I. J. Computer Network and Information Security, **2020, 4, 51-59**
Published Online August 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.04.05

Visual Semagram: An Enhanced Technique for Confidentiality Requirement of Electronic Voting System

Prof. Adewale Olumide S.
Department of Computer Science, Federal University of Technology, Akure, Nigeria
E-mail: adewale@futa.edu.ng

Dr. Boyinbode Olutayo K.
Department of Information Technology, Federal University of Technology, Akure, Nigeria
E-mail: okboyinbode@futa.edu.ng

Salako E. Adekunle
Department of Computer Science, Federal University of Technology, Akure, Nigeria
E-mail: salakoea@futa.edu.ng

Received: 04 March 2020; Accepted: 16 March 2020; Published: 08 August 2020

Abstract: One of the rights of citizens in any democratic society is to freely elect a particular candidate into a specific office for governance. This implies that among the candidates participating in an election, one of them would emerge as a winner based on the specified rules and regulation. The recent reports on the election in different parts of the world revealed that the corrupt politicians and corrupt election officers did manipulate the sensitive results thereby leading to undesired candidate emerge as a winner. This implies that election results had not been adequately secured against an attack such as alteration for false results. This paper reviewed scholarly published work and presented a novel technique using visual semagram to satisfy the confidentiality requirement of the electronic voting system. The mathematical equations on how the three primary additive colours (Red, Green and Blue) could be used to modify and conceal the election results against suspicion and alteration were presented. The significance of this paper included the presentation of a technique that would conceal any sensitive message from attackers' suspicion and scholarly piece of information for further investigation in handling insecurity issues. The future work would involve the implementation and evaluation of the proposed technique to achieve the confidentiality requirement of the e-voting system, and to establish the validity and reliability of proposed technique.

Index Terms: Visual Semagram, Technique, Achieving, Confidentiality, Electronic Voting.

1. Introduction

With The election remains a fundamental platform to elect an individual into an elective position in a democratic society or organisation. The citizens get registered or enrolled as voters that would have legitimate rights to participate in decision making on who governs the society. The voters express their decision on a preferred contestant among many contestants through a vote at different polling booths. At the successful completion of the election, the votes would then be collated at the polling booth for onward transmission through public unprotect networks. The votes from different polling booths would then be summed up at the collation centre for declaration of winner based specified rules and conditions.

The adoption and uses of electronic devices and technologies into voting systems solely depend on specified functional and security requirements. It is expected that an e-voting system must satisfy the fundamental functional and security needs of the users. As human needs vary, so the e-voting requirements must satisfy the needs of every user. Generally, the e-voting functional requirements included convenience, transparency, flexibility, accuracy, auditability and uniqueness among others. Also, the security requirements included authentication, integrity, confidentiality, reliability, simplicity and distribution of authority among others.

The problem of results' suspicion from fraudsters and attackers has becomes a threat to sensitive information. Any sensitive information ought to have been secured from unauthorized alteration. One of the fundamental requirements of electronic voting (e-voting) system is confidentiality. The confidentiality requirement of e-voting system deals with concealment of sensitive election results against attacks such as result-alteration to favour a particular candidate and deformity from corrupt politician and fraudsters. The existence of election results through the public unsecured networks needs to be protected or concealed towards achieving credible and fair election.

However, the existing electronic voting (e-voting) systems have security challenges that are porous to various attacks such as alteration, deformation, and stealing from corrupt politicians, corrupt election officers and fraudsters. Many attempts have been made to tackle the security challenges of the confidentiality requirement of the e-voting system. Reference [13] explained the three fundamental and popular techniques to hide information from suspicion and alteration. These techniques were cryptography, steganography and watermarking as illustrated in Figure 1. Also, Figure 2 showed details of steganography in which visual semagram is a sub-technique.

