An Improved Cybersecurity Model using Cryptography and Steganography with NTRU-LSB Algorithm

Souley Boukari, Jaafaru Bobbo

Abstract - Data and information has become one of the prime targets of hackers due to the sensitive nature of patients’ information. Some methods such as DES, 3DES, Blue fish and AES were used but found to be inefficient. This research aims to reduce the vulnerability of threats and increase the user satisfaction based on Embedding Capacity (EC), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) on patient’s information since healthcare systems are getting very common within the society. Nth Degree Polynomial Ring Unit and Least Significant Bits were used to encrypt a text message into audio file. The research, therefore, developed a hybrid security system that can hide compressed information in audio using NTRU and LSB. The concept of cryptography and steganography was introduced to encrypt the original data by using symmetric key cryptography and to hide that data into an audio file. The proposed model was developed using MATLAB R2018(a) software. The results revealed that the proposed model is more secured in comparison to the existing model. The MSE for the proposed system is 2.4320e-06 as against 2.5321e-06 for the existing model with the peak signal to noise ratio of 156.1154 and 161.0154 for the proposed system. The proposed system has embedding capacity of 0.020 bps, while the existing system is having 2.75 bps. From the result analysis, the proposed system has performed significantly better than the existing system in terms of MSE, PSNR and embedded capacity.

Keywords - Cybersecurity; Nth Degree Polynomial Ring Unit (NTRU); Least Significant Bit (LSB); Cryptography, Steganography, Stego - audio Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), embedded capacity.

1. Introduction

Cyber security has been used interchangeably for information security. Where the latter considers the role of humans in the security process, the former considers this as an additional dimension. However, such discussion on cyber security has important implication as it focuses on the ethical part of the society as a whole. Healthcare sector has become one of the major targets of hackers due to the sensitive nature of patients’ information such as digital patient records, electronic management records, risk management, security tools, and all elements needed for enhanced patients’ information security. Health Information is an information exchange which is linked and managed on internet and its infrastructures [1]. However, protecting information is not an easy task. Health care organisations are quickly confronting security threats and vulnerabilities through the implementation of digitalisation of patient records. The aim of health care systems is to deliver the highest health service to patients anytime from anywhere. Privacy is one of the major factors which have a sub factor in the form of confidentiality which is needed to prevent the disclosure of patient’s sensitive information [2].

In the healthcare sector, data security must be given the highest priority, as it is essential to maintain access rights to data. Improving security in healthcare means maintaining privacy and confidentiality of the patient information, and it helps in preventing threats. The primary objective of the health information technology is to meet three fundamental goals, confidentiality, integrity and availability with the overall aim of achieving security in Health Care.

Therefore, this study uses NTRU and LSB to form a combined cryptography and steganography technique to improve the security of patient’s information.
Cryptography serves the following purposes:

Confidentiality: The principle of confidentiality specifies that only the sender and the intended receiver should be able to access the contents of a message.

Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Non-repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message. Cryptography consists of two types:

a. Symmetric Key Cryptography: When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography. E.g. Data Encryption Standard (DES), AES, Triple DES, Blowfish algorithm.

b. Asymmetric Key Cryptography: When two dissimilar keys are used, that is, one for encryption and the other for decryption, then that mechanism is known as asymmetric key cryptography. Steganography is the art and science of writing concealed messages in such a way that no one, except the sender and intended recipient, suspects the existence of the message, a form of security through hiding the message, i.e., Steganography is a concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information concealed in it. Like cryptography, different types steganography techniques are available based on the hiding techniques, cover medium used etc. Steganography techniques include image steganography, video steganography, text steganography etc. In this paper, we have implemented audio steganography which includes LSB algorithm and Discrete Wavelet Transform (DWT).

