RESEARCH | Article in Press

An Optimum Method of Audio Steganography to Hide Text in Audio

Mst Jannatun Ferdaush

Received: 10 July 2026 / Accepted: 30 August 2026

Abstract

This paper proposes a new technique of audio steganography to improve text hiding in audio files by overcoming the limitations of traditional methods. Audio steganography is crucial for ensuring confidentiality and security in various applications, including personal communications, medical imaging, and digital rights management. This technique is a novel method used by researchers in secret information transmission. In this paper, we present an optimized approach using the amalgamation of the LSB substitution method with some advanced encryption techniques to provide more robustness and embedding capacity. Our approach unites under one cover a special approach of text embedding, having incorporated the new image interpolation technique providing reversibility and a fragile watermark for integrity verification. At the same time, these latter acts to alert the receiver in case tampering has taken place in the course of transmission and provide higher security for the hidden message. The proposed technique can achieve high data-embedding capacity with minimum distortion while preserving strong resistance of both intentional and unintentional data alteration. The experimental results validate that our methodology outperforms the conventional LSB methods in terms of embedding capacity and distortion. It can be applied to secure communication, digital watermarking, and forensic audio analysis. Future work will focus on optimizing data retrieval, expanding compatibility to more audio formats, and improving computational efficiency. This work enhances the study of steganography by presenting a secure text-hiding scheme within audio, enabling secure and reliable data communication.

Keyword: Information Security, Visual Cryptography, Audio Steganography, Secret Im-Age, Reverse Steganography

Introduction

Steganography

Steganography is a process in which secret messages are hidden in communications via a public network in such a way that an eavesdropper, who listens to all communications, cannot detect the presence of a secret message. In contrast to the voluminous literature proposing novel ad hoc steganographic protocols and dissecting vulnerabilities in existing protocols, relatively little work has been done on formalizing steganographic conceptions of security, and none has provided thorough rigorous proofs of security in any non-trivial model. Steganography is the virtuosity and science of entrenching undisclosed messages in a protection message. Following are some examples of steganography applications as diverse as the applications of communication. By using this technology, no one, save the sender and intended recipient realizes the message's existence. You may use this technology to transmit personal messages to anyone, colleague, or accomplice. It also can be used to carry personal data from point X to point Y in a way that

any transmission is undetectable. It can also be applied in network topologies, as will be explained on this page. This can be one of the handiest ways to mask communication between botnets and other systems being controlled by hackers. Since some of the procedural packets are just so common and commonly overlooked, it can potentially be used to further disguise the source and destination of data. Deriving exactly when and how a system was infected through a packet dump itself may take an otherwise well-trained malware analyst hour to weeks. A well-designed network steganographic program could sustain longer lengths of time.

Electronics are advancing in all aspects of our lives. Additionally, e-healthcare is a godsend, which is not only in terms of quality but also in terms of security and data transfer, ensuring that all patients receive the most effective therapies. The stated goal is difficult to fulfill, but if we can overcome difficulties such as electronic patient record (EPR) verification, payloads of medical images, secure transmissions, and precise recovery of sent data for correct diagnosis, we will be rewarded with the greatest healthcare available. Cryptography can solve the security and content authentication problems. Data concealing including inserting EPR, logos, and other significant data in medical photos, may be utilized to improve safety and evade undesirable attention to data [1, 2]. Using traditional hiding schemes, this data embedding could cause medical images to be distorted [3, 4]. Such distortions, particularly in medical photographs [5], cannot be overlooked. We must utilize new data-concealing strategies, ensuring that such a circumstance does not happen.

Problem Definition

Steganography aims to conceal confidential messages inside a cover medium, i.e., an audio file, so that its presence goes unnoticed to the observer. The Least Significant Bit (LSB) substitution method is one of the most widely used and easiest ways of doing this. However, traditional LSB methods are afflicted with certain built-in defects that reduce their strength and security level. One of the key problems is their vulnerability to statistical attacks. Statistical characteristics of the cover audio, such as histograms or sample distribution, can be inspected by attackers to recognize anomalies generated by the embedded information. For instance, naive implementations of LSB can distort the uniform distribution of noise in an audio file, and the secret message can be found using statistical analysis.

Besides, LSB techniques are susceptible to steganalysis techniques that exploit such statistical differences to uncover the hidden information. These techniques might involve examining the frequency domain of the audio signal or more advanced signal processing techniques to identify embedded data. In addition, LSB methods can cause audible distortion if too much data is embedded, or if embedding is not correctly performed. This distortion can be detectable and defeats the aim of steganography, which is to remain undetectable.

To overcome these limitations, more advanced steganographic techniques are needed. These typically involve LSB substitution combined with other techniques such as encryption, additional embedding algorithms of higher complexity, or adaptive strategies that take the characteristics of the cover audio into account.

A basic steganographic model is depicted in the diagram Figure 1 below. Adopted from Steganography Model – Edureka.

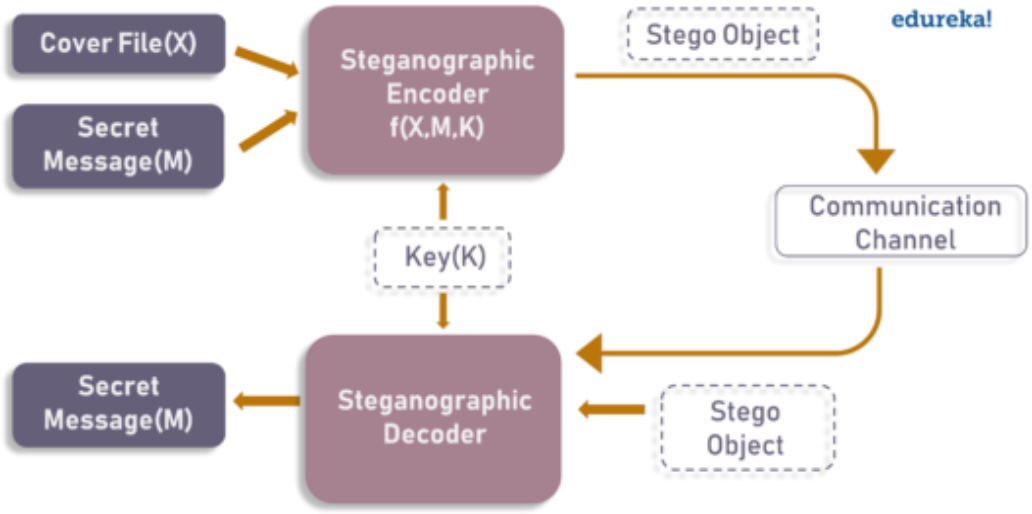


Figure 1. A basic steganographic model.

Related Work

Digital steganography has received a lot of attention. In 1996, the inaugural International Workshop on Information Hiding took place, followed by five further workshops and even a book on the subject. Surprisingly, nothing has been done to formalize steganography, and most of the research is based on heuristic approaches, such as steganography with digital photos, steganography with video systems, etc. Information-theoretic models for steganography have been proposed in a few articles [4, 8, 10, 12], but they are constrained in the same manner that Information-theoretic cryptography is what it's called.

Research Contribution

The main contribution of this research could also be summarized as follows: -

The suggested method allows us to create data concealment optimally. Not only does the proposed method allow us to incorporate EPR, but it also allows us to validate the material using a brittle watermark and hiding. A new picture interpolation technique has been presented to ensure the ability of medical imaging to be reversed. The image for the cover is created by interpolating the cover image's dimensions. Only the non-seed pixels of something like the cover photo are used to embed EPR to assure reversibility. Aside from the EPR, a fragile watermark is included to identify any infringement during transmissions. This watermark guarantees safe delivery. When the watermark placed at the receiving end is not retrieved, any attack on the image is confirmed. If the extracted watermark differs from the sent one, suggesting infringement, a request for retransmission is given to save time; if the implanted and received watermarks are identical, we can extract the EPR. We encrypt EPR to ensure its safety and security utilizing a magic rectangle. The substitution of the least significant bit (LSB) is used for embedding.

This work makes a number of significant contributions to audio steganography and represents significant advances over the traditional LSB methods. The following outlines the major contributions.

1. **Enhanced Security through Advanced Encryption:** The proposed method enhances security through the utilization of advanced encryption techniques in combination with LSB substitution. This extra layer of encryption makes it more difficult to extract the hidden information even if the attackers know that there is a chance of a steganographic message. Specifically, we encrypt EPR to protect and secure it through a magic rectangle.
2. **Improved Reversibility via Image Interpolation:** This proposes a novel image interpolation process

for ensuring the reversibility of medical imaging. The size of the cover is interpolated to produce the image of the cover. It is only non-seed pixels of something like a cover image used to implant EPR to be sure of its reversibility. This is particularly critical in applications like medical imaging, where one has to make sure that the cover audio can be retrieved without losing data.

3. **Data Integrity Verification using Fragile Watermarking:** The method utilizes fragile watermarks to verify embedded data integrity. In addition to the EPR, a fragile watermark is applied to identify any tampering while in transit. The watermark provides secure transit. When the inserted watermark on the receiving end is not gathered, any infringement attack on the picture is recognized. When the deleted watermark is distinct from the watermark which was sent along with the implication of infringement, a retransmission request is given for the sake of saving time. When the received and planted watermarks are similar, we can recover the EPR. This is accomplished to allow the receiver to detect any change or modification to the audio file while sending it.
4. **Optimal Data Concealment:** The scheme allows us to design data concealment optimally.
5. **LSB Embedding:** Least Significant Bit (LSB) replacement is utilized for embedding.

