A Multidisciplinary Journal Publication of the Faculty of Science, Adeleke University, Ede, Nigeria

2015 Edition Vol 2.

Performance Assessment of an Enhanced Crystographic Model for Secure E-Voting

Olaniyi, O.M.
Department of Computer Engineering
Federal University of Technology,
Minna, Niger State, Nigeria
mikail.olaniyi@futminna.edu.ng

Arulogun, O.T., Omidiora, E.O. & Okediran, O.O.
Department of Computer Science and Engineering
Ladoke Akintola University of Technology
Ogbomoso, Oyo State, Nigeria
otarulogun@lautech.edu.ng, eoomidiora@lautech.edu.ng, ookediran@lautech.edu.ng

ABSTRACT
In this paper, we present qualitative performance assessment of an imperceptible and robust crystographic model of secure electronic voting. The performance analysis was achieved based on the degree to which the model meets the generic and functional requirements of secured e-voting system: authentication, integrity, confidentiality and verifiability using exploratory factor analysis, multiple correlations and non-parametric inferential test statistics. Further qualitative assessment results showed that the implemented model possessed capacity to guarantee and validate voters for who they are, guarantees the integrity of elections, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process in developing country where digital divide is significant.

Keywords: Steganography, Crystography, E-voting, Information hiding, Authentication, Confidentiality, Integrity, Verifiability, Cryptography

1. INTRODUCTION

Democracy is the institutionalization of freedom (US. B. of Inter. Info. Programme (2010).The ultimate freedom of the populace to serve as their guardian and forge an ideal path of fair and trusted system of governance. The United Nations Universal Declaration of Human Rights affirmed that: "The foundation of freedom, justice and peace in the world is based on the recognition of inherent dignity of the equal and inalienable rights of all members of the human family" (US. B. of Inter. Info. Programme (2010). Citizens in a democratic system of governance have not only rights to vote, but to participate in the political system that, in turn, protects their freedom and rights through electoral processes. The democratic electoral process rests on a fair, universally acceptable voting system through which the electorate can easily and accurately cast a vote (Olaniyi, Arulogun, and Omidiora, 2012). The most significant and critical phase of democratic electoral process is the voting phase. The integrity of the voting phase is a function of the integrity of the democratic process which depends on requirements such as correctness, robustness to fraudulent behaviors, consistency, transparency and security of entire democratic processes (Malkawi, Khasaweh, and Al-Jarrah, 2009).

To secure e-democratic decision making, design and development of secure and scalable electronic voting systems has been an active research endeavor in literatures using different techniques. In John, Ayo, Ndujuiba, and Okereke (2013), Multifactor Authentication schemes using Smart Card, Fingerprint Biometrics and Personal Identification Number (PIN) were used to provide security and convenience in e-voting system. Similar Multifactor Authentication mechanism using Visual Challenge grid mechanism, one-time personal identification short message service (OTP-SMS) and cryptographic hash functions were used to provide authentication and integrity security requirements to e-voting systems in (Olaniyi, Arulogun, Omidiora, and Adeoye, 2013). In Gunjal & Mali (2012), a multi-layer, secure web based e-voting system was proposed using biometric and wavelet based image watermarking technique in YCgCb color space. In Moayed, Abdul Ghani, and Mahmod (2008), a survey of cryptographic techniques used for e-voting systems was presented.

Similar survey on cryptographic and crystographic models was carried out in Olaniyi, Arulogun,Omidiora, and Okediran (2013). In Olaniyi et al.,(2013) an adaptable, robust and imperceptible secure e-voting model for developing countries like Nigeria was proposed. Crystography is the combination of cryptographic techniques and steganographic techniques to the enhancement of communications security over an insecure enterprise networks.

