







## An Enhanced Steganography Approach for Concealing Audio in Images Using Double Density-Dual Tree Wavelet Transform

Salwa A. AbdAl-Hameed<sup>1</sup>, Hadeel N. Abdullah<sup>1\*</sup>, Najat H. Khalif<sup>1</sup>, Jaafar M. Alghazo<sup>2</sup>

<sup>1</sup> Department of Electrical Engineering, University of Technology, Baghdad 10066, Iraq

<sup>2</sup> Artificial Intelligence Research Initiative, College of Engineering and Mines, University of North Dakota, Grand Forks 58201, ND, USA

Corresponding Author Email: [hadeel.n.abdullah@uotechnology.edu.iq](mailto:hadeel.n.abdullah@uotechnology.edu.iq)

<https://doi.org/10.18280/ria.370516>

### ABSTRACT

**Received:** 14 June 2023

**Revised:** 22 July 2023

**Accepted:** 29 July 2023

**Available online:** 31 October 2023

#### Keywords:

*double density-dual tree wavelet transform, image steganography, secret audio, structural similarity index metric (SSIM), least significant bit*

Steganography, the art of concealing information within another message or physical object to evade detection, has potential applications across multiple digital content types, including text, photos, videos, and audio. The hidden data size significantly influences the difficulty of detection. Conversely, the data amount that can be concealed within an image is largely dependent on the cover image dimensions, a concept often overlooked by steganographers. Despite numerous attempts to improve embedding capacity, the quality of generated stego-images remains subpar, and embedding capacity continues to be restricted by the cover image size. This study introduces an image steganography approach, leveraging double density dual tree wavelet transform (DDDT-DWT), designed to enhance capacity while preserving optimal quality. The performances of discrete wavelet transform (DWT), double density DWT (DD-DWT), and double density dual tree DWT (DDDT-DWT) are implemented, evaluated, and comparatively assessed. Key performance parameters, such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE), are calculated, guiding the selection of the most efficient methodology. The stego-image quality is also measured using the Structural Similarity Index Metric (SSIM). Experimental results indicate that the proposed DDDT-DWT-based method yields superior imperceptibility for the stego image, with a PSNR of 47.8582 and an SSIM of 0.9945. This advancement in steganography presents opportunities for increasingly undetectable and efficient data concealment.

## 1. INTRODUCTION

The communication of secret messages has been around for thousands of years. The main concept of sending secret messages is to send a message where only the sender (transmitter) and receiver can understand the message. With the invention of electronic maSteganographyoncepts of cryptography, steganography, watermarking, and others came to light to conceal the information being transmitted and make it hard for any unauthorized person to detect and understand the hidden messages. In today's connected world, with information being exchanged through the Internet of Things (IoT) over the cloud, the demand for greater security Steganographyng, and the importance of steganography is increasing [1]. Private personal information is used and available in electronic format in many sectors, including banking, health, security, border control, etc. In every sector today, private personal information is sent via Wi-Fi, the internet, the cloud, and other transmission mediums. While in transmission, this data is always susceptible to being accessed by unauthorized persons through hacking attacks. Thus the importance of information security, network security, and cybersecurity is on the top priority list for companies, institutions, governments, and others [2].

The most trending techniques for steganography are watermarking and steganography. Invisible steganography can

be achieved through steganography. Steganography hides the secret messages in other digital media formats known as carriers, cover, innocent, or host. Examples of carriers can be video, audio, image, and text files. Information (Secret messages) is hidden in other information (carriers), which makes the secret message hard to detect. Steganography as a word roots back to its original Greek words "Stegos"="Steganographygrafia"="writing"; thus, steganography is "covered writing". Throughout the paper, carrier files will be referred to as "cover", an embedded secret message will be referred to as "payload," and carrier after the message is embedded in it will be referred to as stego-filetype, i.e., stego-image. The statistical properties of the cover must show no signification variation after the secret message is hidden in it to ensure that the message is concealed. Thus, a stego-file type which is the cover file after embedding the payload into it displays similar statistical properties as the cover-filetype used as a carrier. Only the intended recipient should be able to retrieve the secret message. Least significant bit (LSB) alteration steganography is a widespread technique for steganography [3].

Watermarking hides information (watermark) into other media formats, usually as a measure to protect copyright, and can be visible or invisible. Cryptography is yet another method for concealing secret messages through the use of codes so that only the intended recipient with knowledge of the code can be

able to decrypt and read the message. Recent trends in steganography hiding combines both steganography and cryptography. Durability, capacity, and transparency are the performance metrics of data-hiding algorithms.

Hiding audio into steganography referred to as audio steganography, is a research area still being explored in information security. Hiding images or messages in other images is referred to as image steganography. The steganographic techniques utilize either the spatial domain or the transform domain [4].

In order to hide audio signals in an image, this research suggests a new method of steganography based on dual tree-double density discrete wavelet transform. Audio can be in any format, such as .wav, .mp3, etc., and images can be in any format, such as .jpg, .bmp, etc. The cover image must be significant because audio files may have many samples, even for brief periods. Different types of discrete wavelet transform is used to boost the hiding capacity. This work's primary characteristics are:

- Aims to offer an appropriate, effective way to securely send audio file to its destination while hiding it from hackers.
- The suggested system is appropriate for all audio file formats and won't modify the file size even after encoding.

The rest of the paper is organized as follows: Section 2 details steganography techniques in recent literature, and Section 3 details the proposed method. Section 4 details the proposed algorithms, Section 5 shows the results obtained through the proposed methods and analysis, Section 6 concludes and future work, and Section 8 lists all references used.