By combining these features, the proposed approach is a more robust, secure, and effective solution to audio steganography compared to traditional LSB methods.

Research Scope

The scope of this research is exciting and helpful for the:

1. In the business world Audio data hiding can be used to hide a secret chemical formula or plans for a new invention.
2. Audio data hiding can also be used in the noncommercial sector to hide information that someone wants to keep private.
3. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks.
4. As part of ARTUS1 project, which intends to incorporate animation characteristics into audio and video content.
5. Data hiding in video and audio is of importance to the government for information system security and covert communications, as well as for the protection of copyrighted digital assets.
6. It can also be used in forensic applications to introduce concealed data into audio recordings to verify spoken words and other noises, as well as in the music industry to monitor songs through broadcast radio.
7. Audio (Cover) Wave File Pre-Processing. The 2-bit LSBs of every 8/16-bit audio sample (Chunk) of wave file are replaced with random bit patterns generated by a True Random Number generator (TRNG), the details of which are beyond the scope of this study.

Literature Review

A. Introduction

Audio steganography is a method of concealing information in audio by taking use of limitations in the human auditory system [1]. Since it is not visible to the user, the audio steganography is more challenging than image steganography. The sound quality may be affected as the audio bits are being changed. The masking effect of the Human Auditory System (HAS) states that lower-frequency voices are repressed by higher-frequency voices, which supports the usage of an audio file as the cover. This attribute ensures that the stego file passes the hearing test.

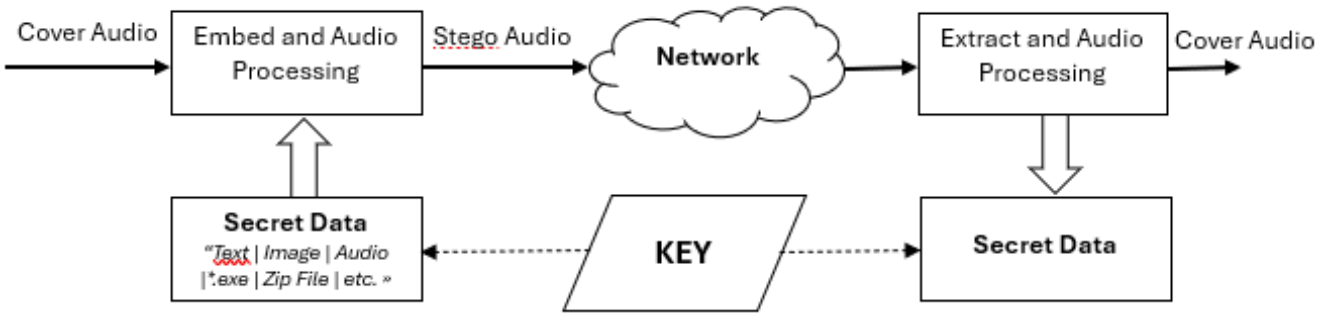


Figure 2. Visual Diagram of Audio Steganographic Model

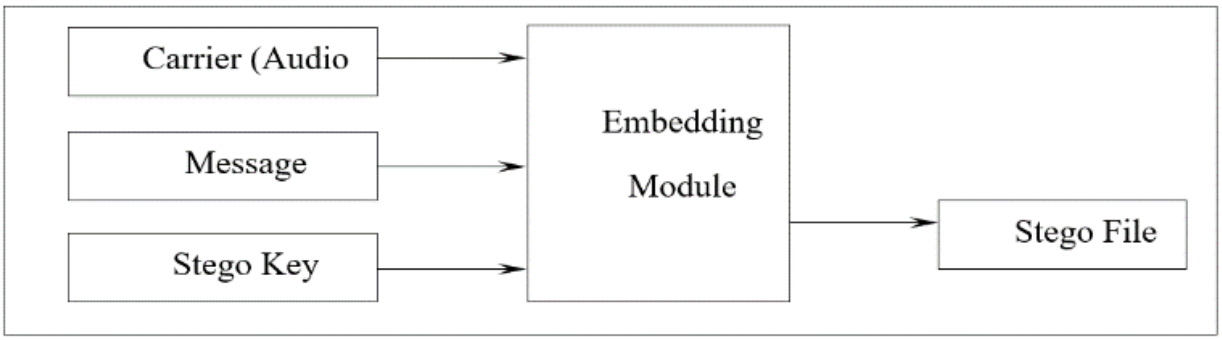


Figure 3. Basic Audio Steganographic Model [2]

The following three qualities of an effective audio steganographic scheme are required: inaudibility of distortion (perceptual transparency), data rate (capacity), and robustness. The magic triangle for data concealment [14] is named after these features (requirements).

B. Historical background

Steganography is the fine art of hiding a concealed message within regular communication. It comes after two Greek words: steganos, which means "covered," and graphia, which means "writing." Steganography is a primeval practice that has been used in many forms to keep communications hidden for thousands of years. For instance: a. The initial use of steganography dates back to 440 BC, when people in ancient Greece scribbled messages on wood and covered it with wax, which served as a layered medium. b. Romans utilized various types of imperceptible inks, and light or heat was used to decode the hidden secrets. c. Microdots were complete documents, photos, and plans that were shrunk to a dot's size, and added to normal paperwork by the Germans during World War II. d. Additionally, null ciphers were used to conceal unencrypted hidden messages within seemingly ordinary communication. We now use a variety of current steganographic techniques and tools to ensure that our information remains private. You must be right in asking if steganography and cryptography are the same things: no, they are two different concepts, and in this research, we are dealing with steganography.

C. Traditional Audio Steganography Techniques

A comparative analysis of digital audio steganography techniques was conducted by Fatiha Djebbar et al [3]. In their research, they discovered that many new steganography techniques have been developed in recent years that are particularly successful in securing digital information. Due to its wide availability and popularity, audio files have been chosen as the main carrier. The goal of audio steganography is to implant

a secret message in a digital audio file. A comparative examination of the literature in audio steganography techniques was presented in this paper. They compiled a summary of each technique's flaws and virtues in order to better characterize its application area. They conclude in their study that frequency domain techniques are better than temporal domain in terms of capacity, imperceptibility and undetectability. Uma Mehta [5] proposes a technique that increases security by requiring all files for data decryption; otherwise, information will not be able to be discovered. The LSB (Least Significant Bit) approach is used to hide information in a media file, which replaces the LSB of audio with binary data. In the geographic realm, steganography techniques based on the LSB are highly common. The Steganographic technique is shown as follows in Figure 4.

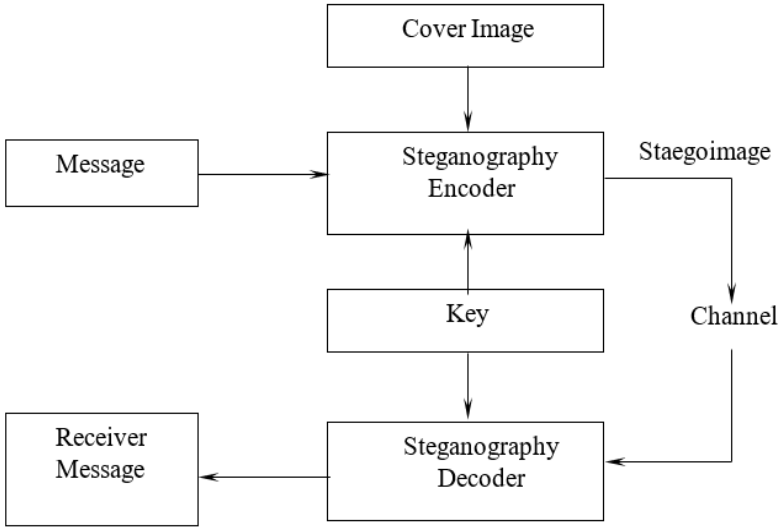


Figure 4. Steganographic Scenario [5]

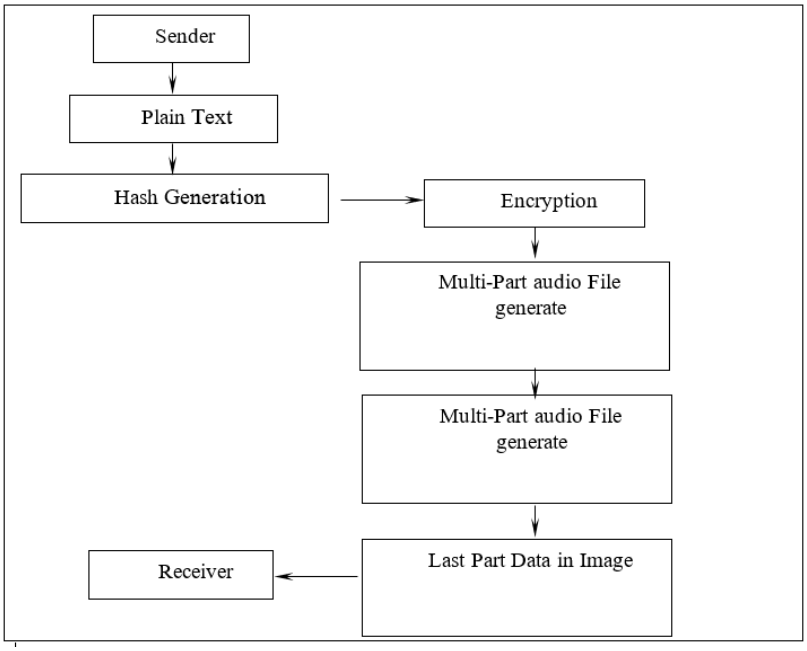


Figure 5. Flow chart of Steganographic process

Palwinder Singh [6] focused on various emerging concepts and recent techniques in audio steganography, such as Parity Coding, Least Significant Bit Coding (LSB), Phase Coding, Echo Data Hiding, and Spread Spectrum. Based on strengths, shortcomings, and concealment rate, they also assess the performance of modern audio steganography techniques. They have also talked about some recent developments, such as Audio Steganography based on Genetic Algorithms.

