Bulletin of Electrical Engineering and Informatics
Vol. 11, No. 1, February 2022, pp. 185~194
ISSN: 2302-9285, DOI: 10.11591/eei.v11i1.3279

Audio steganography with enhanced LSB method for securing encrypted text with bit cycling

Enas Wahab Abood[1], Abdulhssein M. Abdullah[2], Mustafa A. Al Sibahee[3,4], Zaid Ameen Abduljabbar[5,6], Vincent Omollo Nyangaresi[7], Saad Ahmad Ali Kalafy[8], Mudhafar Jalil Jassim Ghrabta[9]
[1]Department of Mathematics, College of Science, University of Basrah, Basrah, Iraq
[2]Department of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[3]Department of Computer Technology Engineering, Iraq University College, Basrah, Iraq
[4]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, China
[5]Computer Science Department, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[6]Shenzhen Institute of Huazhong University of Science and Technology, Shenzhen, China
[7]Faculty of Biological & Physical Sciences, Tom Mboya University College, Homabay, Kenya
[8]Basra Oil Training Institute, Ministry of Oil, Basrah, Iraq
[9]Pharmacy Department, Ashur University College, Baghdad, Iraq

Article Info

Article history:

Received Aug 31, 2021
Revised Dec 2, 2021
Accepted Jan 16, 2022

Keywords:

Audio security
Audio steganography
Bit cycling encryption
LSB steganography

ABSTRACT

Data security pressing issue, particularly in terms of ensuring secure and reliable data transfer over a network. Encryption and seganography play a fundamental role in the task of securing data exchanging. In this article, both steganography and cryptography were combined to produce a powerful hybrid securing stego-system. Firstly, a text message is encrypted with a new method using a bits cycling operation to give a cipher text. In the second stage, an enhanced LSB method is used to hide the text bits randomly in an audio file of a wav format. This hybrid method can provide effectually secure data. Peak signal-to-noise ratio (PSNR), mean squared error (MSE) and structural similarity (SSIM) were employed to evaluate the performance of the proposed system. A PSNR was in range (60-65) dB with the enhanced least significant bit (LSB) and the SSIM had been invested to calculate the signal quality, which scored 0.999. The experimental results demonstrated that our algorithm is highly effective in securing data and the capacity size of the secured text. Furthermore, the time consumption was considerably low, at less than 0.3 seconds.

Corresponding Author:

Enas Wahab Abood
Department of Mathematics, College of Science, University of Basrah
Basrah, Iraq
Email: enaswahab223@gmail.com, enas.abood@uobasrah.edu.iq

1. INTRODUCTION

The process of exchanging data constantly increases through various means of transportation and for various types of data, meaning that the need to secure it also increases. This is especially the case for highly sensitive data such as military data, bank and personal accounts [1]. Digital security emerged to secure the protection of digital data exchanged over the network and transport media [1]. There are innumerable ways to secure data of all kinds, many of them successful. However, there remains considerable security gaps, as well as issues with application, such as memory or time consumption. Steganography and cryptography are the most essential aspects of digital security [2]. Steganography is the covered writing science and invisible communication. The key objective of steganography is to hide data inside an innocent file (which could be an image, a text, audio, and a video) in such a way that its existence is undetectable within the carrier file,

visible only to the authorized user and after the application of the retrieving algorithm [3]. Steganography offers methods for providing secrecy and access restriction. The hidden information is inextricable without sufficient knowledge of the steganography parameters, such as positions, the length of the secret message, and the secret key [2]. The encryption, on the other hand, is a way of transforming the overall view of understood data into a disfigured one, so the encrypted message appears to contain important data that requires deciphering. The encryption would fail if the intruder were to be able to decrypt the cipher message, while Steganography fails to secure data when the attacker detects the presence of a secret data inside the cover file [4], [5]. Thus, for more ensuring data security, steganography and encryption are used together so that any observer would struggle to detect messages and, even upon retrieval, it would remain indecipherable and meaningless [6]. In encryption, there are two kinds of cryptography: symmetric and asymmetric. Symmetric cryptography uses a unique key for encryption and decryption, so its main problem is how to share keys securely. Asymmetric cryptography has two keys, the first is a public key used for encryption and the second is private and used for decryption (i.e. keys are complementary) [7].

Audio steganography is defined as the art of securing data through hiding it in an audio file; the secret data may be an image, a text, a video or even an audio, which is mostly applied to ensure copyright for audio files to protect the rights of the file's owners. The most significant obstacle to all methods of steganography is the extreme sensitivity of the human auditory system (HAS) [8], [9]. To implement audio steganography, many methods can be used, such as least significant bit (LSB), phase coding, echo hiding and spread spectrum coding. The most famous and easily implemented method is LSB, where the bits of secret data are replaced with the LSB of the cover value [10]. The LSB steganography technique is capable of hiding a large amount of data. Unfortunately, these data could be perceived due to the channel noise it causes [11], while the transform domain techniques used the auditory system capabilities in hiding, by putting the low frequencies beside the inaudible high frequencies [12].

