Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 3, June 2021, pp. 1777~1786
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i3.pp1777-1786

Securing audio transmission based on encoding and steganography

Enas Wahab Abood[1], Zaid Ameen Abduljabbar[2], Mustafa A. Al Sibahee[3], Mohammed Abdulridha Hussain[4], Zaid Alaa Hussien[5]
[1]Math Department, College of Science, University of Basrah, Basrah, Iraq
[2,4]Computer Science Department, College of Education for Pure Science, University of Basrah, Basrah, Iraq
[2-5]Neusoft Institute Guangdong, Guangdong, China
[2,3]Shenzhen Institute of Huazhong University of Science and Technology, Shenzhen, China
[2,4]Technical Computer Engineering Department, Al-Kunooze University College, Basra, Iraq
[3]Department of Communication Engineering, Iraq University College, Basrah, Iraq
[5]Information Technology Department, Management Technical College, Southern Technical University, Basrah, Iraq

Article Info

Article history:

Received Jan 23, 2021
Revised Mar 24, 2021
Accepted Mar 29, 2021

Keywords:

Audio steganography
DWT stego
LSB stego
Secure communication
Sound transformation

ABSTRACT

One of the things that must be considered when establishing a data exchange connection is to make that communication confidential and hide the file's features when the snoopers intercept it. In this work, transformation (encoding) and steganography techniques are invested to produce an efficient system to secure communication for an audio signal by producing an efficient method to transform the signal into a red–green–blue (RGB) image. Subsequently, this image is hidden in a cover audio file by using the least significant bit (LSB) method in the spatial and transform domains using discrete wavelet transform. The audio files of the message and the cover are in *.wav format. The experimental results showed the success of the transformation in concealing audio secret messages, as well the remarkability of the stego signal quality in both techniques. A peak signal-to-noise ratio peak signal-to-noise ratio (PSNR) scored (20-26) dB with wavelet and (81-112) dB with LSB for cover file size 4.96 MB and structural similarity index metric structural similarity index metric (SSIM) has been used to measure the signal quality which gave 1 with LSB while wavelet was (0.9-1), which is satisfactory in all experimented signals with low time consumption. This work also used these metrics to compare the implementation of LSB and WAV.

Corresponding Author:

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

1. INTRODUCTION

Information security is a science specialized in securing information that circulates over the Internet from the risks that threaten it. The security of these data and information has become an obsession and a vital topic along with the development of technology and the means of storing and exchanging information in different ways from one site to another across the network [1]. Information security is defined as the science that works to provide information protection from the risks that threaten it. It could be also defined as the barrier that prevents attacks on information by providing the tools and means necessary to protect the information from internal or external risks [2]. Standards and measures are taken to prevent information from reaching the hands of unauthorized persons through communications and to ensure the authenticity and

integrity of these communications. Encryption and steganography are two information security techniques. Encryption is the art of scrambling data to be unrecognizable and vague [3], [4]. Sometimes, the cryptographic methods used supplements such as steganography [5]. Steganography is the art of concealing a secret message with a cover; the message and the cover can be any type of files like a text, an image or an audio file. It is a protection that prevents suspicions of a confidential message presence. Only sender and receiver have a piece of knowledge about the embedded message [2], [6]. Audio files are considered the best media to be used as a cover because of their sensitivity, capacity, and widespread availability [6]. Audio steganography techniques may be categorized into three types. The first category refers to time-domain techniques, which hide messages in the least significant bit (LSB) of each audio file sample that contains the secret message binary bit sequences [7]. Although this audio steganography technique can hide large amounts of data, these data may be simply detected because of channel noise [8]. The second category is transform domain techniques that used hiding effects of the human auditory system by making the low frequencies near the high frequencies inaudible [9]. The third category is a wavelet domain method that uses discrete wavelet transform (DWT) to hide the messages in the LSBs of wavelet coefficients, to enhance the imperceptibility of the message; data should be hidden in hearing integer wavelet coefficients. Moreover, hiding data in silent parts of the audio signal must be avoided. Hiding data in the wavelet domain produced a high embedding rate, but the data extracted by the receiver may contain errors [8], [10]. There are some classic techniques for audio steganography like echo hiding technique, phase coding technique, and spread spectrum technique. Noticing that these techniques induced no noise in the cover audio file and that's why it considered more robust for Steganography achievement [6]. The main idea of converting an image into sound and vice versa revolves around the need to understand the image from another perspective. This helps people with sensory disabilities to perceive the environment and collect information about their surroundings [11].