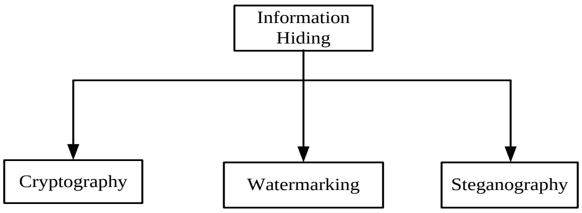


Fig.1. Security system techniques

Cryptography is a security term and it implies the transformation of plaintext (original message) into ciphertext (encrypted message) by using encryption techniques. Cryptography deals with converting a sensitive message into a different disorganized and confusing format with a key. The encrypted message is transmitted to the desired destination through unprotected networks. At the destination end, the receiver decrypts the ciphertext to plaintext using the decryption method shared between the senders and the receivers. The existence of the sensitive message is guessable, thus series of attacks by the fraudsters is inevitable. Once, fraudsters guess the existence of the sensitive message, attacks on encrypted message is possible [13]. The likelihood of attacks on the ciphertext and deformity of the sensitive message is high in cryptography.

Watermarking is a hiding information technique that deals with an impression of images or text on other images or text. This technique raises suspicion for attacks. Watermarking cheaply calls for fraudsters' attacks because the existence of sensitive massage is predictable by the attackers. Similar to cryptography, the possibility of damaging sensitive message secured by watermarking technique is high [4].

Steganography is a scientific technique of hiding within another information or data. The objective of steganography is to conceal sensitive messages in a safe message or carrier in such a way that no one or computer applications could guess the existence. Internet is a standout amongst the most broadly utilized correspondence channel to transmit messages. Information transmission over the Internet has security-related issues as fraudsters could attack sensitive data unlawfully [1]. Due to the simplicity of computerized duplication and alteration, information security turns into an essential issue of discussion.

Then again, steganography covers the confidential message in a medium that is difficult to recognise. The medium could be a picture, video, text and audio [1, 7]. In steganography, texts, images, videos and audio are technically embedded in other texts, images, videos and audio. Additionally, any file format could be embedded in another file format, for example, texts could be embedded in an image, and audio in the video. Generally, there are three approaches to hiding information using steganography. These approaches are injection, substitution, and generation [15].

In the injection approach, the sensitive message is implanted in the insignificant portions of the carrier file. The steganography by injection uses end-of-file (EOF) portion of the carrier file to conceal the sensitive message. The EOF implies that no more information can be read from the data source [15]. In the substitution approach, the insignificant bits of the carrier is substituted with the bits of the sensitive message. Technically, bits' substitution changes the carrier format, thereby drawing the attention of fraudsters for modification. Steganography by generation deals with the transformation of the sensitive message into new information. There is a clear dissimilarity between the original and new message. Generation approach to concealing sensitive message remains technically undetectable by Human Auditory System (HAS), Human Visual System (HVS) and computer programs (e.g Phishing) for modification. Technically, the sensitive message is read and a new message is generated in steganography by generation [15].

In both injection and substitution, carrier files are needed to conceal the sensitive message but in the generation approach, no carrier is needed. Perhaps, steganography by injection and substitution may not sensitive to HAS and HVS, the carrier raises suspicion for attacks because of the high sensitivity of hidden file to detective and destructive computer programs (e.g Phishing) for modification. According to [15], steganography by generation remains a powerful and technically reliable method of hiding information. Steganography by generation involves the creation of a piece of information which may be meaningful or not but the existence of sensitive data is not known. For example, an image may be meaningful or not to Human Visual System (HVS) but the existence of the sensitive message is not known.

The paper would highlight exiting studies on information security and present problems that violate the confidentiality requirement of the e-voting system. This paper would present an enhanced technique to hide the sensitive message from suspicion and generate an image using the bits of the sensitive message and the image would be named “vimago”.

2. Related Works

In [4], the three major hiding information techniques were presented as illustrated in Table 1 based on techniques, strength, applicability and robust. The fundamental significance of steganography over cryptography and watermarking techniques is that sensitive messages do not attract attention from fraudsters for alteration. The visible encrypted message, no matter how unbreakable it might look to anyone, would provoke suspicion. Figure 2 illustrates a common classification of steganographic techniques [8].

Principally, steganography is divided into two; technical and linguistic. The technical steganography deals with hiding sensitive message into an image, audio and video. The technical steganography is simply by injection and substitution approaches. The technical steganography conceals message within another message. In technical steganography, a carrier is needed to conceal the sensitive message. The use of a carrier to conceal sensitive message often leads to its deformity because its bits are required for injection and substitution. Therefore, the attacks are inevitable.

