Proceedings of the 4th International Conference on Computing and Data Science (CONF-CDS 2022)
DOI: 10.54254/2755-2721/2/20220613

Secure Electronic Commerce Transactions Using Pythagorean Triple-based Cryptography and Audio Steganography

Arome Junior Gabriel, Emmanuel Akindoyin Awosola

School of Computing, Federal University of Technology, Akure, Nigeria.

ajgabriel@futa.edu.ng

Abstract. The rapidly increasing utilization of Information Technology (IT) in electronic commerce and other aspects of human existence has led to a rise in worries about the privacy and safety/security of those involved. Due to the alarmingly high frequency with which data or user privacy breaches occur today, conducting online transactions can represent a major threat to buyers' (and even business owners') privacy. Existing solutions to these security issues are still vulnerable to classic phishing scams. As a result, the construction of a robust and efficient audio steganography system for secure electronic commerce transactions is presented in this work. The developed system first encrypts sensitive financial data using the Pythagorean Triple-based Cryptographic (PTC) algorithm, then compresses the resulting cipher-text using the Lempel Ziv Welch (LZW) and Huffman's Compression Algorithms, and finally embeds the compressed file (using one-dimensional Discrete Cosine Transform (DCT)) in a suitable audio-file cover to produce an output (stego file) that is indistinguishable from the cover file. This output can then be exchanged between communicating entities across open networks. The new system has a little or no alteration in its outputs, as evidenced by the Signal-to-Noise Ratio (SNR), in the experimental results gotten.

Keywords: electronic commerce, information security, computer networks, cryptography, Steganography, mathematics

1. Introduction

Without computers and their networks, modern life would be nearly impossible in today's electronic civilization. The Internet is undeniably the backbone of practically all aspects of modern life. Indeed, the fast adoption of IT in practically every facet of life has resulted in a slew of advantages, ranging from increased efficiency and expediency to lower prices.

Indeed, according to research, IT is now employed to give various electronic-services in democratic decision-making, governance, education, medicine and/or health, and even electronic commerce [1-2].

The security (privacy, integrity, availability, or confidentiality) of stored information or transmitted ones, especially in the course of their various e-service implementations is critical to the success of all of these application areas [3].

Information overload, which characterizes today's e-society (Internet), has a number of advantages. However, it can make customers' and businesses' (or merchants') lives miserable and difficult.

DOI: 10.54254/2755-2721/2/20220613

Customers who want to make purchases or conduct online commerce transactions in typical electronic commerce paradigms must first register by providing personal information such as passwords and usernames to the merchant's website. The customer next selects and adds things to their shopping cart. The customer then proceeds to initiate payment by providing his or her bank account information (like credit card type and number). Finally, clients must provide an address to which their things can be delivered. Furthermore, merchants, delivery companies, and even financial institutions participating in the transaction engage in some type of registration that requires them to provide personal information.

The image portrayed thus far suggests that a large amount of personal data is involved, particularly when it comes to electronic commerce or payment. Customers and other e-commerce stakeholders have become more concerned as a result, particularly when it comes to the safety of personal data. Furthermore, clients divulge a great deal of personal info, such as names, phone numbers, credit-card details, products purchased, transaction place and time, addresses, and even behavioral patterns. Unauthorized third parties (attackers or adversaries) with hostile intentions can use this information for further research, which could lead to various forms of cybercrime such as extortion, financial fraud, theft, and even corporate secret leakage to competitors. In various ways, it is required of enterprises that process personal data of customers to state and maintain strict adherence to data protection standards. As a result, addressing these security and privacy concerns has become a top priority for both customers and merchants [1, 4].

The majority of existing solutions are still vulnerable to new cyberthreats, and even issues that bothers on high computational resource demand. Indeed, the majority of extant systems rely on cryptography or steganography. Either of these two techniques are on their own very susceptible to breach by a technically sound attacker. As a result, there is a strong incentive to do research into ways to build more efficient and reliable solutions. Combining steganography and cryptography, towards providing a more robust and efficient response to today's security challenges.