In this paper, we present further qualitative performance assessment of a previous work on imperceptible and robust crystographic model for secure e-voting presented in Olaniyi, et al., (2014) using inferential statistical techniques. The current modified open ballot system of election in Nigeria was studied and an enhanced stegano-cryptographic or crystographic model for secure e-voting systems was developed using information hiding techniques and software engineering process models. Voters of acceptable age range were asked to use the developed secured voting system based the e-voting model. Relevant data were captured and analyzed using inferential data analysis. An imperceptible and robust secured e-voting model for democratic governance was assessed using developing country like Nigeria as a case study with the view of asserting the degree the model fulfill fundamental and social security requirements require for the conduct of free, fair, credible and genuine e-elections (Olaniyi, et al., 2014).

The rest of the paper is organized into the following: Section 2 describes basics cryptographic modeling to secure e-voting systems, Section 3 describes methodologies adopted to carry out the research; Section 4 presents the results and discussion of the model's quantitative assessments and sections 5 concludes and provide recommendations for future research endeavor.

2. CONCEPT OF CRYSTOGRAPHIC MODELLING IN SECURE ELECTRONIC VOTING

Crystography is the synergistic combination of information hiding techniques of steganography and cryptography for enhancing the security of communications over enterprise network (Gabriel, Alese, Adetumbi, and Adewale, 2013). When crystographic information security model is applied to social distributed information system like electronic voting systems, credible and transparent electronic democratic decision making can be deployed to populace (Olaniyi, et al., 2015). In this model shown in Figure 1, Bob (the sender and the voter) sends a secret message P (electronic ballot) to Alice (the receiver and voting administrator).In order to do this, Bob first encrypts the message using an encryption algorithm to produce a cipher text, M. Using a specific steganographic algorithm on cover image, C, Bob identifies redundant bits and embed the desire encrypted information without arousing an eavesdropper (Wendy) suspicion to create the final stego Image. The stego Image is transmitted over a public channel to Alice who can get M through the multiple level of extraction process (Gabriel et al., 2013; Olaniyi et al., 2012).

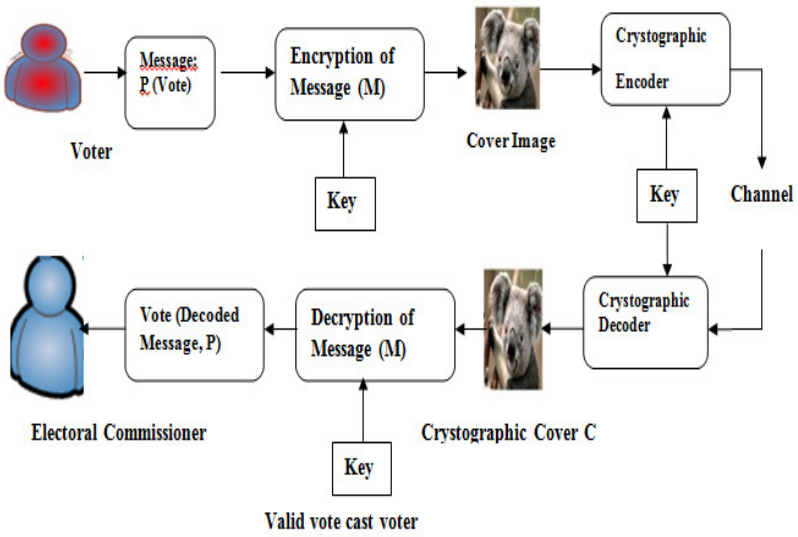

Fig. 1: Crystographic Information Security Model for Secure E-Voting (Source: Olaniyi, et al.., 2012)

3. MATERIALS AND METHODS

In this section, brief description of performance assessment factors, research questions, data collection instrument, method, tools for data analysis are discussed.

3.1 Performance Assessment Factors and Research Questions

The performance assessment factors in this further evaluation is similar to fundamental security issues of e-voting system from voter's end voter's end, the network and at voting system's end presented in Olaniyi et al., (2014). These fundamental technical security issues and social factors issues are:

i. Could voters be verified to be who they claimed they are? i.e. Authentication issue
ii. Could vote casted remain secret? i.e. Issue of confidentiality
iii. Could votes remain unaltered? i. e. Issue of Integrity issue.
iv. Could votes be counted and audited accurately? Issue of Non-Repudiation
v. Could e-voting system developed on the model allow multiple voting? i.e. democratic issue
vi. Could e-voting system developed on the model eliminate rigging attributed to conventional voting? i.e. Issue of rigging?
vii. Could the e-voting model enhance citizen participation?
viii. Could the developed secured e-voting model drive free, fair and credible e-governance?