## 2. RELATED WORK

Rahman et al. [5] reviewed the steganographic methods, including but not limited to the spatial and transform domain embedding methods. The various algorithms for extracting and embedding processes in steganographic systems were reviewed in the work. Steganography is divided into technical and non-technical categories in the study [6], as well as categories based on the subject matter. Steganography problems include payload capacity, mean square error, structural similarity (SSIM), image fidelity (IF), normalized cross-correlation (NCC), robustness, and quality of stego pictures. Chawla and Shukla [7] proposed a scheme for hiding big images into small ones but used Matrix Rotation to scramble the secret image. DWT and Alpha blending are performed on both images. IDWT is then applied to obtain the stego image. Their results indicated a highly secure steganography method with good perceptual visibility, this method can reduce noise in stego images for data concealing without compromising the quality of the cover image. Avci et al. [8] proposed a method for hiding audio data. They proposed the use of DWT to obtain high pass filter coefficients. They then applied the Least Significant Bit (LSB) method to the obtained coefficients. The measurement of the transparency and capacity showed improved results. Least Significant Bit has the drawback of being completely insecure and open to steganalysis. Gharavi and Rajaei [9] proposed a steganographic method that used features from the curvelet transform for the hiding process and was tested for security and robustness using benchmarks. The method was also found to tolerate online robustness attacks. The issues with image steganography utilizing Wavelets and DCT are effectively

addressed by the curvelet transform, but the curvelet transform has a larger computational cost than the wavelet transform. Aiswarya et al. [10] propose a technique to hide an audio signal in Discrete Wavelet Domain of a cover image. The visual difference between the cover image and the stego-image is reported as null. PSNR and MSE measured which show good results. Liao et al. [11] present a new steganography method based on extremum features and twice DWT (Twi-DWT). The second-order difference is used to extract the extremum sequence of the secret message as well as the covert information. The cover signal is decomposed using Twi-DWT to extract the security sequence. The covert information then replaces the security sequence. The achieved stego-audio signal is similar to the original host audio meaning transparency was achieved. Their method was reported to be superior both in embedding capacity and robustness compared with similar methods. Latha et al. [12] proposed using wavelet transform to embed the secret message in the cover image while utilizing the chaotic map to encrypt the secret message prior to embedding it in the cover image for added security. The authors claim the secret message will become very secure due to the chaotic map encryption technique. Tabares-Soto et al. [13] present steganalysis algorithms for detecting whether an image, audio, or video file contains any hidden message through the process of steganographic methods. It is indicated that Cover media, whether audio, image, or video, has different spSteganography that are altered when steganography is performed.

Aslantaş and Hanilçi [14] critically review the steganalysis methods available for detecting alterations in the characteristics of audio and image stego-media against the corresponding original cover media and then to understand the process of hiding information in audio and image media and how to detect it. AlSabhany et al. [15] present a review paper on various steganography methods using the LSB and DWT algorithms. The LSB and DWT-based methods are compared in this paper as well. Its weaknesses include a lack of robustness, susceptibility to noise, scaling, and cropping, and these limitations. Abood et al. [16] present Steganography techniques used for audio steganography. The paper also presented the standards for embedding secret information in audio signals using various audio steganography methods. The authors outline the current Steganography and capacities for audio steganography as well. Despite their ease of use and large payload, they have poor security and imperceptibility. As a result, numerous methods for audio steganography have been created to maximize capacity while boosting visual quality and security. Sun et al. [17] propose a new method for concealing information in digital audio using vector quantization (VQ) and audio-to-image wavelet transform (A2IWT). Their approach consisted of converting the audio cover into an image using wavelet transform and resampling the coefficients. VQ is used to embed the secret data in the image. The complete stego-image is converted back to audio to form the stego-signal. They reported that results indicated their method was both efficient and effective. Alghazo [18] proposes a watermarking-based method to embed secret data in images. For electronic health records (EHRs) applications in a cloud environment. Private patient data is embedded in biomedical images and transmitted in the cloud environment. Quality and impeccability analysis is performed to show the technique's robustness and PSNR analysis. The watermark-based technique was largely impervious to simulated repeated attacks. Hema and Shyry [19] proposed a technique for

steganography with cover images of human skin tone regions. For added security, the authors utilize the Lagrange interpolation encryption. The skin tone regions are for chosen can be used as cover images. The image pixels belonging to the skin region are used to embed the secret message horizontally and vertically. Vector Discrete Wavelet Transform (VDWT) is used for hiding the message. Despite being a potent signal and image processing tool, the discrete wavelet transform (DWT) has three significant drawbacks: shift sensitivity, subpar directionality, and a lack of phase information.

Analysis of the aforementioned studies reveals numerous shortcomings, including decreased imperceptibility and inadequate security against steganalysis methods. This paper proposes a novel mathematical model based on DDDT\_DWT coefficients. Here, rather than using a restricted number of sub-images as in other similar transform domains, the image is changed to several sub-band coefficient matrices, which offers more housing to hide the secret bits.

### 3. PROPOSED METHODOLOGY

#### 3.1 Double-density DWT

The selection of which transform to apply is influenced by many variables, but the complexity of computation and coding efficiency stand out. The quantity of multiplications and additions necessary for the transform's implementation is used to gauge computational complexity. The signal energy's compression level into a limited number of coefficients is known as coding gain [20].