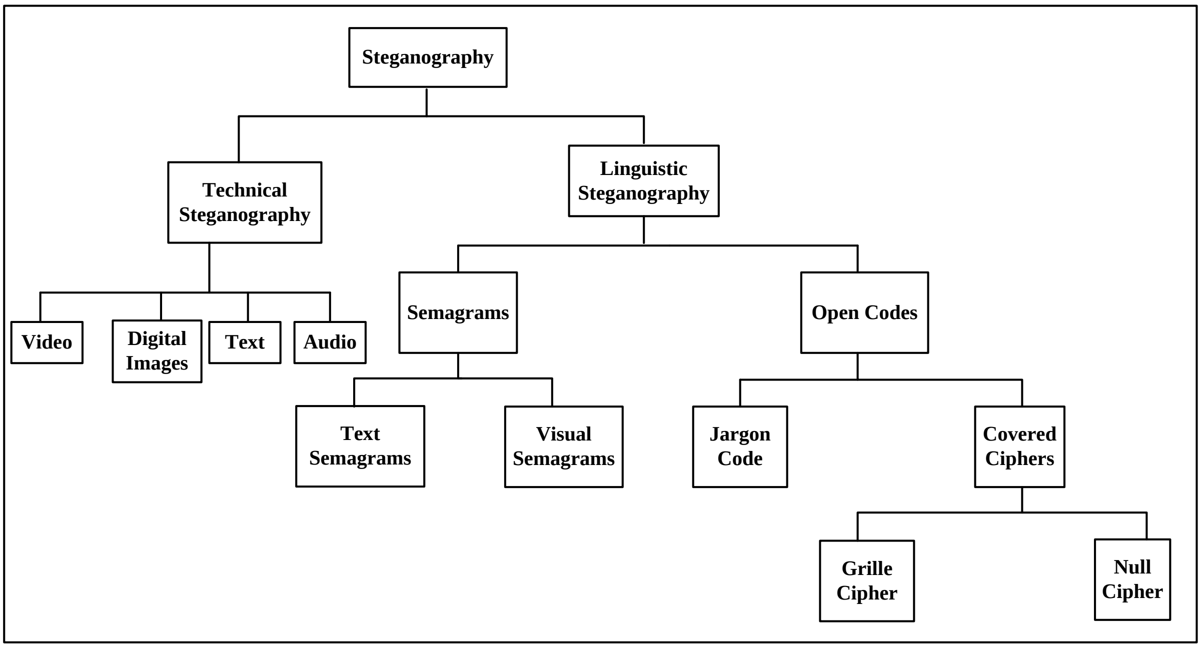


Fig.2. Classification of steganography techniques

The linguistic steganography is a scientific way of using language to conceal the sensitive message. The use of language may include re-arrangement letters, modification of images and sound signals [3]. A language that is incomprehensible by the fraudsters is used to conceal the sensitive message. The language could be in texts, sound and images only comprehensible by the senders and the receivers. Furthermore, linguistic steganography is divided into semagram and open-codes. The open-codes conceal messages in visible texts and subjected to attacks because of the existence of the sensitive message in know. The semagram is further divided into texts and visual. The text semagram conceals a message in a modified-texts. The texts are modified as desired by the senders and the receivers. For instance, upper, lower letters and special symbols may be interchanged to conceal message against attacks. Since the existence of the sensitive message is known, the attacks on the modified-texts are inevitable. This implies that the attacks could result in deformity thereby, leading to false results at the receiver's end.

The visual semagram conceals a sensitive message in images. According to [2], a sensitive message is an image. This implies that visual semagram deals with a transformation of the sensitive message to images. The visual semagram uses generation approach to conceal a sensitive message in an image. The visual semagram does not require a carrier for concealment. The EOF and insignificant bits of any file (image, sound or text) are not required for concealment. This implies that an image produced is not sensitive to HAS and HVS. Therefore, the visual semagram steganography is secured against alteration.