3.2. Study Area and Sample size

The study population comprises of voters of acceptable age range within campus environment at the department of Computer Science and Engineering, LAUTECH Ogbomoso in Oyo State, Nigeria and Computer Engineering department of Federal University of Technology, Minna, Niger state Nigeria. Purposive sample technique is adopted to aid the ease of data collection of the members (users) of the sample size. The users sampled are voter's eligible to vote (of 18 yrs and above) and electorate of current conventional voting system in Nigeria (Olaniyi et al., 2014). Each voter expresses their feeling about the degree to which the developed crystographic model fulfill fundamental requirements of secure e-voting using the following Likert linguistic values: Strong disagree:1, disagree:2,Neutral:3,Agree:4,Strongly Agree:5.

A total of one hundred and ten (110) sample users perceptive analysis form (questionnaire) were distributed for assessment of the e-voting model after exercising pre-election process: voter's registration; election process-voting and post-election process-verifiability on the developed secured in e-voting system based on e-voting model. Users were asked to assess the developed e-voting model both for technical and social factors in section 3.1 that can significantly influence the assertion that the model possessed capacity to guarantee and validate voter's for who they said they are, guarantees the integrity of elections, ensures privacy of the voters, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process.

3.3. Data Collection Instrument

A well-structured user's perceptive analysis form (questionnaire) was designed to capture both technical and social factors of free, fair and credible e-voting system. The questionnaire was tested and validated for reliability using Cronbach's alpha test in SPSS environment. The interpretation of the assessment using benchmark proposed in (Hinton, Brownlow, McMurvay, and Cozens, 2004) is provided for different technical and social factors have been presented in Olaniyi et al., (2014).

3.4. Method and Tools for Data Analysis

Of the one hundred and ten (110) users assessed, only one hundred and two (102) responses were received from users from the duly filled user perceptive analysis forms(questionnaires) and primary data from the duly filled questionnaires was captured, compiled and analysed using Statistical Package for Social Sciences (SPSS) version 11.5 for Windows environment using inferential data analysis. The inferential test statistic techniques were adopted to investigate the impact of extracted security variables on the performance of the developed model using the target population. Exploratory factor analysis, multiple correlations and non-parametric Chi-Square inferential test statistics in SPSS were used to evaluate the degree of security of the e-voting model.

Using exploratory factor analysis, factors that measure the generic requirements of secure e-voting model variables were extracted using principal component analysis and varimax method. Therefore, inference statistics that show the relationships were carried out using Spearman's correlation as well as Chi-Square test statistics on captured non-parametric ordinal data. The exploratory factor analysis involved extraction of six significant factors that measured the generic security requirements in e-voting variables from a list of fifteen using the principal component analysis and Varimax with Kaiser Normalization method.

The inferential statistics that shows the relationships between study variables using the bivariate correlation through spearman's ranking was used to establish the relationship between extracted generic requirements of secure e-voting variables with the secure e-voting performance of the model (through the seventh factor-participation of voters as a result implementation of the developed secure e-voting system). In addition, chi-square test was performed to investigate the impact of consideration of generic security requirements of e-voting on the performance of secure e-voting based on the developed modified model by sampled users. The findings of these inferential data analysis were reported in the next section.

4. RESULTS AND DISCUSSIONS

Factors with eigenvalues greater than 1 (>1) from exploratory factor analysis were extracted and items with correlation coefficients below ± 0.3 were deleted because they were considered to have low contribution to the factors extracted. Table 1 shows correlation coefficients for the six factors extracted: Authentication requirements of secure e-voting, secrecy and confidentiality requirements, verifiability requirements, multiple voting, elimination of rigging (integrity), ubiquitosity of secure e-voting system. Table 2 shows the correlation coefficient using the bivariate correlation through spearman's ranking. In addition, chi-square test was performed to investigate the impact of generic security requirements of e-voting with the performance of secure e-voting based on the developed modified model by sampled users.