In this paper, we propose a hybrid system of cryptography and steganography to strengthen security. A new Algorithm has been produced to implement the cryptography; based upon bits cycling around a concealed point. That concealed point is determined by the user as a key point. The bits before and after the key point are replaced with each other; it is considered as a symmetric method which is low in cost and easy to implement and secure. For additional security, a steganography is added. The LSB is employed for steganography with modifications as a random spreading of bits and a number for the division as a secret key.

The most influential contribution of encryption proposed method is to protect important text messages from being eavesdropped on by attackers, the method is characterized with low costs and increasing the security level using steganography in audio due to its ability to hold a lot of data, as well reducing network resources consumption due to less usage of calculations and memory consuming; time elapsed here was very low, so we recommend it should be used with smart devices.

The paper structure is organized as shown in; section 1 is the introduction, containing principles, definitions and an overview of the study subject; in section 2, a review of previous works is discussed, including encryption and steganography; section 3 includes the proposed system (structure and algorithms). The experimental results and analysis are presented in section 4; finally, the conclusions and future works are outlined in section 5.

2. RELATED WORK

In recent years, there have been several researches about developing algorithms to hide data in an audio signal. A few related works are given here, with the aim to achieve robustness and increased efficiency. Produced a scheme that utilized the concept of Frequency Masking with the coefficients of wavelet of the payload by carrying out a replacement process for indirect LSB to hide sound signals into cover sound signals of speech [13]. It consisted of four steps: decomposition and pre-scaling operations that were done by implementing the discrete wavelet transform (DWT) and the coefficients of the DWT were transformed from decimal to a binary representation. Following this, the wavelet coefficients of the payload were sorted and hidden with an indirect LSB substitution operation. Finally, the output signals were reconstructed by applying the inverse wavelet transform. Although it was effective for securing data, it required the implementation of too many calculations, resulting in high consumption time. Yan *et al*. [14] proposed a novel steganographic algorithm for securing MP3 audio files. Their algorithm was based on the window switching technique, which is a part of the MP3 compression standard for controlling the pre-echo distortion. It works by establishing a relationship between the parity of a secret bit, the type of window, and the secret message is hidden in MP3 audio. The proposed algorithm was compliant with the MP3 compression standard, which made the process of decoding the stego audio correctly done with ordinary MP3 players, while the hidden message could only retrieved by parsing the information of the hiding process without fully decoding it. Tayel *et al*. [15] hid data bits in an LSB audio file and indicated that the size of the cover file and

the message length affected the sound quality of the cover file, and whenever the message size got bigger, the audio became distorted.

Rajput *et al*. [16] proposed two algorithms. In algorithm-I, two data bits of the secret message were hidden each time on the LSB positions of the cover audio file based on the 3 MSBs of the cover audio file, in proposed algorithm-II, those two data bits are hidden on LSB positions of the cover file, and they are based on the compliment of 3 MSBs of the cover file. Its first algorithm-I improved the hiding capacity by covering up two data bits each time, while algorithm-II was robust against attacks because, in conventional algorithms, the hiding process is done linearly, which enables attackers to extract the secret data easily. Its system was immunized but complex, leading to a high computational cost. According to [17] proposed a hybrid system consisting of encryption and hiding. In the encryption phase, the text was encrypted firstly by converting it into a binary code using a dynamic table in a substitution manner, then encrypted it with an AES algorithm based on a dynamic key. The encryption key was generated using corner points. The hiding phase used LSB in the cover image pixels except for the Harris corner points. Hashim *et al*. [18] presented two techniques; one was an enhanced LSB method for allocating bits at random positions, and the other was an advanced encryption standard (AES) which was used to increase the security level of the message. The two systems in [17] and [18] suffered from the complexity and high cost of the AES algorithm employed in them and the generated long keys. Irsan *et al*. [19] purposed an algorithm to encrypt a text message utilizing the chaotic map; the algorithm used the MS map to generate a keystream. Wu *et al*. [20] produced a new steganography method to hide and secure audio files. This method was based on information from iterative adversarial attacks against convolutional neural networks CNNs. The method begins with a flat or a random embedding cost, and then the data is updated based on the attack information until satisfactory security results are satisfied with long time consumption. According [21] proposed a modified eLSB embedding technique to hide a text message in an image file. The modified method encrypts secret messages in two stages. In the first stage, the metadata is generated and the header information is included in the first few bytes of the cover image. In the second stage, the secret message after processing by hashing the frequent words is stored in the cover image using an improved method. While it gives a smaller size of secret data in the cover file, it requires further calculation to implement it.