As the results of election transit from the polling booths to the collation centres and to avoid suspicion and alteration, the research would use a visual semagram technique to hide the election results from the unauthorized populace, unauthorized officers and fraudsters. Unlike commonly used Least Significant Bit (LSB) steganography that changes the positions of the pixels of the carrier (another image) by either substitution or injection method, and raise suspicion on the hidden message, the visual semagram does not modify or change the pixels' positions and no any other image is required to hide the sensitive messages. The visual semagram does not use any other image, no alteration of the bits after EOF maker and insignificant (least) bits, thus, the detection is difficult. When a new image is generated from the original or sensitive message, it does not raise suspicion for attacks by the HVS, HAS and harmful computer programs by the fraudsters. According to Reference [15] highlighted that using steganography by generation could take the sensitive message and transform the sensitive message to coloured pixels that could finally make up any image. For instance, transforming the letter "K" into bits and colour intensity for a particular colour. Intensity is a scientific description of brightness or dullness of a colour. Visual semagram technique creates an image from the bits of sensitive message and does not raise suspicion on the election results as the technique creates its image to convey the election to the relevant authority. Once, there is no suspicion on the hidden message, the probability of subjecting the new image (“Vimago”) to various types of attacks is very low, thereby increasing the confidentiality level of the hidden message.

Reference [10] used cryptographic wavelet watermarking technique to accomplish the confidentiality requirements of the electronic voting system. However, the technique exposed the sensitive message to attacks as fraudsters could easily guess the existence of the sensitive message.

Reference [11] used the Least Significant Bits (LSB) by bits substitution to develop an android platform for a mobile–voting system with cloud-based storage and to hide the election results. In the same opinion, [5] and [12] used Least Significant Bits (LSB) of substitution and injection approaches to hide the election results. The LSB raises suspicion and is sensitive to various attacks resulting in distortion of original results [14].

Reference [6] developed a fingerprint-based voting system and the confidentiality requirement of e-voting was achieved using Advanced Encryption Standard (AES). The AES could expose the sensitive results to various attacks by the fraudsters as the encrypted message raise suspicion of the concealed message.

Reference [9] used space insertion text semagram and an enhanced advance encryption standard (E-AES) to conceal sensitive election results over public networks. The cipher-text transmitted over the public networks would raise suspicion thereby causing the fraudsters and harmful programs to attack the sensitive results and triggering deformity. These attacks and deformities could lead to false results. The existing techniques towards achieving the confidentiality requirements have not been highly secured the sensitive election results from attacks and alteration. The paper presented a novel technique called visual semagram to satisfy the confidentiality requirement of the electronic voting system.

3. Research Motivation

The transmission of a sensitive message through public and unprotected networks could be a cheaper avenue for the fraudsters to attack. Any message that raises suspicion could easily be attacked for alteration. The existing techniques to hide sensitive message are subjected to passive and active attacks. The LSB, cryptographic, enhanced advance encryption standard, text semagram and jargon codes could call the attention of attackers for modification. Also, technical steganography techniques required a carrier to embed a sensitive message. The distortion in the carrier’s characteristics could raise suspicion for attack and eventually leading to modification and undesired candidate emerge as a winner in an election. The paper was motivated to tackle the highlighted problems and provide mathematical techniques for future implementation and evaluation.

4. Research Objectives

The objectives of this research were to:

1. Design a technique that would conceal the sensitive message towards achieving a confidentiality requirement of e-voting system.
2. Formulate mathematical equations for concealing sensitive message.

5. Proposed Technique

The visual “semagramming” is a steganography technique of creating an image using the bits of the sensitive data without involvement of any bits from any other data. The “Vimago” is a pictographic data generated from “semagramming” process. A “semagramming” process is the generation of an image with any desired shape using the bits of the original message. The image obtained from the “semagramming” process is called “Vimago”. The “Vimago” conveys the election results to the relevant authority through the public and unprotected networks thereby preventing any form of fraudulent activity such as alteration. The formation of “Vimago” is achieved by the generation technique among the three techniques of injection, substitution and generation of hiding methods in steganography. The generation technique generates a new set of data which does not raise any suspicion for attacks. Technically, no carrier is needed in visual semagram technique. The bits of the sensitive results are transformed into the pixels of the image. In visual semagram technique, any image regardless of shape and appearances can be created. The image generated has no meaning to the fraudsters for alteration. It is even better if the image has no meaning and not beautiful to the attackers. Also, harmful computer programs would not be able to detect the sensitive message because EOF and insignificant bits are not used to generate the “Vimago”.

The “Vimago” would be generated based on the numerical values (scores) of election results, alphabetic characters of the political parties and contestants’ name encoded in matrix T. Figure 3 shows graphical generation and transmission of “Vimago”.

