Journal of Advances in Mathematics and Computer Science

34(1): 1-26, 2019; Article no.JAMCS.51915
ISSN: 2456-9968
(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

Secure Electronic Voting Using a Hybrid Cryptosystem and Steganography

Oladotun O. Okediran[1*], Adeyemi A. Sijuade[1] and Wajeed B. Wahab[2]

[1]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
[2]Department of Electrical, Electronics and Computer Engineering, Bells University of Technology, Ota, Ogun State, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. Authors OOO and WBW did the conceptual framework design. Author OOO wrote the draft and final copies of the manuscript and did a thorough literature search of all the reference materials used. Author AAS performed the statistical analysis of responses received from respondents. Author WBW did the implementation in Java. Finally, all authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JAMCS/2019/v34i1-230201
Editor(s):
(1) Dr. Sami Ullah Khan, Assistant Professor, Department of Mathematics, COMSATS Institute of Information Technology, Pakistan.
Reviewers:
(1) Jose Ramon Coz Fernandez, University Complutense of Madrid, Brazil.
(2) Michel Riguidel, France.
(3) K. Karthick, GMR Institute of Technology, India.
Complete Peer review History: https://sdiarticle4.com/review-history/51915

Original Research Article

Received: 30 July 2019
Accepted: 05 October 2019
Published: 19 October 2019

Abstract

Conventional voting techniques have been employed over the years in most elections. However, each of these techniques has attendant short comings. The existing conventional voting systems have been subjected to gross abuse and irregularities. Electronic voting (e-voting) which is emerging as an alternative to these conventional voting systems, though highly promising, is not also totally free of flaws; information security issues bordering on privacy, integrity and verifiability of the electronic ballots casted are still significant in most implementations of e-voting systems. In this paper, we developed a security scheme that was based on a hybrid Rivest-Sharma-Adleman (RSA) algorithm and Advance Encryption Standard (AES) algorithm with Least Significant Bit (LSB) replacement algorithm for securing ballot information in an e-voting system. An e-voting system with multiple voting channels which includes poll site voting, mobile voting and remote internet voting was developed in the contextual Nigerian scenario. The electronic ballots casted via the system during experimental usage were encrypted using the hybrid RSA-AES algorithm to circumvent the problems of privacy, integrity and verifiability

**Corresponding author: E-mail: oookediran@lauetch.edu.ng, oookediran@lautech.edu.ng;*

associated with many e-voting systems. The encrypted ballots were then hidden using LSB replacement algorithm to improve their integrity. The image quality of the cover image used and stego image obtained from the security scheme developed was quantitatively assessed using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Correlation. Furthermore, a performance evaluation based on users' perception of the developed e-voting system showed that the system satisfied most of the generic security requirements for electronic voting.

Keywords: Cryptography; e-voting; integrity; privacy; steganography; verifiability.

1 Introduction

The increase in advancement, affordability, accessibility and adaptability of information and communications technologies (ICT) has created a breeding ground for developmental innovations through which critical services that affect our human lives can be provided. ICT has introduced new methods of undertaking many activities by electronic means. Some examples include e-commerce, e-banking, e-learning, e-government, e-democracy, e-voting, e-health and so on. Corresponding to this, is also the innovative porting of such applications to mobile devices such as Smartphones and tablet devices; hence m-commerce, m-banking, m-learning, m-voting and so on. These applications have tremendously changed the way we do many things. There is barely any facet of the world we live in that has not felt the effects of the ICT revolution. Most people are now regular users of computer, mobile phones and keen consumers of ICTs. Also, governments in both the developed and developing worlds have responded by formulating ICT policies, putting in place regulatory frameworks and establishing institutional infrastructures. Their aim is to facilitate and bring order to these e-developments that are rapidly changing the world we live in [1].

One of the e-developments being facilitated by many governments around the world today is electronic participation (e-participation). The adoption of ICT in governance is aimed at the provision of better information and services to citizens with fewer resources through optimization of available resources and infrastructures. This aim could only be achieved through effective e-participation between the governed and the government. E-participation is a technology-mediated interaction among the citizens, formal political spheres and central governing spheres. The mission of e-participation is to endow citizen with privileges of ICT to respond in bottom-up decision processes and develop social as well as political responsibility for their choices [2]. Citizens' participation in electronic governance could be in the following context: information provision, consultation, campaigning, deliberation, polling, electioneering and voting using different electronic methods. E-participation through electronic voting (e-voting) is the use of ICT in the context of public voting in elections or referenda. It has emerged as a significant alternative to conventional voting systems. In times past, different voting systems that are based on traditional paper ballots, mechanical devices, or electronic ballots were developed for elections, but each of these voting systems has their respective attendant problems. In Nigeria for example, most elections are conducted using paper ballots. This conventional voting system has littered the Nigerian electoral history with example of elections being manipulated in order to influence their outcome. Allegations of violence, intimidation, ballot stuffing, under-age and multiple voting, counting error, the complicity of the security agencies and the absence or late arrival of election materials, and so on, often trail these elections [3]. These attendant problems have led to a rapid decline in voters' participation in elections. Using Nigeria as an instance, in the various elections conducted since independence, about half the number of registered voters actually voted during elections [4]. This worrying from a democratic point of view in that, if the reasons for the decline are left unchecked, the mandate of those elected to hold the positions might eventually be questionable. Furthermore, in the developing world, participatory democracy is a major requirement for achieving the millennium development goals (MDGs), particularly, where the majority of the citizenry is disenchanted with the electioneering or democratic processes or governance.

Many e-voting schemes have been proposed and used with various degrees of successes in a number of countries during local elections and referenda. Also, many pilot e-voting and m-voting schemes have been

developed and tested. These schemes have proven that e-voting can undoubtedly enable voters to cast their vote from a place other than the poll site in their voting district, facilitate the casting of the vote by the voter, facilitate the participation in elections by those who are entitled to vote, widen access to the voting process for voters with disabilities or those having other difficulties in being physically present at a poll site, increased voter turnout by providing additional voting channels, reduce overtime, the overall cost to the electoral authorities of conducting an election, deliver voting results reliably and more quickly amongst many other benefits [3,5]. Furthermore, e-voting can enhance polling and votes' security, confidentiality, sincerity and increased cost savings on reduced manpower, logistical materials and tools; and above all instant analysis and reporting.

However, despite these value-added advantages of e-voting, some generic security requirements for voting systems are still contentious in many implementations of e-voting systems. Issue of voters' authenticity; privacy, integrity and verifiability of electronic ballots casted are evident in many systems. E-voting systems are classified as a high impact social information system, whose loss of these vital security parameters could have an adverse effect on the credibility of near and future democratic governance [2]. Consequently, to proffer solutions to the aforementioned security challenges of e-voting, different information security schemes that were based on cryptography, watermarking and steganography have been formulated and proposed. However, express literature survey revealed that most of these schemes are still vulnerable brute force attack, timing attack, session hijacking, replay attack, trapdoor problem, known-plaintext and chosen-plain text attack [6,7,8] and can also be manipulated by eavesdropping.

In this paper, an e-voting system with multiple voting channels which includes poll site voting, mobile voting and remote internet voting was developed in the contextual Nigerian scenario. A hybrid RSA-AES algorithm with LSB replacement algorithm was implemented to provide a security scheme for the system. RSA is an asymmetric encryption algorithm and one of the most secure for encryption. It uses a pair of keys: one for encrypting and another for decrypting, but it is computationally slow due to complex calculations involved by its large key size (1024 bits and more). On the other hand, AES is a symmetric algorithm that uses the same key for encrypting/decrypting the information and is very fast computationally due to its small key size, but it suffers from the exchange of keys. Hybridizing the two algorithms solves the inherent limitations in each; RSA was used for the exchange of keys while AES was used for encrypting and decrypting information. The encrypted ballot is then be hidden using LSB replacement algorithm for imperceptibility and enhanced security of the ballots. The LSB algorithm is a spatial domain-based steganography technique that embeds messages in the least significant bit of the pixel of a cover image. Section two presents review of relevant literature to this research; Section three details the research methodologies employed in the development of the security scheme and the e-voting system; Section four presents the results and Section five summarized and concludes the paper.

2 Literature Review

2.1 E-voting and security concerns

As the computing and communicating techniques progress rapidly, increasing emphasis has been placed on developing voting schemes that use the information and communications technology resources for providing more efficient voting services than conventional paper-based voting methods. Furthermore, the explosion of the internet culture worldwide has caused many to question why ballots can't be cast in the same manner as goods are ordered on the web-from home or from work? Voters see themselves as customers and expect the government to make the business of voting more convenient. In the past decade various types of electronic voting, particularly remote voting, have won considerable attention as possible additional voting methods that promise to make the electoral process simpler and more efficient for political parties, candidates, election administration, and most importantly, for electors. Many types of Internet or remote electronic voting schemes have been implemented with varying degrees of success. While some systems have worked well, pilot of prototypes in other jurisdictions have been cancelled, some even before they were introduced, because of concerns on security issues.

The design of an e-voting system must satisfy a number of competing for security criteria in the three phases of an election process. Organisation for the Advancement of Structured Information Standard (OASIS) in 2003, defined a conceptual perspective for e-voting. The OASIS consortium is a standard for the structured interchange among hardware, software, and service providers who engage in providing election or voter services to public or private organizations. [9] conceptualized of e-voting to be made of three phases which are pre-voting, voting and post voting.

a) *Pre-voting phase* which involves election declaration, candidate nomination, referendum options and voters' registration. In this phase are security requirements for:

   i. Authenticity: Only selected voters may vote and the electronic voting system must provide proof with the use of appropriate authentication mechanisms that a selected voter is the one that cast the vote [10];
   ii. Eligibility: Only eligible voters are permitted to vote [10,11,12,13].

b) *Voting phase* which involves ballot information, voter authentication, vote casting and confirmation. In this phase are security requirements for:

   i. Uniqueness: No voter should be able to vote more than one time [10,11,12,13,14,15,16];
   ii. Verifiability: A system is verifiable if voters can independently verify that their votes have been counted correctly. The most verifiable systems allow all voters to verify their votes and correct any mistakes they might and without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out, but not corrected or might allow verification of the process by party representatives but not by individual voters [17];
   iii. Security: Throughout the voting process, a vote can't be tampered with [3,18];
   iv. Fairness: The electronic voting system must not provide any information for the outcome of an election process during the election process. No one can learn the voting outcome before the tally [13].

c) *Post-voting phase* which involves election counts, results and audit. In this phase are security requirements for:

   i. Privacy**:** After casting a vote, no one should be able to link the voter to this vote. The e-voting system must provide anonymity mechanisms so that the voter could not be traced back by his vote. There should be no way to derive a link between the voter's identity and the marked ballot [10,11,12,13,15,16,19];
   ii. Integrity: Once a voter cast a vote, no alternation to this vote is permitted [3,18];
   iii. Accuracy: All valid votes are counted correctly. The electronic voting system must count all votes and must count them as casted. A voter's vote cannot be altered, duplicated, or removed. Of course in a real electronic voting system appropriate error thresholds must be set that will indicate the validity of an election process [11,13,15,16,19,20].