The relatively new field of Double Density DWT (DD\_DWT) shows promise in removing some of the limitations of wavelets. DD\_DWT offers more design options and hence can combine all desirable transform features. Discrete-time signals are subjected to the DD\_DWT using the oversampled analysis and the synthesis filter bank. Three analysis filters make up the analysis filter bank:  $h_0(n)$  stands for the low pass filter,  $h_1(n)$  and  $h_2(n)$  for the high pass filters. As the input signal  $X(N, N)$  travels through the system, the analysis filter bank decomposes it into three subbands, each down-sampled by 2. It is implemented as 1-D row transform followed by a 1-D column transform on the data obtained from the row transform. A 2-D separable transform is equivalent to two 1-D transforms in series. Figure 1 shows the filter bank structure for the computation of a two-dimensional DD\_DWT [21].

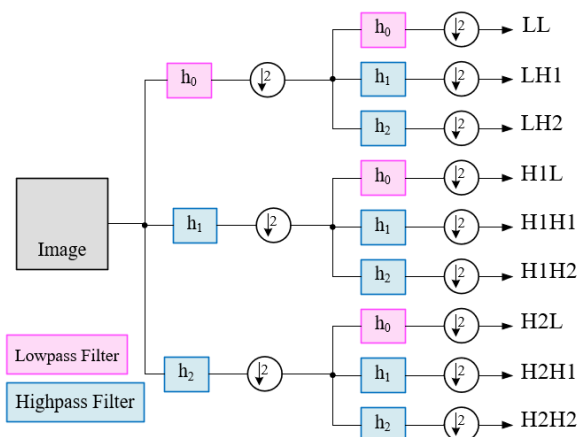


Figure 1. Filterbank structure for the double-density DWT

#### 3.2 Double density-dual tree wavelet transform

The fundamental DWT and its extensions DD\_DWT have at least two significant shortcomings. They are (i) a lack of shift-invariance, which causes the energy distribution between DWT coefficients at various scales to significantly vary even with small shifts in the input signal, and (ii) a poor directional selectivity for diagonal features due to the wavelet filters being separable and real. Using the undecimated form of the dyadic filter tree is an established means of offering shift invariance. Nevertheless, it still has far higher computation needs than the fully decimated DWT, and the output information also has large redundancy, making further processing expensive. Dual-Tree Discrete Wavelet Transform (DT-DWT) is a shift invariance method that is more computationally effective. When filtering multidimensional signals, the DT-DWT also provides substantially superior directional selectivity. In conclusion, it possesses the following characteristics: (i) Approximate shift invariance; (ii) Good directional selectivity in two dimensions; and (iii) perfect reconstruction (PR) employing short linear-phase filters.

The dual-tree DWT and the double-density DWT offer different qualities and benefits. The double-density complex, also known as the double-density dual-tree DWT (DDDT\_DWT), was created by combining the two transforms. By doing this, we are then a Wavelet use the double-density complex wavelet transform Waveletlement complex and directional wavelet transform [22].

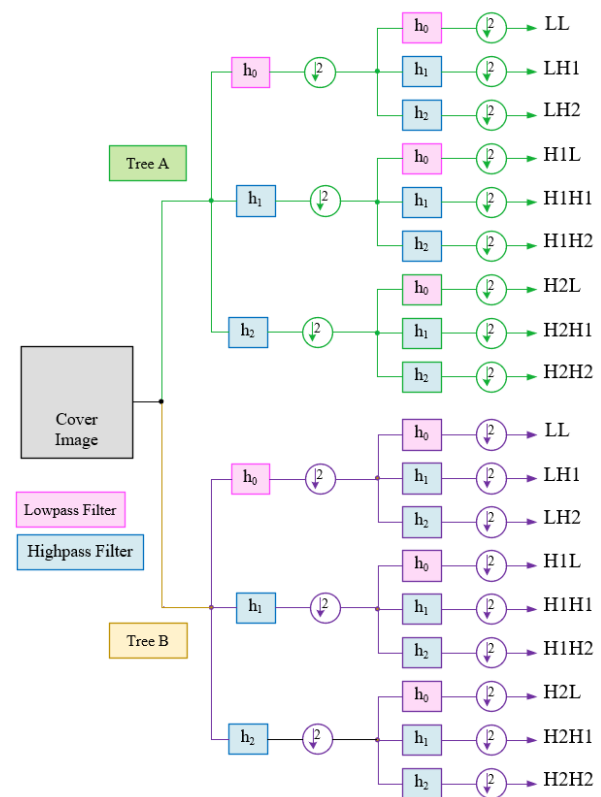


Figure 2. Filterbank structure for the double-density dual tree DWT

To implement the DDDT\_DWT, we must first design an appropriate filter bank. We have already seen in the previous sections what sort of filter bank structure the double-density DWT is associated with (specifically that it is made up of one lowpass filter and two highpass filters), which means that we

are going to move on to the characteristics of the dual-tree DWT. The primary foundation of the dual-tree DWT is the concatenation of two critically sampled DWTs. We build a filter bank that executes several iterations concurrently to achieve this [21]. The oversampled filter bank is illustrated in Figure 2.

In contrast to Double Density DWT, which is based on a single scaling function (low pass) and two unique wavelets (high pass), 2-D DT\_DWT is based on two distinct scaling functions and two distinct wavelets. The cover picture is divided into nine sub-bands that are labeled LL, LH1, LH2, H1L, H1H1, H1H2, H2L, H2H1, and H2H2, respectively, upon application of 2-D DD\_DWT. The Double Density Dual-Tree DWT (DDDT\_DWT) combines the DT\_DWT and DD\_DWT characteristics. Two parallel, oversampled iterated filter banks make up the DDDT\_DWT's structure. First, a 1-D DDDT\_DWT decomposition is performed on each row of the cover image, with one decomposition using the real component of DDDT\_DWT to represent reality and the other using an imaginary decomposition. Following the 1-level decomposition, four times as many wavelets as the standard 2-D DD\_DWT are obtained.