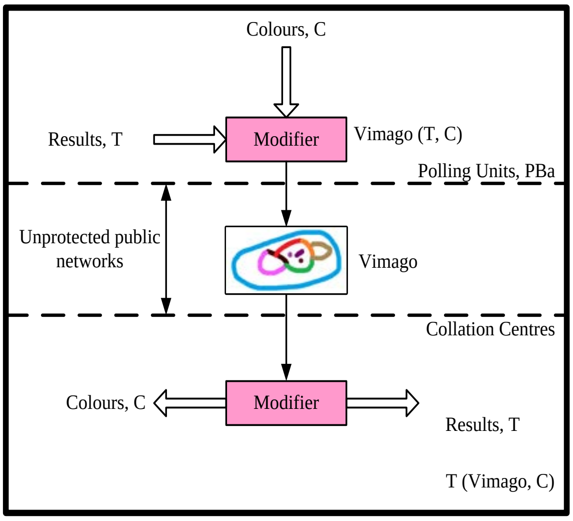


Fig.3. Vimago machine

Basically, the generation of "Vimago" would involve different intensities of primary additive colours, Red (R), Green (G) and Blue (B). This implies that different intensities of R, G and B would be added to produce a 24-bits image. Thus, R, G and B would have 8 bits each. Figure 4 shows a 24-bit combination of R, G and B colour intensities.

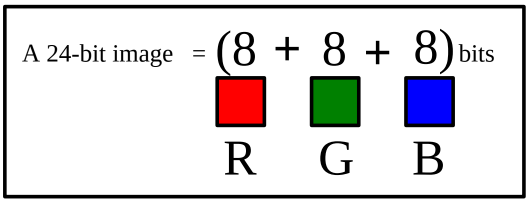


Fig.4. Vimago RGB bits

Using these 8 bits, there would be 28 (256) possible different colour combination of intensities for each colour. This implies that 256 (0 to 255) different colour intensities could be formed for each R, G and B. The characters of the sensitive results are first converted to America Standard Codes for Information Interchange (ASCII). The numeric values would then be transformed into a matrix. The elements of the matrix would further be transformed into bits (zeros and ones).

Mathematically, a “Vimago” could be generated as follows:

$$T_B = \varphi(matrix\,T) \tag{1}$$

TB is the binary message of matrix T, φ is binary converter and matrix T is the ASCII equivalent of the original and sensitive message.

$$T_B = \begin{bmatrix} TB_{11} & TB_{12} & TB_{13} & TB_{14} & \cdots & TB_{R1} \\ TB_{21} & TB_{22} & TB_{23} & TB_{24} & \cdots & TB_{R2} \\ TB_{31} & TB_{32} & TB_{33} & TB_{34} & \cdots & TB_{R3} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ TB_{C1} & TB_{C2} & TB_{C3} & TB_{C4} & \cdots & TB_{C} \end{bmatrix} \tag{2}$$

$$T_B = \begin{bmatrix} 000\ 000\ 00\ 000\ 000\ 00\ 000\ 00\ 000 & 0000\ 000\ 000\ 00\ 000\ 00\ 000\ 0000 & \cdots & TB_{R1} \\ 001\,100\ 00\,100\ 001\,10\ 000\,10\ 001 & 0011\ 000\,110\ 00\ 010\ 01\,110\ 0001 & \cdots & TB_{R2} \\ 011\,100\ 01\ 011\,100\ 01\ 011\,10\ 001 & 1111\,100\,111\ 00\ 010\,11\,100\ 0100 & \cdots & TB_{R3} \\ 011\,100\ 01\ 011\,100\ 01\ 011\ 00\ 001 & 0000\ 000\ 011\,10\,111\ 00\ 010\ 0011 & \cdots & TB_4 \\ \vdots & \vdots & & \vdots \\ 000\,111\ 00\ 010\,111\ 00\ 011\,111\,11 & 1111\,100\ 011\,10\ 001\ 01\,110\ 0010 & & TB_C \end{bmatrix} \tag{3}$$

Each element of T_B (e.g TB_{11}) would then be converted to RGB HexCode required for a particular colour intensity.

