National College of Ireland

Secure Transmission of Data using Audio Steganography and Cryptography

MSc Internship
Cyber Security

Manmeet Kumar
Student ID: x21113602

School of Computing
National College of Ireland

Supervisor: Arghir Nicolae Moldovan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Manmeet Kumar		
Student ID:	X21113602		
Programme:	MSc Cyber Security	**Year:**	2022-2023
Module:	MSc Internship		
Supervisor:	Arghir Nicolae Moldovan		
Submission Due Date:	15/12/2022		
Project Title:	Secure Transmission of Data using Audio Steganography and Cryptography		
Word Count:	7161	**Page Count:**	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Manmeet
Date: 15/12/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Secure Transmission of Data using Audio Steganography and Cryptography

Manmeet Kumar
x21113602

Abstract

Digital information such as images, text, and audio are shared through networks in this age of technology. This data transmission over the internet is vulnerable to eavesdropper interception and improper manipulation. So, security of data has become a prominent subject of research. Much study has gone into finding the best solution for text secrecy, integrity, and dependability. Audio steganography is one such approach for securely conveying or hiding sensitive data. Audio steganography is used to conceal critical info by embedding it in an audio recording. In this research study, a system is implemented that combines encryption of data and audio steganography to keep the confidentiality and integrity of exchanged data. Here, a system is implemented in which the secret data is firstly encrypted, and then the cipher data is incorporated inside an audio track by using the LSB (Least Significant Bit) technique. This study also examines how well-known encryption algorithms (AES-256, Twofish, Blowfish, and Triple DES), as well as how files of different file types & sizes (txt, docx, pdf, and jpg) affect the PSNR value. The proposed system is assessed and tested by computing the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio). Spectrogram is used for visual evaluation of audio files to evaluate if the secret data hidden in the audio cover file affects the frequencies present in the audio files. The results reveal that there is no noticeable distortion when the encrypted files are buried inside the cover audio file. Also, different file types have noticeable impact on the PSNR value than different encryption algorithms.

Keywords: Audio Steganography, LSB encoding, Encryption, File types, PSNR.

1 Introduction

Since it was first made available to the public, the internet has grown swiftly, and cybersecurity has become a constant issue. Every day, millions of human beings utilise the internet, and gigabytes of data are shared. As the quantity of persons and data shared through the internet grows, information security becomes a major concern. The 3 pillars of data security are "Confidentiality, Integrity, and Availability". An intruder can intercept critical text messages or data transferred over the internet, compromising confidentiality. As a result, ensuring the secrecy of the text messages or data over internet becomes critical. Two of the most frequent and successful methods for securing sensitive data include cryptography and steganography.

Cryptography is known as the art of hidden writing. In this procedure, a specific algorithm is utilised to encrypt the chosen message, after encryption the cipher data along with the secret key is shared to the recipient of the message. Using the same method and secret key, the recipient can decrypted the cipher message to get the original message [1]. The following are the fundamental objectives of cryptography:

- Confidentiality: No one should be able to view the message except the intended recipient.
- Integrity: Only the authorized individual is allowed to change or modify the important information or data.
- Authorisation: The identification of the recipient must be confirmed to ensure that the person reading or receiving the communication is the intended recipient.
- Availability: The availability means that if an authorised person needs the data, they should be able to obtain it without difficulty or interference.
- Non-repudiation: A methodology or procedure for proving that a communication came from a reliable source.

Steganography is the act of concealing the existence of digital data by inserting it into a different media format, such as audio, images, text, or videos. If the digital media containing the embedded data is examined, there will be no indication that any information is buried. Therefore, the person will not try to decrypt the data. Audio steganography, video steganography, and image steganography are the three types of steganography. This proposal is centred on the implementation of audio steganography. As the name indicates, audio steganography is the practise of hiding a secret inside audio tapes. Any digital material may be represented by a bit sequence. In general, two actors are engaged in audio steganography: Sender and Receiver. The secret data or message is inserted in audio file by the sender, and the secret data or message is extracted from the audio file by the receiver [2].
There are several methods for doing effective steganography, including the DWT (Discrete Wavelength Transform), Multi-Level Clustering (MLC), Dual Key Approach, and Least Significant Bit (LSB) and One of the traditional ways for steganography audio is LSB (Least Significant Bit). Because of its simplicity, it has piqued the curiosity of many scholars [3].