### 3.3 Least significant bit

The most straightforward method for including data in a digital image file is the least significant bit (LSB) coding. LSB coding enables a significant quantity of data to be encoded by replacing the least significant bit of each sampling point with a binary message. The LSB data hiding technique is one of the simplest methods for inserting data into digital signals in noise-free environments. It merely embeds secret message bits in a subset of the LSB planes of the image stream, one of the numerous data-hiding techniques proposed to embed the secret message within the audio file. With this method, a secret message is substituted for the LSB of each sample's binary sequence in the digitized audio file. Consider the case where we are interested in hiding the letter "A" in a digitized audio file where each sample is represented by 16 bits (binary equivalent: 01100101). In that situation, the binary equivalent of the letter "A" in each bit is substituted for the LSB of eight successive samples, each of which is 16 bits in size.

### 3.4 The proposed model

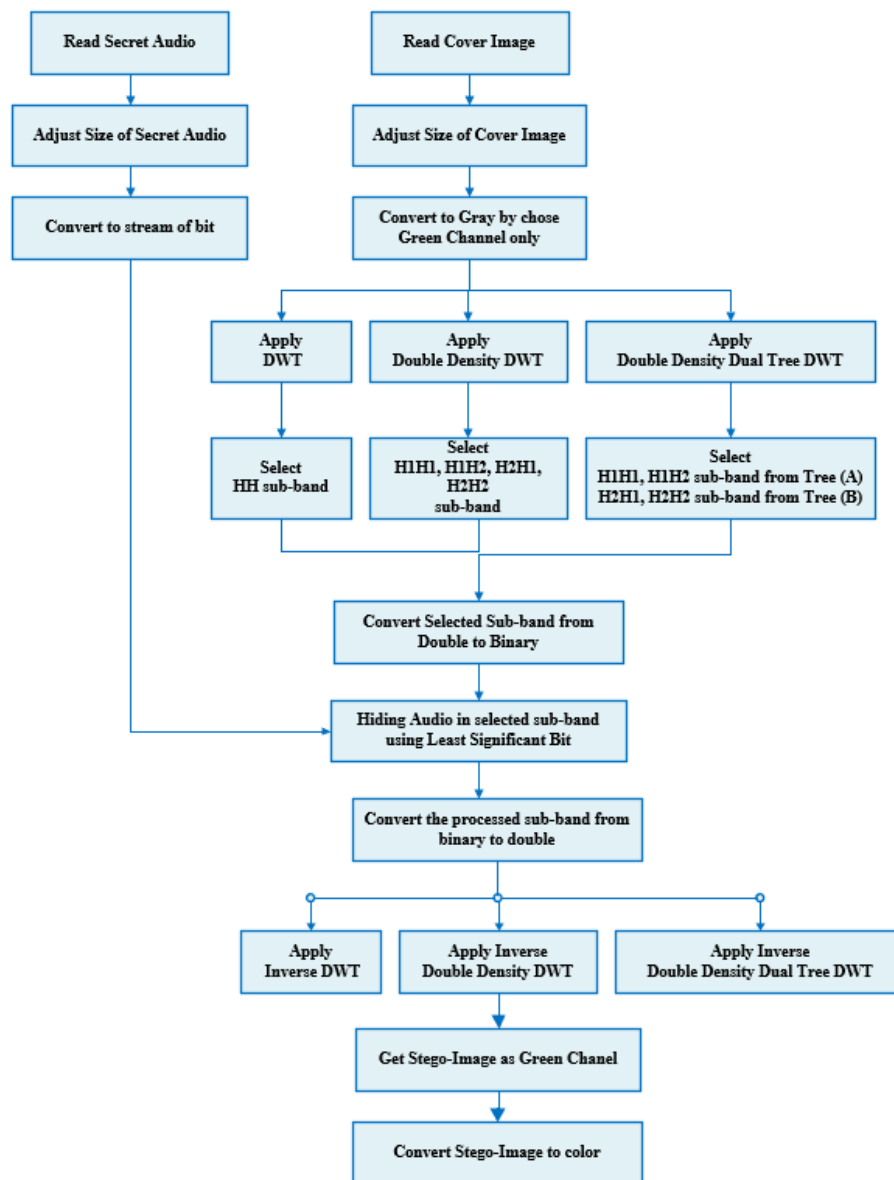


Figure 3. Block diagram for the proposed system model

Both temporal domain and transform domain steganography techniques are common. The cover object is transferred to a different domain, such as the frequency domain, to obtain the transformed coefficients in the transform domain. The hidden information is concealed by manipulating these coefficients. The coefficients are then subjected to the inverse transformation to produce stego signals. The actual sample values of temporal domain techniques are altered, making them more vulnerable to attacks than transform domain approaches. The present research investigates the viability of concealing an audio clip behind a digitally colored image. Audio files can be of various forms, but Wave files (.wav) are the most popular. The steganography technique will embed the audio file into the cover image without requiring a password or stego-key, regardless of the audio file format used. The LSB approach removes the audio file bits from the created stego-image and inserts them into an image. Figure 3 depicts the methodology that is suggested in this paper.

In the following steps, a method for embedding an audio file into the cover image by using Wavelet Transform:

#### A. Audio Processing

1. Read the audio file with (.wav) type.
2. Adjust the audio file length with the same length for each file, and reshape for the 2D array with a suitable size ( $N \times M$ ).
3. Convert the audio file from Double data type into Binary wave data type.