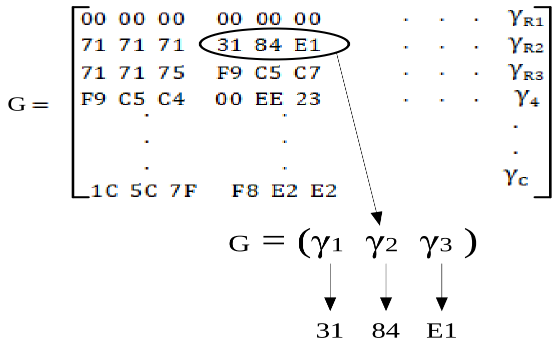
$$\gamma = \sigma(T_B) \tag{4}$$

δ is the RGB HexCodes translator/converter and γ is the RGB HexCodes generated from T_B.

$$\gamma = \begin{bmatrix} 00\ 00\ 00 & 00\ 00\ 00 & \cdots & \gamma_{R1} \\ 71\ 71\ 71 & 31\ 84\ E1 & \cdots & \gamma_{R2} \\ 71\ 71\ 75 & F9\ C5\ C7 & \cdots & \gamma_{R3} \\ F9\ C5\ C4 & 00\ EE\ 23 & \cdots & \gamma_4 \\ \vdots & \vdots & & \\ 1C\ 5C\ 7F & F8\ E2\ E2 & & \gamma_C \end{bmatrix}$$

Each element of γ is divided into 3 components (values) to represents R, G and B intensities.

$$G=(\gamma_1, \gamma_2, \gamma_3) \tag{5}$$


G =
00 00 00 00 00 00 . . . γR1
71 71 71 31 84 E1 . . . γR2
71 71 75 F9 C5 C7 . . . γR3
F9 C5 C4 00 EE 23 . . . γ4
1C 5C 7F F8 E2 E2
γC
G = (γ1 γ2 γ3)
31
84
E1

$$\gamma_1 = (V_{red}) : V_{red} \text{ is red intensity}$$
$$\gamma_2 = (V_{green}) : V_{green} \text{ is green intensity}$$
$$\gamma_3 = (V_{blue}) : V_{blue} \text{ is blue intensity}$$

As components of G vary, a different combination of colour intensities are produced, thereby resulting in different colours for different data.

Therefore,

$$\text{Vimago } L_{n1}(\gamma_1),\ L_{n2}(\gamma_2),\ L_{n3}(\gamma_3) \tag{6}$$

Where L_{n1}, L_{n2}, and L_{n3} are the locators for R, G and B colour intensities. The locators are used to place a particular colour at a specific location to form an image. Figure 5 shows election results and semagramming module while Figure 6 shows the result and semagramming sequence diagram of the proposed e-voting system.