The feature of redundancy is what makes video and audio data ideal carriers for steganography [4]. Because of the presence of duplication, the cover audio input used before and after steganography sounds identical [4]. Because the HAS (Human Auditory System) is significantly delicate than that of the HVS (Human Visual System), audio steganography is regarded much challenging than video or picture steganography [5]. Although a lot of research study has been performed in the subject of encryption and steganography, malicious attackers are continually finding complex and new ways to exploit publicly available and undisclosed vulnerabilities.

1.1 Research Question

Que - How can the security and authenticity of crucial data be preserved during transmission utilising audio steganography and cryptography. Also, how different encryption algorithms and file types affect the PSNR value?

The proposed system's goal is to ensure data secrecy during transmission by combining audio steganography with data encryption. Steganography gives some level of secrecy, but if the malicious actor discovers that the steganography is being used, he/she could rapidly decipher it. To counter it, the data is first encrypted and then it is hidden inside a cover file. In the proposed approach, files of different file types and sizes (txt, docx, pdf, and jpg) is encrypted using different types of encryptions (AES-256, Twofish, Blowfish, and Triple DES) and then by using LSB method, cipher data is embedded within cover audio files. The use of different types of files and encryption algorithms adds the novelty to this research.

This research paper also describes the results of experiments with secret data concealment utilizing data encryption and audio steganography. The produced stego audio's PSNR was compared to the original cover audio's PSNR to see how effectively the data is hidden in the cover audio file.

1.2 Report Structure

The layout of the research paper is defined below:
Section 2 of the paper includes an extensive literature assessment of past work in the subject of steganography and cryptography. The next part, Section 3, discusses the research methods used to get the intended outcomes. The following two parts, Sections 4 and 5, cover the design requirements of the suggested solution as well as the implementation phase. The final two sections, 6 and 7, represent the learning results, conclusions, and future work that may be performed to overcome them.

2 Related Work

To understand the novelty of the study, a full literature review is required to understand about the relevant efforts and work carried out by the other researchers who’ve already done and published research in the field of cryptography and steganography. Only by

analysing prior research in the relevant domains can new techniques be discovered or invented, or existing work be improved.

2.1 Steganography

Steganography is at the heart of the suggested approach; it is the way of concealing information or data in a audio cover file, picture or video file. Steganography is sometimes mistaken with cryptography, however the two are extremely distinct.

2.1.1 Audio File

Using audio for steganography is a tough task since the HAS (Human Auditory System) is regarded to be significantly sensitive than the HVS (Human Visual System). As per (Asad et al., 2011) [4], because of the existence of repetition, audio steganography is conceivable. To accomplish audio steganography, a technique that operates against the HAS should be applied; the technique should meet capability, transparency, and resilience. The amount of info or data that can be contained within a cover audio file is known as capability; how effectively the info or data is integrated is known as transparency; and the embedded secret info or data ability to survive assaults is known as robustness [4]. There are several audio files formats available, with .wav and .mp3 being the most often used for steganography. (Lindawati and Siburian, 2017) [6] have employed both .mp3 and .wav files as a cover audio file for steganography in their research paper. They employed PSNR to assess the quality of the reconstructed file which is an audio file. This research revealed that steganography is of bad quality if the value of psnr is 30 dB or less and that audio hiding quality is greater in WAV files over MP3 files. [6].