To design an audio steganography system for protecting electronic commerce transactions, this study proposes combining Pythagorean Triple-based Crypto (PTC) with DCT, LZW, and the Huffman's algorithm.

2. Related works

There are a lot of extant works in the literature that are connected. The majority of these works have flaws that act as weaknesses or downsides. In [5], Akinyede et al. presented an electronic payment system that uses the AES encryption technique for security. Their system, on the other hand, was not assessed. Furthermore, the usage of simply AES raises suspicion among malicious individuals. It is necessary to equip such a system with the capability of concealing the existence of covert communication. In the endeavor to find a solution to the security concerns, the writers of [6] and [7] each contributed their quota. However, their steganography technology is ineffective, as some of their outputs are distorted and could raise suspicion. Furthermore, the work in [7] only permits the usage of one audio file type (.wav), which is a limitation in and of itself. Despite the fact that the authors of [8] published a research paper aimed at improving the capacity of low-bit encoding audio-steganography, their method has a considerable computational cost, especially as the amount of the input secret message grows larger.

The authors of the paper [9] devised a method for encrypting text files and storing the cipher-text generated in a digital object. Their goal was to create a secure system that combined the strengths of cryptography and steganography. As a cover file, an mp3 audio file was used. Their system has the disadvantage of producing low-quality stego-files as outputs. Besides, only MP3 file formats were used as cover media.

Three LSB approaches were analyzed and designed by the authors of [10]. The main purpose of their research was to figure out how to use the 3rd LSB approach to embed image files in audio cover files. However, the characteristics of the cover file was drastically different from the output stego-file.

DOI: 10.54254/2755-2721/2/20220613

This indicates that their system is not very robust and may be vulnerable to statistical analysis. Aside from that, only.WAV files were used.

In [11], Adeboje et al. developed an audio steganography system that may use two (2) different file formats as cover files. The authors tested their technique using the MP3 and MP4 file formats. Other audio file formats should be investigated to see whether they are suitable.

Gabriel et al. developed more attack-resistant systems that integrate post-quantum cryptography as well as steganography to allow for the security of information against conventional or even quantum attacks in the cloud computing domain [3], as well as e-voting systems [4].

Gabriel et al. in [12] carried out a study that resulted in the development of a two-stage steganography scheme for secure info exchange. In these two investigations, however, only photographs/images were considered as cover files.

More research is needed to develop a similar approach for audio or video data. The authors in [13] presented a new symmetric cryptography technique for ensuring the security of messages. In this study, encryption /decryption keys are generated using the Pythagorean triple (an extension of the famous Pythagorean theorem). The technique proposed is quite simple, and is expected to be computationally inexpensive.

This current study therefore seeks to combine the new Pythagorean triple-based crypto algorithm with audio steganography to develop a two-layer robust system for securing electronic commerce transactions over public/enterprise networks.

3. The proposed secure E-commerce system

The Electronic Transaction Network Model, the Threat Model, the Specific Objectives, and the Proposed System Architecture/Design are the four sub-titles that address the proposed system design covered in this section IV.

3.1. The electronic transactions network model

There are four (4) major entities or actors in the proposed system. In terms of the transaction, communication is limited to these entities. The Merchant S, who is usually the business owner or service provider, the Customer D, who makes purchases or requests services, and the financial agencies or banks B, who handle transaction payment issues, are the entities in question. As well as delivery agencies (DA), who handle the delivery of purchased things to the customer's address or location. The majority of communication between these entities takes place through the open Internet.

3.2. The threat model

In this paper, we regard the major threat to be an adversary who is a malicious entity/individual with the ability to: 1) compromise any of the entities involved in this e-commerce scenario, and/or 2) eavesdrop messages exchanged between the entities involved in the transaction, with the goal of deducing and retrieving information on users' private lives, for the purpose of blasphemy or financial gain. As a result, it is necessary to recognize and counter the adversary's threats. to be more specific.