Table 1: Rotated Component Matrix by Varimax with Kaiser Normalization

		Component		
	Extracted Security Variable	1	2	3
1	Authentication Requirements of Secure E-voting System	.757		
2	Secrecy and Confidentiality Requirements of Secure E-voting System	.802		.273
3	Non-Repudiation and Verifiability Requirements of Secure E-voting System	.403	.615	
4	Multiple voting	.135		
5	Elimination of Rigging attributed to manual voting system	.616	.332	.279
6	Ubiquitosity of Secure E-Voting System	.609		
7	Participation of Voters as a result of Implementation of the developed Secure E-voting System			.922

Table 2: Total Variance of the Considered Factors using Principal Component Analysis

Component	*Initial Eigenvalues*		
	Total	**% of Variance**	**Cumulative %**
1	2.261	32.294	32.294
2	1.160	16.571	48.865
3	1.133	16.182	65.047
4	0.832	11.881	76.928
5	0.682	9.739	86.667
6	0.545	7.788	94.455
7	0.388	5.545	100.000

From Table 2, the authentication requirement of secure e-voting has an Eigen value of 2.261 and a percentage of variance of 32.294 ,Secrecy and confidentiality requirements has an Eigen value of 1.160 and a percentage of variance of 16.571, verifiability requirements has an Eigen value of 1.133 and a percentage of variance of 16.182, multiple voting has an Eigen value of .832 and a percentage of variance of 11.881, elimination of rigging (integrity) has an Eigen value of .682 and a percentage of variance of 9.739,ubiquitosity requirements has an Eigen value of .545 and a percentage of variance of 7.788.

Also, multiple correlations were used to establish the relationship between authentication requirements, secrecy and confidentiality requirements, verifiability requirements, multiple voting, elimination of rigging (integrity), ubiquitosity of secure e-voting service generic security requirements factor with secure e-voting performance of the model (through the seventh factor- participation of voters as a result implementation of the developed secure e-voting system).The results of these relationships are summarized with corresponding correlation coefficients are tabulated in Table 3.

From Table 3, the following relationships and implications were observed and deduced respectively:

a) There was significant positive relationship between authentication requirement of secure e-voting with secure e-voting performance of the model with correlation coefficient of 0.203 with significance value of 0.05.i.e. (r = 0.203, P-value < 0.05). This implies that as the voters attempted to express their unique e-democratic choices through usage of secure e-voting system, their identity was uniquely authenticated and validated with the developed secure e-voting system based on modified crystographic technique. This finding is in agreement with the work of Linu & Anilkumar, (2012) which established that authentication security requirement represents the most critical security issue of secure e-voting.

b) There was highly significant positive relationship between secrecy and confidentiality requirement of secure e-voting with secure e-voting performance of the model with correlation coefficient of 0.272 with significance value of 0.01 (r = 0.272, P-value < 0.01). This implies that as the voters attempted to express their unique e-democratic choices through usage of secure e-voting system their privacy and anonymity were preserved by the developed secure e-voting system based on the developed modified crystographic technique. The secret e-ballot was maintained and protected from the view of an eavesdropper. This finding is in agreement with the assertion of the imperceptibility basis of steganographic systems. Truly secure steganographic system should be imperceptible neither by human eye nor by statistical attacks (Nagham, Abid, Ahmad, & Osamah, 2012).

c) There was significant positive relationship between non-repudiation and verifiability requirement of secure e-voting with secure e-voting performance of the model with correlation coefficient of 0.151 with significance value of 0.005.i.e. (r = 0.151, P-value < 0.005). This implies that after the voter expressed their secret e-democratic choices through usage of secure e-voting system they also have tendency to independently verify secretly, the inclusion and removal of their preference in the final tally. This finding is in agreement with the consensus of the notion of end-to end verifiability requirement of secure e-voting in literature (Kremer, Ryan, and Smyth, 2010; Chaum, Ryan, and Schneider, 2005) .The notion of allowing voters and election observers to verify, independently of the hardware and software running that ballots are recorded, tallied and declared accurately.