In many of the existing e-voting models and schemes, security issues of privacy, integrity and verifiability of the electronic ballots are still evident. Furthermore, most of the existing security models proposed and developed to proffer solutions to these issues are still vulnerable to brute force attack, timing attack, session hijacking, replay attack, trapdoor problem, known-plaintext, chosen-plaintext attack and manipulations by eavesdropping. However, voting systems must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. Hence there is a dire need of a foolproof security mechanism for electronic voting.

2.2 Cryptography

Cryptography is the science of keeping secrets secret [21]. An original message is known as the plaintext, while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is

known as enciphering or encryption; restoring the plaintext from the ciphertext is deciphering or decryption; a cipher is a pair of algorithms that create the encryption and the reversing decryption [22]. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. Providing confidentiality is not the only objective of cryptography. Cryptography is also used to provide solutions for other information security problems [21]:

i. *Data integrity*. The receiver of a message should be able to check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or for parts of it.
ii. *Authentication*. The receiver of a message should be able to verify its origin.
iii. *Non-repudiation*. The sender should not be able to later deny that he/she sent a message.

Generally, there are three types of streams in cryptography: symmetric key, asymmetric key and hashing.

Symmetric-key cryptography uses a single secret key for both encryption and decryption purpose. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher [23]. Data manipulation in symmetric cipher is faster as they generally use shorter key lengths. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps for each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret [22,24]. Examples of symmetric-key encryption algorithm are AES, Data Encryption Standard (DES) and Triple DES (3DES).

On the other hand, asymmetric key cryptography uses two keys: one is the public key and another one is the private key. Receiver's public key is used by the sender for encrypting the message and receiver's own private key is used for decrypting the message at the receiver. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security [22]. In asymmetric any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key [21]. Public key algorithms are fundamental security ingredients in modern cryptosystems, applications and protocols assuring the confidentiality, authenticity and non-reputability of electronic communications and data storage. Example of this class of encryption algorithm includes RSA, Diffie–Hellman key exchange protocol, Elliptic curve techniques, El-Gamal to mention but a few.

2.2.1 Description of the RSA algorithm

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n) + 1$; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C [22]:

$$C = M^e \bmod n \tag{2.1}$$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

i. It is possible to find values of e, d, and n such that $M^{ed} \bmod n = M$ for all $M < n$.
ii. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.

iii. It is infeasible to determine d given e and n.

The first requirement is to find a relationship of the form:

$$M^{ed} \bmod n = M \tag{2.2}$$

The preceding relationship holds if e and d are multiplicative inverses modulo φ (n), where φ (n) is the Euler totient function. For p, q prime, φ(pq) = (p - 1)(q - 1). The relationship between e and d can be expressed as

$$ed \bmod \varphi(n) = 1 \tag{2.3}$$

This is equivalent to saying

$$ed \equiv 1 \bmod \varphi(n)$$
$$d \equiv e^{-1} \bmod \varphi(n)$$

That is, e and d are multiplicative inverses mod φ (n). It may be noted that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to φ (n).

$$\text{Equivalently,} \quad \gcd(\varphi(n), d) = 1. \tag{2.4}$$

In summary the essential ingredients of the RSA scheme are:

p, q, two prime numbers	(private, chosen)
$n = pq$	(public, calculated)
e, with gcd(φ (n), e) = 1; $1 < e <$ φ (n)	(public, chosen)
$d \equiv e^{-1}$ (mod φ (n))	(private, calculated)

The private key consists of {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates $C = M^e \bmod n$ and transmits C. On receipt of this ciphertext, user A decrypts by calculating $M = C^d \bmod n$.

2.2.2 Description of the AES algorithm

Compared to public-key ciphers such as RSA, the structure of AES and most symmetric ciphers is quite complex and cannot be explained as easily as many other cryptographic algorithms [22]. The AES is based on the Rijndael cipher [25]. The Rijndael cipher is an iterated block cipher and supports different block and key sizes. Block and key sizes of 128, 160, 192, 224 and 256 bits can be combined independently. The only difference between Rijndael and AES is that AES supports only a subset of Rijndael's block and key sizes. The AES fixes the block length to 128 bits, and uses the three key lengths 128, 192 and 256 bits.

Rijndael is an iterated block cipher [21]. The iterations are called rounds. The number of rounds, which we denote here by N_r, depends on the block length and the key length. In each round except the final round, the same round function is applied, each time with a different round key. The round function of the final round differs slightly. The round keys $key_1, \ldots, key_{Nr}$ are derived from the secret key k by using the key schedule algorithm. Rijndael is byte-oriented [21]. Input and output (plaintext block, key, cipher-text block) are considered as one-dimensional arrays of 8-bit-bytes. Both block length and key length are multiples of 32 bits. We denote by N_b the block length in bits divided by 32 and by N_k the key length in bits divided by 32. Thus, a Rijndael block consists of N_b words (or 4. N_b bytes), and a Rijndael key consists of N_k words (or 4. N_k byte). Table 1 shows the number of rounds N_r as a function of N_k and N_b:

AES with key length 128 bits (and the fixed AES block length of 128 bits) consists of 10 rounds. The round function of Rijndael, and its steps, operates on an intermediate result, called the *state*. The *state* is a block of N_b words (or 4. N_b bytes). At the beginning of an encryption, the variable *state* is initialized with the

plaintext block, and at the end, *state* contains the ciphertext block. The intermediate result *state* is considered as a 4-row matrix of bytes with N_b columns. Each column contains one of the N_b words of *state*. An encryption with Rijndael consists of an initial round key addition, followed by applying the round function (N_r - 1) - times, and a final round with a slightly modified round function.

Table 1. Number of rounds N_r as a function of N_k and N_b

N_k	N_b				
	4	**5**	**6**	**7**	**8**
4	10	11	12	13	14
5	11	11	12	13	14
6	12	12	12	13	14
7	13	13	13	13	14
8	14	14	14	14	14

The round function is composed of the *SubBytes*, *ShiftRows* and *MixColumns* steps and an addition of the round key. In the final round, the *MixColumns* step is omitted. A high level description of the Rijndael algorithm follows:

byteString *Rijndael*(byteString *plaintextBlock; key*)

i. *InitState*(*plaintextBlock; state*)
ii. *AddKey*(*state; key*$_0$)
iii. for $i \leftarrow 1$ to N_r - 1 do
iv. *SubBytes*(*state*)
v. *ShiftRows*(*state*)
vi. *MixColumns*(*state*)
vii. *AddKey*(*state; key*$_i$)
viii. *SubBytes*(*state*)
ix. *ShiftRows*(*state*)
x. *AddKey*(*state; key*$_{Nr}$)
xi. return *state*;

2.3 Steganography

Steganography is the art and science of hiding communication; It is the art and science of hiding the existence of information into information [26]. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits that are, those that can be modified without destroying that medium's integrity [27]. The information is embedded in a cover or carrier object so that no one can understand the presence of information. A key is used for embedding procedure without which the adversary cannot be able to detect the embedded message [28]. The altered new object is called stego-object. Image, audio, video and so on can be the cover objects [28,29,30]. For steganography algorithms, three concepts are required that contend with each other [31]:

i. Capacity: indicates the information quantity that the cover object can hide.
ii. Robustness: refers to the amount of modifications that a stego-object can withstand before hidden information destruction.
iii. Imperceptibility: A steganographic process is imperceptible when human eye cannot distinguish between the cover image and the stego-image. This parameter is measured by the MSE and PSNR. The MSE is calculated by the following expression:

$$MSE = \frac{1}{MN}\sum_{i=1}^{i=M}\sum_{j=1}^{j=N}(C(i,j) - S(i,j))^2 \quad (2.5)$$

Where C is the cover image and S is the stego -image, M and N are the numbers of lines and columns of C and S. The PSNR is computed using the following equation:

$$PSNR = 10Log\left(\frac{max^2}{MSE}\right) \quad (2.6)$$

where *max* is the maximum pixel value of the image. The PSNR increases when MSE decreases, this means that a higher PSNR value is a sign of a better degree of imperceptibility of the steganographic algorithm. The human visual system (HVS) cannot detect any distortions in stego-images having PSNR that goes beyond 36 dB.

Based on cover object, steganography is classified as image, audio, text, video, and protocol steganography [28]. Among them, image steganography is a popular one as it can achieve the three concepts which contend with each other: capacity, imperceptibility, and robustness [32]. The image steganography methods are of two types depending on domain type: spatial domain based techniques and frequency domain based techniques. In spatial domain-based technique, the message is embedded in the intensity of pixels of the images straightly while in the frequency domain based technique, images are converted into the frequency domain and then the messages are embedded in the transform coefficients [33]. Among many spatial domain based techniques, LSB (Least Significant Bit) method is the widely applied method. In this technique, messages are embedded in the least significant bit of the pixel of the cover image. To embed more messages, two or more pixels of the cover image can be allocated, but this kind of allocation can degrade the image fidelity as well as imperceptibility [33]. Some of the available frequency domain based techniques are Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) [34].