In the frequency domain, the cover file is transformed to the frequency domains of fast Fourier transform (FFT), discrete cosine transform (DCT), or DWT to acquire the transformed coefficients. These coefficients are used for hiding secret messages. To retrieve the secret message, an inverse transform is applied to the cover coefficients to gain hidden data. There are many differences between time and frequency domain techniques, for example, the time domain is more effective with attacks than the latter because the sample values are modified [12]. Furthermore, the encoding operation could be utilized to change the appearance of data files from the image to audio, audio to text, or vice versa to create a new shape that is unrecognizable and more secured. Some of these operations include audio-to-image transform methods based on the DWT and the discrete fourier transform (DFT) of an audio signal, inverse fast fourier transform (IFFT), and inverse discrete fourier transform (IDFT), which are used to calculate the original audio signal [13]. These methods are mostly used with the application of vision that aids technology for the blind, for image recognition based on its sound patterns or the creation of an image or audio signature [13], [14]. This work proposed a new method to transform the audio into an image file with an red–green–blue (RGB) format in the time domain. Subsequently, the image is hidden within an audio file using two techniques, namely, the LSB technique in the time domain, and the substitution technique in the wavelet domain. Also, to show the efficiency of the proposed system in terms of securing data, a statistical analysis is used in this paper for testing the transformation method and comparisons between hiding using LSB and wavelet. This work contributes to finding an inexpensive way and simple to convert data from voice to image with the aim of preserving it and keeping it securely without consuming the network or computer resources in saving and transmission. That is, whatever the size of the resulting image (which was mostly less than the original size), it will be hidden inside a cover file and sent to the receiver where the size of the cover file will be kept. For this, the proposed method guaranteed the integrity and security of data with fewer efforts and computations.

The paper is structured as follows; section 1 includes an overview and definitions for the research subject, section 2 discusses a review of previous studies on transformation and steganography. The proposed system structure is described in section 3. Section 4 presents the experimental results and analysis. Finally, the conclusions and future works are shown in section 5.

2. RELATED WORKS

Several studies have been submitted to implement a high level of security to protect different kinds of data. Several systems, including those that rely on encryption by making data incomprehensible, the transformation to change data forms and hide information continue in developing. In this work, only transformation and steganography methods are merged to secure data.

2.1. Transformation studies 1

Peng *et al*. [15] proposed a method that transformed a digital audio signal by converting it into an image using virtual optical parameters. Their method depended on wave position and length, as well the

sensitivity of discrete fresnel diffraction (DFD). The basic idea was come from a space-variant Fresnel transform optical processor (SVFTOP) where the information sheet is an encoded sound map. The 1D audio wav was encoded as a 2D matrix as a 2D sound map (2SM) that would be stored as an information sheet represented an ordinary image [15]. Khan *et al*. [14] proposed an algorithm to recognize images based on their generated sound patterns blind people who are suffering from visual perception lacking. The algorithm generated an audio signature from an image with two phases. In the first phase, edge detection is processed in all directions (horizontal, vertical, and diagonal) using the Sobal operator. Then, the length and orientation of each edge are determined. In the second phase, three audible frequencies are generated on each edge direction (namely, horizontal, vertical, and diagonal), then played as a sound [14]. Ya-Nan used edge detection with canny operator and image segmentation to process images, the author then mapped the image to voice patterns. This could be used in the vOICe system by helping blinds in obtaining some information by training to hear these patterns of sound to recognize images [16]. Zhang *et al*. [13] proposed a novel image-sound conversion method that reduced the complexity of image-sound conversion computation. Their method takes DFT for each column of an image as an audio signal and IFFT is used to retrieve the audio signal. This method was effective and successful in real-time performance as a part of the vOICe technology for the blind.