Table 1. Summary and evaluation of Audio Steganography methods.

Hiding Domain	Methods	Strengths	Weaknesses	Hiding Rate
Temporal Domain	Low bit encoding	Simple and Easy way of hiding information with a high bit rate	Easy to extract and destroy	16 kbps
	Echo hiding	Resilient to lossy data compression algorithm	Low security and capacity	40-50 bps
Frequency Domain	Magnitude spectrum	Longer messages to hide and less likely to be affected by errors during transmission	Low recovery quality	3 kbps
	Tone insertion	Imperceptibility and concealment of embedded data	Lack of transparency and security	250 bps
	Phase spectrum	Robust against signal processing manipulations and data retrieval needs the original signal	Low capacity	333 bps
	Spread spectrum	Provide better robustness	Vulnerable to time-scale modification	20 bps
	Cepstral domain	Robust against signal processing operations.	Perceptible signal distortions and low robustness	54 bps
Wavelet Domain	Wavelets coefficients	Provide high embedding capacity	Lossy data retrieval	200 kbps
Codecs Domain	Codebook modification	High robustness	Low embedded rate	2 kbps
	Bitstream hiding	High robustness	Low embedded rate	400 bps

Coding in the LSB format: It is possible to use the least significant bit because most alterations do not result in perceptible changes to the sounds. Another approach is to make use of human limitations.

Figure 6. The signal level comparisons between a WAV carrier file before the LSB coding

Figure 7. The signal level comparisons between a WAV carrier file after the LSB coding

It is feasible to encrypt communications utilizing frequencies that are unique undetectable audible to humans. Messages can be buried inside sound files using frequencies above 20.000 Hz and will not be identified by human inspections [16]. Multiple LSB steganography was utilized by S.S. Divya and M. Ram Mohan Reddy to hide audio and written text Cryptography is used to provide security. The two of them new substitution techniques offered increased the capability of cover audio for inserting more data. Message bits were inserted into several and varied LSBs in this case. For data embedding, these approaches used up to 7 LSBs. The results show that the techniques increased the capacity of data hiding of cover audio by 35 to 70% when compared to the traditional LSB methodology, which uses 4 LSBs for data embedding. Cryptography was implemented using the RSA algorithm [8].

For audio steganography, Muhammad Asad suggested a three-layered scheme based on least significant bit replacement. The secret message to be conveyed was passed through two layers before being embedded within the cover message in the third layer [9]. Pooja P. Balagurgi and Sonal K. Jagtap integrated two aspects of network security, cryptography, and steganography to develop a two-level encryption technique for user data. The combination of the LSB approach and the XORing method demonstrated an additional level of security [10]. S. Imaculate Rosalinel and M. Ashok Raj proposed a method for hiding a secret message in the cover image using Adaptive Pixel Pair Matching. The most well-known LSB approach had its drawbacks, such as increased distortion and reduced embedding efficiency. The Optimum Pixel Adjustment Process (OP AP) approach later overcame this [11]. Gunjan Nehru and Puja Dhar developed a deep look at audio steganography techniques using LSB and genetic algorithm methodology. Their investigation of audio steganography approaches employing various algorithms, such as the genetic algorithm approach and the LSB approach, provided the basis of their research [12].

P. T. Yu et al. proposed a work in the spatial domain of a color image in which a binary watermark was encoded, and the neural network was trained using a set of training patterns. The difference in intensity between the blue component of the central pixel and the other pixels in the window was used as the training pattern. There are 9 input vectors and 1 output vector in each training pattern. The trained neural network extracts watermarks from legal picture owners [13]. C.C. Chang and I.C. Lin devised a novel image data watermarking system based on neural networks and Discrete Wavelet Transforms (DWT). A pseudo-random 8 noise generator was used to pick a coordinate set S from DWT decomposition (PRNG). To train the network, a training set was created, with each training pattern containing eight input vectors and four predicted outputs. The watermark was embedded using the trained network [14].

The flaws of the previous procedure, as well as how they differ from the present method, will be explained here. The human ear is extremely sensitive to noise and can often detect even the least amount of noise inserted into a sound file, hence conventional approaches like as echo concealment, spread spectrum, and parity coding have significant shortcomings in terms of resilience. Because the secret message is only encoded in the first signal segment, phase coding has the main disadvantage of poor data transmission rate. As a result, this approach is only utilized for transferring a modest amount of data. The Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of the audio file with a binary message, among the various information hiding techniques proposed to embed secret information within audio files. As a result, the LSB approach enables a significant amount of secret data to be encoded in an audio file.

To use LSB to hide confidential information, follow these steps:

a. Create a bit stream from the audio file.

b. In the secret information, convert each character into a bit stream.
c. In the secret information, replace the LSB bit of the audio file with the LSB bit of the character.

The proposed approach is more secure and efficient for hiding secret information from hackers and sending it to the intended recipient in a secure and undetected manner. This suggested technique also ensures that the file size does not change after encoding and it may be used with any audio file format [7].

D. Audio Steganography Evaluation

Signal-to-noise ratio is high (SNR): SNR stands for signal-to-noise ratio, which is defined as SNR dB = 2 log 10 V signal V noise, where Vsignal and Vnoise are the measured signal and noise voltages, respectively. Audio steganography employs the audio file as a host (cover) file in embedding, which is not simple and might be regarded a challenge (HAS) due to the sensitivity of the Human Auditory System. The Human Auditory System detects audio file fluctuation over a power range of more than one billion to one and a frequency range greater than one thousand to one. It does, however, have flaws, and a wide dynamic range can contribute to data concealment (Bender et al., 1996). Because of their high level of redundancy and high data transmission rate, as well as their huge size in comparison to other multimedia files, audio files make good host files for hiding. Later, we'll go through a few techniques.

Efficiency is determined by a set of norms known as requirements. In most algorithms, there are a set of specific requirements that must be met. Transparency, capacity, robustness, and algorithm complexity are the four criteria. In steganography, hiding capacity is the most important property, followed by transparency and security, while resilience is more important in watermarking. For example, increasing capacity reduces transparency, and vice versa. A decent steganographic system must strike a balance between these objectives, which is difficult to accomplish in a single method. The signal-to-noise ratio SNR is used to assess the performance of the procedures under consideration [17]. The SNR value represents the amount of distortion caused by embedded data in the cover audio signal sc (m, n). The following equation gives the SNR value:

$$SNR_{dB} = 10\log_{10}\left(\frac{\sum_{n=1}^{N}|s_c(m,n)|^2}{\sum_{n=1}^{N}|s_c(m,n)-s_s(m,n)|^2}\right)$$

Where ss(m, n) is the stego-audio signal such as: m = 1, ...M and n = 1, ...N, where M is the number of frames in milliseconds (ms) and N is the number of samples in each frame.

Maximum permissible concealing rate in given temporal domain SNR values software for steganography [18] and [19] are shown in Table I. The cover audio files are WAV format speeches that range in duration from 4 to 10 milliseconds and are sampled at 16 kHz with 16 bits per sample. Before being embedded, the hidden message in both s-tools and Steghide software is compressed and encrypted.

Table 2. Objective performance of audio Steganography software.

Software	Hiding Rate (Kbps)	SNR
H4PGP	32	53.50
S-tools	18	68.44
Steghide	18	57.80

Figure 8 shows the noise level caused by the embedding in the cover voice signal. Most audio steganography algorithms based on frequency domain use a perceptual model to calculate the acceptable amount of data embedding without altering the audio signal, to control the distortion generated by the embedding process. Frequency masking is used by many audio steganography methods [20], [21], [22], and [23] and auditory masking [24], as the steganography embedding perceptual model.