d) There was significant negative relationship between multiple voting requirement of secure e-voting with secure e-voting performance of the model with correlation coefficient of -0.026 with significance value of 0.05.i.e. (r = -0.026, P-value < 0.005). This implies that as the voters attempted to express multiple e-democratic choices through the usage of secure e-voting system, their inconsistency with the tenet of true democratic rule of a unique vote for a voter was denied by the developed secure e-voting system based on modified crystographic technique. This finding is in agreement with the notion of democratic tenet of e-voting as established in Okediran, Omidiora, Olabiyisi,Ganiyu, Alo, (2011); Abdul Hamid, Adebayo,Ugiomoh, and AbdulMalik, (2013).

e) e) There was significant positive relationship between elimination of rigging (integrity) requirement of secure e-voting with secure e-voting performance of the model with correlation coefficient of 0.184 with significance value of 0.05.i.e. (r = 0.151, P-value < 0.005). This implies that e-democratic decision making process through the usage of secure e-voting system based on the developed modified crystographic technique ensured integrity of ballot from the threat of eavesdropper and attacker en-route from near and remote voter as well as voting servers. This finding is in agreement with the notion of preserving the election canvas and e- ballots form modification en-route to the election server in literature (Tohari, Jainkun, & Song, 2009; Patil, 2010; Okediran, et al., 2011).

The Chi-Square test characteristic analysis was achieved by measuring the performance of secure e-voting based on the developed modified model against major six variables found after factors analysis. In addition, a null and an alternative hypothesis were formulated as:

Null Hypothesis
The performance of secure e-voting model is not dependent on identified generic variables of secure e-voting.

Alternative Hypothesis
The performance of secure e-voting model is dependent on identified generic variables of secure e-voting.

Table 4 shows the result of chi-square test characteristics in SPSS of the performance of secure e-voting with six variables found after factors analysis. It is clear from Table 4, that all the six extracted variables had a significance value less than 0.005 at 5% level of significance, thus the null hypothesis is rejected. Therefore, the performance of secure e-voting model is dependent on the identified generic variables of secure e-voting.

Table 3: Correlation Coefficients of extracted generic security requirements variables

Spearman's rho	***1***	***2***	***3***	***4***	***5***	***6***	***7***
Authentication Requirements	1.000						
Secrecy and Confidentiality Requirements	0.230 (*)	1.000					
Non-Repudiation and Verifiability Requirements	0.052	0 .134	1.000				
Multiple voting	-0.034	0.015	0.256(**)	1.000			
Elimination of Rigging attributed to manual voting system	0.211 (*)	.384(**)	0.270(**)	-0.091	1.000		
Ubiquitosity of Secure E-Voting System	0.220 (*)	0.250(*)	0.130	-0.030	0.171	1.000	
E- participation of voters due to the developed secure e-voting System	**0.203 (*)**	**0.272(**)**	**0.151(*)**	**-0.026(*)**	**0.184(*)**	**0.072(*)**	**1.000**

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed). a Listwise N = 102

Table 4: Chi-Square Test Statistics for six variables found after factors analysis

	Authentication Requirements of Secure E-voting System	*Secrecy and Confidentiality Requirements of Secure E-voting System*	*Non-Repudiation and Verifiability Requirements of Secure E-voting System*	*Elimination of Rigging attributed to manual voting system*	*Multiple voting*	*Ubiquitosity of Secure E-Voting System*
Chi-Square(a)	124.961	119.863	135.549	102.020	53.784	162.216
Df	4	4	4	4	4	4
Asymp. Sig.	.000	.000	.000	.000	.000	.000

0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 20.4.