2.2. Steganography studies

The principle of steganography appeared and continued to be developed as a mechanism for protecting the information of any type of files. Audio steganography is used to hide audio signals. The basic requirements of an audio steganography system are the imperceptibility of the secret message, the hiding capacity should be maximized, optionally, the hidden data preferred to be encrypted, and either or both the message and the cover file must be an audio signal [14]. Some researchers have considered the time domain of the audio file data as a good choice for hiding secret messages. Thus, the most common method was LSB that used by K. Gopalan who used LSB for embedding an audio message in a cover utterance file. The secret message was compressed and hidden in the samples of the cover utterance by altering one bit in each sample according to the data bits with a key, which was also used to retrieve the hidden bits at the receiver side [17]. Santosa and Bao [18] proposed an audio steganography approach based on DWT for audio-to-image conversion. In their approach, the host audio signal is transformed into an image and then hidden in an image, which is then transformed back into an audio signal [18]. In 2015, Sinha *et al*. [19] proposed the LSB method for concealing encrypted text messages. First, the text message was encrypted using a Vigenère cipher algorithm. Second, the text message was embedded into a cover of an audio file using the LSB method. To increase the security level, the audio file was manipulated with Blum Blum Shub pseudorandom number generator to transpose the places of the samples [19]. Naseri *et al*. [20] presented a new securing strategy based on watermarks for quantum images. They aimed to hide data using the LSB and the most significant bit (MSB). The authors simulate and test their system with peak signal-to-noise ratio (PSNR) calculation to ensure its security and applicability compared with the previous studies found in that period [20].

In the frequency domain, Viswanathan [21] produced a model for hiding a text message in audio files in frequency domain format (FFT). The message was hidden in the FFT high coefficients as watermark information. This method could prevent tampering and resisting malicious attacks whilst retaining the hidden message with no distortions [21]. Wang introduced a quantum representation called QRDA of digital audio. The representation used two entangled qubit sequences to store the information of amplitude and time information that belongs to a digital audio signal that has a single-channel [22]. Chaharlang *et al*. [23] presented a steganography–steganalysis system for audio signals. This system consists of two main components, steganography, and steganalysis. In steganography, the cover audio signal was divided into quantum frames with a specific length, and the embedding data are spread in the least significant fractional qubit of the amplitude of selected samples in each frame. The selection operation depended on the triangular number sequence. The steganalysis component produced a steganalyzer that was used to detect the embedding operations. These operations were performed by steganography component and a feature extraction scheme to calculate the power feature of quantum audio signal frames. This quantum model was simulated and tested many times with different wave files [23]. Abdulrazzaq *et al.* [24] studied a method that included compression–encryption of an image in an audio file. The image file was compressed by the GMPR technique that used the discrete cosine transform and high-frequency minimization encoding scheme. The steganography technique was used for hiding a compressed image in an audio file of standard "*.wav" format because of its high capacity as a carrier medium. The hiding algorithm was based on the LSB technique in a variable and multiple LSB layers [23].

Previous methods are characterized by the presence of relative immunity against most of the attacks. Amongst the problems that exist in the literature, the security problem of the encryption key or accuracy in retrieving data, and the time consumption and complexity of calculations. In this paper, a simplified and

efficient method is presented to convert files into another type to protect them from snoopers. The method converts the audio file into an image then hides it within another audio file with two methods and produces a comparison between them. The conversion method preserves the accuracy and size when converting, increasing storage efficiency after merging, and concealing them with another file. This is to take the size of one file instead of two files.

3. PROPOSED SYSTEM

The proposed system consists of two phases: transformation and steganography where the message and cover files were audio file format. In the transformation stage, the audio message is converted into an RGB-image file, and then it is hidden in an audio cover file in the steganography phase. There are two techniques for this phase one in the time domain and the other in the frequency domain.

3.1. Transformation phase

The secret audio file is transformed into an image with RGB format by using some formulas to transform every single sample of the audio file into a sample of an image (pixel) (i.e. transformed a value in the range [−1, 1] to three numbers in the range [0.255] as an image pixel. The introduced algorithm is given in algorithm 1.

Algorithm -1: the proposed transformation method

1. Initially create a Matrix for empty image with dimension n×n×3, where n=√M , M is the length of audio file
I_RGB (1: n, 1: n, 1: 3) = zeros
2. For each sample Ai in audio file is manipulated with these formulas:
I_R=integer part (Ai*256)
I_G=integer part(fraction part (Ai) *256)

$$I\_B = \begin{cases} 255 & , \quad A \geq 0 \\ 0 & , \quad A_i < 0_i \end{cases}$$

These variables represent a pixel in RGB image I_RGB.
3. i=i+1
4. Goto 2
5. End

The operation of multiplication with 256 is to get the nearest integer number in the range [0.255] which is desirable for format uint8 that represents the image format.

ex1: A = 0.95672
I_R=244
I_G=235
I_B= 1 i.e. the pixel is [244, 235, 1]
ex2: A= -0.52372
I_R=134
I_G=18
I_B= 0 i.e. the pixel is [134, 18, 0]