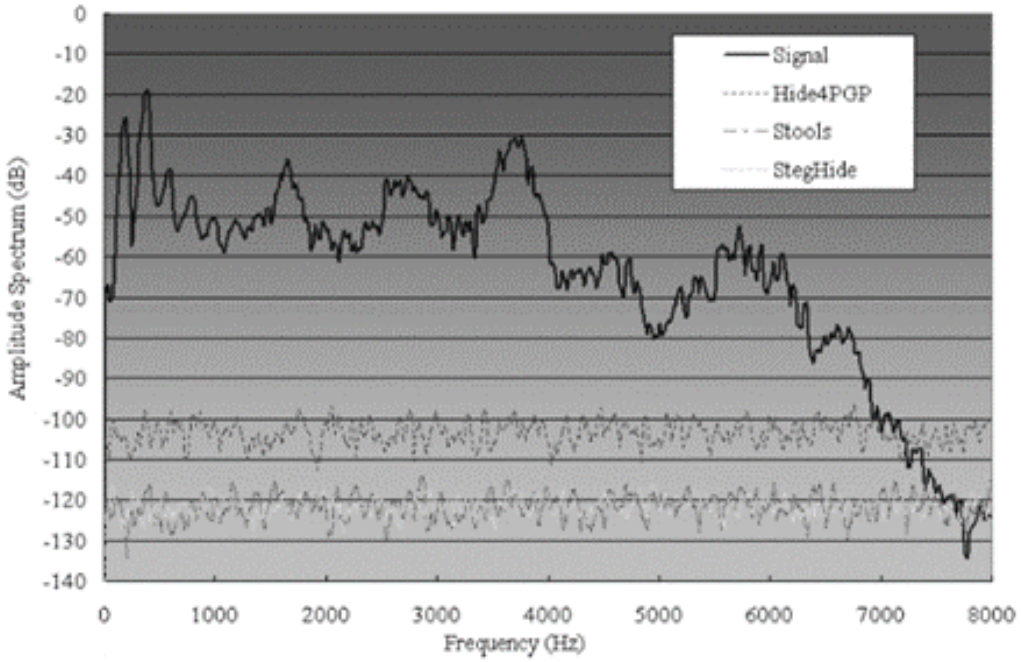


Figure 8. Noise level in a speech frame induced by the software tool appearing in Table 2

Furthermore, some frequency domain techniques, such as phase embedding, indirectly come into phase features, such as robustness to basic linear signal operations like magnification/amplification, attenuation, filtering, resampling, and so on. Encoder domain approaches ensure embedded data's durability against compression and noise addition in more demanding environments, such as real-time applications. When creating a robust steganographic system, these two features are expressly pursued. However, if a voice encoder/decoder is present in the network, embedded data integrity in the encoder domain may be jeopardized. Furthermore, if a speech augmentation algorithm such as echo or noise reduction is installed in the network, concealed data may be transformed.

The following are a few factors to keep in mind to avoid simple recognition of embedded data:

1. Good steganography adopts that the cover used to conceal messages does not raise any suspicions among adversaries. Creating new cover audio before data embedding is a simple way to avoid a known-carrier assault. By comparing the original with the stego audio file, publicly available cover audio signals may jeopardize the steganography system's dependability.
2. The tolerance of the Human Auditory System (HAS) to common sound changes (e.g., loud sounds tend to mask out quiet sounds) [1] has two effects on the audio steganography system: (1) Stenographers take advantage of the fact that noise created by frequency masking data embedding is often undetectable, and (2) lossy audio data compression, such as MPEG/Audio encoding, removes masked frequencies and hence the embedded data [25].

3. A simple listening test can compromise the steganographic system if it is hidden in soundless gaps of audio signal or high LSB layers of audio samples.
4. Prior to the embedding process, adding an encryption layer strengthens the security of steganographic systems and types hidden message detection more difficult. The randomness of encrypted data is often strong, which fits in keeping with the audio file's nature [26].
5. Information that is embedded in an indeterministic manner is difficult to extricate [20]. As a result, discovering the existence of a steganographic message does not always imply that it will be extracted.

Table 2 summarizes the strengths and weaknesses of the strategies examined. The application and employed channel transmission conditions influence elements such as security considerations about hostile channel attacks, robustness, or larger concealing capacity.

E. Recent Advancements in Audio Steganography

Deep Learning-Based Techniques: Deep learning techniques have dominated most fields in the last few years, such as audio processing and steganography. Deep learning-based algorithms, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been applied to enhance the security and efficiency of steganography systems for audio. CNNs can be used to train complex features from sound signals and conceal hidden messages in unobtrusive locations, thus making them steganalysis-resistant.

RNNs can, however, capture temporal dependencies of sound data, allowing for more resilient and high-capacity schemes for steganography. Autoencoders, which are a type of neural network, have also been applied to audio steganography by learning a compressed representation of the audio signal and embedding secret data within this representation.

These deep learning approaches are generally better than traditional approaches in terms of security, capacity, and resilience because they can learn statistical properties of the audio signal and make it more difficult for the attacker to identify the presence of hidden messages.

However, there are drawbacks to deep learning methods as well, such as increased computational demands and the need for extensive training data.

F. Conclusion

In the past, we have seen that the bulk of similar works depend on improving the prediction efficiency with additional characteristics. The truth is that, for example, certain papers have no photographs, these features do not necessarily exist. It is also very risky to use social media information since it is easy to make a replacement account on these media to trick the identification mechanism. That's why I only decided to reflect on the article body to see if false news can be accurately described.

Materials and Method

The LSBs were chosen for substitution since they contribute the least to the computation of the cover file's statistical value.

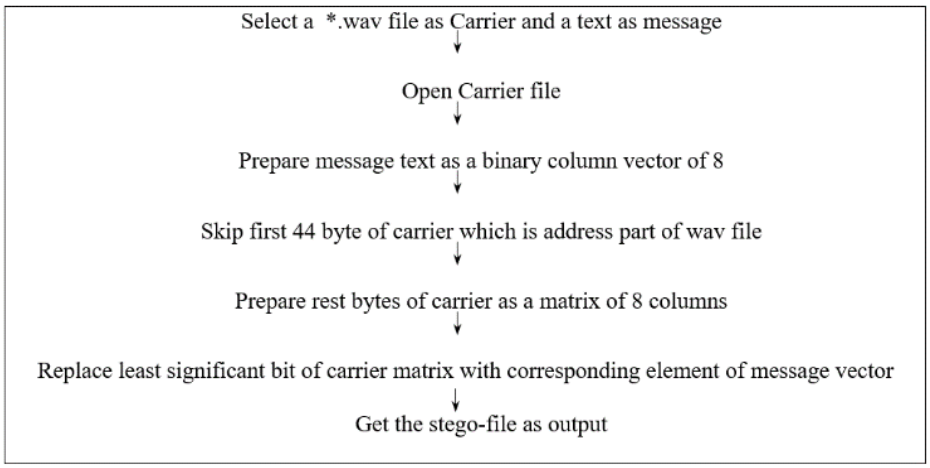


Figure 9. Flowchart of LSB modification Technique for Audio Steganography

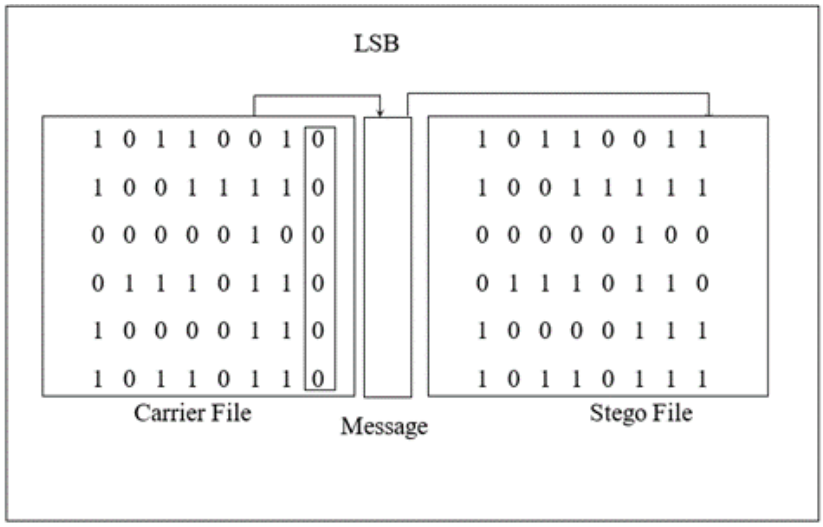


Figure 10. LSB modification procedure for Audio Steganography

A pdep instruction can be used in LSB steganography encoding to extend the secret message bits and insert them at the least significant bit positions of each subword. The secret message is decoded using a pex instruction that extracts the least significant bits from each subword and reconstructs it.

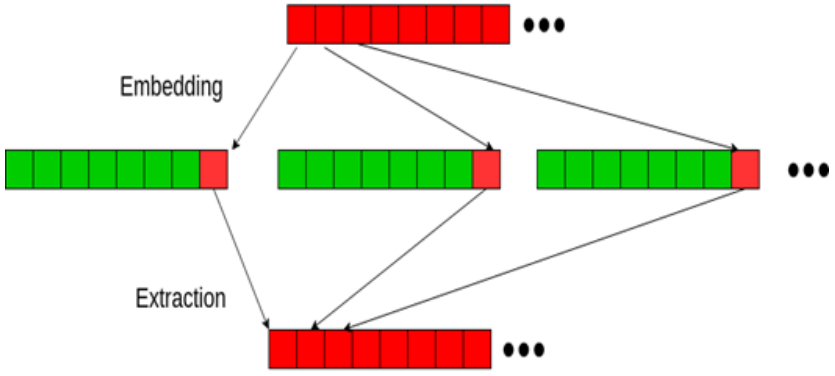


Figure 11. Visualization of LSB modification procedure for Audio Steganography

The stego-file hasn't been audibly changed, as far as we can tell. Furthermore, the graphical depiction demonstrates that there is no significant differences between the input carriers file and the output stego-file.