2.1.2 Low Bit Encoding

One of the most popular ways of audio steganography is LSB. LSB gives the best in class un-detectability [7] which is useful if the attacker obtains the audio file, but the issue is that it is not as strong or enough resistant and has a rate of low embedding.
In 2012, (Nosrati et al., 2012) [8] study looked at the core concepts and methods of audio steganography, such as spread spectrum, parity coding, echo data hiding, LSB, and phase coding. It also investigated current advancements in the industry. “Embedding data between frames in an MP3 file”, “Considering Parity and XORing of LSB's”, “Audio Wave Steganography”, “Modifying Quantized Spectrum Values of MPEG/Audio Layer III”, “Genetic Algorithm-Based Audio Steganography”, “Quantized frequency domain embedding and reversible integer transforms”, and others were among them. In 2011, (Ahmed and Ali, 2011) [9] suggested a Secure information hiding system (SIHS) where the secret data or message was hidden in an image with the use of LSB technique. By randomly distributing the message's bits throughout the image, this approach improves on the LSB method by rendering it difficult for unauthorised users to decrypt the original data or message. The discrete logarithm technique is used to compute the position of the bits within the pixels to insert the message. The proposed approach generates a stag-key, which will be used for message embedding and extraction. The major themes of this

research paper were the LSB technique and image steganography. Considering that LSB is vulnerable to steganalysis, several additional safeguards are necessary.
In 2012, research study by (Balgurgi and Jagtap 2012) [10] advocated integrating the least significant bit methodology with the method of XORing. Because LSB is quite simple to employ but prone to steganalysis, it is employed in conjunction with the method of XORing to prevent this issue. The Least significant bits are treated to an operation of XOR in this manner and based on the result and the message bit to be encapsulated, the LSB of the data sample would either modified or left intact. This method may be made more secure against detection by combining multiple data-hiding mechanisms. This study by (Datta et al., 2015) [11] improves on prior work. They proposed incorporating 2 data bits at once onto cover media to improve capacity and employing numerous layers of LSB encoding to increase resilience. Because bitwise operations are used for extraction, it is quite difficult to acquire the real information or data with this approach. The perceived clarity of stego audio file is preserved by final bit correction and flag configuration. In all these studies, security may be enhanced by applying strong encryption, as using the LSB method alone can result in data theft via steganalysis.

In 2016, study by (Jadhav and Rawate, 2016) [12] provided an exciting strategy for incorporating all necessary info in the cover audio's selected spots in 2016. The embedding position was determined using the top 3 bits of MSB of the cover cover file. They added an extra key which is a secret key utilizing CES (Chaotic Encryption Scheme), which boosted security. The private data or message was 1st encrypted utilizing CES and after that incorporated within a 16-bit pattern utilizing an audio file of WAV type in their investigation. This technique lacks security since LSB is vulnerable to steganalysis and the CES is considered to be risky encryption. Then, in 2017, research by (Rajput et al., 2017) [7] carried forward [12]'s study and provided an effective method of implementing audio steganography. Two algorithms were provided in the proposed work: Algorithm-I inserts 2 secret message bits of data at one time on the positions of LSB of porter audio file depending on the porter audio's 3 MSBs. This method increased embedding capacity by inserting 2 data bits at the same time. Algorithm-II inserts 2 data bits on the places of LSB of the porter audio, depending on the compliment of 3 MSBs of carrier audio. This method improves resistance against assaults. Extra security is offered by utilising a key which is secretin nature.

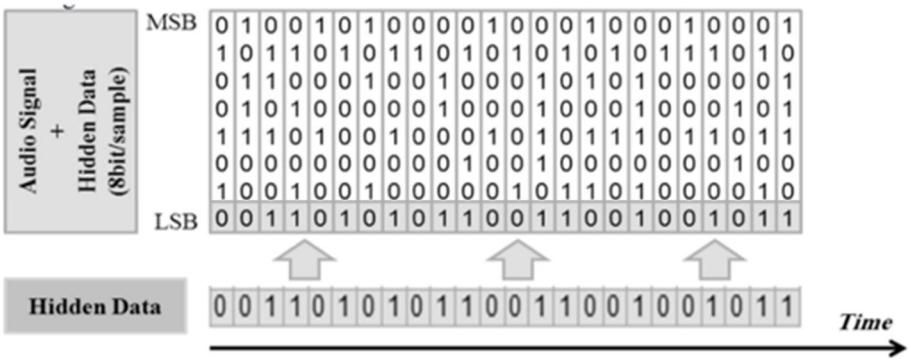

Figure 1: LSB in 8bits per sample signal is overwritten by one bit of the embedded data.[3]