#### B. Image Processing

1. Read colored cover images with any type (.jpg, .png) into the program.
2. Adjust the cover image size to a suitable size ( $N \times M$ ).
3. Convert the colored cover image into a gray-scale image by choosing the green channel.
4. Apply one type of DWT to the cover image to get the approximate and details sub-bands of cover image, which will be used to embed the audio file. In Wavelete will be used three types of wavelet transforms and compare between them to get a more efficient method; these types are:
  - Discrete Wavelet Transform (DWT).
  - Double Density Discrete Wavelet Transform (DD\_DWT).
  - Double-Density Dual-Tree Discrete Wavelet Transform (DDDT\_DWT).

#### C. Embedding processing

1. Select any part of the approximate sub-band of the cover image. In this work, the selection is as follows:
  - ❖ Select HH subband for Wavelet Transform.
  - ❖ Select H1H1, H1H1, H2H1, H2H2 subbands for Double Density Wavelet Transform.
  - ❖ From Tree (A), select H1H2, H2H2 subbands, and from Tree (B), select H2H1, H2H2 subbands for Double Density Dual Wavelet Transform.
2. Convert the selected sub-bands from the Double to the Binary data type.
3. Embed the secret audio into the processed sub-band of the cover image. LSB techniques are used to embed the stream binary of audio files into 5<sup>th</sup>, 6<sup>th</sup>, 7<sup>th</sup>, 8<sup>th</sup> bits of each byte in the image. XORing the 8LSB bit, 7LSB, 6LSB, and 5LSB bits of the byte in the sub-band of the cover image

with the first four bits in the audio file, the operation is continued until all the bits of the audio file embedded in the cover image.

4. Convert the processed (HH, HH8, HH16) sub-bands from the Binary data type to the Double data type.
5. Apply Inverse DWT to get stego-image.

#### D. Extraction Process

1. Read colored stego-image.
2. Convert the colored stego-image into the gray-scale image.
3. Apply the same type of DWT applied in the embedding process.
4. Take the chosen subband's encrypted secret audio bits.
5. Convert to decimal to obtain the secret audio's estimation coefficients.
6. Find the inverse DWT for the estimation coefficients from step 4 while taking zeroes into account for the detailed coefficients. Secret audio is the end outcome.

#### E. Performance Evaluation

The proposed system evaluates results with design metrics measures. The approach is also assessed based on how closely the retrieved hidden audio resembles the original audio. This correspondence between the retrieved hidden audio and the original audio is measured. The following objective measurements are frequently employed to assess the outcomes:

##### • Mean Square Error (MSE)

The sum of the square of the difference between the original secret audio and the recreated secret audio is used to calculate the mean square error (MSE), which is then divided by the total number of samples as shown below:

$$MSE = \frac{1}{N} \sum_{i=0}^{N-1} (R_i - O_i)^2 \quad (1)$$

where,  $R_i$  is the reconstructed signal;  $O_i$  It is the original signal, and  $N$  is the number of signal samples. T The better the reconstructed signal accurately mimics the original signal, the lower the value of MSE signifies.

##### • Peak Signal to Noise Ratio (PSNR)

The PSNR is used to evaluate the quality of the stego-image. For an  $M \times N$  grayscale image, apply the PSNR between Cover-Image ( $C_{i,j}$ ) and Stego-Image ( $S_{i,j}$ ), by using this equation:

$$PSNR = 10 \log_{10} \frac{M \times N}{\sum_{i=1}^M \sum_{j=1}^N (C_{i,j} - S_{i,j})^2} \quad (2)$$

##### • Structural Similarity Index Metric (SSIM)

SSIM is a more accurate gauge of image quality than established metrics like MSE and PSNR. While SSIM views picture deterioration as a perceived change in structural information, PSNR calculates the perceived errors. The concept of structural information holds that the pixels are strongly interdependent, particularly when they are close together in space. SSIM evaluates the quality of X, with respect to Y, by computing a local spatial index that is defined as follows:

$$SSIM(x, y) = [l(x, y)]^\alpha \cdot [c(x, y)]^\beta \cdot [r(x, y)]^\gamma \quad (3)$$

The  $l(x,y)$  index is related to luminance differences,  $c(x,y)$  with contrast differences, and  $r(x,y)$  with structure variations between  $x$  and  $y$ . where  $\alpha$ ,  $\beta$ , and  $\gamma$  are parameters that define the relative importance of each component.

- **Signal to Noise Ratio (SNR)**

The highest value of SNR indicates a lesser difference in original and extracted audio.

$$SNR = 10 \log_{10} \frac{M \times N}{\sum_{i=1}^M \sum_{j=1}^N (C_{i,j} - S_{i,j})^2} \quad (4)$$