5. CONCLUSION AND RECOMMENDATIONS FOR FUTURE RESEARCH WORK

This paper has successfully presented qualitative performance assessment of crystographic model of electronic voting for delivery of transparent and credible e-democracy. The fundamental technical secured e-voting requirements of voter's authentication, vote confidentiality, vote integrity and verifiability as well as functional requirements of secure e-voting systems like scope for rigging, democracy are preferential assessment factors to impact electorate choice were investigated. Correlation analysis was used to investigate the relationship between extracted variables and the performance of the developed secure e-voting model. Spearman's ranking was used to establish the relationship between extracted generic requirements of secure e-voting variables with the secure e-voting performance of the model and chi-square test was used to investigate the impact of consideration of generic security requirements of e-voting on the performance of secure e-voting based on the developed modified model by sampled users.

The findings of correlation analysis and spearman's ranking show that the extracted variables had a positive and significant relationship with the performance of the developed secure e-voting model. The chi-square test characteristic of all the six extracted variables had a significance value less than 0.005 at 5% level of significance, thus the null hypothesis was rejected. Therefore, the performance of secure e-voting model is dependent on the identified generic variables of secure e-voting. The findings of this paper will make steganographers, software developers and government in making sound decision on what to consider in designing , developing and administration of secure e-voting systems for future free, fair and credible e-democratic decision making through e-voting. The developed secured electronic voting model in Olaniyi et al., (2015), if implemented in future e-democratic decision making in developing countries will help increase the level of citizens' participation in the elections and ensure a better, faster, easier and more efficient means of voters' registration ,voting and auditing compare to existing manual method of voting.

In future, further qualitative performance evaluation of other information hiding techniques like watermarking should be carried out. The result should be compared with the developed crystographic model for government and its election authority to ensure increased public participation, ensure political trust and confidence while demystifying problems of insecurity in e-democratic making in future elections.