The above methods have a relative immunity to most attacks. Among the problems found in the literature are the issue of encryption key security or accuracy in data retrieval, as well as the time-consuming and complexity of computational operations. In this paper, a simplified, low complexity, and effective method for encrypting the text file is presented to protect it from snoopers and this hybrid system produced much security for the message and ensuring its reliability and integrity. The method selects a point from the symbol bits to rotate the bits before and after it to produce a new symbol and then hides it inside another audio file in a randomly modified LSB method. It is difficult to determine the spread of bits or the rotation point unless the snooper has comprehensive information about it. They would also require knowledge about how to convert the audio file to the American standard code for information interchange (ASCII) code used in the system.

3. PROPOSED SYSTEM

In this article, a hybrid system is proposed to protect text message transmission between two entities using two security techniques: encryption and audio steganography. The text message is encrypted using a new algorithm based on exchanging bits position around key-point which is then hidden inside a cover sound file in the time domain using a modified LSB method with random distribution. The proposed system involves two stages illustrated in Figure 1.

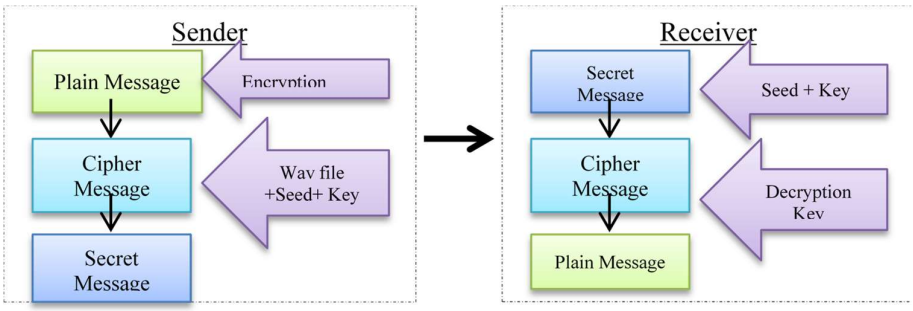

Figure 1. The general diagram of the system

3.1. Key exchange stage

Elliptic curve cryptography (ECC) is used once to encrypt the keys for being exchanged between the sender and receiver, the sender encrypts the keys with the public key and sends them to the receiver, who in turn decrypts them using the secret key. ECC is an encryption algorithm that produces encryption keys by using curve points, explained in the following steps [22], [23]:

a. Point generation: the irreducible polynomial equation is used to get the n-number of points for obtaining elliptic curve.
b. Key generation: both public key and private keys are generated.
c. Encryption: the three keys (of the suggested algorithm) are encrypted with the public key by the sender to protect it from unauthorized parties.
d. Decryption: is decrypted the cipher text (three encrypted keys) with a private key by the receiver.

Although the ECC algorithm is an asymmetric algorithm and it uses two keys, it is a computationally inexpensive, less time-consuming algorithm than other asymmetric algorithms, and it is used only once to exchange keys and thus does not affect the system's lightness, speed, and security.

3.2. Secure message delivery stage

3.2.1. Cryptography technique

The first security technique was the encryption of a plain text message using a proposed algorithm that works on the plain character itself to get a cipher character. As known, each readable character in the computer needs 7 bits to be represented like (a6 a5 a4 a3 a2 a1 a0) in the proposed method. The arrangement of these bits changed to get a new character. The encryption algorithm is illustrated as shown in:

– Sender side algorithm (1-a):

a. Selecting a point as encryption key which is a number between 1 and 6 as a point of cycling, let be M=3.
b. Cutting the bits before point M and placing it at the end of the new character.
   A= (a_6 a_5 a_4 a_3 / a_2 a_1 a_0)
   B= (- - - a_6 a_5 a_4 a_3)
c. The rest of A`s bits are placed at the start of the new character:
   B= (a_2 a_1 a_0 a_6 a_5 a_4 a_3)
   Ex: ASCII code of the character ('b') is 98 and its binary code is ('1100/010'), supposing that the key is 3 so, the new binary will be ('010/1100') which is 44 of the character ','. The operation is repeated to all characters of the message to get the cipher message.
d. The cipher message is hidden in a sound file (as explained in the next subsection) and sent to the receiver.
e. end

– Receiver side algorithm (1-b):

After receiving the audio message by the recipient, the cipher text message is extracted (unhidden) from the cover file and decrypted by the decryption key which is:

Decryption key=Encryption key+1:

B= (b_2 b_1 b_0 / b_6 b_5 b_4 b_3) cipher character

A=(b_6 b_5 b_4 b_3 / b_2 b_1 b_0) plain character

Then, the binary code is transformed to an ASCII code, which will be transformed to characters of the plain text message.