In the year 2019, research by (Sobin and Manikandan, 2019) [13] conducted a comparison & analysis of two distinct audio steganography methods. The first integrated steganography and cryptography concepts to create a new app for audio steganography. They advocated employing a variety of security levels. The hidden message was encrypted on the first level of security with the RSA technique and then placed in a cover audio file with typical audio steganography by LSB method. In the 2nd way, they created a powerful genetic algo which is on the basis of LSB data concealing strategy and disguised the info or message as audio. When the data are analysed, the 2nd method—the Genetic Algorithm—showed a far superior PSNR ratio than the 1st method, which uses the RSA algorithm. As a result, the second option is preferable. Furthermore, RSA is a terrible solution for little audio files. (Mohajon et al., 2018) [14] takes a similar method of utilising a genetic algorithm. They employed a genetic method, but with a symmetric security key of K bits. They used a genetic algorithm in their study to put the info or message into the audio file, and they increased the security by utilising a K-bit key of security that may provide within 8 & 15 MSB positions when message bits were compared. Very limited information was offered by them about if they utilised per-existing encryption algorithm or developed their own.

Another intriguing technique was presented in 2019 research by (Anwar et al., 2019) [15]. The goal of this study was to create an Android app which allows marking of frame, Encryption of dynamic key, and the LWT insertion of data which is secret in nature into audio file. In place of manually inputting the value of Dynamic key throughout the deciphering procedure, the communication might be deciphered utilising a designated frame. During the course of process of testing, it was observed that using this strategy might result in up to 20% audio loss. Because this initiative is still in its early stages, further investigation is necessary.

There were various inventive and intriguing techniques tried to develop and apply the LSB methodology of audio steganography. Other new and intriguing ideas are explored in [16], [17], and [18]. These studies concluded that LSB is insufficiently safe on its own because to its low resilience, low insertion rate, and vulnerability to steganalysis. For fail-safe circumstances, another technique or extra security procedures are necessary.

2.1.3 DWT Algorithm

The discrete wavelet transform (DWT) technology is relatively new in comparison to LSB-based alternatives, and many researchers are attempting to enhance it. The capacity to break the data into low- and high-frequency elements is the essential capability of DWT. Although the top area contains the elements of signal's edge, the bottom parts contain the majority of the signal's data. Majority of the signal's data is once again divided into 2 parts. For each partition, the algorithm of DWT is employed, initially vertically followed by the directions horizontally.

During 2014, this study by (Geethavani et al., 2013) [19] introduced a revolutionary approach of combining audio steganography with cryptography components. First, the information or data that must be sent is encrypted using a tweaked blowfish method. The

corresponding output ciphertext is then disguised within a cover file of audio type utilising the DWT method. After receiving the stego audio, the initial information or data is recovered via the reverse technique. The downsides of using DWT include higher degrees of distortion in audio than LSB, that leads in more incorrect data.

In the year of 2016, a study by (E. et al., 2016) [20] suggested using a hybrid approach that combines techniques of steganography and cryptography to give 2 levels of protection. The suggested method first encrypts the secret info or data with AES, considered to be the most secure method till now, before concealing it inside grey picture with the "PVD-MPK" and "MSLDIP-MPK" approaches. The results of the performed experiment indicated that the suggested strategy might be used to embed substantially a lot more info than approaches currently in usage, and it greatly improves the quality of visual of the stego image. One disadvantage of this study is that it only concentrated on picture steganography and solely on grayscale photos.

DWT is used for a variety of research purposes, however it has significant downsides, such as more audio distortion than LSB, which leads to more erroneous data. However, there are some advantages to adopting DWT, such as temporal frequency representation.