3.2.1. The privacy of customers must be protected. That means the opponent should be unable to obtain any information about individual customers' consumption patterns or trends. Even the merchant M should not have a fine-grained understanding of the personal details of his clients.

3.2.2. *The integrity of the messages transferred must be 100% guaranteed.* As a result, every receiver-entity must validate the sender-legitimacy. entity's Modification attempts, FDI, MMA, replay, and other common cyber-attacks must be detected and/or thwarted.

DOI: 10.54254/2755-2721/2/20220613

3.3. The specific objectives of this research

The specific goal of this project is to provide an efficient secure e-commerce transactions system that can ensure high-level security of sensitive data sent between business transacting entities through public open/enterprise networks.

3.4. The proposed system design

The difficulty of safe electronic commerce transactions is depicted in this paper using the famous prisoners' problem, in which Alice (the sender) and Bob (the receiver) are two captives who want to talk about how to escape. While discussing/communicating, Alice and Bob must do everything they can to avoid arousing the suspicions of the jail keeper/supervisor (Wendy), who will send them into solitary incarceration.

Bob (the sender) represents client systems used by both customers and merchants in our proposed safe e-commerce transaction framework. A client system wants to send a secret message M (products chosen for purchase, customers' location/address, customers' credit card information, or even the merchant's bank details) to Alice (the receiver), who represents the server system of the designated Trusted Agent (TA) or Trusted Third Party (TTP).

Bob encodes the personal information or financial transaction data using the Pythagorean Triple based Cryptography (PTC) Algorithm, to produce a cipher-text, Y, in order to allow for a covert transmission of information between these three entities (Merchant, Customer, and the TA).

The generated cipher-text is then compressed by Bob using Huffman's technique. The Lempel Ziv Welch compression technique is then applied to the output. These significantly reduce the size of the cipher-text. Finally, the steganography system's robustness to statistical analysis is improved, and the human auditory system's ability to detect distortion in its final output (stego-file) is considerably decreased or eliminated.

As a cover file C, Bob the sender (merchant/customer) selects a suitable audio file. The encoded and compressed surreptitious message was hidden in the digital.M4A/.MP3 audio signal using the Spread-Spectrum method. This approach utilized in this study changes the frequency spectrum of the audio cover file such that it bounces between frequencies quickly. It recognizes the low frequencies of the audio signal frames in this way and constructs a final output stego-file S by hiding/embedding bits of the cipher-text in them without generating audible distortions (that is, without raising Wendy's suspicion).

The resulting stego-image, S, is sent across a public channel (which Wendy/cyber-criminals watch) and is only received by Alice if Wendy has no suspicions about it. Once Alice receives S, she can use the extraction procedure to retrieve the original plain-text message, as shown in Figure 1 on the right-hand side of the figure at the receivers' section of the system's architecture.

The embedding procedure represents a steganography system's most difficult task. This is because the final stego-file output must be as close to the original audio cover file as possible. Wendy, the illegal eavesdropper, must not notice any distortion.

Two key processes are carried out, as indicated in Figure 1, on both the merchant/customer and Trusted Agents' sides of the secure electronic commerce transactions system: the Cryptography and Steganography procedure.