3.2.2. Steganography technique

Audio steganography is the second part in securing step of the system, the cipher message is hidden in a sound file of a stereo channels in *.wav file format. A modified LSB method is used to hide bits in random positions in the cover file in the second channel. The LSB is chosen by dividing each sample value with a number which represents a Key for LSB detection. The stego algorithm steps are carried out, as demonstrated in:

– Sender side algorithm(2-a):

a. Converting the ASCII of the encoder message into binary representation:
   [30 35 20 …] = [0011110 0111000 1110011…]
b. Generating a set of random locations for the distribution of message bits based on the number of its bits as the generation number key.
c. For each value in the cover file y(i), i is a random position, bits of cipher message characters bit(h) , steps are done as:
   – y`(i)=y(i) *100000

- Taking the integer part (z) of y`(i) , transforming it to binary and putting the rest fraction (if there is a remainder) in x :
- z=binary(int(y`(i)))
- Hiding the bit(h) in the LSB of z.
- y`(i)=decimal (z) + x
- y(i)=y`(i)/100000

d. Forming the cover file from the samples and send it to the recipient.
e. end

Remark: The wav file capacity for hiding messages varies according to the sampling rate of the wav file and the length of the plain message. The text character takes 7-bits in binary representation, so if we have a wav file of the sampling rate at about 44100 samples per second, one second is capable of hiding more than 6200 characters. In this system, because of the random distribution of the message bits, they became difficult to collect, unnoticeable, and hard to arrange with less noise in the cover file. Figure 2 shows the sound file with the different lengths of the hidden messages.

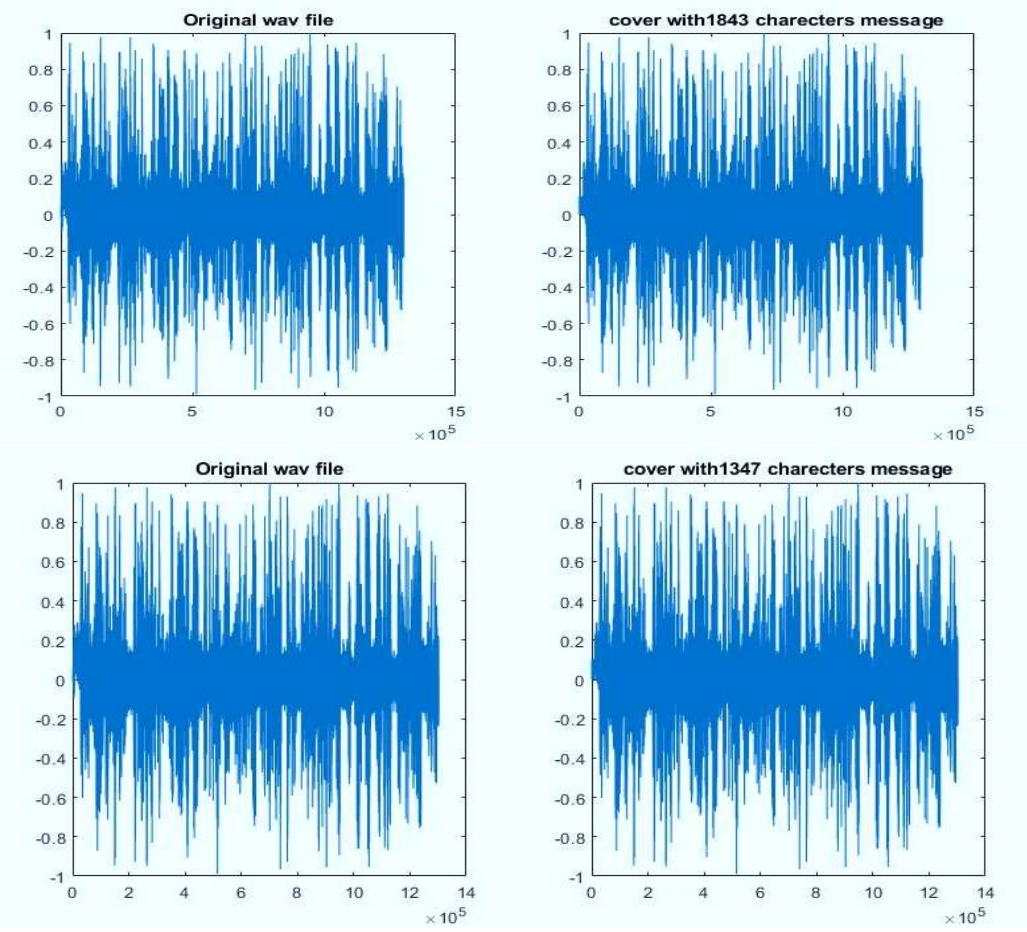

Figure 2. A cipher messages with lengths 1843 and 1347 character inside the cover file

- Receiver side algorithm(2-b):