2.3.1 The least significant bit replacement algorithm

The Least Significant Bit replacement algorithm is a commonly used straightforward steganographic algorithm used to embed secret information inside a cover medium [35]. In this method, the least significant bits of the original data in the cover medium are altered based on the secret message. In the case of digital images, the alteration is done only at the least significant bits of the original image so as to reduce the effect of degradation of the original image. By inserting the secret message only at the least significant bits, the perceptibility of the original image is not much affected. The description of the modulus operandi of the algorithm is as follows:

Let C be the original 8-bit grayscale cover-image of $M_c \times N_c$ pixels represented as

$$C = \{x_{ij} | 0 \leq i < M_c, 0 \leq j < N_c, x_{ij} \in \{0, 1, \ldots, 255\}\} \quad (2.7)$$

M be the n-bit secret message represented as

$$M = \{m_i | 0 \leq i < n, m_i \in \{0; 1\}\} \quad (2.8)$$

Suppose that the *n-bit* secret message M is to be embedded into the k-rightmost LSBs of the cover-image C. Firstly, the secret message M is rearranged to form a conceptually *k-bit* virtual image M' represented as

$$M' = \{m_i' | 0 \leq i < n', m_i' \in \{0, 1, \ldots, 2^k - 1\}\}, \quad (2.9)$$

Where $n' < M_c \times N_c$. The mapping between the *n-bit* secret message $M = \{m_i\}$ and the embedded message $M' = \{m_i'\}$ can be defined as follows:

$$m_i^{'} = \sum_{j=0}^{k-1} m_{i\times k+j} \times 2^{k-1-j} \tag{2.10}$$

Secondly, a subset of n' pixels $\{x_{l1}', x_{l2}', \ldots, x_{ln}'\}$ is chosen from the cover-image C in a predefined sequence. The embedding process is completed by replacing the k LSBs of x_{li} by m_i'. Mathematically, the pixel value x_{li} of the chosen pixel for storing the *k-bit* message m_i' is modified to form the stego-pixel x_{li}' follows:

$$x_{li}' = x_{li} - x_{li} \bmod 2^k + m_i' \tag{2.11}$$

In the extraction process, given the stego-image S, the embedded messages can be readily extracted without referring to the original cover-image. Using the same sequence as in the embedding process, the set of pixels $\{x_{l1}', x_{l2}', \ldots, x_{ln}'\}$ storing the secret message bits are selected from the stego-image. The k LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits. Mathematically, the embedded message bits m_i' can be recovered by:

$$m_i' = x_{l1}' \bmod 2^k \tag{2.12}$$

2.4 Related works

Tohari et al. [36] proposed a security conscious mobile voting scheme to meet the requirements for integrity, confidentiality and anonymity security requirements for electronic voting. The scheme leveraged on small-key sized Ecliptic curve cryptographic algorithm for direct and faster encryption of votes in the mobile device and secure data transfer between the voters' end and the electoral office's end.

Purusthomata and Alwyn [37] developed a secure internet-based e-voting system using an identity-based encryption system to satisfy security requirements for privacy, anonymity, eligibility, fairness, verifiability and receipt freeness of electronic voting. The e-voting system experimented the use of a public key infrastructure that was based on a unique voter's identification number.

Sujata and Banshidhar [38] proposed an e-voting protocol based on the blind signature to meet security requirements of privacy, anonymity, eligibility, fairness, verifiability and uniqueness of secure e-voting. The protocol is an improvement over the YES/No e-voting protocol using bitwise XOR operation for vote generation and blind signature for voter authentication.

Gina et al. [39] designed an identity based secured e-voting protocol that was founded on two bilinear pairing cryptographic algorithms to meet privacy, eligibility, transparency, accuracy, and uniqueness requirements for secure e-voting. The protocol uses threshold encryption scheme and blind signature bilinear cryptographic primitives as main construction blocks.

Patil [40] developed a cryptography-based voting protocol to guarantee voters' privacy, authenticity, verifiability and integrity requirements for secure electronic voting. The developed protocol uses a blind signature, to guarantee the voters' privacy and ballot confidentiality as well as digital signature to authenticate the voter.

Okediran et al. [3] proposed a multifaceted e-voting system using a number of electronic devices including private computer network, web and mobile. The security scheme implemented for the system was based on RSA and proxy servers as firewall.

Katiyar et al. [41] fused steganographic and cryptographic techniques to resolve authentication security requirements of an online e-voting system using both secret key and voters biometric fingerprint template as the cover. The work embeds voter's identification number and SHA256 hashed secret key created during registration on voters' fingerprint template as distinct and final stego image.

Alok and Atul [42] proposed a combined cryptography and steganography scheme for mobile voting. The scheme was based on face and voice biometric recognition for authentication and ECC encryption for vote integrity and image steganography for confidentiality.

Mallick and Kamilla [43] combined steganographic and cryptographic techniques to proffer confidentiality and integrity security requirements for e-services. The work employed LSB spatial image domain steganographic technique that was pre-encrypted with symmetric block cipher.

Rura et al. [44] developed a secured e-voting system which was founded on the core security requirements for electronic voting as well as non-functional requirements such as non-coercibility, receipt-freeness and universal verifiability by experimentation with two different steganographic tools which are F5 and Outguess on five different types of images. The work explored the principles of secret ballot theory, image steganography, visual cryptography and threshold decryption cryptosystems in Java.

Gupta et al. [45] developed a blind signature based cryptographic scheme to provide voter's anonymity and ballot confidentiality in a secure e-voting system. The protocol utilised blind signature to guarantee the voters' privacy and ballot confidentiality and digital signature to authenticate the voter.

Sodiya et al. [46] developed an e-voting architecture for secure e-voting. Security considerations for the system were targeted on ensuring privacy, receipt-freeness and non-coercion. A security model based on Ecliptic curve and probabilistic encryption were proposed to avert the aforementioned security concerns. The architecture employed ECC and El-Gamal Cryptosystem to encrypt voters vote prior to transmission to voting authority for later decryption at tally phase.

Sulthana and Kanmani [47] developed a secure online voting scheme with integration of facial biometrics with fingerprint for authentication. An asymmetric encryption algorithm, RSA and video steganography were implemented incorporated into the system to enhance security.

Swamminathan and Dinesh [48] developed a model for secure online voting with hybridization of image steganography and SHA 256 hash algorithm. The voting system uses LSB technique of steganography to embed voters' PIN, secret key and voter biometric fingerprint template into cover image.

Prabha and Ramamoorthy [49] enhanced the work of [41] which suffer from hashing speed limitation, by replacing MD5 with SHA 256 and provides authentication for voters by using biometrics (iris) prior to embedding both hashed key and voters identification number to produce the final stego image.

Linu and Anilkumar [50] proposed a multimodal face and fingerprint biometric technique to proffer solution to the problem of authentication in an online e-voting model. The model improved on methodology proposed in [41] using multimodal biometrics of face and fingerprint and MD5 hashing algorithm. The model authenticates voters' biometric face and fingerprint using principal component algorithm and Gabor filtering algorithm respectively.

Nivedtha and Meyyapan [51] developed a unison media and domain technique for encrypting and hiding data in a cover medium using image processing methodology. The developed technique combined DES cipher and LSB steganographic technique to encrypt secret image prior to hiding in the cover mage in spatial domain.

Olaniyi et al. [52] designed a secure electronic voting system that catered for the security concerns of erring voter's authentication and integrity of vote transmitted over insecure wireless medium. Multifactor authentication and cryptographic hash functions were combined to secure the developed e-voting system by the authors.

Neha [53] proposed a unison media and domain secure model for online voting system using a fusion of cryptography and steganography. The evolved voting model utilised MD5 hashing algorithm to optimize speed of key encryption and LSB technique to hide built in randomly generated image for each voter.

Kharmate et al. [54] proposed a smart e-voting system, which was entirely works on digital data. AES algorithm was used for voter's data encryption process. This system can examine validity and eligibility of the voter, the inactive votes and illegal user was stayed out of the system.

Fashoto et al. [55] implemented an e-voting model for elections in a tertiary institution. The voting model considered basically the security requirements for privacy and confidentiality of voters and ballots casted respectively. RSA encryption was implemented to ensure the aforementioned security requirements.

Alhasnawi and Alkhalid [56] introduced a practicable method for secure online voting system using biometrics, cryptography and steganography. The underlying techniques involved in developing the system include extraction of fingerprint feature using the Particle Swarm Optimization (PSO) algorithm. The extracted features are then encrypted a unique voters' Personal Identification Number (PIN) and the Candidate Number using ECC. Finally, multiple chaotic logistic maps was used by the authors to generate a random hiding locations and the Least Significant Bit technique is used for hiding the encrypted voter's information inside a cover image to produce a stego image, which is sent over the insecure channel.

Rura et al. [57] developed an online voting system based on image steganography and visual cryptography. The e-voting system developed by the authors incorporated data security techniques that includes password hashed based scheme, visual cryptography, F5 image steganography and threshold decryption cryptosystem.

Sundar et al. [58] proposed a secure e-voting system that satisfies basic security requires for electronic voting. RSA and Md5 Algorithms using random number generators were implemented to encrypt voters' particulars and casted ballots.

After a thorough review of the above mentioned related works, it was established that most of these works developed schemes and models for providing fundamental security requirements for electronic voting that includes confidentiality, integrity, authentication and verifiability. However, most of these schemes are still vulnerable to various attacks and eavesdropping. Many of the security schemes and models built around an encryption algorithm are still vulnerable to packet sniffing, keylogging, meet-in-the-middle attacks, chosen plaintext attack, brute force attack and frequency analysis. On the other hand, many of the security schemes and models they were built around both cryptography and steganography still contends with the underlisted issues:

i. Low robustness against statistical attack from statistical steganalyst and low robustness against image manipulation which might destroy the hidden message from its destination.
ii. For those implemented with unilateral stego medium as well as spatial domain, the hiding process is prone to manipulation by an eavesdropper. Furthermore, they lacks non-repudiation requirement for information security.

In this paper, an e-voting system with a security scheme built on a hybrid cryptosystem and steganography was developed, with an attempt to proffer a more robust scheme in fulfilling the security requirements for electronic voting which may in turn also be a solution to the above mentioned limitations of the reviewed related works.