REFERENCES

1. Abdul Hamid, S. M., Adebayo, O. B., Ugiomoh, D. O., & AbdulMalik,M.D. (2013). The Design and Development of Real time e-voting System in Nigeria with emphasis on Security and Result Veracity. International Journal of Computer Network and Information Security, 5(5), 9-18.
2. Amer, A. & El-gendy, H. (2013). Towards a fraud prevention e-voting system. nternational Journal of Advanced Computer Science and Applications, 4(4), 147-149.
3. Chaum, D. ,Ryan, P. Y. A. & Schneider, S. (2005). A Practical Voter-Verifiable Election Scheme. In Proceedings of 10th European Symposium On Research In Computer Security, ESORICS'05, 3679 of Lecture Note in Computer Science (LNCS), Springer, (pp. 118–139.). Springer.
4. Gabriel, A. J, Alese, B. K., Adetumbi, A.O. & Adewale, O. S. (2013). Post-Quantum Crystography: A combination post-quantum cryptography and steganography, , In proceedings of the IEEE 8th International Conference for Internet Technology and Secured Transactions(ICITST-2013) (pp. 449-452.). USA: IEEE.
5. Gunjal, B. L. & Mali, S. N. (2012). Secure e-voting System with Biometric and Wavelet based Watermarking Technique in Ycgcb color space. In proceedings of IET International Conference on Information Science and Control Engineering (icisce 2012),, (pp. 1-6).
6. Hinton, P., Brownlow, C., McMurvay, I., & Cozens, B. (2004). SPSS explained. East Sussex, England: Routledge Inc.
7. John, N. S., Ayo, C. K., Ndujuiba C., & Okereke, C. E. (2013). Design and Implementation of a Unified e-ID Card for Secure Electronic Voting System (MUSES). International Journal of Computer and Information Technology (IJCIT) , 2(6), 1131-1135.
8. Kremer, S., Ryan, M. & Smyth, B. (2010). Retrieved November 17th, 2012, from Retrieved online from http://www.lsv.ens-cachan.fr/Projects/anr-ote/PUBLIS/KRSesorics10.pdf
9. Linu, P., & Anilkumar, M. N. (2012). Authentication for Online Voting Using Steganography and Biometrics. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 1(10), 26-32.
10. Malkawi, M., Khasaweh, M. K. & Al-Jarrah, O. (2009). Modelling and Simulation of a Robust E-Voting System. Communication of Information Management Association (IBIMA) Journal, 8, 198-206.
11. Moayed, M. J., Abdul Ghani, A. & Mahmod, R. (2008). A survey on cryptography Algorithms in Security of Voting System Approaches. International Conference on Computational Sciences and Its Applications (ICCSA), (pp. 190 – 200).
12. Nagham, H. A. (2012). Image Steganography Techniques: An Overview. International Journal of Computer Science and Security, 6(3), 168-187.
13. Okediran, O. O. Omidiora, E. O., Olabiyisi, S. O. Ganiyu R.A. & Alo, O. O. (2011). A Framework for a Multifaceted Electronic Voting System. International Journal of Applied Sciences (IJSA), 1(4), 135-142.
14. Olaniyi, O. M. Arulogun, O.T. & Omidiora, E. O. (2012). Towards an Improved Stegano-Cryptographic Model for Secure Electronic Voting, 4(3). African Journal of Computing and ICTs, 4(3), 23 – 32.
15. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O. & Okediran, O. O. (2014). Performance Assessment of an Imperceptible and Robust Secured E-Voting Model, 3(6), 127-132. International Journal of Scientific and Technological Research (IJSTR), 3(6), 127-132.
16. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O. & Okediran, O. O. (2013). A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System. Covenant Journal of Informatics and Communication Technology (CJICT),, 1(2), 54-78.
17. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O. & Okediran, O.O. (2015). Implementing Generic Security Requirements in E-Voting Using Modified Stegano-Cryptographic Approach, 7(1),. International Journal Of Information and Computer Security (IJICS), 7(1), 64-90.
18. Olaniyi, O. M., Arulogun, O.T., Omidiora, E.O. & Adeoye,O. (2013). Design of Secure Electronic Voting System using Multifactor Authentication and Cryptographic Hash Functions. International Journal of Computer and Information Technology (IJCIT), 2(6), 1122-1130.
19. Patil, V. M. (2010). Secure Electronic Voting System by using Blind Signature and Cryptography for Voter's Privacy and Authentication. Journal of Signal and Image Processing, 1(1), 1-6.
20. Tohari, A., Jainkun, H., & Song, H. (2009). An Efficient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography. In Proceedings of Third International Conference on Network and System Security, , 2009 (pp. 474-479). IEEE Computer Society.
21. US. B. of Inter. Info. Programme, (2010). DemocracyInBrief .Retrieved July 2014, 24, from http://www.ait.org.tw/en/201001-DemocracyInBrief.pdf (24th July 2014)

Biographical Notes

Olayemi M. Olaniyi is a Lecturer in the Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria. He obtained his B. Tech in 2005 and M.Sc. in 2011 in Computer Engineering and Electronic and Computer Engineering respectively. He had his PhD in Computer Security from the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria in 2015. He has published in reputable journals and learned conferences. His areas of research includes: Computer Security, Intelligent Systems, Embedded Systems and Telemedicine.

Oladiran T Arulogun is an Associate Professor in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He was a visiting Research scholar at Hasso-Plattner Institute, Potsdam, Germany in 2012. He has published in reputable journals and learned conferences. His research interests include Networks Security, Mobile IPv6, Wireless Sensor Network and its applications.

Oluwasayo E. Omidiora is currently a Professor of Computer Engineering in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Sc. Computer Engineering in 1991. He obtained his M.Sc. and Ph.D in 1998 and 2006 respectively. He has published in reputable journals and learned conferences. His research interests are in Soft Computing and Biometrics systems.

Oladotun O. Okediran is a Lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Tech. Computer Engineering, M.Tech. and Ph.D in 2002, 2008 and 2011 respectively. He has published in reputable journals. His research interests include: Computational optimization, e-commerce, biometrics- based algorithms and their applications to e-voting systems.