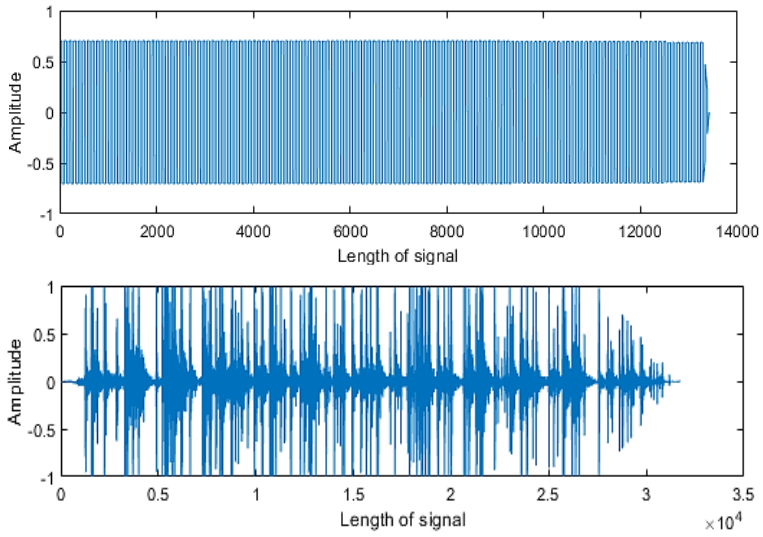
After the transformation is completed, the resulting image I_RGB is stored as an image of *.TIFF format to still retain all details of the original information. Then, it will be hidden in an audio cover file. On the receiver side, the transformation process is reversed by using a division operation to return the value of the secret sample as follows:

$$x = sgn * ((I\_R + (I\_G/256))/256) \quad (1)$$

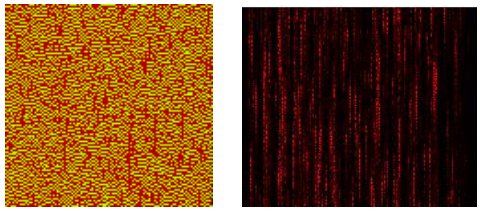
where sgn is either +1 or −1 based on the value of I_B, that is, if it is 0 or 255, respectively. Figure 1 shows the audio file before and after transformation.

3.2. Steganography phase

The cover audio file is a "* .wav" format which is consisting of many samples in each duration (frame) and that makes it suitable for hiding big data. The LSB and DWT methods are implemented to hide data according to the cover file domain (time and frequency), as well as producing a comparison between these methods to show their efficiency in hiding.



(a)



(b)

Figure 1. Audio file VS its image: "beep.wav" and "applause_y.wav":
(a) before transformation and (b) after transformation

3.2.1. LSB method

The audio signal is analog. Therefore, to use the signal digitally in computers, the analog signal is sampled periodically in time to transform it into a sequence of samples using a digital converter [23]. Each sample represents the high capacity of the signal in the given time unit. In the LSB method, the samples of the cover audio file and the pixel of the secret image are transformed into binary, the LSB of the cover sample will be replaced with one bit from the message`s bits as shown in Figure 2.

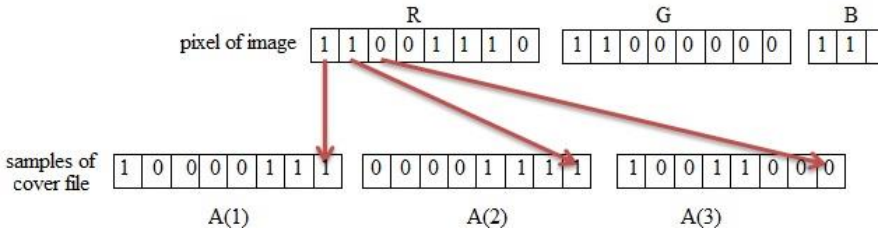


Figure 2. Replacement of message bits with cover message bits

In this phase, the secret bits were distributed randomly in the cover file to increase the imperceptibility of a steganography system by reducing the degree of distortion in the cover file and by making it difficult to track down the hidden data. The generation of a random position is performed with a seed number. It is chosen depending on the number of image bits to obtain a series of random numbers used as locations for hiding bits. To generate these locations, we applied MATLAB function "randi". For retrieving the data again, the bits are collected and reconstructed to form the original file that represented a secret image.