At the receiver side, a seed number (which is the length of message bits) is used to generate random numbers representing the locations of message bits, the bits are collected and re-arranged to form the cipher characters as an ASCII coding as shown in:

a. Using the seed number to generate a set of locations of the message bits.
b. For each value in the random position of the cover file y(i):
   - y`(i)= y(i)*100000

– z`= int( y`(i)) , taking integer part of the division operation.
– Transform z` to binary.
– messege_bit(i)= LSB of z.

c. Arrange the message bits to build the ASCII representation of the ciphered characters.
d. Send the cipher text to decryption algorithm 3.a to get plain message.
e. end

4. DATA STEGANOGRAPHY STANDERS

4.1. Peak signal to noise ratio

Peak signal to noise ratio (PSNR) metric calculates the ratio of the noise between the same signal before and after making changes on it to expose any distortion after change [22], [24]. It is computed with the formula:

$$PSNR(x,y) = 10log_{10}\left(\frac{M^2}{MSE}\right)$$

Where M takes the highest value of the x samples while MSE represents the mean square error between x,y and it is computed by:

$$MSE = \frac{\sum_{i=1}^{M} \|x(i)-y(j)\|^2}{M}$$

Where x is the original wav file before hiding while y is after hiding.

4.2. Structural similarity index metric

Structural similarity index metric (SSIM) is an image quality metric and it is considered the preferred option of all the traditional measures, such as PSNR and MSE. This metric takes the image distortion as a change in the structural data of that image. The SSIM idea is dependent on the principle that the spatially closed image pixels have strong interdependencies. That way, this metric is able to measure any minor change [25]. The SSIM formula calculates the changes between the secret image before and after processed as shown in:

$$SSIM = \frac{(2\underline{x}\,\underline{y}+c_1)(2\sigma_{xy}+c_2)}{(\sigma_x{}^2+\sigma_y{}^2+c_2)(\underline{x}^2+\underline{y}^2+c_1)}$$

Where $c1 = (k1L)^2$, and $c2 = (k2L)^2$ are constants to evade null dominator. L is 255 which is the high value of the pixels and 1 for the audio file. k1 and k2 have default values (0.01 and 0.03) respectively. The identical score of this metric is 1, which decreases to −1 as a whole difference.
Remark: x and y could be the secret image before sending and after retrieving or the cover file before and after hiding, according to the desired measurable.

5. EXPERIMENTAL RESULTS AND ANALYSIS

5.1. Cryptography analysis

The algorithm 3.2.2 was written for retreiving the cipher text from the cover and decrypted with 3.2.1 to get the plain text. The Table 1 shows that the text message was retrieved seccesfully and completly, the SSIM was used to measure the similarity for the text messeges between sender and receiver. The SSIM values for all different sized messeges were (1) which means the system was reliable and accurate in retreiving.

Table 1. The SSIM values of the secret messeges from sender to receiver

Message size (number of the characters)	SSIM
450	1
1001	1
2056	1
2503	1
3050	1

5.2. Steganography results

In this paper, the secret message is a text message that is firstly encrypted by a new method depending on a bit cycling to get the cipher text that is embedded in a cover file. The cover file must be audio (*.wav) file format. The system was experimented with different lengths of messages and sizes of cover files; in each experiment the files are chosen so the number of samples of the audio file (size) must be at least 7 doubles of the amount of character in the text message to ensure the reliability and efficiency of the proposed algorithms. The system simulation was executed using MATLAB R2018a on an Intel® Core™ i7-3520M and CPU @2.90GHz with 8.00 GB Ram. For the characteristic analysis of the proposed system, some metrics, such as peak signal to noise ratio (PSNR), mean squared error (MSE), and structural similarity (SSIM), were used.

The PSNR ratios for different length messages before and after encryption and exchanged from sender to receiver and decryption were infinity which means the messages were transmitted completely with no loss [5], [26]. Also, The PSNR, MSE, and SSIM were calculated for the audio file before and after embedding the message for a different length of them. PSNR scored 60-65 dBs for hiding different lengths of messages within the same audio file while MSE gave values less than 9e-7, this is considered very high compared to the minimum acceptable ratio of 20 dB, recommended by the International Federation of the Phonographic Industry (IFPI) [27], [28]. On the other hand, the SSIM gets very close to 1 for all cover files. From above, we conclude that the ratios scored excellent results and that ensures the system imperceptibility and noiseless requirement, Table 2.