DOI: 10.54254/2755-2721/2/20220613

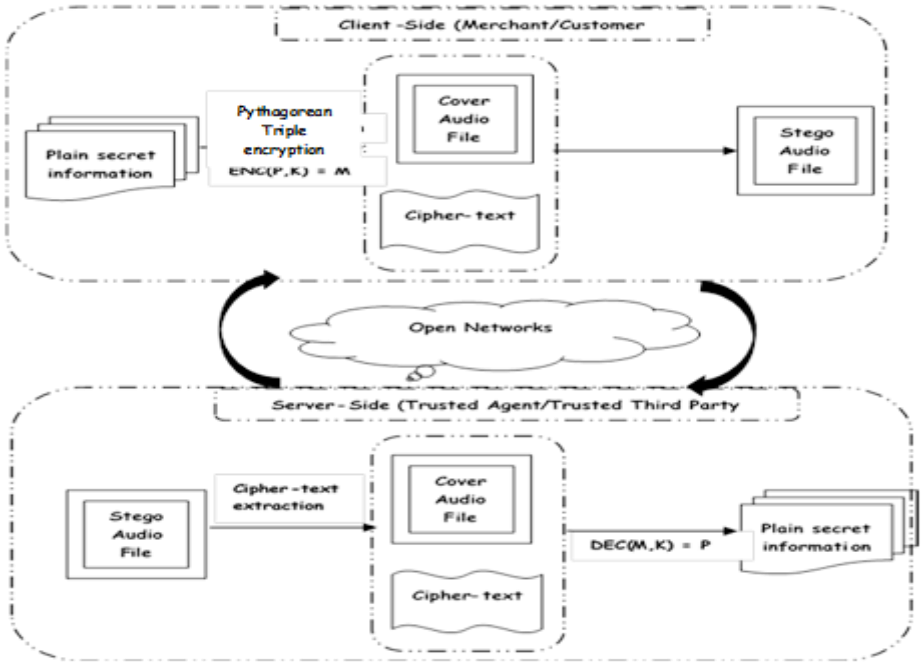

Figure 1. Architecture of the proposed Secure Electronic Commerce Transaction System.

4. The proposed Pythagorean theorem-based crypto-Scheme

The study in [16] presented a vivid study on the use of Pythagorean triple for encryption/decryption of messages. These thoughts/ideas are summarized and presented in this section of the current article.

4.1. Pythagorean triple

The "hypotenuse" is the triangle's longest side; hence the formal definition of the famous Pythagorean theorem is given as: “the square of the hypotenuse in a right-angled triangle is equal to the sum of the squares of the other two sides”. The length of the third side of a right-angled triangle can be deduced/calculated if we are given the dimensions of the first two (2) sides. A "Pythagorean Triple" is a collection of positive integers **a**, **b** and **c** that agrees with the Pythagorean rule: $a^2 + b^2 = c^2$.

The smallest Pythagorean Triple for instance is 3, 4, 5. This is true especially since;

$$3^2 + 4^2 = 5^2$$

$$9 + 16 = 25$$

The list of Pythagorean triples includes, but is not limited to; (3, 4, 5), (9, 40, 41), (19, 180, 181) and even (36, 323, 325).

Scaling up a collection of triples is the simplest approach to making more Pythagorean Triples. For instance, 3, 4, 5 can be scaled up by 2 to yield 6, 8, 10. This also satisfies the formula $a^2 + b^2 = c^2$.

4.2. Pythagorean triple crypto

The New Pythagorean Triple Crypto scheme encrypts and decrypts a message with the same key utilizing symmetric cryptography methods.

An ordered triple of the form $x, y, z \in z^3$ such that equation holds, is referred to as a Pythagorean triple [14].

$$x^2 + y^2 = z^2 \tag{1}$$

The common explanation of equation 1 is that it has only one solution (x_1, y_1, z_1).

DOI: 10.54254/2755-2721/2/20220613

For every random pair of positive integers p and q, Euclid's principle, which really is a foundational rule for Pythagorean triples can be used to generate a Pythagorean triple. Here, p > q, as represented by the integers defined in equations (2-4);

$$x = p^2 - q^2 \tag{2}$$

$$y = 2pq \tag{3}$$

$$z = p^2 + q^2 \tag{4}$$

The Pythagorean Theorem, which states that there is only one fundamental solution (x, y, z) for any p and q, can be extended using the New Pythagorean Triple method. This definition can be re-stated using the New Pythagorean Triple algorithm formulas as follows: for any numbers p and q, there are at least two fundamental solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) or (x_1, y_1, z_1), (x_2, y_2, z_2) and (x_3, y_3, z_3). Encryption and decryption keys can easily be created and utilized in a simple symmetric cryptosystem using these techniques.