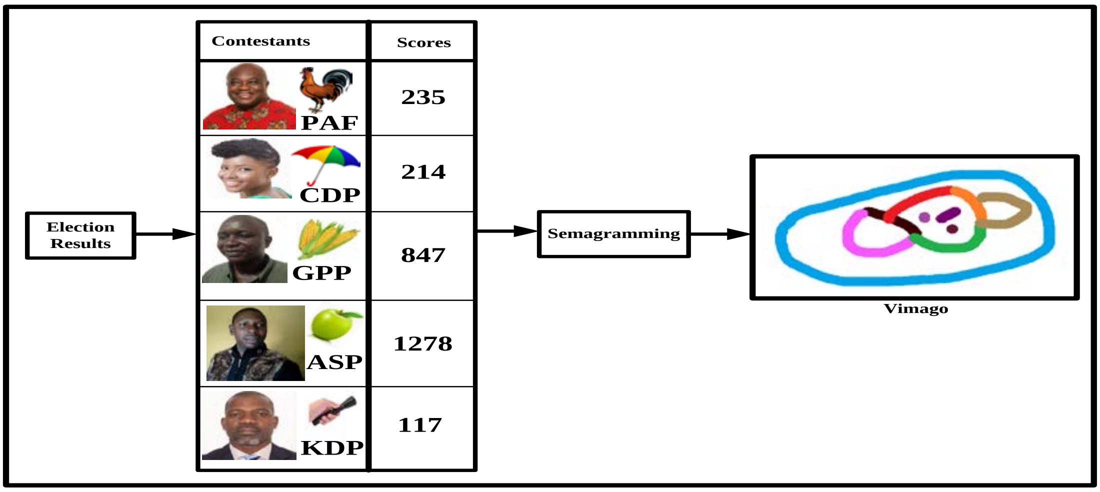


Fig.5. Election results and semagramming module

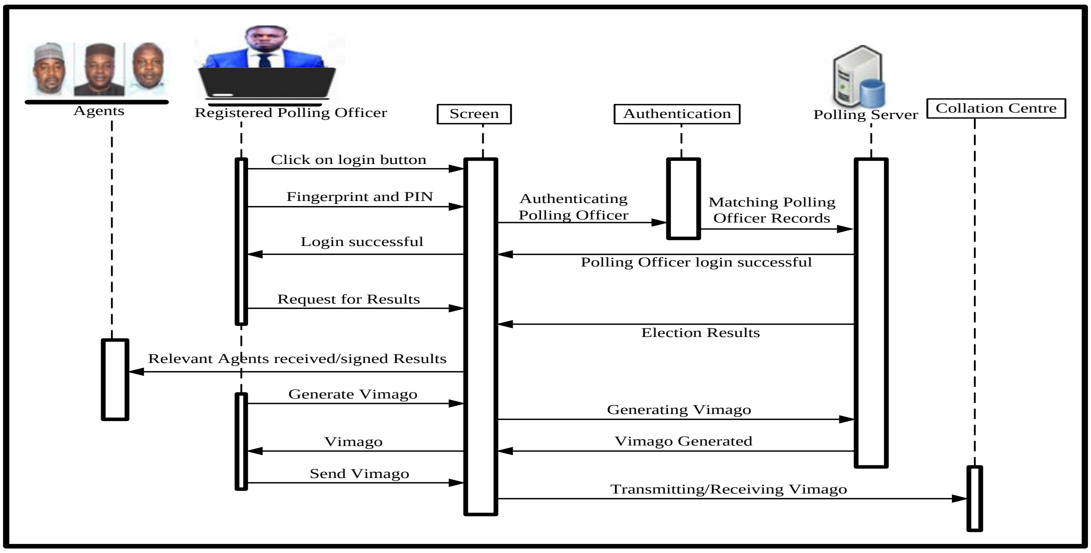


Fig.6. Result and semagramming sequence diagram

6. Conclusions

Steganography is a fundamental and technological technique of hiding sensitive data from attacks. The concealment of sensitive election results against attacks and deformity by the fraudsters and corrupt politicians would guarantee a credible and fair election. This paper presented a visual semagram technique as a measure to secure election results from suspicion, attacks and deformity. Scientifically, the proposed technique used the intensities of the primary additive colours (Red, Green, and Blue) and the bits of the original message to generate an image of any desired shape and conceal the sensitive results over public and unprotected networks. This research advances from the existing applications of LSB, text semagram, jargon codes, grille-cipher and encryption to hide any sensitive messages that raise suspicion for attacks. The suspicion could instigate forceful and illegal modification on the hidden message.

7. Future work

This paper presented a visual semagram technique towards achieving the confidentiality security requirement of the electronic voting system. The future work would focus on the implementation of visual semagram technique presented in this paper to conceal the election results against attacks and alteration, and to establish the validity and reliability of proposed technique.

Acknowledgement

The researchers acknowledge the persons whose photographs have been used in this research. Thank you for your co-operation.

References

[1] Anderson, R. J., & Petitcolas, F. A. P. (2008). On the limits of steganography, Institute Electrical and Electronics Engineers (IEEE), 16, 474–481.

[2] Cerkez, P. S. (2013). Do you see what I see?. 2013 IEEE Applied Imagery Pattern Recognition Workshop (AIPR). Retrieved August 22, 2018 from https://ieeexplore.ieee.org/document/6749313/

[3] Gary, C. K. (2014). An overview of steganography for the computer forensics examiner. Retrieved on April 10, 2018 from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.90.8113.

[4] Hardikkumar, V. D. (2012). Steganography, Cryptography, Watermarking: A Comparative Study. *Journal of Global Research in Computer Science*, 3(12), 33-35.

[5] Jadhav, A. D., Ambavane, P. R., Patil, M. A., Shewale, K. G., & Vishwasrao, S. P. (2014). Online voting system based on biometrics using adhar card data. *International Journal of Emerging Trends in Science and Technology*, 1(2), 128–133.

[6] Jaya, C., Milind, K., and Pranali, T. (2017). Fingerprint based voting system. *International Journal of Research in Science and Engineering*, 3(2), 108–114.