Table 2. The PSNR, MSE and SSIM calculated for different size of message embedded in an audio cover file of length (3 seconds) with (48000) Fs before and after hiding

Message size (number of the characters)	PSNR	MSE	SSIM
450	65.0516	3.1249e-07	0.9997
1001	60.6343	8.6411e-07	0.9996
2056	60.63	8.6420e-07	0.9995
2503	60.6335	8.6427e-07	0.9994
3050	60.6332	8.6433e-07	0.9994

The bit-interpolation process changes the value of the sample by 0.00001 only when the LSB is different and this small value may cause a little noise in the cover file. Using a smaller message and a larger cover file leads to a reduction in the file distortion. In addition, the statistical analysis and experiments proved the effectiveness of the system in securing data and the little noise caused by the hidden message. The noise can also be reduced by using a larger multiplication in the step in 3.2.2 :(y`(i)=y(i) *100000) to get the least possible effect of the replaced bits.

5.3. Computational costs

The experiments also showed that the time consumption for the system both in cryptography and steganography varies proportionally with messages length, as showed in Table 3, Figure 3. We can see that the average time of whole system in encryption and hiding last for less than 0.3 seconds, which is less than what was obtained by [20] (approximately 0.42 hours on average). Although the processor we used is much less efficient than the processor was used by them in the specifications (Nvidia GPU Titan X, an Intel(R) Core(TM) i7-6900K CPU of 16 cores, memory of 64 GB) and this makes our method better and more efficient in terms of speed and the possibility of using it in tablets, lightweight, and smart devices.

Table 3. The time consumption (seconds) of the proposed system for different message lengths

No. of message characters	Elapsed time			
	Encryption	Decryption	Hiding	Unhide
450	0.0091	0.0028	0.022	0.039
1001	0.0088	0.0066	0.0942	0.0722
2056	0.0173	0.0115	0.161	0.109
2503	0.015	0.0142	0.181	0.11
3050	0.0182	0.0161	0.1942	0.14

The significant keys used in the proposed system were three, the encryption key which is used for text message distortion, multiplication number, and a seed number for producing a set of random numbers were used as locations to spread message bits inside the cover file. To expose the message on the receiver's end, the keys would be necessary, or else mission is too difficult.

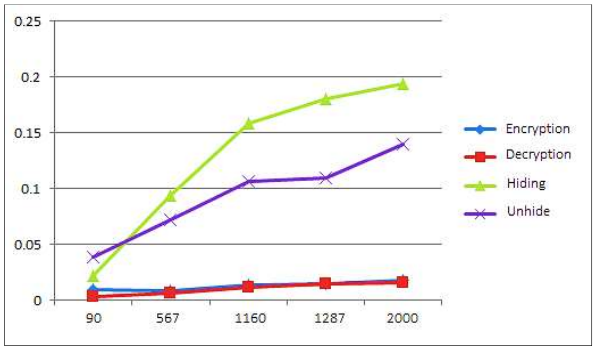

Figure 3. Elapsed time for securing messages vs message size and fixed audio file size 3 seconds with frequency sampling 48000

6. CONCLUSION

This system is suitable for securing different types of data, such as text or images. The secret messages were hidden with less distortion in the cover file that may result from the changes in values of samples. The statistical analysis experiments for the values of PSNR were proved system ability which recorded a value greater than 60; as well as MSE which indicates that there is a lack of distortion. The SSIM scale, whose values were about 0.999, confirms the system success in hiding, and any attempt to reduce the resulted noise could affect the ability of message recovery. The fully secured messages were retrieved completely, as confirmed with the PSNR ratio, which records infinity between sent and received messages of different lengths. Furthermore, the execution time was very low, making it suitable for use with lightweight devices.

REFERENCES

[1] F. Q. A. Alyousuf, R. Din, and A. J. Qasim, "Analysis review on spatial and transform domain technique in digital steganography," *Bulletin of Electrical Engineering and Informatics,* vol. 9, no. 2, pp. 573-581, 2020, doi: 10.11591/eei.v9i2.2068.

[2] M. Umamaheswari, S. Sivasubramanian, and S. Pan-diarajan, "Analysis of Different Steganographic Algorithms for Secured Data Hiding," *International Journal of Computer Science and Network Security IJCSNS*, vol. 10, no. 8, pp. 154-160, 2010.

[3] R. Din and A. J. Qasim, "Steganography analysis techniques applied to audio and image files," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 4, pp. 1297-1302, 2019, doi: 10.11591/eei.v8i4.1626.

[4] C. Gong, J. Zhang, Y. Yang, X. Yi, X. Zhao, and Y. Ma, "Detecting fingerprints of audio steganography software," *Forensic Science International: Reports*, vol. 2, p. 100075, 2020, doi: 10.1016/j.fsir.2020.100075.

[5] E. W. Abood, W. A. Khudier, R. H. Jabber, and D. A. Abbas, "Securing Hill encrypted information With Audio steganography:a New Substitution Method," *Journal of Physics Conference Series*, vol. 1591, no. 012021, pp. 1-8, 2020, doi: 10.1088/1742-6596/1591/1/012021.