3 Methodology

Finding appropriate research methodologies is critical in drawing up model solutions/systems to identified problems [59]. This research applies the Systems Development Life Cycle (SDLC) approach to derive a secure electronic voting system that would solve a real life problem. The SDLC in systems engineering, information systems and software engineering, is the process of creating or altering systems, and the models and methodologies that people use to develop these systems [60]. More specifically, SDLC is a methodology

for design and implementation of an information system [61]. This work employed the iterative waterfall model.

3.1 Requirements definition

Prior to the design of any voting system, a comprehensive and detailed set of requirements have to be developed. The design requirements of the developed e-voting system in this work are divided into two groups, namely, generic and system-specific. The generic requirements are those requirements that apply to any voting system. The system-specific requirements, on the other hand, are those requirements that are specific to the developed system. The generic requirements catered for by the system are privacy, authenticity, integrity/accuracy, democracy and verifiability which have all been expressly defined in Subsection 2.1. The system-specific requirements, on the other hand, are those requirements that are specific to the developed system. The system-specific requirements of the system allow:

i. *Multi-user:* A number of voters can vote simultaneously;
ii. *Accessibility:* The system can be accessed by voters from any location using secure internet and/or mobile devices;

3.2 Framework design for the system

The framework design was done to determine applications architectural framework. The emerging framework from this design process is a representation of the structure for the realization of the defined goal. An integral part of the model design is the infrastructural model architecting in which model(s) were developed on the framework. The models are graphical model developed using unified modeling language (UML).

3.3 Applications development

Applications were developed and deployed to test the framework developed. The applications were developed using Java, JavaScript, HTML 5, PHP v6, MySQL server 2012, HTTP SMS gateway and Android Studio and SDK tool.

3.4 Security scheme for the developed E-voting system

The security considerations of the system for securing end to end messaging was based on the implementation of an hybrid RSA-AES encryption algorithm with LSB replacement algorithm. RSA was used for exchange of keys while AES was used for encrypting and decrypting information. The encrypted ballots were then hidden using LSB replacement algorithm for imperceptibility and enhanced security of the ballots. The encryption/embedding and extraction/decryption processes for the security scheme are depicted below:

A. Encryption and Embedding Process

i. Create a RSA key pair; a private key and a public key.
ii. Generate a random key for AES.
iii. Create an AES cipher to encrypt a text string with the AES key.
iv. Encrypt the message with the AES key.
v. Encrypt the AES key with the RSA public key.
vi. Using LSB, read the selected cover image and the encrypted message of steps i – v above which is to be embedded in to the cover image; the output image after embedding is referred to as stego image.
vii. Convert the encrypted message into cipher text by using secret key shared by receiver and sender.
viii. Convert the encrypted message in (vii) above into binary form.

ix. *Find LSBs of each RGB pixels of the cover image.*
x. *Embed the bits of the encrypted message into bits of LSB of RGB pixels of the cover image.*
xi. *Continue the procedure until the encrypted message is fully hidden into cover file.*

B. Extraction and Decryption Process

i. *Read the stego image.*
ii. *Find LSBs of each RGB pixel of the stego image.*
iii. *Find and retrieve the LSBs of each RGB pixel of the stego image.*
iv. *Continue the process until the message is fully extracted from stego image.*
v. *Extracted the encrypted data.*
vi. *Decrypt the AES key with the RSA private key.*
vii. *Decrypt the message entered with AES key in order to read the original message.*

The crypto-steganographic security scheme described above is depicted in Fig. 1 below.

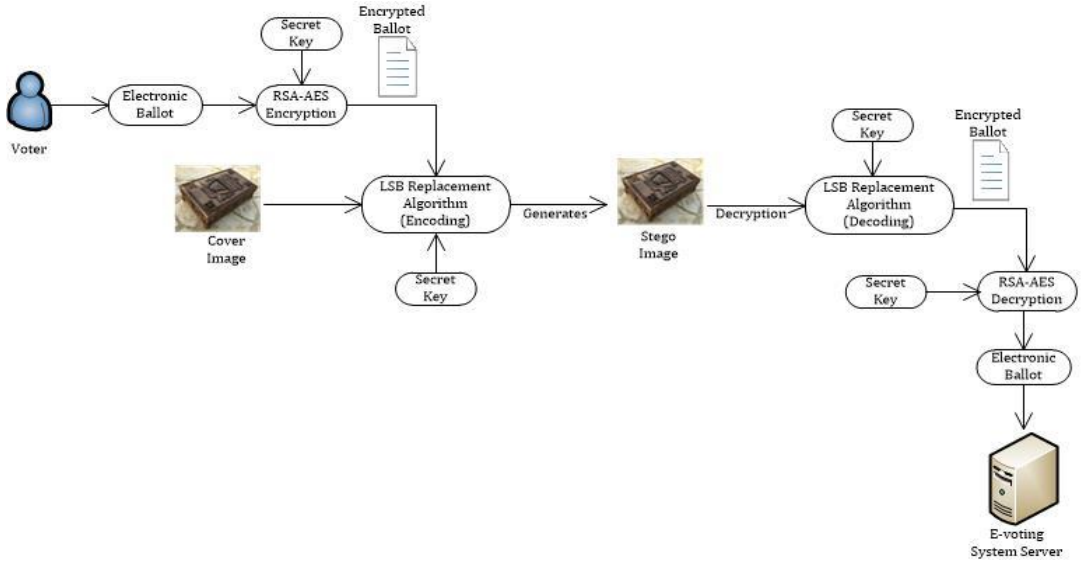


Fig. 1. The developed crypto-steganographic security scheme

3.5 Performance testing and evaluation

Users perception of the developed system were collected after experimental usage to ascertain if the core values desired in voting systems are inherent in the developed e-voting system. This was accomplished by administering a questionnaire based on a psychometric scale (a 5-point Likert rating scale). The following research questions bothering on whether the developed e-voting system fulfilled the generic security requirements desirable in voting systems were raised in the questionnaire administered:

i. Can votes casted remain unaltered? Requirement for *"Integrity"*.
ii. Can a validated vote be included in the final tally? Requirement for "*Accuracy"*.
iii. Can voters be verified to be who they claimed they are? Requirement fo*r "Authenticity"*.
iv. Can the developed e-voting system permits only eligible voters to vote and only vote only once? Requirement fo*r "Democracy"*.
v. Can the developed e-voting developed ensure that neither election authorities nor anyone else can link any ballot to the voter who cast it? Requirement fo*r "Privacy"*.

vi. Can the developed e-voting system ensure that no voter can prove that he or she voted in a particular way? Requirement for *"Secrecy/non-coercion"*.
vii. Can the developed e-voting allow voters to independently verify that their votes have been counted correctly? Requirement for "*Verifiability"*.

Furthermore, the following questions bothering on social factors were raised in the questionnaire:

i. Could e-voting system developed eliminate rigging and other problems associated with conventional voting systems?
ii. Could the e-voting system enhance citizen participation in electioneering processes?
iii. Could the developed e-voting system impel free, fair and credible e-elections?

4 Results and Discussion

4.1 Architectural framework of the developed E-voting system

The developed architectural framework of the e-voting is presented in Fig. 2 below. The functional structure of the framework is described as follows:

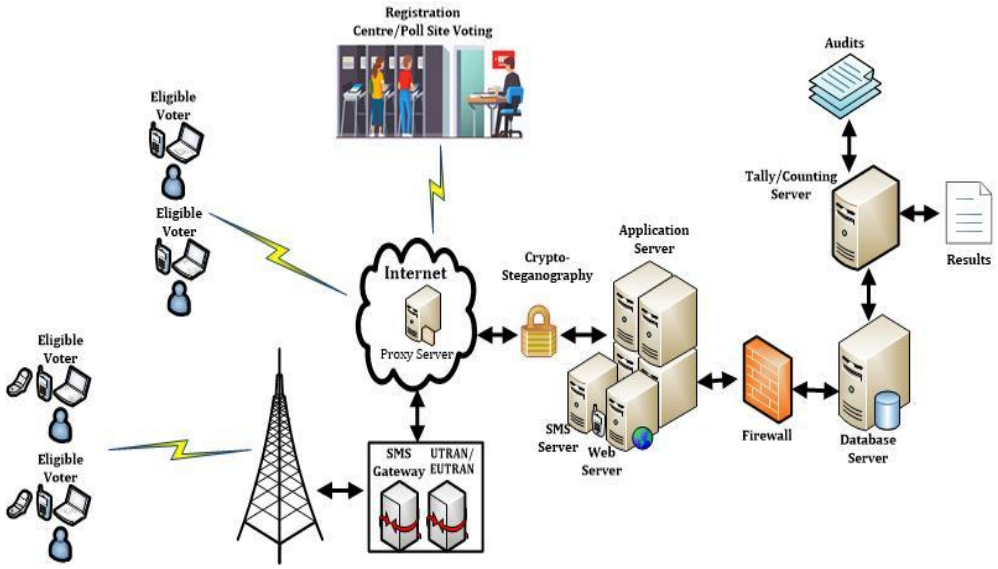


Fig. 2. Architectural framework of the developed E-voting system

Voters' registration for the developed e-voting requires all eligible voters to have a duly registered (as required by the Nigerian Communications Commission) subscriber identity module (SIM) card number and a National Identification Number (NIN). Furthermore, biodata and biometric fingerprints capture of all eligible voters is a core requirement for all voters at this phase. Updated copies of databases containing these two public records (SIM number and NIN) will be available on the application and database servers at the electoral body by relevant authorities. This is very essential for voters' verification and authentication purposes during voting. Electronic voters' registration can only be accomplished under the supervision of electoral officials. A unique Voter Identification Number (VIN) will be generated for each voter after a successful registration process. The VIN is one of the credentials for authentication during the voting phase.