[7] Katzenbeisser, S., & Petitcolas, F. A. P. (2000). Information hiding techniques for steganography and digital watermarking. Boston: Artech House Inc.

[8] Lip, Y. P., Kok, O. C., Tan, F. A., & Delina, K. (2011). An enhanced embedding method using inter-sentence, inter-word, end-of-line and inter-paragraph spacing. *International Journal of the Physical Sciences (IJPS),* 6(36), 8130–8142.

[9] Oke, B. A., Olaniyi, O. M., Aboaba, A. A., & Arulogun, O. T. (2019). Securing electronic voting system using crystographic technique. *Journal of Science, Technology & Education (JOSTE),* 7 (1), 88 – 105

[10] Olayemi, M. O., Taliha, A. F., Aliyu, A., and Olugbenga, J. (2016). Design of secure electronic voting system using fingerprint biometrics and crypto- watermarking approach. *International Journal of Information Engineering and Electronic Business,* 8(5), 9–17, 2016.

[11] Ragunath, G., Aarthi, R., & Dhanalakshmi, A. S. (2014). A+Votz–google android platform for a mobile - voting system with cloud based storage and data hiding features. *International Journal of Engineering Development and Research*, 2(2), 2318–2323.

[12] Shweta, A.T., Nikita, P. J., & Topannavar, P. S. (2014). Steganography and biometric security based online voting system. *International Journal of Engineering Research and General Science*, 2(3), 110–114.

[13] Suraj, K. D., & Vivek, C. (2017). Steganography, cryptography and watermarking: A review. *International Journal of Innovative Research in Science, Engineering and Technology*, 6(2), 2595– 2599.

[14] Syed, M. H., Salihah, Y., Syed, B., Mehvish, S., & Zahid, G. K. (2017). Analysis of LSB and DWT steganography techniques over various attack. *International Journal of Advance Engineering and Research Development*, 5(1), 1–3.

[15] Youssef, B. (2013). Steganography & the art of deception: a comprehensive survey. *International Journal Latest Trends Computing*, 4(3), 128 – 139.

Authors' Profiles

Adewale Olumide Sunday is a Professor of Computer Science, Department of Computer Science, School of Computing, Federal University of Technology (FUTA), Akure, Nigeria. He has Ph.D. in Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria in 2002; M.Tech in Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria–1998; BSc Computer Science with Mathematics Ogun State University (Now OOU), Ago Iwoye, Nigeria, in 1991. His Research/Areas of Interest are Cyber Security, Software Engineering, E-Learning and Digital Library. He is a member of many professional bodies. He is a member of Institute of Electrical and Electronic Engineers and Association of Computer Machineries (135763); Member, Infonomics Society, United Kingdom; Member, Computer Professional & Registration Council of Nigeria (CPN). At present, Prof. Adewale is the Dean, School of Computing, Federal University of Technology, Akure (FUTA), Nigeria.

Olutayo Boyinbode (PhD) is an Associate Professor at the Department of Information Technology, Federal University of Technology, Akure, Nigeria. Her research interests are Mobile and Ubiquitous Learning, Mobile Networks, Machine Learning and Internet of Things for Development ((IoT4D). She has several publications in reputable peer-reviewed journals and has also served as a reviewer to several peer reviewed journals. She is a professional member of Association for Computing Machinery (ACM) and Institute of Electrical and Electronics Engineers (IEEE).

Salako E. Adekunle received a degree (B.Eng) in Electrical and Computer Engineering, Master of Technology (M.Tech) in Computer Science from Federal University of Technology, Minna, Niger State. At present, he is a PhD student in Computer Science at the Federal University of Technology, Akure, Nigeria. He is a member of the Nigeria Computer Society and Teachers Registration Council of Nigeria (TRCN). His research interests include Biometric Security, Educational Technology and Control Technology. He has published papers in reputable local and international journals and his published textbooks included Introduction to Computer Logic, Learning Pascal Made Easy, A Handbook on Symbolic Logic and BASIC Programming Language.

How to cite this paper: Adewale Olumide S., Boyinbode Olutayo K., Salako E. Adekunle, "Visual Semagram: An Enhanced Technique for Confidentiality Requirement of Electronic Voting System", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.4, pp.51-59, 2020. DOI: 10.5815/ijcnis.2020.04.05