2. Related Works

Due to the importance and sensitive nature of information in the healthcare sector, different methods, algorithms and models have been proposed by different authors to ensure that digital information is secured. The security of the Healthcare Systems and medical applications is considered by applying information hiding methods. The constraints in securing medical and healthcare applications using steganography, watermarking, and cryptography are listed. But these techniques need to be designed in such a way that can guarantee the least acceptable alteration in the medical data [3].

In their study, Babatunde, et al. [4], employ 3DES, Least Significant Bit (LSB), techniques to improve the Security of Medical Data. The result obtained shows that a double layered security system offers more security strength and makes it difficult for cyber-attack. Moreover, there is a need for a faster and more secure technique as their solution is too slow and might cause more havoc than the advantage it offers.

Sivaranjani and Radha [5], study various techniques used for securing data and how biometrics can be used for hiding data are examined. The study helps in understanding the QRS Complex detection of heart beat, filtering the signal in the heartbeat, discussing how various encryption techniques like RSA, DES, Triple DES, are used for encryption of patient data over network to secure transmission so as to try implementation of the same technique using Biometric Key Generation.

Abdulsalam et al., [6] in their study, addressed the issue of confidentiality in regard to medical data in Electronic Healthcare Record (EHR) system using transform domain watermarking technique, Linde Buzo Gray (LBG) algorithm for authentication and Huffman compression for data reduction.

Demyana et al., [7] examined a new technique for hiding medical information in an image with less variety bits. This study will attempt to extend the proposed system to a steganography technique that can have confirmation module alongside encryption and decryption.

Krishnan and Abdullah, [8] in their study, present an Enhanced Security in Audio Steganography by using Higher Least Significant Bit to improve security and robustness by embedding bits of secret message in higher LSB of a cover audio. Nevertheless, this work did not focus on developing more efficient, higher LSB scheme with better PSNR, MSE to improve Audio Steganography.

Omotosho et al., [9] in a study presented an e-prescription system that addresses some challenges pertaining to the patient’s privacy protection in the process of drug prescription. The developed system uses spread spectrum image steganography algorithm with Advanced Encryption Standard (AES) key implementation to provide secure means of delivering medical prescription to the prescriber and the pharmacists so as to consider the use of Audio and Video Spread Spectrum Steganography and performance evaluation of the developed system using appropriate metrics.

Nawlesh and Kalpana [10] presented an e-prescription system that addresses some challenges pertaining to the patient’s privacy protection in the process of drug prescription. The developed system
uses spread spectrum image steganography algorithm with Advanced Encryption Standard (AES). The proposed method recovers the cover image losslessly after extraction of patient information, thereby showing better results as compared to the other methods.

Jero et al. [11] proposed a steganography approach based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to hide patient confidential information along with the Electrocardiogram (ECG) data. The approach aims at less distortion to the watermarked signal so that the diagnosability is not lost and also at maximum retrieval of the patient information.

Ahmad et al., [12] in their study proposed methods to protect medical data by using the shared secret mechanism and steganography for 2 and 1 bit LSB. The experimental results show that they produce relatively good quality (similarity) in terms of Peak-Signal-Noise-Ratio (PSNR).

3. Methodology

This work is aimed at improving the security of information hidden under audio medium. This work uses Discrete Wavelet Transform (as the file compression method), Least Significant Bit and NTRU cryptosystem to hide text file in an audio carrier. The NTRU encryption of Bernstein et al. [13] is used to scramble the original bits to text file, the text file is converted to ASCII binary and cipher which is encoded into low and high frequency passes obtainable for effective hiding with the single level DWT algorithm. Figure 1. below presents the proposed cyber security model in a health care system.

3.1. Working Principle of the Proposed System

This study provides an improved security to healthcare information using NTRU encryption scheme and DWT algorithm. The benefit of using both NTRU encryption scheme and DWT algorithm is that it is used to create communication between parties which gives a minimised threat of destroying the media and theft of secret data during transmission.

The aim is to conceal the availability of secret data (text lexicons) encoded in digital audio file (carrier) since, audio medium is the most common form of communications and information exchange.