[6] S. M. H. Alwahbani and H. T. I. Elshoush, "Hybrid Audio Steganography and Cryptography Method Based on High Least Significant Bit (LSB) Layers and One-Time Pad-A Novel Approach," *Proceedings of SAI Intelligent Systems Conference. Intelligent Systems and Applications*, pp. 431-453, 2018, doi: 10.1007/978-3-319-69266-1_21.

[7] S. A. A. Ghani, R. D. Abdul-Wahhab and E. W. Abood, "Securing Text Messages Using Graph Theory and Steganography," *Baghdad Science Journal*, vol. 19, no. 1, pp. 189-196, 2021, doi: 10.21123/bsj.2022.19.1.0189.

[8] C. T. Jian, C. W. Chuah, N. Ab. Rahman, and I. R. A. Hamid, "Audio Steganography with Embedded Text," *IOP Conference Series Materials Science and Engineering*, vol. 226, no. 1, p. 012084, 2017, doi: 10.1088/1757-899X/226/1/012084.

[9] K. Thangadurai and G. S. Devi, "An analysis of LSB based image steganography techniques," *International Conference on Computer Communication and Informatics*, 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751.

[10] M. Pooyan and A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform," *IEEE International Symposium on Signal Processing and Information Technology*, 2007, pp. 600-603, doi: 10.1109/ISSPIT.2007.4458198.

[11] S. Jiang, D. Ye, J. Huang, Y. Shang, and Z. Zheng, "Smart Steganogaphy: Light-weight generative audio steganography model for smart embedding application," *Journal of Network and Computer Applications*, vol. 165, p. 102689, 2020, doi: 10.1016/j.jnca.2020.102689.

[12] J. Chaharlang, M. Mosleh, and S. R. Heikalabad, "A Novel Quantum Audio Steganography-Steganalysis Approach Using LSFQ-based Embedding and QKNN-based Classifier," *Circuits, Systems, and Signal Processing*, vol. 39, pp. 3925-3957, 2020, doi: 10.1007/s00034-020-01345-6.

[13] D. M. Ballesteros and J. M. Moreno, "Highly transparent steganography model of speech signals using Efficient Wavelet Masking," *Expert Systems with Applications*, vol. 39, no. 10, pp. 9141-9149, 2012, doi: 10.1016/j.eswa.2012.02.066.

[14] D. Yan, R. Wang, X. Yu, and J. Zhu, "Steganography for MP3 audio by exploiting the rule of window switching," *Computers & Security*, vol. 31, no. 5, pp. 704-716, 2012, doi: 10.1016/j.cose.2012.04.006.

[15] M. Tayel, A. Gamal and H. Shawky, "A proposed implementation method of an audio steganography technique," *18th International Conference on Advanced Communication Technology (ICACT)*, 2016, pp. 180-184, doi: 10.1109/ICACT.2016.7423320.

[16] S. P. Rajput, K. P. Adhiya and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio," *International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, 2017, pp. 1-6, doi: 10.1109/ICCUBEA.2017.8463948.
[17] F. A. Abdullatif, A. A. Abdullatif, and A. Al-Saffar, "Hiding Techniques for Dynamic Encryption Text based on Corner Point," *Journal of Physics Conference* Series, vol. 1003, no. 012027, pp. 1-10, 2018, doi: 10.1088/1742-6596/1003/1/012027. 2018.
[18] J. Hashim, A. Hameed, M. J. Abbas, M. Awais, H. A. Qazi and S. Abbas, "LSB Modification based Audio Steganography using Advanced Encryption Standard (AES-256) Technique," *12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 2018, pp. 1-6, doi: 10.1109/MACS.2018.8628458.
[19] M. Y. T. Irsan and S. C. Antoro, "Text Encryption Algorithm based on Chaotic Map," *Journal of Physics: Conference Series*, vol. 1341, no. 6, pp. 1-8, 2019, doi: 10.1088/1742-6596/1341/6/062023.
[20] J. Wu, B. Chen, W. Luo and Y. Fang, "Audio Steganography Based on Iterative Adversarial Attacks Against Convolutional Neural Networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2282-2294, 2020, doi: 10.1109/TIFS.2019.2963764.
[21] J. R. Jayapandiyan, C. Kavitha and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," *IEEE Access*, vol. 8, pp. 136537-136545, 2020, doi: 10.1109/ACCESS.2020.3009234.
[22] M. A. Al Sibahee *et al*., "Lightweight Secure Message Delivery for E2E S2S Communication in the IoT-Cloud System," *IEEE Access,* vol. 8, pp. 218331-218347, 2020, doi: 10.1109/ACCESS.2020.3041809.
[23] M. A. A. Sibahee *et al*., "Promising Bio-Authentication Scheme to Protect Documents for E2E S2S in IoT-Cloud," *IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2020, pp. 1-6, doi: 10.1109/ICSPCC50002.2020.9259519.
[24] H. K. Amal and Q. A. Iman, "A novel technique for speech encryption based on k-means clustering and quantum chaotic map," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 160-170, 2021, doi: 10.11591/eei.v10i1.2405.
[25] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, 2004, doi: 10.1109/TIP.2003.819861.
[26] F. J. Farsana, V. R. Devi, and K. G. Kuttapan, "An Audio Encryption Scheme Based on Fast Walsh Hadamard Transform and Mixed Chaotic Keystreams," *Applied Computing and Informatics*, 2019, doi: 10.1016/j.aci.2019.10.001.
[27] S. Katzenbeisser and F. A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking/Stefan Katzenbeisser," *EDPACS the EDP audit, control and security newsletter*, Boston, 2000, vol. 28, no. 6, pp. 1-2, doi: 10.1201/1079/43263.28.6.20001201/30373.5.
[28] S. Hemalatha, U. D. Acharya, and A. Renuka, "Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image," *Procedia Computer Science*, vol. 47, pp. 272-281, 2015, doi: 10.1016/j.procs.2015.03.207.