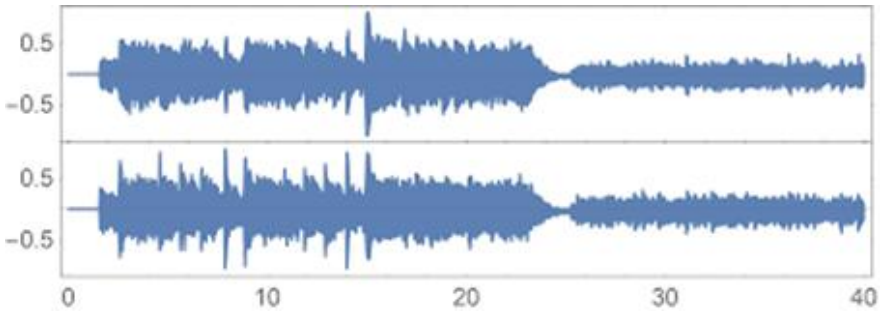


Figure 12. Graphical depiction of the secret message

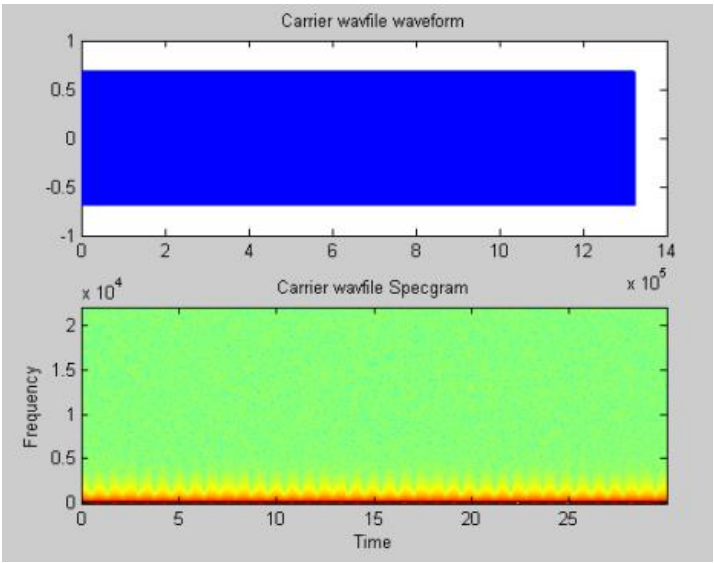


Figure 13. Graphical Representation before text message encoded

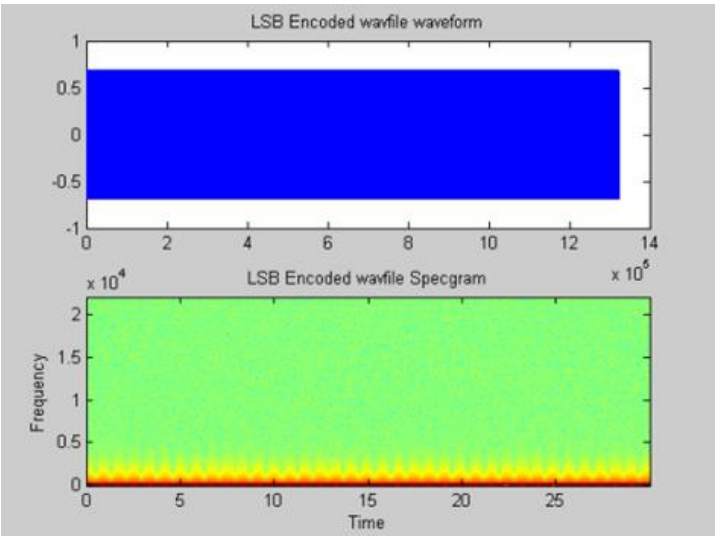


Figure 14. Graphical Representation after text message encoded

Encryption Mechanism and Integration with Steganography: To further protect the hidden message, an encryption process is applied before the steganography process. EPR in this study is encrypted using a 'magic rectangle' technique. 'Magic rectangle' encryption involves reorganizing the information into a rectangle and then successively applying a series of substitutions and permutations so that the content is not visible. The step-by-step process in the encryption is as follows:

1. The EPR data is first translated into a binary stream.
2. This binary stream is then structured into a rectangle of pre-specified dimensions.
3. The columns and rows of the rectangle are permuted with a secret key.
4. Substitution operations are performed on the rectangle elements with the secret key.

This encryption process ensures that even if the steganographic embedding is discovered, the message concealed within is secure from being accessed without the proper decryption key. The integration of the mechanism of encryption with the steganography process is as follows:

1. The EPR information is encrypted first using the 'magic rectangle' technique.
2. The encrypted binary stream is embedded in the audio cover file using the LSB substitution method.
3. During the embedding process, the least significant bits of the audio samples are replaced with the encrypted data bits.

This sequential steganographic embedding and encryption process provides a layered security system, with it being even more difficult for an attacker to access the original data.

Experiment Results

The cover file in this manner is audio, whereas the message inside is an image signal. It can be done by applying the Discrete Wavelet Transform (DWT) on the watermarked audio stream. Using the iterative equations below, one-directional DWT of any stage can be computed from the coefficients of the DWT of the preceding stage [9].

$$WL(n,j) = \sum_m WL(m, j-1) h_0(m-2n)$$

$$WH(n,j) = \sum_m WL(m, j-1) h_1(m-2n)$$

$WL(n,j)$

Where is the nth scaling coefficient at the jth Stage,

$WL(n,j)$

is the nth wavelet coefficient at the jth Stage,

and h0(n) and h1 are the dilation coefficients corresponding to the scaling and wavelet functions, respectively.

In figures. 15(a) and 15(b), histograms of the cover picture and the stego image were plotted. The MSE and PSNR values were determined for various n values. Table 3 illustrates the MSE and PSNR values for each steganographic procedure, as well as the time required.

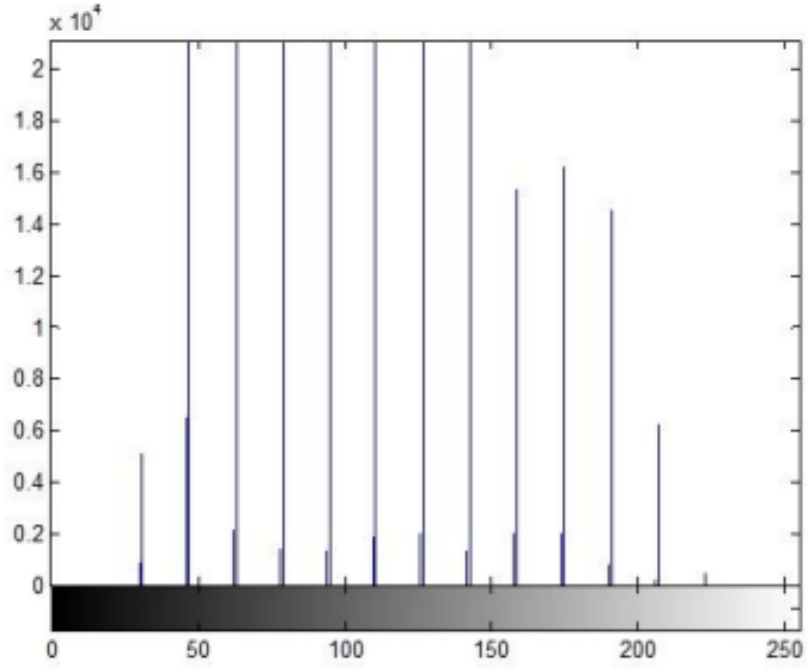


Figure 15(a). Histograms of the cover picture and the stego image

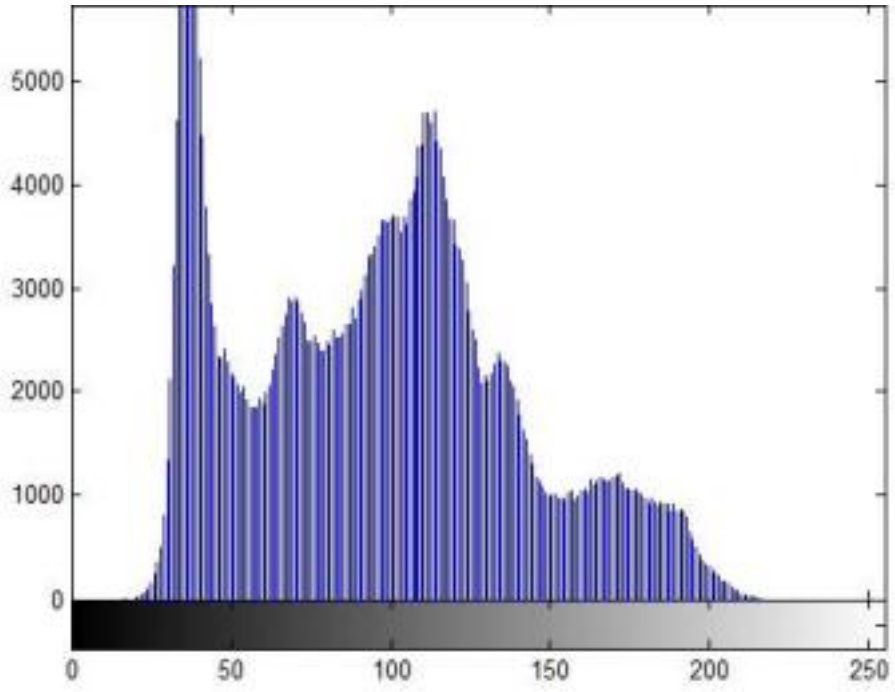


Figure 15(b) histograms of the cover picture and the stego image

Table 3. MSE and PSNR values, as well as the time spent for each value of n.