The audio cover medium is chosen due to its ability to take advantage of bits replacements features such as LSB and HVS available to several formats of audio communication today. This steganography utilised special tools such as Discrete Wavelet Transform (DWT) and NTRU Encrypt to pre-process, compress and transform both the secret message and the cover medium for increased security against third party attacks and data/information quality retention. The performance of the proposed algorithm will be evaluated based on Krishnan and Abdullah, (2016) using different sizes of data types like text and audio file.
3.2. NTRU Encryption Algorithm for Crypto-Steganography System

Step 1: Puts the message in the form of polynomial m whose coefficients are chosen modulo p between \(-p/2\) and \(p/2\) (centered lift).

The text message is then compressed using Huffman algorithm.

\[ Mc = H(m) \]

where Mc is compressed message.

Step 2: Encrypt the message as \( Ec = Pu \ast R + Mc \) (modulo q) where R is any N X N random matrix.

Before secret message transmission at the sender-side, the text message is transformed into a polynomial \((m)\) with coefficients selected modulo \(p\) in the range \(-p/2\) and \(p/2\) (centered lift). Another, small polynomial \((r)\) is selected at random in order to obscure the message. Eventually, the secret message \((m)\) will be encrypted \((e)\) using the Equation 1:

\[ \begin{align*}
    e &= r \ast h + m \pmod{q} \\
\end{align*} \]  

\( (1) \)

At broadcast-side, for successful transmission of the secret data, two small polynomials \(f\) and \(g\) are chosen from the truncated polynomials ring \((R)\). The inverse of \(f\) modulo \(q\), and the inverse of \(f\) modulo \(p\) is calculated as follows:

\[ f \ast f^{-1} = 1 \pmod{q} \]  

\[ f \ast f^{-1} = 1 \pmod{p} \]

The product of these polynomials can be expressed by the Equation 2.

\[ h = p \ast ((Fq) \ast g) \pmod{q} \]  

\( (2) \)

Therefore, the key generations for the encrypted message \((e)\) can be defined as follows:

**Private Key:** The pair of polynomials \(f\) and \(fp\).

**Public Key:** the polynomial \(h\).

The public and private keys generated are secret which is known to the sender and intended receiver of the message \((e)\) when transmitted in audio carrier as stego-object.

3.3. NTRU decryption of Crypto-Steganography System

Step 1: Compute \( A = F \ast Ec \pmod{q} \) and choose the coefficients in the range \(-q/2\) to \(q/2\).

Step 2: Decrypt the message \( D = Fp \ast A \pmod{p} \).

Step 3: Decompress \( Mc = H^{-1}(D) \).

At the receiver’s side of the proposed crypto-steganography, the private polynomial \(f\) is used to generate a polynomial \(a = f \ast e \pmod{q}\). The coefficients to be selected must be in the range of length \(q\). The recipient generates another polynomial \(b = a \pmod{p}\) in order to reduce each of the coefficients of \(a\) modulo \(p\). The second private polynomial \(fp\) is used to 0 generate the polynomial \(c = fp \ast b \pmod{p}\), which the original form of secret data transmitted from the sender under audio carrier described in the next subsection.

3.4. Architecture of the Proposed System

The entire activity for embedding the encrypted secret message into the audio file carrier to minimize suspicion of third party using LSB is depicted in Table 1 below:

| Table 1. The algorithm of the Crypto-steganography |
|-----------------------------------------------|
| **Input:** Audio samples and Text files       |
| **Output:** secret message and stego key      |
| 1. INPUT compressed audio files for secret message carrier and text file |
| 2. BREAKDOWN the audio vector into congruent portions in signal transform domain with ID DWT. |
| 3. CREATE Binarization of the audio files selected |
| 4. Estimate LSBs position of cover medium      |
| 5. Select the lexicon content of the Text string |
| 6. CONVERT the lexicon into ASCII and Binary representations |
| 7. GENERATE the Nth Truncated polynomial ring for the matching lexicon bits |
| 8. EMBED the combined lexicon portions of the scrambled text file into the audio cover LSBs positions accordingly. |
| 9. BROADCAST the stego-object to the receiver-side as initiated from sender-side with stego key |
| 10. DELIVERY of the secret data by the sender to the receiver. |
| 11. The receiver EXTRACTS the secret message from stego-audio file. |
| 12. RETRIEVE original secret data or plain Cipher text. |
3.5. Operational flowchart of the proposed system (sender)

The activities flowchart depicting the whole processes of the crypto-steganography using audio carrier and text file as secret message at the sender level is depicted in Figure 2. below:

4. Operational Flowchart of the Proposed System (receiver)

The flowchart for retrieving and reversing text lexicons secret data embedded in an audio cover medium is illustrated in Figure 3.
5. Result and Discussion

The work is implemented using MatLab stimulator R2018 (a) and the following results were obtained and discussed below. The original message (text) is encrypted and embedded into an audio cover which is then transmitted via email as a stego audio. At the receiving end, a cover audio is received and decrypted to original text message.

The LSB based steganography alone is ineffective for hiding secret messages in audio signals because it is susceptible to attack from unintended parties whenever large scale noise results. But, the introduction of the NTRU Encrpt algorithm extends the security of undercover transmission and communication. Again, the bits displacements of audio file with encrypted text file were attained by slight modifications of original sound signal at high spectrum, which are unnoticeable to HAS.

Test Case/ Sample 1:

The histogram plot for the original text and audio file embedded with secret message for the sample 1 is illustrated in Figure 4. below

The reason is that the bits in text lexicon have the same makeup as audio carrier bits substituted.

Test Case/ Sample 2:

The audio file (cover and stego) for Sample 2 (Figure 5.) and text file before and after steganography indicates that the two audio files are imperceptible to HAS as shown in Figure 4.2. In the case before steganography, the histogram plot of Sample 2 commenced with the maximum amplitude of −0.9 to +0.9 and decreased to -0.3 to +0.3 at 14000 seconds. After embedding, the relative distribution of audio wave signal is the same except for the indicated concealed secret message.

Test Case/ Sample 3:

The histogram plot of Sample 3 (Figure 6.) indicated the least amplitude at the start and finish after 1800 seconds. The maximum values of amplitude were recorded at -0.9 and +0.9 after 2100 seconds and 1300 seconds respectively. However, the same wave signal distribution is observed after steganography. This is indicative of relative similarity between original audio Sample 3 and stego-object. This implies that hidden secret data cannot be identified by HAS as illustrated in Figure 6.
Test Case/ Sample 4:

From Figure 7., the analysis of two wave plot (histogram) of both the cover and stego files differences cannot be easily differentiated by HAS. The histogram plot of Sample 4 at the beginning amplified to maximum values of -1 and +1 at time of 7000 seconds. It reduced to -0.5 and +0.5 amplitude for a period of 4000 seconds. The final lap of the audio wave signal showed high amplitude of -0.9 to 0.8 in 12000 seconds. Similarly, the distribution of sound wave signal is similar but slightly different in the last 4000 seconds. The reason for this difference is that the bits of secret data (text lexicons) are embedded at the LSBs positions of the carrier file (Sample 4). The goal confused HAS about the existence of secret data realized by NTRU encryptions of the secret message.

Figure 7. Histogram plot of audio Sample 4 before and after steganography

In all audio samples selected for this proposed cryptosystem implementation, there are relative small disparities between the auditory qualities of either sound file (before and after steganography process). The amplitude of both audio files are relatively the same within the range of (-0.1 to 0.7). The rate of noise spread fall within the same audio spectrum as the original, which makes it difficult for the HAS to detect. The maximum number of audio samples spread in audio signal spectrum remains the same after embedding of the text file at 60000 bits. Consequently, audio based steganography with NTRU Encrypt is effective for concealing secret messages over an audio carrier because of the low chances of attacks through the exploitation of HAS.