3.2.2. DWT method

In this method, the cover file and the encoded message are converted into the DWT. The cover conversion is done in three levels as presented in Figures 3 (a) and (b). Subsequently, random locations are selected similarly as in the LSB method. This selection is to distribute image wavelet coefficients in the cover file. Then, the audio file is reconstructed again using inverse transformation and sent the resulted sound file to the recipient. At the recipient side, a DWT transform is applied again, and the coefficients of the secret image are extracted, manipulated with inverse transform, and the secret image is retrieved successfully.

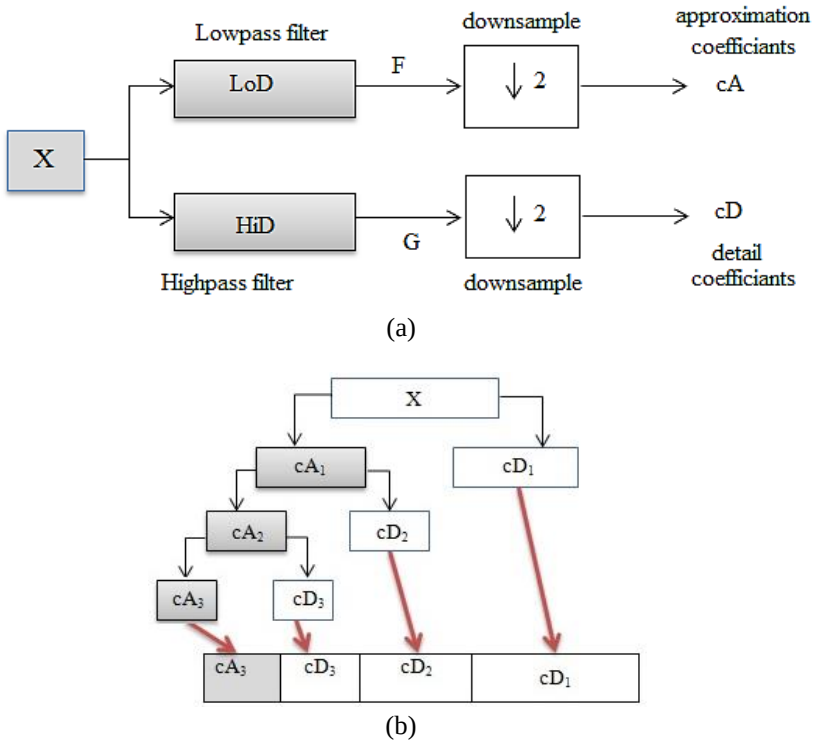


Figure 3. Shows signal multi-level decomposition diagram (DWT): (a) decomposition of signal X with the low pass filter Lo_D and the high pass filter Hi_D to yield the approximation and detail coefficients for one level and (b) level-3 decomposition of signal X

4. EXPERIMENTAL RESULTS AND ANALYSIS

The system is implemented with MATLAB2018 on Intel® Core i7-3520M CPU 2.90 GHz 8.00 GB Ram of memory. The results are tested against varying sized audio secret files from 26 KB–4.5 MB with a cover audio file of 4.9MB. Recall that the transformation process was transforming the audio into a RGB image, and then embedded it in a cover with two stego methods, which are; LSB and DWT. Both methods have their characteristics and disadvantages that will be discussed in terms of statistical analysis methods.

4.1. Characteristics of transformation

The audio secret file is transformed into an RGB image with format *.TIFF. Hence, the entire file format is changed to be a new completely different file from the original one. If snoopers and attackers can extract the file from the cover one, then they will have an incomprehensible image as meaningless data. On the other hand, if the snoopers extract the bits, group them into sound, and listen to them, then it won't be apparent because of the random scattering of the values. For this, the only authorized user who knows the conversion algorithm and distribution key can extract the data and recover the audio file from the cached image [24]. The type * .tiff is used to store the image that resulted from converting the audio file because it preserves all the values of the image without compression, thereby making it suitable to retain all the details of the original file. Moreover, despite its large size compared to the rest of the image types, the image file is slightly less than the original audio file when converting. The conversion time is variable according to the file size as shown in Table 1.