N (LSB Bits)	MSE	PSNR (db)
1	1.5894e+004	14.1790
2	3.8599e+003	20.3254
3	915.1061	26.5765

4	222.9934	32.7083
5	48.5570	39.3287
6	8.9208	46.6871
7	0.9932	56.2210
8	0	∞

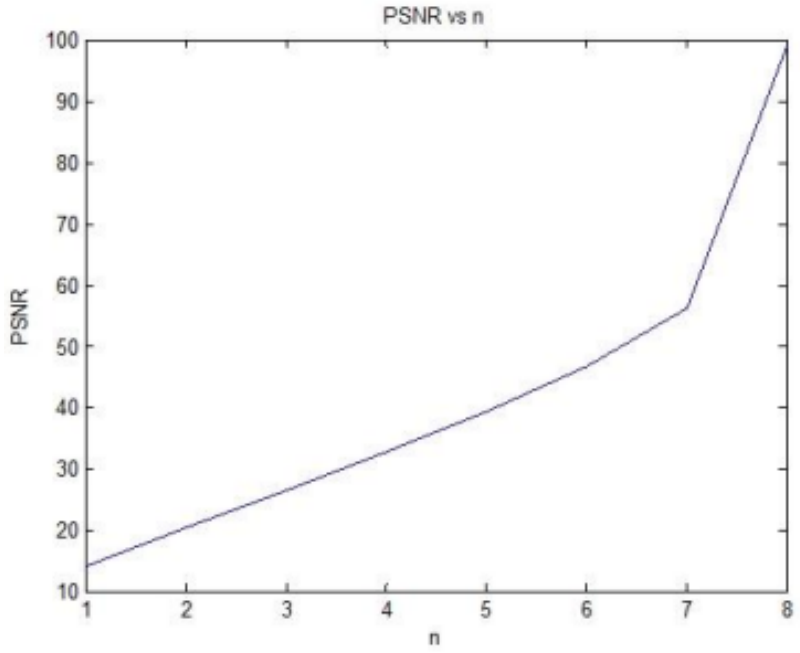


Figure 16(a). Plot of MSE vs ^{n}

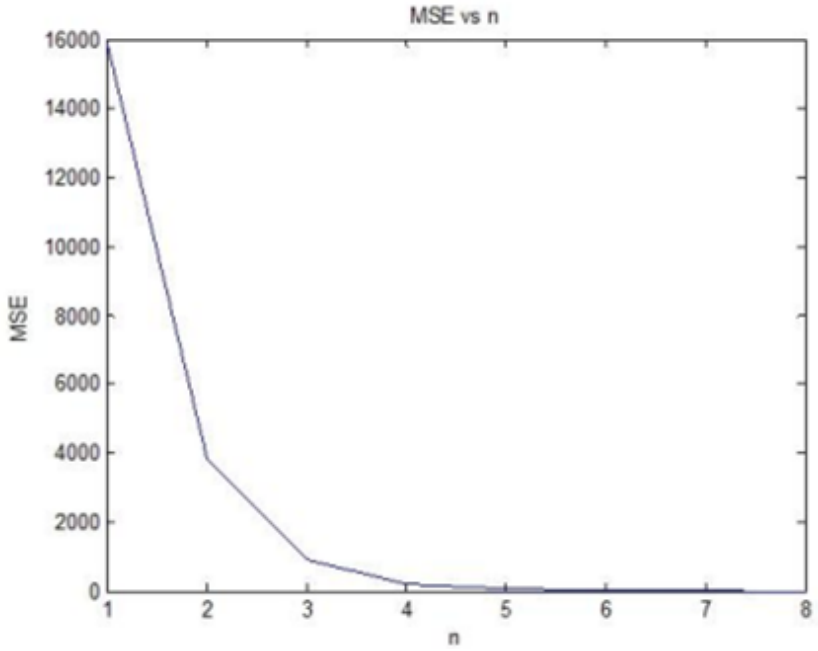
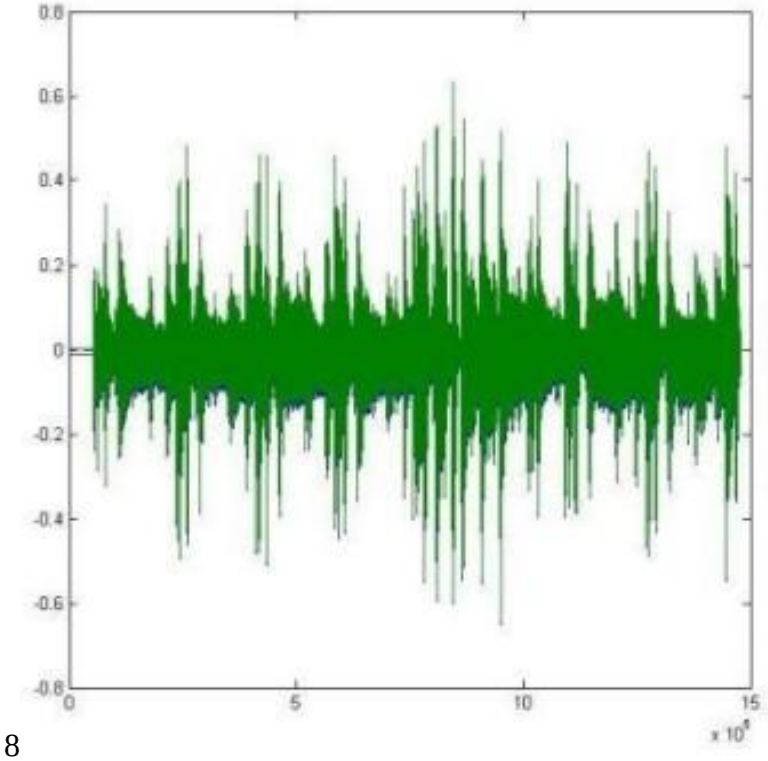