Voting can be done through the system either under the supervision of the electoral commission officials at designated poll sites or remotely by SMS or internet. Remote internet voting requires the use of a computer or a Smartphone that is equipped with a fingerprint reader. On Election Day, poll site voters cast their electronic ballots at designated Poll sites. After successful verification of the voter's credential by supervisory officials of the electoral body, the voter can proceed to cast his/ her ballot on the voting interface by selecting the choice candidate/political party and a fingerprint scan. A remote internet voter runs the uniform resource locator (URL) for the e-voting system through a web browser on a computer or Smartphone (with Google's android). The web application prompts the voter to download the voting application package. After installation on the voter's device, the voting application will request the voter's credentials that include SIM number, NIN and a fingerprint scan of the voter documented during voter's registration process. If there is a match amongst these three, the voting interface will pop up for the voter to select the choice candidate/political party.

A remotes SMS voter will request for the candidates' list for the election being held using an assigned keyword sent to the SMS premium number designated for the e-voting system. The SMS must be sent from the voter's end using the SIM number documented during the voters' enrollment phase. Each candidate is assigned a candidate's code which is randomly generated and assigned to each candidate's name. No two voters will receive the same candidate's code for a particular candidate. Only verified voters will receive the candidates' list and the corresponding candidates' code. Ballot casting is done via SMS by concatenating the NIN and candidate's code. The electronic ballots casted via the system during experimental usage will be encrypted using a hybrid RSA-AES algorithm to circumvent the problems of privacy, integrity and verifiability associated with many e-voting systems. The encrypted ballots will then be hidden using LSB replacement algorithm to improve their integrity. The activity diagram depicting the functional structure of the architecture is depicted in Fig. 3.

4.2 System implementation

This Subsection presents sample graphical user interface (GUI) of the implementation of the e-voting system. The voters' enrollment and sample registered voters credentials are depicted in Fig. 4A and 4B respectively while the Poll site voting interface is depicted in Fig. 4C. The voting application request web page for a remote internet voter using a computer is depicted in Fig. 4D and Fig. 4E shows the installed voting application for a remote voter using a computer. Fig. 4F depicts the voting application for a remote internet voter using a smart phone.

4.3 Performance evaluation by users' assessment

The study population comprises of users of acceptable voting age (18 years and above) who had at one time or the other participated in an electioneering process in Nigeria. This population is taken from students of the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. A total of one hundred and twenty questionnaires were distributed for evaluation of the e-voting system after experimental usage for desired generic security and functional requirements as well as social factors. Backend data and information were made able for post-voting evaluation of the e-voting system.

Of the one hundred and twenty questionnaires that were administered, one hundred and four responses were received from respondents. The users' perception of the developed e-voting system was carried out, the intent of which is to collate an objective evaluation of the adequacy of the system in providing a platform for the delivery of secure, free, fair, transparent and credible e- election. Primary data from the dully filled questionnaires was captured, compiled, and analyzed using SPSS version 12 for Windows environment. Cronbach's alpha test was used to test for the reliability analysis (internal consistency) of grouped Likert items that measures desirable security requirements for e-voting.

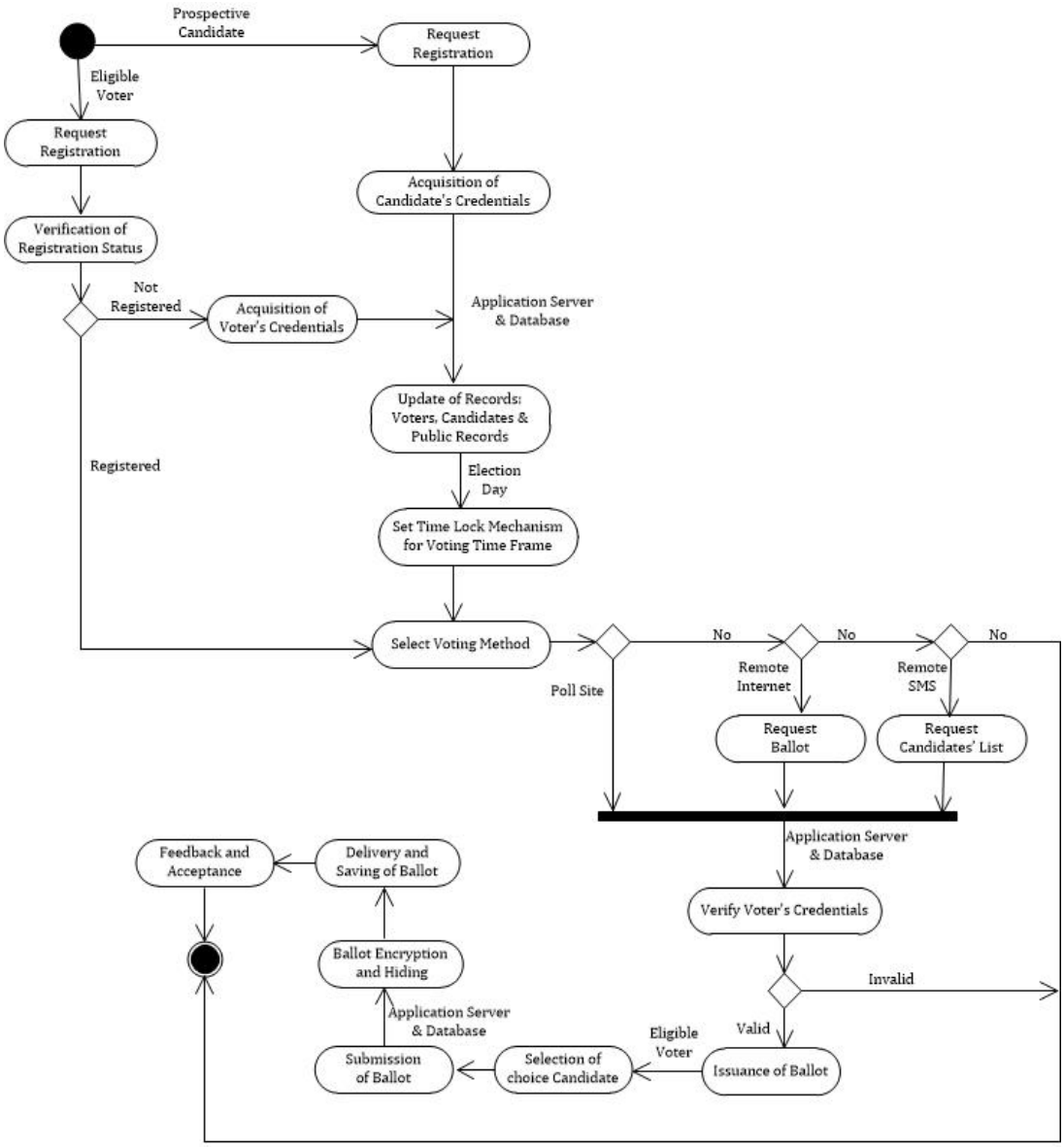
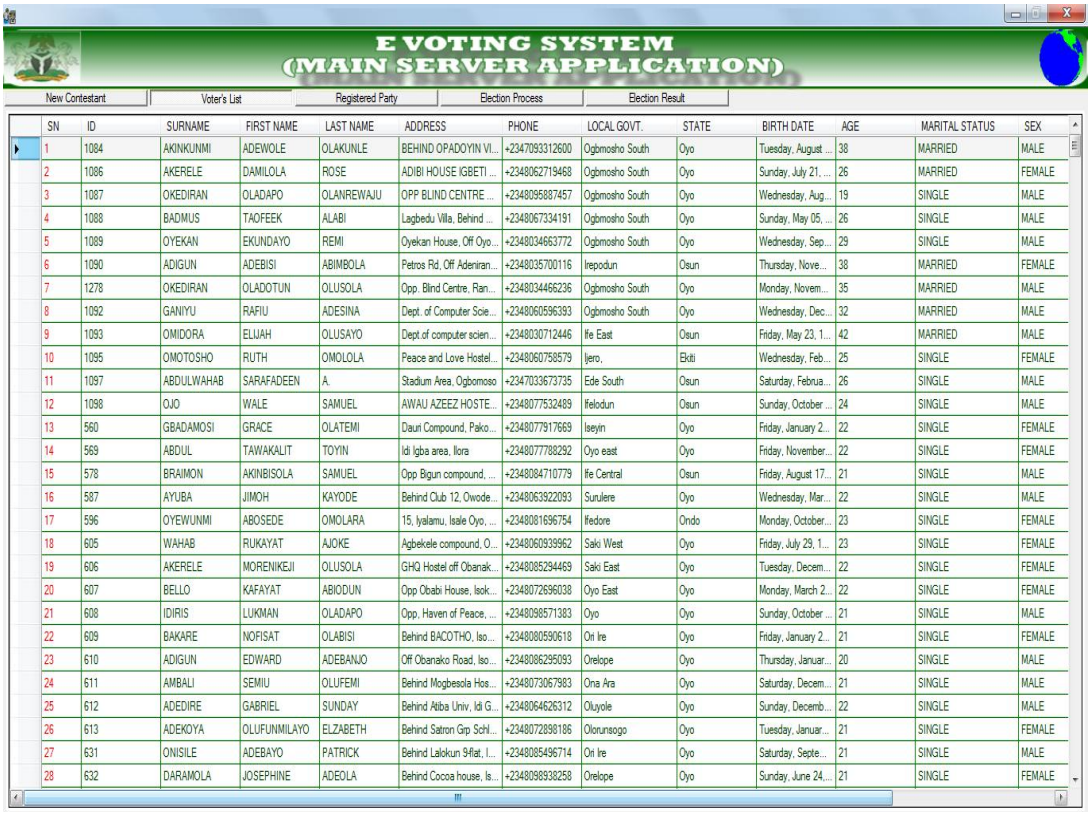