Given $x^2 + y^2 = z^2$ and $gcd(x, y) = 1$, there exist a number z such that;

$$\begin{cases} z = x + u \\ z = y + v \end{cases} \tag{5}$$

where $\gcd(x, y) = 1$ and $\gcd(y, v) = 1$.
here, gcd denotes the greatest common divisor. Now with these, we can safely have;

$$\begin{cases} x + u = y + v \\ x - v = y - u \end{cases}$$

marking $y - u = x - v = \lambda$, then:

$$\begin{cases} x = v + \lambda \\ y = u + \lambda \end{cases} \tag{6}$$

Equation (7) can then be derived by replacing x in equation (5) and (6),

$$z = u + v + \lambda \tag{7}$$

When combined, equations 6 and 7 will yield 8.

$$\begin{cases} x = v + \lambda \\ y = u + \lambda \\ z = u + v + \lambda \end{cases} \tag{8}$$

The new fundamental solutions to the Pythagorean theorem are represented by in equation 8. Substituting these values for x, y and z respectively in equation 1, will yield:

$$(u + \lambda^2) + (u + \lambda^2) = (u + v + \lambda)^2$$

which can even be further reduced to yield:

$$\lambda^2 = 2vu \tag{9}$$

The values of v and u will be chosen in such a way that they produce λ, from which the Pythagorean fundamental solutions are derived:

$$\begin{cases} v = 2p^2 \\ u = q^2 \end{cases}, v > u, \gcd(p, q) = 1 \tag{10}$$

Going back to substitute these values of *u* and *v* in 9, we get:

$$\lambda^2 = 4p^2q^2$$

which will then imply that:

DOI: 10.54254/2755-2721/2/20220613

$$\lambda = \pm 2pq \tag{11}$$

Also, if at this stage, we substitute for u, v, and λ in equation 8, then we can obtain:

$$\begin{cases} x = 2p^2 \pm 2pq \\ y = q^2 \pm 2pq \\ z = 2p^2 + q^2 + \pm 2pq \end{cases} \tag{12}$$

According to the traditional definition of the Pythagorean triple, there is only one essential solution (x, y, z) for p and q. (one is odd, the other is even).

However, if equation 8 is used, the Pythagorean triple can be rewritten as:

There exist at least two important solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) for all values p and q (one of which is odd and the other even) that may be stated in the form of New Pythagorean Triple formulas:

There is a specific scenario for the numbers p and q in which we have three fundamental solutions: Table 1 displays a sample of Pythagorean triple solutions with the values (3, 1), (5, 3), (7, 2), and (8, 2). (7, 4). Table 2 displays the English alphabet number encodings that will be utilized for encryption and decryption in the future.

Table 1. New Pythagorean triple algorithm.

p	q	x_1	y_1	z_1
3	1	24	7	25
5	3	80	39	89
7	2	126	32	130
7	4	154	72	170
p	q	x_2	y_2	z_2
3	1	12	-5	13
5	3	20	-21	29
7	2	70	-24	74
7	4	42	-40	58
p	q	x_3	y_3	z_3
3	1	6	8	10
5	3	30	16	34
7	2	28	45	53
7	4	56	33	65

Table 2. The English alphabet.

a	b	c	d	e	f	g
0	1	2	3	4	5	6
h	i	j	k	l	m	n
7	8	9	10	11	12	13
o	p	q	r	s	t	u
14	15	16	17	18	19	20
v	w	x	y	z		
21	22	23	24	25		

DOI: 10.54254/2755-2721/2/20220613

4.3. Illustration of encryption/decryption with the Pythagorean triple crypto scheme

The mathematical relations in equations 13 and 14 depicts the encryption and decryption procedures respectively:

$$c = m + k(mod26) \tag{13}$$

$$m = c - k(mod26) \tag{14}$$

where, m stands for the plaintext message, c stands for the ciphertext produced at the end of encryption, while k stands for the encryption/decryption key.

For illustration purpose, we demonstrate the encryption procedure for the plaintext message; "Emmanuel University of Technology".