Figure 16(b) Plot of PSNR vs ^{n}



8

Figure 16(c). Original audio signal as cover

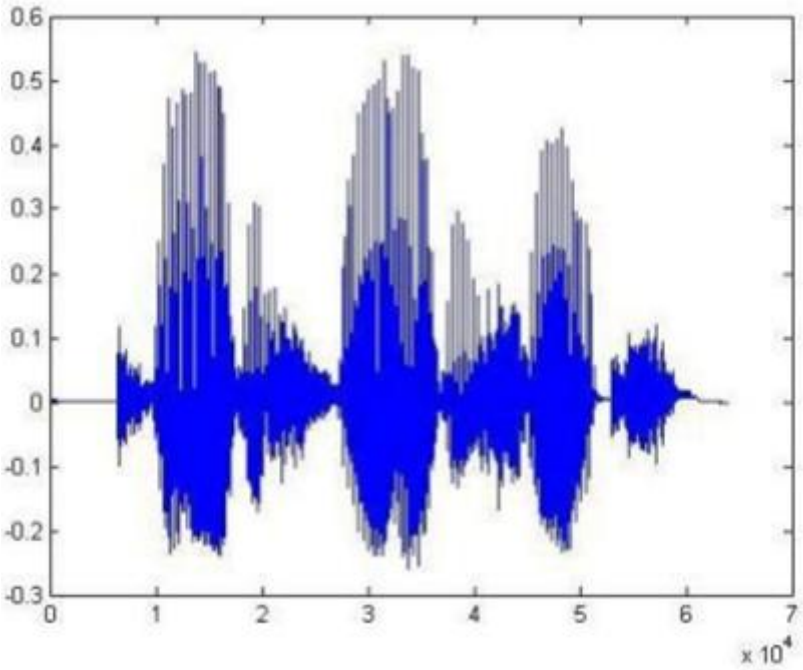


Figure 16(d). Watermark audio signal as message

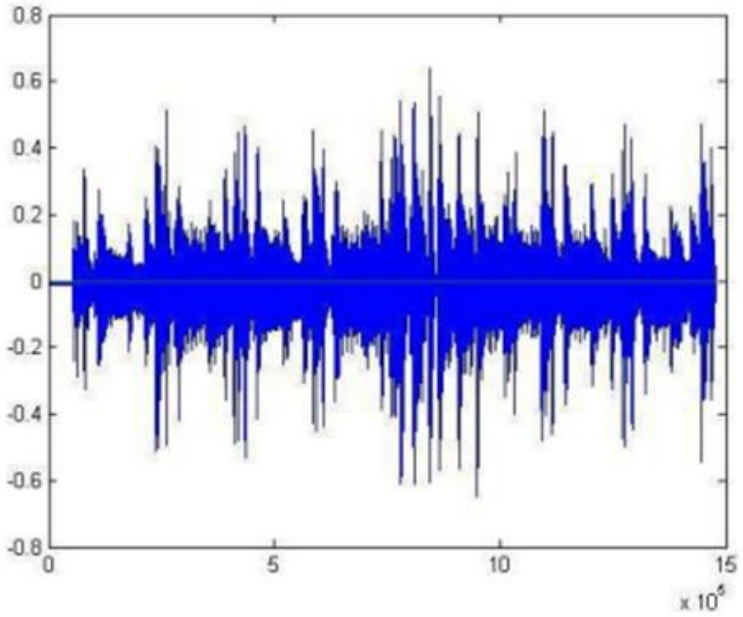


Figure 16(e). Audio in audio watermark signal

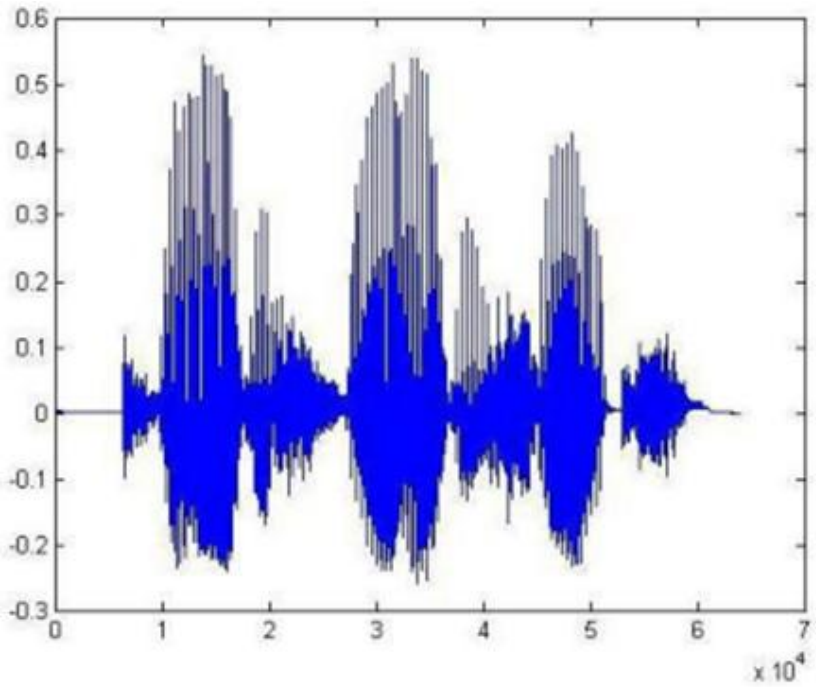


Figure 16(f). Recovered audio watermark signal

Steganalysis Test: To provide a better evaluation of the resistance of the proposed method to steganalysis, we employed different steganalysis techniques other than histogram analysis. Specifically, we employed the following techniques:

1. **RS Analysis:** RS analysis is a statistical technique for the detection of hidden messages in steganographic media. It involves analyzing trends in the data embedding to discover deviations from the predicted statistical features of the cover medium.

2. **Machine Learning-Based Steganalysis:** Machine learning algorithms, such as Support Vector Machines (SVMs) and Random Forests, were trained to predict whether audio samples have a hidden message or not. These algorithms learn complex features from the audio data and can detect slight changes typical of steganography.

The results of the steganalysis test are as follows:

1. RS analysis found no significant anomalies from the statistical properties of the stego audio that are expected, which confirms that the method is immune to this type of steganalysis.
2. The steganalysis machine learning-based algorithms were low in accuracy for uncovering concealed messages, further ensuring the security of the proposed method.

These results, coupled with the histogram analysis, provide a more rigorous assessment of the resistance of the proposed method to steganalysis and make the research more robust.

Algorithms

This section refers to the algorithms that were used during the classification process.

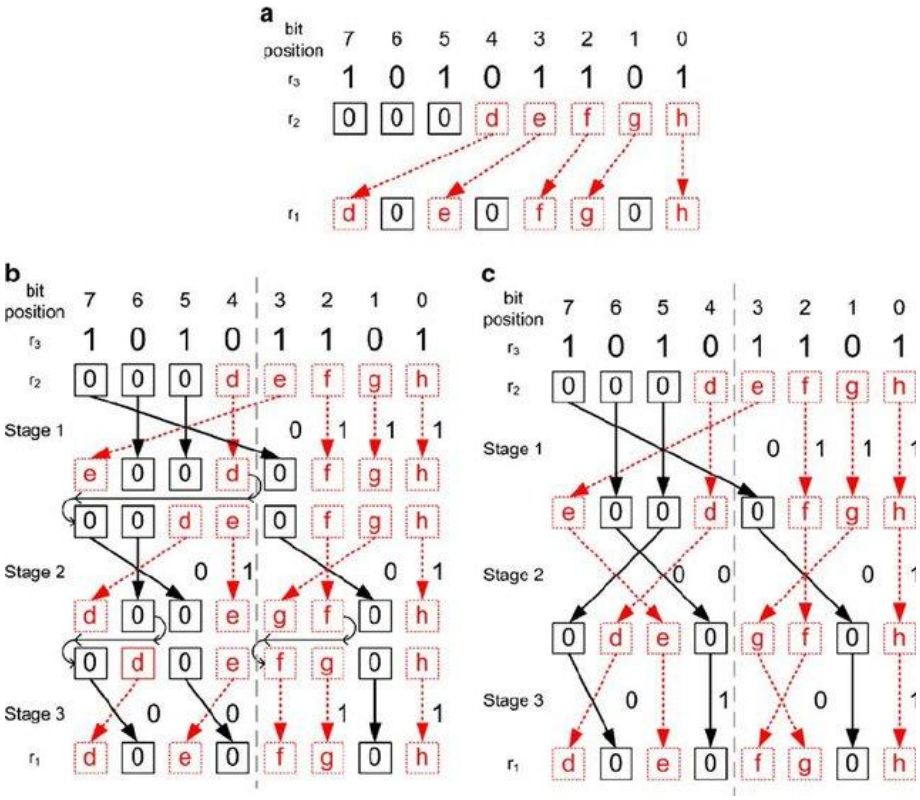


Figure 17. Decision Tree (DT)

The research utilizes Least Significant Bit (LSB) substitution for steganography and a "magic rectangle" encryption method.

Steganography Algorithm (LSB Substitution): LSB substitution method is used to embed secret messages within audio files. The least significant bits of the audio samples are replaced with the secret message bits. The LSBs are chosen because they give the minimum to the statistical value of the cover file and thus produce minimal distortion. The process involves using pdep instruction for encoding to insert secret message bits into the least significant bit positions of each subword. Decoding is done using a pex

instruction to extract the least significant bits from each subword and restore the secret message.

Encryption Algorithm ("Magic Rectangle"): For extra protection for the hidden message, an encryption technique is applied before the steganography. Specifically, EPR data is encrypted with a "magic rectangle" technique. The "magic rectangle" encryption is rewriting the data in a rectangular format and then jumbling it up with a series of permutations and substitutions to conceal the original data.

The encryption process involves the following steps:

1. The EPR data is then converted into a binary stream.
2. The binary stream is then mapped into a rectangle of fixed size.
3. The rows and columns of the rectangle are rearranged based on a secret key.
4. Substitution operations are performed on the elements of the rectangle, also based on the secret key.

The integration of the encryption mechanism with the steganography process is as follows:

1. EPR data is encrypted in the first place using the "magic rectangle" technique.
2. The encrypted binary stream is then embedded into the audio cover file using the LSB substitution method.
3. During embedding, the least significant bits of audio samples are replaced with the data bits of the encrypted data.

Other Algorithm:

- Decision Tree (DT) is also mentioned in the field of classification.

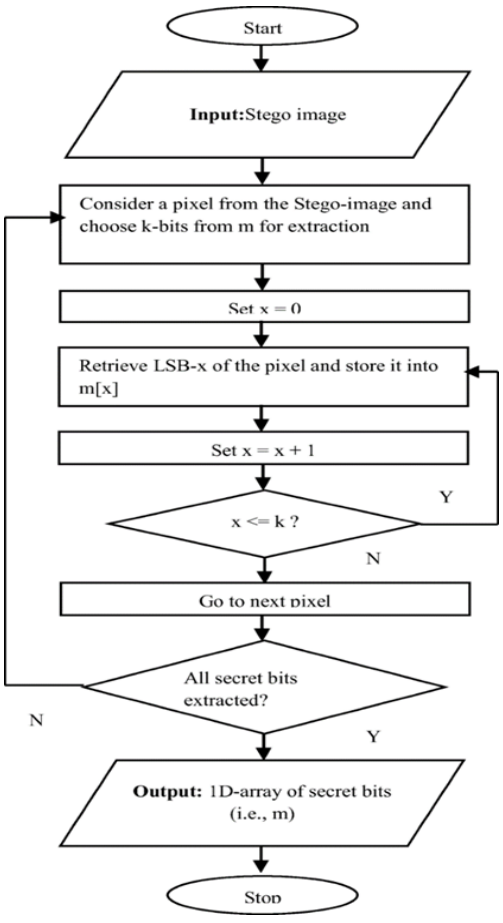


Figure 18. Flowchart of the algorithms used

Results and Discussion

The substitution approach, where nearly all of the bits of the concealment file remained replaced with the message bits, is the most well-known method of steganography implementation. The LSBs were chosen for substitution since they donate the smallest to the cover file's statistical value computation. Multiple LSBs were swapped to boost the data hiding capabilities of cover files. However, using these strategies led to additional distortion. Because LSB replacement is vulnerable to both intentional and unintended attacks, an answer was presented to hide data in deeper levels. More distortion in the concealment file resulted from hiding data in deeper levels of the concealment. Some algorithms were presented at the time that not only did they hide data in deeper layers, but also changed it by eagerly changing specific supplementary sections of the cover file to reduce the distortion.

Audio became popular as a cover file due to its wide availability in practice and its natural masking effect. Furthermore, the masking effect occurs when low-frequency audio is muted by higher-frequency noise. The underlying issues of the substitute technique remained even after the adoption of audio as a cover. As a result, many variations of the traditional LSB approach have been implemented in an attempt to improve its robustness. Combining encryption and steganography added an extra layer of security. As a result, the memo to be buried in the cover was first encoded and then concealed in the cover audio. Researchers began to combine soft computing techniques with steganography around this period. Though a single soft computing technique was used in conjunction with another to achieve a specified aim. GA became the first choice for combining with steganography to build an optimum approach. The different strategies, on the other hand, differ in their fitness function selection and GA rationale. Also developed was a steganography technique for mobile phones. The method's key benefit is its high embedding channel capacity, using only one LSB of the host audio sample results in a capacity of 44.1 kbps. The method's obvious flaw is its low robustness, which stems from the fact that random changes to the LSBs invalidate the coded system. Furthermore, integrated watermarks are unlikely to survive digital-to-analogue conversion and subsequent analogue-to-digital conversion. The basic version of this method has a very tiny algorithmic delay because LSB can now be used in real-time applications. This technique is a suitable and optimum starting point for steganographic audio signal applications as well as steganalysis.