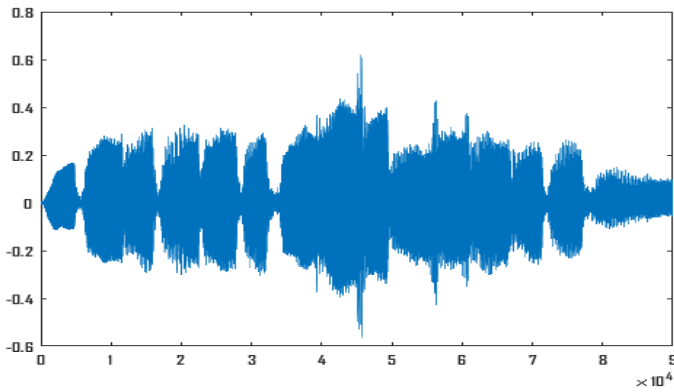


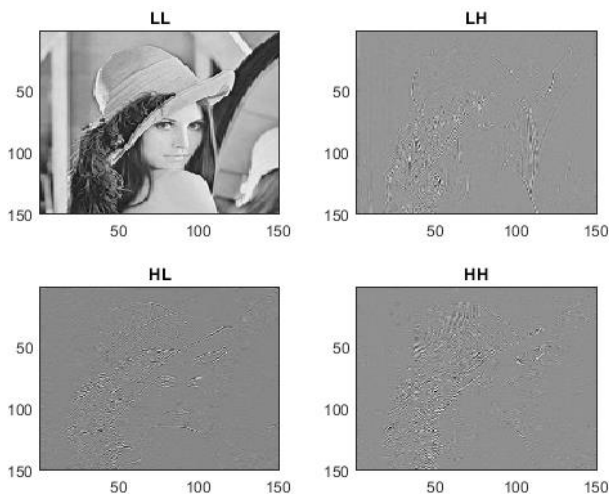
Figure 4. Secure audio signal file

#### 4. SIMULATION RESULTS AND PERFORMANCE EVALUATION

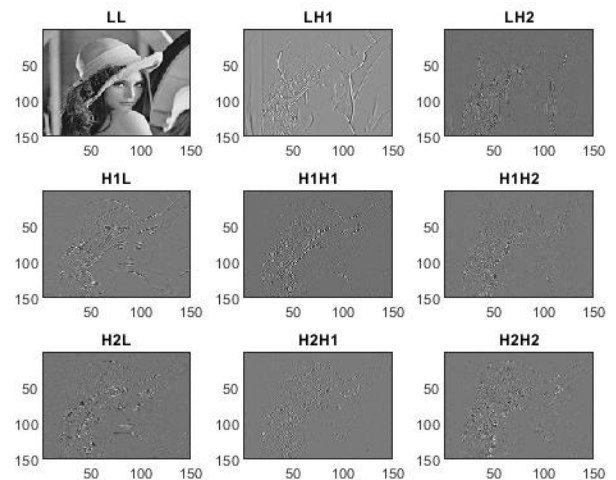
The proposed work has been implemented using MATLAB programming language, a 90KB audio file with (.wav) format, as shown in Figure 4. Lena cover-image are used with 300×300 Size, as shown in Figure 5. Lena images that have undergone various types of wavelet decomposition are displayed in Figure 6 below. The sub-bands result in Wavelet cover image after applying 2D wavelet transform, DD\_DWT, and DDDT\_DWT, respectively.



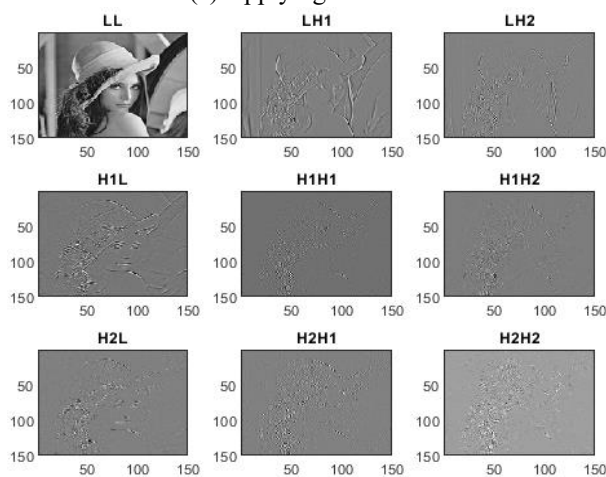
Figure 5. Cover image



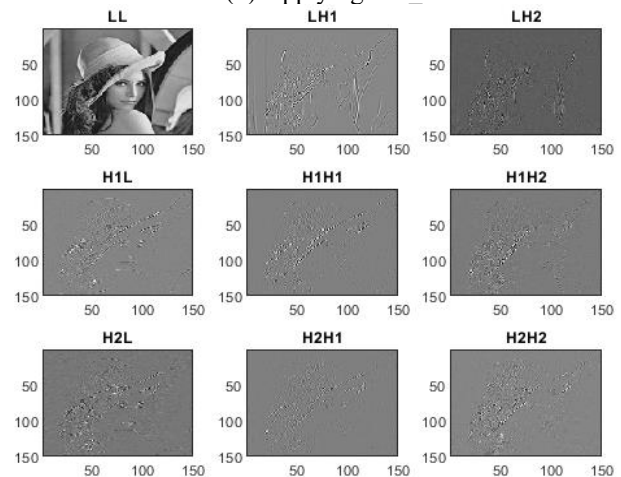
(a) Applying DWT



(b) Applying DD\_DWT



Tree-A Subbands of Image



Tree-B Subbands of Image

(c) Applying DDDT\_DWT

Figure 6. Lena Cover-image after applying a) DWT, b) DD\_DWT, c) DDDT\_DWT

When audio is encrypted and hidden in the LL band, the image is warped. This is because the LL band of the picture component contains crucial information, and any alterations made to the LL band will cause the final image to distort. This makes it simple for an intrusive party to identify the presence of sensitive data. In the meantime, distortion is reduced when audio is buried in the LH band. Finally, when the audio was compared to the HH band, it revealed very little deformation since the HH band carries less significant data and any alterations made had little to no impact on the final image. Thus, we came to the conclusion that we should use the HH band to conceal our hidden audio samples. Figure 7 represents the stego-image for 2D wavelet transform, DD\_DWT, and DDDT\_DWT, respectively.