Fig. 3. Activity diagram of the developed E-voting system

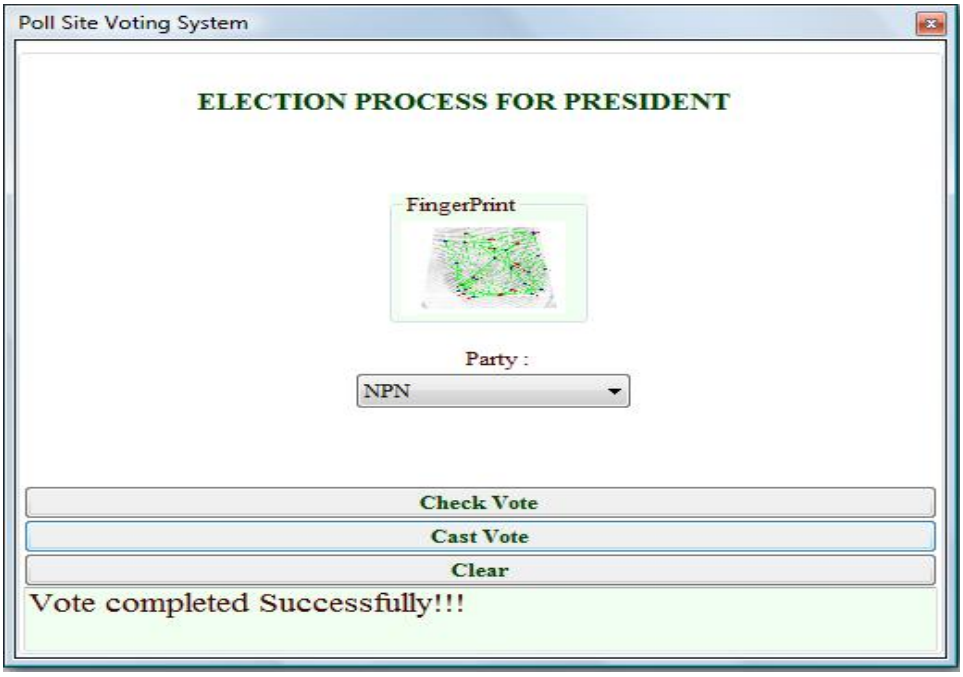
The percentage of users that believed the e-voting model is capable of ensuring voters' privacy and authenticity is 79.59% and 81.37% respectively. The percentage of users that submitted that the integrity, accuracy and verifiability of ballots casted can be guaranteed by the e-voting system is 81.37%, 82.17% and 81.19% respectively. 84.15% of users agreed that the model would not disfranchise any eligible voter and that all voters can only vote once. Over eighty percent (86. 87%) of users submitted that the voting system cannot allow rigging and other similar irregularities. 83.33% and 80.41% of users opined that the e-voting will enhance and increase citizens' participation and credibility of elections respectively, if implemented for large scale elections. The analyses of responses from respondents are represented in the bar chart of Fig. 5.

(A)

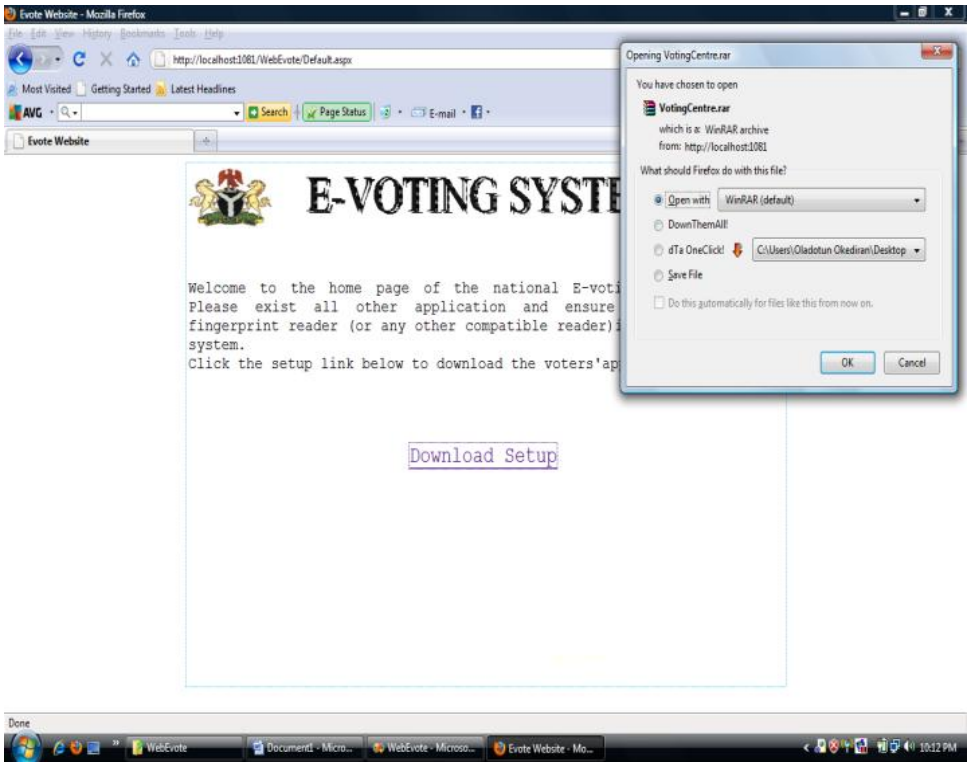


SN	ID	SURNAME	FIRST NAME	LAST NAME	ADDRESS	PHONE	LOCAL GOVT.	STATE	BIRTH DATE	AGE	MARITAL STATUS	SEX
1	1084	AKINKUNMI	ADEWOLE	OLAKUNLE	BEHIND OPADOYIN VI...	+2347093312600	Ogbmosho South	Oyo	Tuesday, August ...	38	MARRIED	MALE
2	1086	AKERELE	DAMILOLA	ROSE	ADIBI HOUSE IGBETI ...	+2348062719468	Ogbmosho South	Oyo	Sunday, July 21, ...	26	MARRIED	FEMALE
3	1087	OKEDIRAN	OLADAPO	OLANREWAJU	OPP BLIND CENTRE ...	+2348095887457	Ogbmosho South	Oyo	Wednesday, Aug...	19	SINGLE	MALE
4	1088	BADMUS	TAOFEEK	ALABI	Lagbedu Villa, Behind ...	+2348067334191	Ogbmosho South	Oyo	Sunday, May 05, ...	26	SINGLE	MALE
5	1089	OYEKAN	EKUNDAYO	REMI	Oyekan House, Off Oyo...	+2348034663772	Ogbmosho South	Oyo	Wednesday, Sep...	29	SINGLE	MALE
6	1090	ADIGUN	ADEBISI	ABIMBOLA	Petros Rd, Off Adeniran...	+2348035700116	Irepodun	Osun	Thursday, Nove...	38	MARRIED	FEMALE
7	1278	OKEDIRAN	OLADOTUN	OLUSOLA	Opp. Blind Centre, Ran...	+2348034466236	Ogbmosho South	Oyo	Monday, Novem...	35	MARRIED	MALE
8	1092	GANIYU	RAFIU	ADESINA	Dept. of Computer Scie...	+2348060596393	Ogbmosho South	Oyo	Wednesday, Dec...	32	MARRIED	MALE
9	1093	OMIDORA	ELIJAH	OLUSAYO	Dept.of computer scien...	+2348030712446	Ife East	Osun	Friday, May 23, 1...	42	MARRIED	MALE
10	1095	OMOTOSHO	RUTH	OMOLOLA	Peace and Love Hostel...	+2348060758579	Ijero,	Ekiti	Wednesday, Feb...	25	SINGLE	FEMALE
11	1097	ABDULWAHAB	SARAFADEEN	A.	Stadium Area, Ogbomoso	+2347033673735	Ede South	Osun	Saturday, Februa...	26	SINGLE	MALE
12	1098	OJO	WALE	SAMUEL	AWAU AZEEZ HOSTE...	+2348077532489	Ifelodun	Osun	Sunday, October ...	24	SINGLE	MALE
13	560	GBADAMOSI	GRACE	OLATEMI	Dauri Compound, Pako...	+2348077917669	Iseyin	Oyo	Friday, January 2...	22	SINGLE	FEMALE
14	569	ABDUL	TAWAKALIT	TOYIN	Idi Igba area, Ilora	+2348077788292	Oyo east	Oyo	Friday, November...	22	SINGLE	FEMALE
15	578	BRAIMON	AKINBISOLA	SAMUEL	Opp Bigun compound, ...	+2348084710779	Ife Central	Osun	Friday, August 17...	21	SINGLE	MALE
16	587	AYUBA	JIMOH	KAYODE	Behind Club 12, Owode...	+2348063922093	Surulere	Oyo	Wednesday, Mar...	22	SINGLE	MALE
17	596	OYEWUNMI	ABOSEDE	OMOLARA	15, Iyalamu, Isale Oyo, ...	+2348081696754	Ifedore	Ondo	Monday, October...	23	SINGLE	FEMALE
18	605	WAHAB	RUKAYAT	AJOKE	Agbekele compound, O...	+2348060939962	Saki West	Oyo	Friday, July 29, 1...	23	SINGLE	FEMALE
19	606	AKERELE	MORENIKEJI	OLUSOLA	GHQ Hostel off Obanak...	+2348085294469	Saki East	Oyo	Tuesday, Decem...	22	SINGLE	FEMALE
20	607	BELLO	KAFAYAT	ABIODUN	Opp Obabi House, Isok...	+2348072696038	Oyo East	Oyo	Monday, March 2...	22	SINGLE	FEMALE
21	608	IDIRIS	LUKMAN	OLADAPO	Opp, Haven of Peace, ...	+2348098571383	Oyo	Oyo	Sunday, October ...	21	SINGLE	MALE
22	609	BAKARE	NOFISAT	OLABISI	Behind BACOTHO, Iso...	+2348080590618	Ori Ire	Oyo	Friday, January 2...	21	SINGLE	FEMALE
23	610	ADIGUN	EDWARD	ADEBANJO	Off Obanako Road, Iso...	+2348086295093	Orelope	Oyo	Thursday, Januar...	20	SINGLE	MALE
24	611	AMBALI	SEMIU	OLUFEMI	Behind Mogbesola Hos...	+2348073067983	Ona Ara	Oyo	Saturday, Decem...	21	SINGLE	MALE
25	612	ADEDIRE	GABRIEL	SUNDAY	Behind Atiba Univ, Idi G...	+2348064626312	Oluyole	Oyo	Sunday, Decemb...	22	SINGLE	MALE
26	613	ADEKOYA	OLUFUNMILAYO	ELZABETH	Behind Satron Grp Schl...	+2348072898186	Olorunsogo	Oyo	Tuesday, Januar...	21	SINGLE	FEMALE
27	631	ONISILE	ADEBAYO	PATRICK	Behind Lalokun 9flat, I...	+2348085496714	Ori Ire	Oyo	Saturday, Septe...	21	SINGLE	MALE
28	632	DARAMOLA	JOSEPHINE	ADEOLA	Behind Cocoa house, Is...	+2348098938258	Orelope	Oyo	Sunday, June 24,...	21	SINGLE	FEMALE