Table 1. Collapsed time and size for various audio file

Size of message	Size after transformation	transformation time(s)
26 KB	11 KB	0.01
50 KB	48 KB	0.05
94 KB	90 KB	0.07
253 KB	267 KB	0.12
4.96 MB	2.53 MB	0.39

4.2. Characteristics of steganography

4.2.1. Peak dignal to noise ratio (PSNR)

PSNR is used to calculate the noise ratio for the cover file before and after hiding to expose visual distortion after hiding [25]. PSNR is computed with the (2):

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

where M is the biggest value of the x samples. mean square error (MSE) is the between, y. Where x represents the original audio file and y is stego file is given by:

$$\mathrm{MSE} = \frac{\sum_{i=1}^{M}\|x(i)-y(j)\|^2}{M} \quad (3)$$

4.2.2. Structural similarity index metric (SSIM)

SSIM is a quality metric used with images. It is better than traditional measures, such as MSE and PSNR. SSIM considers image degradation as a change in structural information. Its work is based on the idea that spatially close image pixels have strong interdependencies. For this, any subtle change could be measured using this metric. The SSIM is calculated between the encrypted secret image and the retrieved image at the recipient side as given below:

$$\mathrm{SSIM} = \frac{(2\underline{x}\,\underline{y}+c_1)(2\sigma_{xy}+c_2)}{(\sigma_x{}^2+\sigma_y{}^2+c_2)(\underline{x}^{\,2}+\underline{y}^2+c_1)} \quad (4)$$

where $c1 = (k1L)^2$, and $c2 = (k2L)^2$ are both constant to avoid null dominator. L is the high range of the pixel values, which is 255. k1 and k2 have default values of 0.01 and 0.03, respectively. The identical sound score value is 1, which decreases to −1 as sounds change [26]. The statistical analysis results showed good quality for signal hiding as in Table 2.

Table 2. Statistical analysis values for PSNR, MSE, SSIM, and time consumption for applying LSB and DWT stego methods

	With LSB				With DWT			
Size of message	PSNR	MSE	SSIM	Time(s)	PSNR	MSE	SSIM	Time(s)
26 KB	112.07	6.1985e-12	1	6.9	26.47	0.0023	0.9999	0.35
50 KB	84.1311	3.872e-09	1	12.8	24.23	0.0037	1.0	0.4
94 KB	84.1330	3.861e-09	1	15.1	24.011	0.004	0.9999	0.41
253 KB	81.121	7.7232e-09	1	22.9	20.53	0.0089	1	1.15
4.96 MB	81.122	7.7226e-09	1	43.9	20.19	0.0096	0.9997	1.2

The results showed that these techniques are robust and capable of withstanding the attacks. Table 2 contains the statistical results of hiding different-sized audio messages within a cover file of size 4.69 MB. The time consumption for the two methods is obviously different, and the time of DWT is lower than that of LSB, indicating that the former is better with online systems and smart devices than the latter. The average PSNR values for both methods were above 20 dB as shown in Table 2. This level is recommended by the international federation of the phonographic industry (IFPI) [12], [27]. The size of the secret files was between (26 KB-4 MB) which were hidden in a cover audio file of size 4.96 MB and all were with one channel with a sample rate ranged between (11200- 48000). However, it is very clear that the LSB method scored a better range (81–112 dB) in PSNR than DWT, which also obtained an acceptable score (20–26 dB) (this means less noise in the cover file).

In SSIM, The LSB method has a better similarity index for the retrieved image because its score value for all hidden files is 1 as given in Table 2, which indicates its effectiveness in maintaining the integrity of the transmitted data. DWT has recorded rates between 0.9 and 1, which is a very little difference.

Nevertheless, the use of this method in audio files is good because it is not greatly affected by such a subtle change. Figure 4 shows an audio message that was hidden in a cover audio file.