Firstly, the message encoding for the word "Emmanuel university of technology" is computed and presented as in Table 3:

Table 3. Presented.

e	m	m	a	n	u	e	l	u	n	i
4	12	12	0	13	20	4	11	20	13	8
v	e	r	s	i	t	y	o	f	t	e
21	4	17	18	8	19	24	14	5	19	4
c	h	n	o	l	o	g	y			
2	7	13	14	11	14	6	24			

The next step would be to generate the encryption/decryption key. This can be done by randomly choosing two integer values for and p and q. If for instance we choose 5 and 3 respectively,

These numbers would be fed into the new Pythagorean triple formulas;

$$\begin{aligned} x_1 &= 2p^2 + 2pq \\ y_1 &= q^2 + 2pq \\ z_1 &= 2p^2 + q^2 + 2pq \end{aligned} \qquad \begin{aligned} x_2 &= 2p^2 - 2pq \\ y_2 &= q^2 - 2pq \\ z_2 &= 2p^2 + q^2 - 2pq \end{aligned} \qquad \begin{aligned} x_3 &= 2pq \\ y_3 &= p^2 - q^2 \\ z_3 &= p^2 + q^2 \end{aligned}$$

$$(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3)\ (mod26)$$

The encryption key can be easily created in the following format:

$$x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3$$

to obtain;

$$(80, 39, 89, 20, -21, 29, 30, 16, 34)(mod26)$$

and finally, the key;

$$(2, 13, 11, 20, 5, 3, 4, 16, 18)$$

The message is now being translated into numerical form. Table 2 is used to turn each letter of the text into a number. The values in table 4 are obtained.

In a nutshell, the resultant ciphertext which is GZXUSXIBCPVGYWVMJGQSEYHKRETQTJ is then implanted in a carefully chosen audio-cover file by means of the steganography component (of the proposed system) to obtain a stego-audio-file which to the Human Audio System (HAS) has the same feel/quality as the original the audio cover file. This final output (stego-file) is then securely transmitted to the recipient.

The recipient first extracts the ciphertext from the stego-file received. Then to decode the ciphertext, the recipient must possess the number pair (p, q) = (5, 3) with which to derive the decryption key.

DOI: 10.54254/2755-2721/2/20220613

Table 4. Message encryption.

e	m	m	a	n	u	e	l	u	n	i
4	12	12	0	13	20	4	11	20	13	8
2	13	11	20	5	3	4	16	8	2	13
6	25	23	20	18	23	8	1	2	15	21
G	Z	X	U	S	X	I	B	C	P	V
v	e	r	s	i	t	y	o	f	t	e
21	4	17	18	8	19	24	14	5	19	4
11	20	5	3	4	16	8	2	13	11	20
6	24	22	21	12	9	6	16	18	4	24
G	Y	W	V	M	J	G	Q	S	E	Y
c	h	n	o	l	o	g	y			
2	7	13	14	11	14	6	24			
5	3	4	16	8	2	13	11			
7	10	17	4	19	16	19	9			
H	K	R	E	T	Q	T	J			

5. System implementation

The project was implemented using the MATLAB software running in a Windows 10 OS setup with 4GB of RAM, a 2.16GHz Intel processor, and a 250GB hard disk. In this experiment, the cover media was picked from two (2) different digital audio file types (.mp3 and.m4a). To allow for the evaluation of our approach, secret text files with various features were embedded in the chosen audio cover files.

The stego files (audio files included in the stego files) were assessed. After assessing the proposed approach, the stego file (audio file) preserves its original size, and the volume of info which the proposed system can effectively/efficiently hide was observed to be reasonably large.

Standard performance metrics such as, *computing time*, *compression-ratio*, *bit-per-character*, as well as *signal-to-noise ratio*, were employed for appraising the proposed system. We observed that the proposed system performed sufficiently well in terms of these performance metrics.