6. Conclusion and Further Research

In conclusion, this study developed an improved cybersecurity model, that is, the combination of cryptography (NTRU encryption algorithm) and steganography (LSB Audio encoding technique) to improve information security in health care sector. The problem caused by cyber-attacks on information related to health issues. The result in this study shows that this improved model offers more security strength and make successful cyber-attack to be more difficult. With this model, healthcare information embedded into the cover audio can easily be retrieved without any suspicion of the carrier. In future, there is need to experiment other positions for hiding secret messages in the carrier medium to avoid high decryption skills of attackers and promote integrity of secret messages. This can be in the area of spatial and domain transformation functions such as Discrete Cosine Transform and Fourier Transform. There is need to implement NTRU cryptosystem on longest vector problems such as factorization and discrete logarithms.

References

[1]. Samydurai, A., Revathi, K., Prema, P., Arulmozhiarasi, D. S., Jency, J., & Hemapiya, S. (2015, March). Secured Health Care Information exchange on cloud using attribute based encryption. In 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-5). IEEE.
[2]. Barua, M., Lu, R., & Shen, X. (2013, December). SPS: Secure personal health information sharing with patient-centric access control in cloud computing. In 2013 IEEE global communications conference (GLOBECOM) (pp. 647-652). IEEE.
[3]. Sajedi, H. (2018). Applications of data hiding techniques in medical and healthcare systems: a survey. Network Modeling Analysis in Health Informatics and Bioinformatics, 7(1), 6.
[4]. Babatunde, A. O., Taiwo, A. J., & Dada, E. G. (2018). Information security in health care centre using cryptography and steganography. arXiv preprint arXiv:1803.05593.
[5]. Sivaranjani, B., & Radha, N. (2017, October). Securing patient's confidential information using ECG steganography. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 540-544). IEEE.
[6]. Abdulsalam, Y.S. Ahmed, A. Mkall, O.O.(2017). Developing a Secure Distributed Electronic Healthcare System Using Information Hiding Techniques. Proceedings of the iSTEAMS Multidisciplinary Research nexus Conference.
[7]. Wadie, D. M., Taha, I., & El Deeb, H. (2016). Hybrid Cryptography and Stenography Healthcare Application. International Journal of Advancements in Computing Technology, 8(1), 41.
[8]. Krishnan, S., & Abdullah, M. S. (2016). Enhanced security audio steganography by using higher least significant bit. *J Adv Res Comput Appl ISSN (online)*, 2(1), 39-54.

[9]. Omotosho, A., Adegbola, O., Mikail, O. O., & Emuoyibofarhe, J. (2015). A secure electronic prescription system using steganography with encryption key implementation. *arXiv preprint arXiv:1502.01264*.

[10]. Kumar, N., & Kalpana, V. (2015). A novel reversible steganography method using dynamic key generation for medical images. *Indian Journal of Science and Technology*, 8(16), 1. DOI: 10.17485/ijst/2015/v8i16/61974.

[11]. Jero, S. E., Ramu, P., & Ramakrishnan, S. (2014). Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. *Journal of medical systems*, 38(10), 132. DOI 10.1007/s10916-014-0132-zs

[12]. Ahmad, T., Studiawan, H., Ahmad, H. S., Ijthadie, R. M., & Wibisono, W. (2014, October). Shared secret-based steganography for protecting medical data. In *2014 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)* (pp. 87-92). IEEE.

[13]. Bernstein, D. J., Chaungsatiansup, C., Lange, T., & van Vredendaal, C. (2017, August). Ntru prime: reducing attack surface at low cost. In *International Conference on Selected Areas in Cryptography* (pp. 235-260). Springer, Cham.