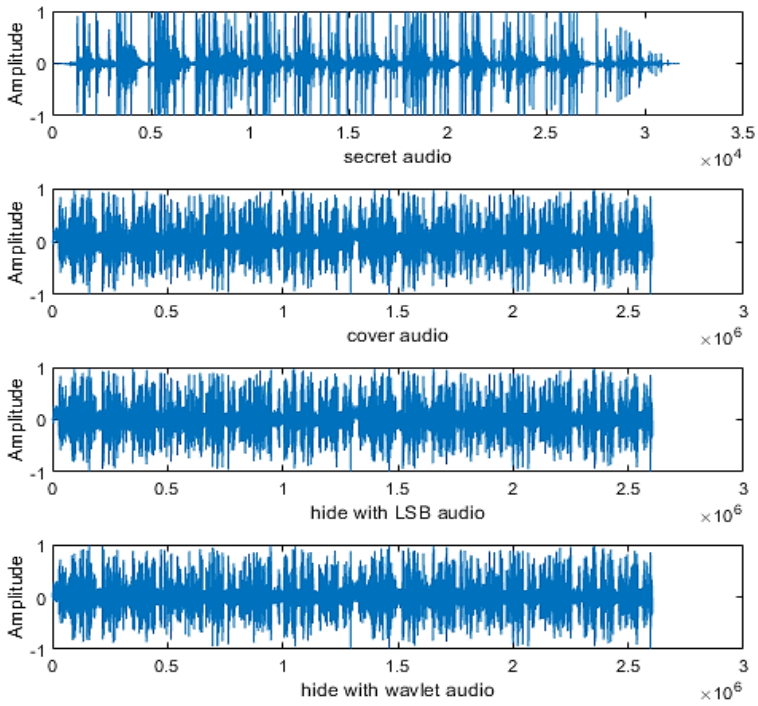


Figure 4. The secret audio and cover audio after hiding with LSB and DWT

5. CONCLUSION

A new and secured transformation method is proposed in this work. This transformation is changing the type of a secret message from audio into image format with type *.Tiff that keeps all its details and values. The introduced method enables robustness for sending an audio message securely with a size less than the original audio file and in meaningless form. Moreover, to get more security two high and secured capacity audio steganography methods were performed, namely; LSB and DWT. These methods achieved good scores for PSNR, MSE, and SSIM metrics, thereby proving its efficiency in sending audio files without exposing its existence. The two methods were compared to show which one is the best in hiding and show the differences between the stego methods studied in this paper. Besides, the system's performance against some attacks is discussed. The experimental results reflected that the secret audio is extracted and reconstructed without any distortion in mostly all tested audio files, especially with LSB stego. For further work, we suggest investing strong mathematical operations in analyzing and representing data for producing a new method of security.

REFERENCES

[1] B. V. Varun, A. M.V., A. C. Gangadhar, and P. U., "Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices," *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 2019, pp. 1391-1395, doi: 10.1109/ICCT46805.2019.8947111.

[2] 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.

[3] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018, pp. 1-9, doi: 10.1109/ICOEI.2018.8553910.

[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, 2020, doi: 10.1016/j.fsir.2020.100075.

[5] W. Sun, R. Shen, F. Yu, and Z. Lu, "Data Hiding in Audio Based on Audio-to-Image Wavelet Transform and Vector Quantization," *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2012, pp. 313-316, doi: 10.1109/IIH-MSP.2012.82.