BIOGRAPHIES OF AUTHORS

Enas Wahab Abood received the bachelor's and master's degrees in computer science from Basrah University, Iraq, in 2005 and 2011, respectively. Her research interests include image processing, sound processing, encryption systems, similarity measures, NLP, graph theory. She has many articles in different aspects of computer science. She can be contacted at email: enas.abood@uobasrah.edu.iq

Abdulhssein M. Abdullah A professor in Computer and Information Technology Department: Computer Science, Basrah-Iraq. His research scopes are digital signal processing, natural languages, speech, and pattern recognition, and semantic web. He can be contacted at email: abduihussein.abdullah@uobasrah.edu.iq.

Mustafa A. Al Sibahee current position at college of big data and internet, Shenzhen Technology University, Shenzhen-China. Department of Computer Technology Engineering, Iraq University College, Basrah, Iraq. Received his, Ph.D. 2018, from Huazhong University of Science and Technology, Wuhan-China. From April-2019 to March-2021, was a postdoctor at Shenzhen Huazhong University of Science and Technology, Research Institute, Shenzhen-China. His research interests include computer networks and information security, internet of things and wireless sensor networks (WSNS). He can be contacted at email: mustafa@sztu.edu.cn.

Zaid Ameen Abduljabbar received the bachelor's and master's degrees in computer science from University of Basrah, Iraq, in 2002 and 2006, respectively, and the Ph.D. degree in computer engineering from the Department of Computer Science and Technology, Huazhong University of Science and Technology, China, in 2017. His research interests include cloud security, searchable encryption systems, similarity measures, Internet of Things, secure computation, biometric, and soft computing. He has published regular articles for more than 40 IEEE International Conferences and High-quality articles in SCI journals, and he holds 3 international patents and 2 International Computer Software Copyright. He has always served as a reviewer for several prestigious journals, and has served as the PC Chair/PC member for more than 25 international conferences. He has got the Best Paper Award that published in the 11th International Conference on Green, Pervasive, and Cloud Computing (GPC16), Xian, China, in May 2016. Also, he participated as a visiting scholar programme for international researchers to Huazhong University of Science and Technology and Shenzhen Institute in 2018 and 2019. He can be contacted at email: zaid.ameen@uobasrah.edu.iq.

Vincent Omollo Nyangaresi received his bachelors degree in telecommunication and information engineering in 2010 and a masters degree in information technology security and audit in 2018. His first doctorate degree is in information technology security and audit. He is currently pursuing his second doctorate degree in computer science. His research interests include machine learning, computer networks and security protocols, telecommunication engineering and systems modeling. He has published over 40 research articles in peer reviewed journals, conferences and symposiums. He can be contacted at email: vnyangaresi@tmuc.ac.ke.

Saad Ahmed Ali Kalafy degree in Computer Science from Basra University, Iraq, in 2001, and a Master's degree in Computer Engineering from the Department of Electrical and Computers, Kashan University, Iran, in 2018, and currently a PhD student at Tabriz University. His research interests include cloud security, searchable encryption systems, internet of things, secure computing, networking, and control algorithms. He can be contacted at email: Saad.Kalafy@gmail.com.

Mudhafar Jalil Jassim Ghrabta He received a Ph.D degree in Center for Biomedical Imaging and Bioinformatics, Huazhong University of Science and Technology, Wuhan, China. He received his master degree of information technology from SRM University, India, Chennai 2015, and got B.S. degree of computer science from Al Mustansiriyah University, Baghdad, Iraq, in 2005. His current research interests include artificial intelligence, machine learning, data mining and image processing. He is Program Committees Members for 23 International Conferences. His current teacher at Ashur university in Baghdad-Iraq. He can be contacted at email: mudhafar.jalil@au.edu.iq.