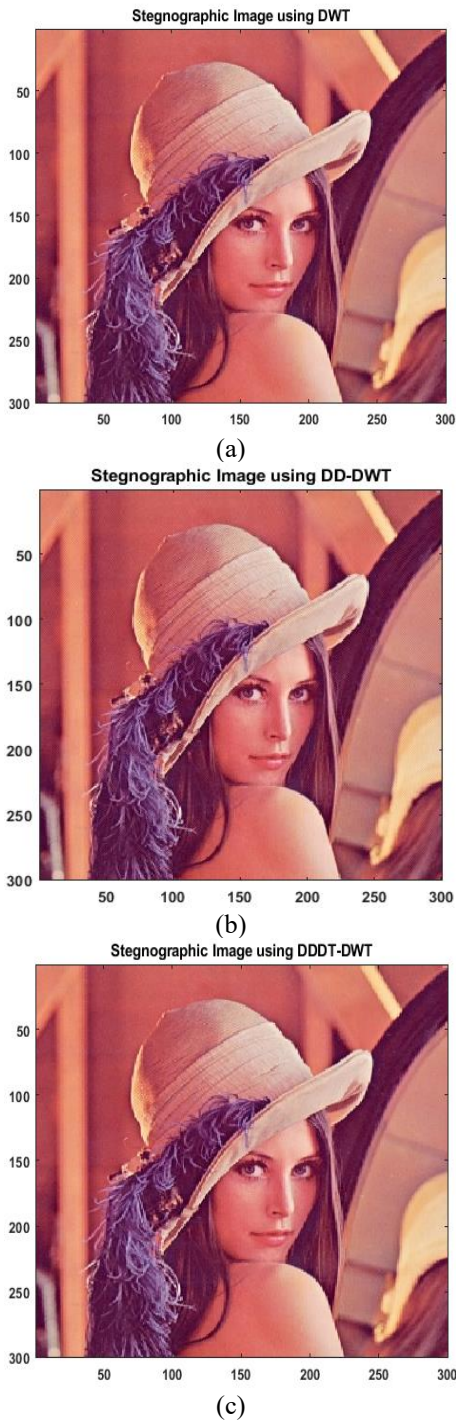


Figure 7. Steganographic image based on; a) DWT, b) DD\_DWT, c) DDDT\_DWT

### 5. COMPARISON BETWEEN PREVIOUS STUDIES WITH PROPOSED WORK

We made a comparison between previous studies and our proposed work in terms of audio sample and cover image used, Table 1 below demonstrates that the MSE and PSNR values vary depending on the audio sample. The suggested method determines PSNR between the Cover and Stego picture to guarantee imperceptibility. Greater PSNR values accomplish the reduction of noise in the stego picture goal and hence reveal an undetectable difference between the cover and stego images that is imperceptible to the human visual system.

The proposed DWT techniques' PSNR and SSIM values show how resilient the work is. The SSIM value of the hidden audio shows that the receiver retrieves the data one by one. When the results are contrasted with tried-and-true techniques, it is found that the proposed DWT, DD\_DWT, and DDDD\_DWT approaches are more sophisticated. As a result, it is found that DDDT\_DWT is a much superior method since it increases the steganographic process' payload through data compression.

Table 1. Comparison between previous studies with proposed work

Algorithm	Cover Image	Audio Samples	Stego Image		
			MSE	PSNR (dB)	SSIM
Proposed DWT	Lena 300×300		7.1387	39.5946	0.9858
Proposed DD-DWT	Lena 300×300	90000	5.6999	40.5721	0.9790
Proposed DDDD-DWT	Lena 300×300		1.0648	47.8582	0.9945
Proposed DWT	Lena 256×256		4.9219	41.2095	0.9907
Proposed DD-DWT	Lena 256×256	65535	2.3925	44.3424	0.9950
Proposed DDDT-DWT	Lena 256×256		0.9332	48.4313	0.9954
[4]	Lena 512×512	65535	-	38.6	0.935
[11]	Lena 512×512	93359	-	41.03	-

### 6. CONCLUSION

The major objective of this work is to identify a method for hiding any format of the secret audio file in the cover picture so that the image file does not undergo any discernible modifications as a result of hiding the secret audio. The paper concluded that LSB was mainly used in the spatial domain, while DWT and DD\_DWT, and DDDT\_DWT, respectively were mainly used in the transform domain. It also concluded that Steganography domain was mainly used in steganography due to its simplicity and high embedding capacity. This research suggests a high-capacity, safe, and reliable image steganography method. It provides positive results for each metric, making it an effective means to deliver audio files without making their existence known. As evidenced by the experimental findings, it has been determined that the proposed steganography technique predominates. In terms of visual steganography, the wavelet decomposition has proven to be a successful, systematic technique.

The PSNR and SSIM values provided by the proposed DWT approaches demonstrate the work's resilience. The

hidden audio's SSIM value demonstrates that the data is retrieved one by one at the receiver. The proposed DWT, DD\_DWT, and DDDT\_DWT approaches are discovered to be more advanced when the findings are compared to established methods. Thus, it is determined that DDDT\_DWT is a significantly better method because it enhances the payload of the steganographic process through data compression.

In Future it is necessary to evaluate the proposed method against many attacks, including histogram equalization, cropping, occlusion, translation, etc. According to the testing findings, recovering secret audio without significant distortion is usually possible.