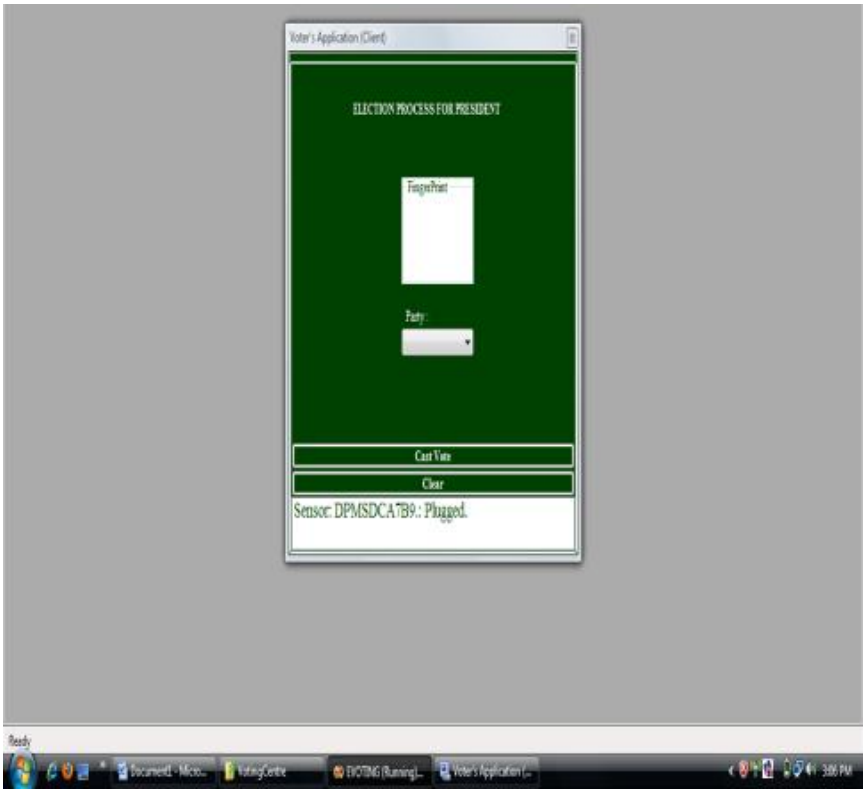
(B)


Poll Site Voting System
ELECTION PROCESS FOR PRESIDENT
FingerPrint
Party :
NPN
Check Vote
Cast Vote
Clear
Vote completed Successfully!!!

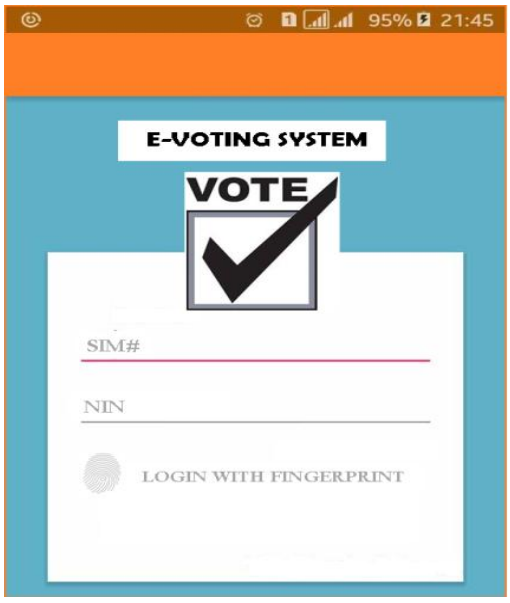
(C)


Evote Website - Mozilla Firefox
Evote Website
E-VOTING SYSTE
Welcome to the home page of the national E-voti
Please exist all other application and ensure
fingerprint reader (or any other compatible reader)
system.
Click the setup link below to download the voters'ap
Download Setup
Opening VotingCentre.rar
You have chosen to open
VotingCentre.rar
which is a: WinRAR archive
from: http://localhost:1081
What should Firefox do with this file?
Open with
WinRAR (default)
DownThemAll!
dTa OneClick!
Save File
Do this automatically for files like this from now on.
OK
Cancel
Done

(D)



(E)



(F)

Fig. 4. Sample GUI of the Implementation of the E-voting system

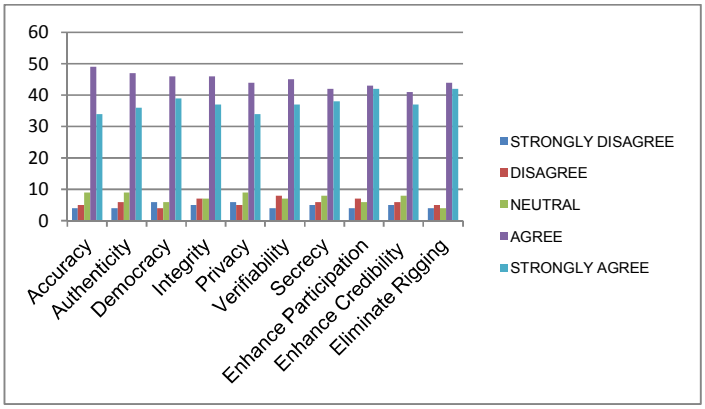


Fig. 5. Analysis of users' performance assessment

Cronbach's alpha was used to measure internal consistency of the security requirements variables accessed via the administered questionnaire. The results of the reliability test for the measures suggest that all the measures are reliable. The alpha coefficients for the measures ranged from 0.75 to 0.79 as presented in Table 2. According to the rules of thumb of [62] values greater than 0.7 are considered "acceptable" level of internal consistency of measure.

Table 2. Reliability test of parameters used in users' performance assessment

Variables	Cronbach's alpha coefficient	[62] Definition
Authenticity and Democracy	0.7718	Acceptable
Integrity and Accuracy	0.7521	Acceptable
Privacy and Secrecy	0.7452	Acceptable
Verifiability and Elimination of Rigging	0.7904	Acceptable

4.4 Performance analysis of deployed security scheme

The performance measure of steganographic systems are measured along the three key parameters mentioned in Subsection 2.3. These are capacity, robustness and imperceptibility. The image quality of the cover image used and stego image obtained from the security scheme developed was assessed by computing the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). A sample cover image used and its equivalent stego image are depicted in Fig. 6 below.

A: Cover Image 8 Bit Grayscale

B: Stego Image 8 Bit Grayscale

Fig. 6. Cover and stego image in grayscale

The MSE is quantifying the difference between values implied by an estimator and the true values of the quantity being estimated. MSE measures the average of the squares of the "errors". The PSNR scales the MSE according to the image range. A higher PSNR indicates that the quality of the stego image is similar to the cover image. Table 3 depicts the computed MSE, PSNR and correlations for three different sample cover images and their respective stego image. It may be noted here that Correlation, determines the extent to which the cover image and the stego image are close to each other even after embedding data.

Table 3. Quality measurements on cover image and stego image

Cover Image	Stego Image	MSE	PSNR (dB)	Correlation
Liverpool.bmp	*StegoLiverpool.bmp*	2.1885	44.74	0.9995
Anfield.bmp	*StegoAnfield.bmp*	4.0186	49.44	0.9988
Emboss1892.bmp	*StegoEmboss1892.bmp*	3.6771	46.17	0.9982

5 Conclusion

Elections and voting are the most critical functions of democracy. In any consensus-based society during electioneering processes, of utmost importance is that the election process must maintain a balance between fairness and performance. Also, the voting systems must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. Many manual voting systems have been developed and used for elections in time past, but each of them has attendant problems. E-voting is significantly becoming the choice alternative to these conventional systems. However, with the growth of information technology, electronic voting systems are susceptible to malicious attacks/threats which can undermine the integrity of the voting process, and hence, the election results. Many security schemes and models have been proposed and developed for securing electronic voting. These schemes and models were based on cryptography, watermarking, steganography or a combination of two of them.

However, express literature survey revealed that most of these schemes are still vulnerable brute force attack, timing attack, session hijacking, replay attack, trapdoor problem, known-plaintext and chosen-plain text attack. This paper implemented a secure scheme for securing electronic voting by combining a hybrid cryptographic scheme with an image steganography technique. Besides improving security, steganography component of the scheme makes data transmission over the network during an election process become less suspicious too. The evaluation of the e-voting system in which the developed security scheme was implemented showed that the system satisfied majority of the security requirements for electronic voting.

The direction of future works can be tuned towards satisfying the information security requirement for availability. Ensuring availability in information systems also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down. Furthermore, quantifying the computer network and infrastructure resources needed to accommodate the implementation requirements of the security scheme proposed in this paper for large scale e-elections is also a visible research area.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Okediran OO, Ganiyu RA. E-agriculture reviewed: Theories, concepts and trends. FUOYE Journal of Engineering and Technology. 2019;4(1):125-130.

[2] Dimitrios Z, Dimitrios L. Securing e-Government and e-Voting with an open cloud. Government Information Quarterly. 2011;28:239-251.

[3] Okediran OO, Omidiora EO, Olabiyisi SO, Ganiyu RA, Alo OO. A framework for a multifaceted electronic voting system. International Journal of Applied Science and Technology. 2011;1(4):135-142.

[4] Azeta AA, Azeta VI, Oluwaseun O, Azeta AE, Ayeni GA. Implementing an E-democracy system in Nigeria. Proceedings of the 11th International Conference on Electronic Government and National Security, Nigeria Computer Society (NCS), Osun State, Nigeria. 2013;98–103.