This research concludes that there are numerous encryption approaches accessible to secure data at this time. Technology developments and novel concepts such as quantum cryptography have given data security a whole new dimension. This cryptographic technique's strength originates from the fact that no one can read (or steal) the information without changing its content. This change warns communicators of the risk of hackers, resulting in highly secure data transfer. We explored several cryptographic algorithms (encryption standards), encryption techniques for audio data, and certain encryption standards that have been employed for audio data encryption for network security purposes in this research work. With the use of these algorithms, one can create their method by modifying current ones to make audio data safer. This research paper proposes and presents a novel audio file encryption technique. This novel technique uses an advanced random procedure to encrypt data. The method is not vulnerable to statistical attacks, according to statistical analysis utilizing MSE, PSNR, correlation, and entropy. A brute-force attack on the technique is also unfeasible due to the large number of possible keys. Our experiments suggest that the proposal is effective. It's a quick and easy method that can nevertheless provide enough protection for audio files. The proposed audio cryptography approach can be used with audio steganography in the future. The combined

solution will protect not just the audio but also the text hidden within it.

Substitution approach, in which nearly all of the concealment file bits remained replaced by message bits, is the most renowned method of deployment of steganography. Substitutions were performed using the LSBs since these contribute least in the statistical value calculation of cover files. One or more than one LSBs were replaced for improving data-hiding property in cover files. However, deployment of these techniques introduced additional distortion. As LSB replacement is vulnerable to malicious and accidental attacks, a solution was proposed to hide data in deeper levels. More distortion in the concealment file was induced by hiding data in deeper levels of the concealment. Some algorithms were then demonstrated which not only embedded information in deeper levels but also changed it by changing some support parts of the cover file actively to reduce the distortion. Audio was liked as a cover file because it was readily accessible in practice and had a natural masking property.

Second, the masking impact is formed if low-frequency noise is masked with higher-frequency sound. The underlying issues of the substitute scheme remained even if sound was being used as camouflage. As such, several derivatives of the initial LSB technique were employed in attempts to make the technique more resistant. The inclusion of encryption as well as steganography allowed for an additional layer of safety. As a result, the memo to be concealed in the cover was first encoded and then concealed in the cover audio. Researchers began to combine soft computing techniques with steganography during this time. While one soft computing technique was used along with another to achieve a specified goal.

GA was the go-to choice to combine with steganography to create an optimal solution.

The diverse approaches, though, differ in their choice of fitness function and justification of GA. Another cell phone steganography approach was also created. The greatest strength of the technique is its large embedding channel capacity, using only one LSB of the host audio sample provides an embedding capacity of 44.1 kbps. The most obvious flaw in the technique is its low robustness due to the fact that random modification to the LSBs ruins the coded system. Besides, embedded watermarks cannot survive digital-to-analogue conversion followed by analogue-to-digital conversion.

Conclusion

In this paper, we've shown how important Steganography is in today's world. Audio steganography remains the practice of hiding a message within an audio file. When the LSB approach is used with other cryptographic methods like as encryption and decryption, one of the most effective and secure transport networks is created. (i) The LSB approach causes distortion in the audio cover file when utilized directly. (ii) Although the parity approach appears to be an effective technique with a high SNR, it also has a large data rate. (iii) The XORing approach demonstrates that utilizing more uwe can, by using more than a single LSB layer for data embedding, you can increase the capacity of the cover audio, but you'll be confined to a single audio format. wav. (iv) The method of embedding text in the fourth and fifth layers with the same and different data, as well as encryption and decryption of the secret message using a public key cryptographic algorithm, is a cost-effective method with low noise distortion and a high SNR and PSNR ratio. (v) When paired with GA, LSB supports a variety of file formats, including .aiff, .wav, and.AU. This approach extends the message length up to 1000 characters. This approach, however, has considerable computational complexity.

Future Scope

The results reveal that even with the changes made to the direct use of LSB, there is still room for development in terms of highly secure data retrieval, better robustness, higher data rate, full recovery of cover audio, and compatibility with various audio formats.

Refrences

[1] S. S. Divya and M. R. M. Reddy, "Hiding text in audio using multiple LSB steganography and providing security using cryptography," *International Journal of Scientific & Technology Research*, vol. 1, no. 6, pp. 68–70, 2012.

[2] P. Jayaram, H. R. Ranganatha, and H. S. Anupama, "Information hiding using audio steganography—A survey."

[3] F. Djebbar, B. Ayad, H. Hamam, and K. A. Meraim, "A view on latest audio steganography," in *International Conference on Innovations in Information Technology*, 2011, pp. 409–414.

[4] N. Kaur and S. Behal, "Audio-technology techniques survey," *International Journal of Engineering Research and Applications*, 2014.

[5] U. Mehta and D. Sihag, "Multi-part data hiding in audio steganography," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 9, pp. 8037–8039, 2014.

[6] P. Singh, "A comparative study of audio steganography techniques," *International Research Journal of Engineering and Technology*, vol. 3, no. 4, pp. 581–585, 2016.

[7] P. Jayaram, H. R. Ranganatha, and H. S. Anupama, "Information hiding using audio steganography—A survey," *The International Journal of Multimedia & Its Applications*, vol. 3, pp. 86–96, 2011.

[8] S. S. Divya and M. R. M. Reddy, "Hiding text in audio using multiple LSB steganography and provide security using cryptography," *International Journal of Scientific & Technology Research*, vol. 1, pp. 68–70, Jul. 2012.

[9] M. Asad, J. Gilani, and A. Khalid, "Three layered model for audio steganography," in *2012 International Conference on Emerging Technologies (ICET)*, 2012.

[10] P. P. Balgurgi and S. K. Jagtap, "Intelligent processing: An approach of audio steganography," in *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*, Oct. 2012, pp. 1–6.

[11] S. Imaculate Rosaline and M. Ashok Raj, "Adaptive pixel pair matching based steganography for audio files," in *2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT)*, Jan. 2013, pp. 1–5.

[12] G. Nehru and P. Dhar, "A detailed look of audio steganography techniques using LSB and genetic algorithm approach," *International Journal of Computer Science Issues*, vol. 9, pp. 402–406, Jan. 2012.

[13] P. T. Yu, H. H. Tsai, and J. S. Lin, "Digital watermarking based on neural networks for color images," *Signal Processing*, vol. 81, pp. 663–671, 2001.

[14] H. B. Kekre, A. Athawale, S. Rao, and U. Athawale, "Information hiding in audio signals," *International Journal of Computer Applications*, vol. 7, no. 9, Oct. 2010.

[15] E. Franz, A. Jerichow, S. Möller, A. Pfitzmann, and I. Stierand, "Computer based steganography," in

Information Hiding, Lecture Notes in Computer Science, vol. 1174, pp. 7–21, 1996.

[16] D. Kahn, "The history of steganography," in *Proceedings of the First International Workshop on Information Hiding*, Cambridge, U.K., May–Jun. 1996, *Lecture Notes in Computer Science*, vol. 1174, pp. 1–7.

[17] Y. Hu and P. Loizou, "Evaluation of objective quality measures for speech enhancement," *IEEE Transactions on Speech and Audio Processing*, vol. 16, no. 1, pp. 229–238, 2008.

[18] "Steganography tools." [Online]. Available: JJTC Security Steganography Tools. [Accessed: Sep. 7, 2026].

[19] "Steghide." [Online]. Available: Steghide Project. [Accessed: Sep. 7, 2026].

[20] F. Djebbar, K. Abed-Maraim, D. Guerchi, and H. Hamam, "Energy based text-in-speech spectrum hiding using speech mask properties," in *ICSRA*, China, May 2010.

[21] F. Djebbar, H. Hamam, K. Abed-Maraim, and D. Guerchi, "Controlled distortion for high-capacity data-in-speech spectrum steganography," in *6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Germany, Oct. 2010.

[22] H. Matsuka, "Spread spectrum audio steganography using sub-band phase shifting," in *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Pasadena, CA, USA, Dec. 2006, p. 36.

[23] X. Li and H. H. Yu, "Transparent and robust audio data hiding in subband domain," in *Proceedings of the Fourth IEEE International Conference on Multimedia and Expo (ICME)*, New York, NY, USA, 2000, pp. 397–400.

[24] M. Pooyan and A. Delforouzi, "Adaptive digital audio steganography based on integer wavelet transform," in *Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*, vol. 2, pp. 283–286, 2007.

[25] R. Krenn, "Steganography and steganalysis," Jan. 2004. [Online]. Available: Robert Krenn—Steganography and Steganalysis. [Accessed: Sep. 7, 2026].

[26] H. Farid, "Detecting steganographic messages in digital images," Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001. [Online]. Available: Dartmouth Technical Report TR2001-412. [Accessed: Sep. 7, 2026].

Authors and Affiliations

Mst Jannatun Ferdaush[1]

✉ Mst Jannatun Ferdaush
jannatunferdaush304@gmail.com

[1] University of South Wales, Cardiff, CF24 2FN, UK