## REFERENCES

- [1] Maisa'a Abid Ali, K.A., Alabaichi, A., Abbas, A.S. (2020). Dual method cryptography image by two force secure and steganography secret message in IoT. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(6): 2928-2938. <http://doi.org/10.12928/telkomnika.v18i6.15847>
- [2] Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S. (2020). A survey of moving target defenses for network security. IEEE Communications Surveys & Tutorials, 22(3): 1909-1941. <https://doi.org/10.1109/COMST.2020.2982955>
- [3] Abduldaim, A.M., Abdulrahman, A.A., Tahir, F.S. (2022). The effectiveness of discrete Hermite wavelet filters technique in digital image watermarking. Indonesian Journal of Electrical Engineering and Computer Science, 25(3): 1392-1399. <http://doi.org/10.11591/ijeecs.v25.i3.pp1392-1399>
- [4] Hemalatha, S., Acharya, U.D., Renuka, A. (2015). Wavelet transform based steganography technique to hide audio signals in image. Procedia Computer Science, 47: 272-281. <https://doi.org/10.1016/j.procs.2015.03.207>
- [5] Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A.A., Ahmed, A., Haleem, M. (2023). A comprehensive study of digital image steganographic techniques. IEEE Access, 11: 6770-6791. <https://doi.org/10.1109/ACCESS.2023.3237393>
- [6] Dhawan, S., Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2): 63-87. <https://doi.org/10.1080/19393555.2020.1801911>
- [7] Chawla, A., Shukla, P. (2014). Comparison of Arnold and matrix rotation using DWT image steganography. International Journal of Scientific & Engineering Research, 5(2): 1062-1066
- [8] Avci, D., Tuncer, T., Avci, E. (2018). A new information hiding method for audio signals. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, pp. 1-4. <https://doi.org/10.1109/ISDFS.2018.8355361>
- [9] Gharavi, H., Rajaei, B. (2018). A robust steganography algorithm based on curvelet transform. In Electrical Engineering (ICEE), Iranian Conference on, Mashhad, Iran, pp. 1624-1628. <https://doi.org/10.1109/ICEE.2018.8472443>
- [10] Aiswarya, T., Mansi, S., Talekar, A., Raut, P. (2017). Steganographic technique for hiding secret audio in an image. International Journal for Research in Engineering Application & Management (IJREAM), 3(4): 1-6.
- [11] Liao, M., Dong, X., Chen, J., Zeng, D. (2019). An audio steganography based on Twi-DWT and audio-extremum features. In 2019 Chinese Control Conference (CCC), Guangzhou, China, pp. 8882-8888. <https://doi.org/10.23919/ChiCC.2019.8866035>
- [12] Latha, R., Premkumar, R., Anand, S. (2018). An efficient wavelet transform based steganography technique using chaotic map. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, pp. 1-7. <https://doi.org/10.1109/ICCTCT.2018.8551076>
- [13] Tabares-Soto, R., Ramos-Pollán, R., Isaza, G., Orozco-Arias, S., Ortíz, M.A.B., Arteaga, H.B.A., Grisales, J.A.A. (2020). Digital media steganalysis. Digital Media Steganography, pp. 259-293. <https://doi.org/10.1016/B978-0-12-819438-6.00020-7>
- [14] Aslantaş, F., Haniççi, C. (2022). Comparative analysis of audio steganography methods. Journal of Innovative Science and Engineering, 6(1): 122-137. <http://dx.doi.org/10.38088/jise.932549>
- [15] AlSabhany, A.A., Ali, A.H., Ridzuan, F., Azni, A.H., Mokhtar, M.R. (2020). Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Computer Science Review, 38: 100316. <https://doi.org/10.1016/j.cosrev.2020.100316>
- [16] Abood, E.W., Abduljabbar, Z.A., Al Sibahee, M.A., Hussain, M.A., Hussien, Z.A. (2021). Securing audio transmission based on encoding and steganography. Indonesian Journal of Electrical Engineering and Computer Science, 22(3): 1777-1786. <http://doi.org/10.11591/ijeecs.v22.i3.pp1777-1786>
- [17] Sun, W., Shen, R.J., Yu, F.X., Lu, Z.M. (2012). Data hiding in audio based on audio-to-image wavelet transform and vector quantization. In 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Piraeus-Athens, Greece, pp. 313-316. <https://doi.org/10.1109/IIH-MSP.2012.82>
- [18] Alghazo, J.M. (2019). Intelligent security and privacy of electronic health records using biometric images. Current Medical Imaging, 15(4): 386-394. <https://doi.org/10.2174/1573405615666181228121535>
- [19] Hema, M., Shyry, S.P. (2023). A hybrid multimedia image encryption technique using singular value decomposition-linear sparsity regularization (SVD-LSR). Soft Computing, 1-11. <https://doi.org/10.1007/s00500-023-07937-z>
- [20] Khalaf, N.H., Abdullah, H.N., Tawfeeq, Q.S., Abdullah, A.N. (2022). Enhancement of radar signal detection using double-density dual-tree DWT. In 2022 2nd International Conference on Computing and Machine Intelligence (ICMI), Istanbul, Turkey, pp. 1-5. <https://doi.org/10.1109/ICMI55296.2022.9873729>
- [21] Abdullah, H.N., Hasan, M.F., Tawfeeq, Q.S. (2008). Speckle noise reduction in SAR images using double-density dual tree DWT. Asian Journal of Information Technology, 7(7): 281-284.
- [22] Abdullah, H.N., Hasan, M.F., Tawfeeq, Q.S. (2008). SAR image denoising based on dual tree complex wavelet transform. Journal of Engineering and Applied Sciences, 3(7): 587-590.