6. Conclusion and recommendation

Financial crime and fraud occur at an alarmingly high incidence in today's computerized world, which is concerning. Information leakage, privacy breaches, and massive losses of money and other valuables have been reported on a near-daily basis. Existing approaches have a number of flaws and are ineffective. The development of an audio steganography security architecture for ensuring secure and privacy-preserving electronic commerce transactions across open business networks is described in this study. As cover media, this work employed two separate audio file types (.M4A and.MP3).

This proposed approach would be extremely valuable in safeguarding and communicating massive amounts of sensitive financial information amongst business transacting entities while avoiding the suspicion of fraudsters and other unauthorized individuals with malevolent intent. Future study will examine the prospect of combining Post-Quantum Cryptography with DCT Steganography, as well consider the use of videos or text files as cover media.

References

[1] B. Hampiholi, G. Alpar, 2017. “Privacy-preserving webshopping with attributes”. DOI: 978-1-5386-1027-5/17. *IEEE* 2017.

DOI: 10.54254/2755-2721/2/20220613

[2] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, O. S. Adewale, 2013. Post-Quantum Crystography; A combination of post-quantum cryptography and steganography, The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), Technically Co-Sponsored by IEEE UK/RI Computer Chapter, 9th-12th December 2013, London, UK, 454-457.

[3] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, O. S. Adewale Post-Quantum Crystography based Security Framework for Cloud Computing, Journal of Internet Technology and Secured Transactions (JITST), 2015, 4(1), 351-357.

[4] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, O. S. Adewale, O. A. Sarumi 2019. Post-Quantum Crystography System for Secure Electronic Voting, Open Computer Science, DeGruyter 9:292-298.

[5] R. O. Akinyede, O. S. Adewale, B. K. Alese (2014). Building a Secure Environment for Client-Side E-Commerce Payment System using Encryption System. Proceedings of the World Congress on Engineering 2014 **Vol I**, WCE 2014, July 2 - 4, 2014, London, U.K.

[6] D. Wheeler, D. Johnson, B. Yuan, P. Lutz, (2012). Audio Steganography Using High Frequency Noise Introduction. Thomas Golisano College of Computing & Information Sciences Rochester Institute of Technology, Rochester NY, RIT Scholar Works, retrieved on 14/09/2018 : http://scholarworks.rit.edu/other/302.

[7] D. Ghanwat, and R. S. Rajan, (2013). "Spread Spectrum-based Audio Steganography in the Transformation Domain". *Global Journal of Advanced Engineering Technologies*, 2(4):66-77. 2013.

[8] R. F. Olanrewaju, H. A. Othman, K. R. Suliman, (2013). Increasing the Hiding Capacity of Low-bit encoding Audio Steganography using a Novel Embedding Technique, World Applied Sciences Journal, 2013, 21(26) : 79-83.

[9] P. E. Kresnha, and A. Mukaromah, (2014). A Robust Method of Encryption and Steganography using ElGamal and Spread Spectrum Technique on MP3 Audio File. In Proceeding of Conference on Application of Electromagnetic Technology, 2014, 3(9):11-15.

[10] L. Kumari, D. Goyal, S. Gyan, (2013). Analysis and Design of Three LSB Techniques for Secure Audio Steganography. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 2013, 2(2): 44-55.

[11] O. T. Adeboje, A. O. Adetunmbi, A. J. Gabriel, (2020). Embedding Text in Audio Steganography System using Advanced Encryption Standard and Spread Spectrum. International Journal of Computer Applications (0975-8887). DOI:10.5120/ijca2020919. **Volume 177**, Number 41. Pp 46-51. 2020.

[12] A. J. Gabriel, A. O. Adetunmbi, P. Obaila, (2020). A Two-Layer Image-Steganography System for Covert Communication Over Enterprise Network. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. DOI: 10.1007/978-3-030-58817-5_34.

[13] A. Luma and B. Raufi (2014). "Data Encryption and Decryption Using New Pythagorean Triple Algorithm". Proceedings of the World Congress on Engineering 2014 **Vol I**, London, U.K.