[6] R. Mishra and P. Bhanodiya, "A review on steganography and cryptography," *2015 International Conference on Advances in Computer Engineering and Applications*, 2015, pp. 119-122, doi: 10.1109/ICACEA.2015.7164679.
[7] P. P. Balgurgi and S. K. Jagtap, "Audio steganography used for secure data transmission," *Proceedings of International Conference on Advances in Computing*, 2013, pp. 699-706, doi: 10.1007/978-81-322-0740-5_83.
[8] S. Jiang, D. Ye, J. Huang, Y. Shang, and Z. Zheng, "SmartSteganogaphy: Light-weight generative audio steganography model for smart embedding application," *Journal of Network and Computer Applications*, vol. 165, 2020, doi: 10.1016/j.jnca.2020.102689.
[9] 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*, 2016, pp.431-453, doi: 10.1007/978-3-319-69266-1_21.
[10] F. Djebbar, B. Ayad, H. Hamam, and K. Abed-Meraim, "A view on latest audio steganography techniques," *2011 International Conference on Innovations in Information Technology*, 2011, pp. 409-414, doi: 10.1109/INNOVATIONS.2011.5893859.
[11] A. Cazan, R. Varbanescu and D. Popescu, "Algorithms and Techniques for Image to Sound Conversion for Helping the Visually Impaired People - Application Proposal," *2007 14th International Workshop on Systems, Signals and Image Processing and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services*, 2007, pp. 471-474, doi: 10.1109/IWSSIP.2007.4381143.
[12] 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.
[13] X. Zhang, J.Wang, X. Duan, and Y. Sun, "An Efficient Method of Image-Sound Conversion Based on IFFT for Vision Aid for the Blind," *Lecture Notes on Software Engineering*, vol. 2, no. 1, pp: 54-57, 2014, doi: 10.7763/LNSE.2014.V2.94.
[14] Z. Khan, S. Singh, and G. Agarwal, "Image Recognition by Sound Pattern Generated by the Image," *International Journal of Computer Applications*, vol. 7, no. 12, pp. 10-14, Oct. 2010, doi: 10.5120/1301-1609.
[15] X. Peng, Z. Cui, L. Cai, and L. Yu, "Digital audio signal encryption with a virtual optics scheme," *Optik-International Journal for Light and Electron Optics*, vol. 114, no. 2, pp. 69-75, 2003, doi: 10.1078/0030-4026-00224.
[16] Y. Tian, "A Vision Substitution Method for the Blind Based on Image Edge Detection and Sound Mapping," *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*, 2011, pp. 209-212, doi: 10.1109/CICSyN.2011.53.
[17] K. Gopalan, "Audio steganography using bit modification," *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03)*, 2003, pp. II-421, doi: 10.1109/ICASSP.2003.1202390.
[18] R. A. Santosa and P. Bao, "Audio-to-image wavelet transform based audio steganography," *47th International Symposium ELMAR*, 2005, pp. 209-212, doi: 10.1109/ELMAR.2005.193679.
[19] N. Sinha, A. Bhowmick, and B. kishore, "Encrypted information hiding using audio steganography and audio cryptography*," Int J Comput Appl*, vol. 112, no. 5, pp. 49-53, 2015, doi: 10.5120/19666-1387.
[20] M. Naseri, *et al.*, "A new secure quantum watermarking scheme," *Optik*, vol. 139, pp. 77-86, 2017, doi: 10.1016/j.ijleo.2017.03.091.
[21] V. Viswanathan, "Information hiding in wave files through frequency domain," *Applied Mathematics and Computation*, vol. 201, no. 1-2, pp: 121-127, 2008, doi.org/10.1016/j.amc.2007.12.003.
[22] J. Wang, "QRDA: quantum representation of digital audio," *Int. J. Theor. Phys*, vol. 55, no. 3, pp. 1622-1641, 2016, doi: 10.1007/s10773-015-2800-2.
[23] J. Chaharlang, M. Mosleh, and S. R. Heikalabad, "A Novel Quantum Audio Steganography–Steganalysis Approach Using LSFQ-Based Embedding and QKNN-Based Classifier," *Circuits Syst Signal Process*, vol. 39, pp. 3925-3957, 2020, doi: 10.1007/s00034-020-01345-6.
[24] S. T. Abdulrazzaq, M. M. Siddeq, and M. A. Rodrigues, "A Novel Steganography Approach for Audio Files," *SN Computer Science*, vol. 1, no. 2, pp. 1-13, 2020, doi: 10.1007/s42979-020-0080-2.
[25] M. A. Al Sibahee, *et al*., "Lightweight Secure Message Delivery for E2E S2S Communication in the IoT-Cloud System," in *IEEE Access*, vol. 8, pp. 218331-218347, 2020, doi: 10.1109/ACCESS.2020.3041809.
[26] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multiscale structural similarity for image quality assessment," *The Thrity-Seventh Asilomar Conference on Signals, Systems &* Computers, vol. 2, pp. 1398-1402, 2003, doi: 10.1109/ACSSC.2003.1292216.
[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 in Artech House*, vol. 28, no. 2, pp. 1-2, 2000, doi: 10.1201/1079/43263.28.6.20001201/30373.5.

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.

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.

Mustafa A. Al Sibahee received the Bhd. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2018. He is currently a Researcher with the Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China. He is also a Lecturer with the Department of Communication Engineering, Iraq University College, Basrah, Iraq. His research interests include computer networks and information security, computer network measurements, machine learning algorithms applications, wireless sensor networks (WSN), software dened networking (SDN), embedded systems, and cyber physical systems (CPS).

Mohammed Abdulridha Hussain received the bachelor's degree from the Department of Computer Engineering, College of Engineering, University of Basrah, Basrah, Iraq, in 2004, the master's degree in computer science and engineering from the School of Information Technology, Guru Gobind Singh Indraprastha University, Delhi, India, in 2009, 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. He is currently a Lecturer with the Department of Computer Science, College of Education for Pure Science, University of Basrah. His research interests include network security, data security, cloud security, and networking.

Zaid Alaa Hussien received the B.Sc. degree in computer engineering from the University of Basrah, Iraq, in 2004, the M.Tech. degree in computer science and engineering from Guru Gobind Singh Indraprastha University, India, in 2009, and the Ph.D. degree in computer engineering from Department of Computer Science and Technology, Huazhong University of Science and Technology, China, in 2017. He is currently working as the Head of the Information Technology Department, Management Technical College, Southern Technical University, Iraq. His research interests include cloud security, searchable encryption systems, authentication and integration data in cloud, the Internet of Things, and network security. He is a Reviewer of several journals and international conferences.