[5] Buchsbaum TM. E-voting: International developments and lessons learnt. Proceedings of Workshop on Electronic Voting in Europe –Technology, Law, Politics and Society, Austria; 2004. Available:www.subs.emis.de/LNI/Proceedings/Proceedings47/ Proceeding.GI.47-4.pdf

[6] Longe OB, Roberts ABC, Onifade OFW, Kaka O, Isiaka RM. Framework for the development of a hybrid chaotic image scheme for multimedia data encryption. Proceedings of 3rd International Conference on ICT Applications, Obafemi Awolowo University, Ile-Ife, Osun State, Nigeria. 2008;3:150–154.

[7] Longe OB, Boateng R, Dada EG, Olaniyan O, Olaseni O. Stegacrypt: A reduced least significant bit insertion rate carrier for transmitting embedded information. The Journal of Computer Science and Its Application: An International Journal of the Nigeria Computer Society (NCS). 2010;17(1):1–12.

[8] Longe OB. On the use of image-based spam mails as carriers for covert data transmission. Computing and Information Systems Journal. 2011;15(1):1–5.

[9] OASIS. Election Markup Language (EML) 4.0a. Organization for the Advancement of Structured Information Standards; 2003.

[10] Gritzalis D. Principles and requirements for a Secure E-voting system. Computers & Security. 2002;21(6):539–556.

[11] Cranor LF, Cytron RK. Sensus: A security conscious electronic polling system for the internet. Hawaii International Conference on System Sciences. 1997;3:560.

[12] Dini G. A secure and available electronic voting service for a large-scale distributed system. Future Generation Computer System. 2003;19(1):69–85.

[13] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. In Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, Springer-Verlag. 1992;718:244–251.

[14] Karlof J, Naveen S, Wagner D. Cryptographic voting protocols: A systems perspective. Proceedings of the Fourteenth USENIX Security Symposium (USENIX Security 2005); 2005. Available:http://www.cs.berkeley.edu/~nks/papers/cryptovoting-senix05.pdf

[15] Karro J, Wang J. Towards a practical, secure, and very large scale online election. Computer Security Applications Conference, Annual. 1999;161.

[16] Hwang LM, Chang C. Security enhancement for anonymous secure E-voting over a network. Computer Standards & Interfaces. 2003;25(2):131–139.

[17] Mitrou L, Gritzalis D, Katsikas SK. Revisiting legal and regulatory requirements for secure E- voting. In SEC '02: Proceedings of the IFIP TC11 17th International Conference on Information Security, Deventer, The Netherlands. Kluwer, B.V. 2002;469–480.

[18] Okediran OO. Mobile phones: A panacea for the implementation of E-voting in Nigeria. Asian Journal of Computer Science. 2019;4(1):1-15.

[19] Chaum D. Elections with unconditionally secret ballots and disruption equivalent to breaking RSA. In Proceedings of Computer Science on Advances in Cryptology-EUROCRYP. 1987;177–182.

[20] Jan J, Tai C. A secure electronic voting protocol with IC cards. Journal of Systems and Software. 1997;39(2):94–101.

[21] Delfs H, Knebl H. Introduction to cryptography: Principles and applications. Second Edition, Springer-Verlag Berlin Heidelberg; 2007.

[22] Stallings W. Cryptography and network security: Principles and practice. Seventh Edition, Pearson Education Limited; 2017.

[23] Biggs N. Codes: An introduction to information communication and cryptography. Springer; 2008.

[24] Paar C, Pelzl J. Understanding cryptography: A textbook for students and practitioners. First Edition, Springer-Verlag; 2010.

[25] Daemen J, Rijmen V. The Rijndael Block Cipher, AES Proposal; 1999.

[26] Reddy VL, Subramanyam A, Reddy PC. Implementation of LSB steganography and its evaluation for various file formats. International Journal of Advanced Networking and Applications. 2011;2(5):868-872.

[27] Fridrich J, Goljan M, Soukal D. Searching for the Stego Key. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. Security, Steganography, and Watermarking of Multimedia Contents VI. 2004;5306:70–82.

[28] Anderson RJ, Petitcolas FA. On the limits of steganography. IEEE Journal of Selected Areas in Communications. 1998;16(4):474-481. Special Issue on Copyright & Privacy Protection. 1998;474-482.

[29] Kaur S, Bansal S, Bansal RK. Steganography and classification of image steganography techniques. IEEE International Conference on Computing for Sustainable Global Development (INDIACom), 5-7 March 2014, New Delhi, India; 2014.

[30] Kothari L, Thakkar R, Khara S. Data hiding on web using combination of steganography and cryptography. International Conference on Computer, Communications and Electronics (Comptelix), 1-2 July 2017, Jaipur, India; 2017.

[31] Provos N, Honeyman P. Hide and seek: An introduction to steganography. IEEE Security and Privacy Journal. 2003;32-44.

[32] Akhtar N, Khan S, Johri P. An improved inverted LSB image steganography. International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 7-8 Feb. 2014, Ghaziabad, India; 2014.

[33] Lee YK, Chen LH. High capacity image steganographic model. Visual Image Signal Processing. 2000;147:03.

[34] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal Processing. 2010;90(3):727-752.

[35] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recognition. 2004;37(3):469–474.

[36] Tohari A, Jainkun H, Song H. An efficient mobile voting system security scheme based on elliptic curve cryptography. In Proceedings of Third International Conference on Network and System Security, IEEE Computer Society. 2009;474-479.

[37] Purusthomata BR, Alwyn RP. Design and implementation of secure internet based voting system with user anonymity using identity based encryption system. Proceedings of IEEE International Conference on Services Computing, IEEE Computer Society. 2009;474-481.

[38] Sujata M, Banshidhar M. A secure multi authority electronic voting protocol based on blind signature. International Conference on Advances in Computer Engineering. 2010;271-273.

[39] Gina GG, Roberto G, Gonzalo ID. Identity based threshold cryptography and blind signatures for electronic voting. WSEAS Transactions on Computers. 2010;9(1):62-71.

[40] Patil VM. Secure electronic voting system by using blind signature and cryptography for voter's privacy and authentication. Journal of Signal and Image Processing. 2010;1(1):1-6.

[41] Katiyar S, Meka KR, Barbuiya FA, Nandi S. Online voting system powered by biometric security using steganography. Proceedings of The Second International Conference on Emerging Applications of Information Technology, IEEE Computer Society. 2011;288-291.

[42] Alok K, Atul K. A novel approach for secure mobile-voting using biometrics in conjunction with elliptic curve crypto-stegano scheme. International Journal of Technology And Engineering System (IJTES). 2011;2(1):8-11.

[43] Mallick PK, Kamilla I. Crypto steganography using linear equation. International Journal of Computer and Communication Technology. 2011;2(8):106-112.

[44] Rura L, Isaac B, Haldar MK. Secure electronic voting system based on image steganography. Proceedings of IEEE Conference on Open Systems (ICOS2011). 2011;80-85.

[45] Gupta N, Kumar P, Chhokar S. A secure blind signature application in E-voting. In Proceedings of the 5th National Conference, Computing for National Development, March 10-11, 2011, Bharati Vidyapeeth Institute of Computer Applications and Management, New Delhi. 2011;1-4.

[46] Sodiya A, Onashoga S, Adelani DI. Secure E-voting architecture. Eighth International Conference on Information Technology: New Generations, IEEE Computer Society. 2011;342-347.

[47] Sulthana SS, Kanmani S. Evidence based access control over web services using multi security. International Journal of Computer Applications. 2011;17(3):1-7.

[48] Swamminathan B, Dinesh CD. Highly secure online voting system with multi-security using biometric and steganography. International Journal of Advanced Scientific Research and Technology. 2012;2(2):195-203.

[49] Prabha SM, Ramamoorthy S. A novel data hiding technique based bio-secure online voting system. Proceedings of International Conference on Computing and Control Engineering (ICCCE 2012). 2012;1-4.
Available:http://www.iccce.co.in/Papers/ICCCECS143.pdf

[50] Linu P, Anilkumar MN. Authentication for online voting using steganography and biometrics. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET). 2012;1(10):26-32.

[51] Nivedtha R, Meyyapan T. Image security using steganography and cryptography techniques. International Journal of Engineering Trends and Technology. 2012;3(3):366-371.

[52] Olaniyi OM, Arulogun OT, Omidiora EO, Oludotun A. Design of secure electronic voting system using multifactor authentication and cryptographic hash functions. International Journal of Computer and Information Technology. 2013;2(6):1122–1130.

[53] Neha G. Study on security of online voting system using biometrics and steganography. International Journal of Computer Science and Communication. 2014;5(1):29-32.

[54] Kharmate BB, Shaikh SS, Kangane PR, Anant T. A survey on smart E-voting system based on fingerprint recognition. International Journal of Innovative Research in Computer and Communication Engineering. 2015;3(9):8093-8100.

[55] Fashoto SG, Adeyeye M, Uzoka FE, Usthman FH. Securing a scalable E-voting system using the RSA algorithm: The case of a group voting process in a Tertiary School. Computer Technology and Application. 2016;7:11-27.

[56] Alhasnawi MK, Alkhalid AS. Secure online voting using steganography and biometrics. International Journal of Current Engineering and Technology. 2017;7(3):1097-1104.

[57] Rura L, Issac B, Haldar MK. Online voting system based on image steganography and visual cryptography. Journal of Computing and Information Technology. 2017;25(1):47–61.

[58] Sundar NA, Kishore MV, Suresh C. A secure E-voting system using RSA and Md5 algorithms using random number generators. International Journal of Applied Engineering Research. 2018;13(11): 9468-9473.

[59] Finkelstein A, Kramer J, Nuseibeh B. Software process modeling and technology. Research Studies Press Ltd. Taunton, Sommerset, UK; 1994.

[60] Post G, Anderson D. Management information systems: Solving business problems with information technology. Fourth Edition, New York: McGraw-Hill Irwin; 2006.

[61] Whitman ME, Mattord HJ. Principles of information security. Third Edition, Cengage Learning EMEA; 2009.

[62] George D, Mallery P. SPSS for windows step by step: A simple guide and reference. 11.0 update. (4th Ed.), Boston: Allyn & Bacon; 2003.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
https://sdiarticle4.com/review-history/51915