2.2 Encryption

Encryption is a critical component of the suggested approach; it is the process of turning clear text into a ciphertext utilising encryption keys. Decryption is the process of obtaining the original message by utilizing the decryption key. Encryption ensures that the information being sent remains private.

(Torvi et al., 2016) [21] secures data transfer using a novel text steganography approach. It uses XOR encryption to encrypt the payload before employing steganography. The straightforward yet effective technique is utilised here. However, writing lacks the randomization that audio steganography may give. There are several encryption techniques available to ensure data secrecy. They are picked based on the criteria. (Abood and Guirguis, 2018) [22] compares several algorithms based on the structure, key size, number of rounds, block size, flexibility, and features to find which is best for encryption. "DES", "DH", "E-DES", "RSA", "T-DES", "ECC", "RC4", "RC2", "BLOWFISH", "SEAL", "DSA", "RC6", and "AES" were the algorithms used. After analysing numerous aspects, the author claims that the method was chosen on the basis of criteria. "AES", "Blowfish", "RC4", "E-DES", and "TDES" are the most efficient in terms of time for encryption, speed, adaptability, and security. The results reveal that AES encryption is superior in terms of all the aspects. AES method offers outstanding security, is least resistant to assaults, and has the greatest avalanche effect, making it perfect for text encryption when secrecy and integrity are important, as demonstrated by (Semwal and Sharma, 2017) [23]. A novel mix of LSB embedding and Rijndael text encryption is exhibit by (Hashim et al., 2018) [24]. Employing the LSB bit for substitute with payload bits using the MSB (most significant bits). The encryption of the text using AES before embedding improves its security. Text alone is fragile; thus, the plain text is encrypted with AES to ensure resilience. AES will be utilized for encryption based on the artefacts.

Taking inspiration from the previously described studies, this research offered a method that will eliminate the constraints of the previously discussed publications. This suggested paradigm is designed with safety at every level in mind. A hybrid security technique including steganography and cryptography is used to protect the transport of sensitive data. The secret data file will be encrypted using several encryption methods before being embedded into audio files using the LSB technique. To investigate the effect of these factors on PSNR values, several file types and encryption techniques are utilized.

3 Research Methodology

The difficulty with the advancement of technology is the confidentiality and integrity of data. Much research has been conducted to ensure data security and integrity, as stated in the preceding section. Because the described methodologies have both strengths and drawbacks, a new strategy is required to address all the shortcomings in present methodology. To ensure the secrecy and integrity of hidden data, a unique type of audio steganography is developed. The suggested approach employs a mix of steganography and encryption for effective message or data transfer with little sacrifice on carrier quality and strong protection of the secret message or data from attackers. The encryption algorithm is utilised to encrypt the message or data, which ensures secrecy, and the technique of audio steganography is utilised to conceal the message or data for more imperceptibility. The method seeks to increase imperceptibility and the security of critical message or data while making no obvious modifications to the cover file.

Visual studio code editor, a Microsoft source-code editing tool, is necessary for application development [25]. The Kali Linux tool "Steghide" a steganography application that conceals bits of a data file within some of the least relevant bits of another file, is also required. This tool hides data file in such a way that its presence is not apparent and cannot be verified. Steghide can also help with digital forensics investigations [26].

3.1 Encryption

Encryption is a means of encrypting data so that it can only be deciphered by authorized entities. In technical terms, it is the method by which human-readable text to unreadable text, also known as ciphertext. In proposed solution, data files are encrypted using 4 well-known and used encryption algorithms. Those 4 encryption algorithms are AES-256, Twofish, Blowfish, and TripleDES. According to the literature analysis completed in the preceding section, these four encryption algorithms are the best in class algorithms which could be employed in situations where data integrity and secrecy are of the utmost importance [22]. Following an examination of the literature on various cryptographic algorithms, the decision to adopt these four algorithms was taken. The reason for utilising 4 different encryption techniques is to explore the impact of these different algorithms on the resulting PSNR value. The greater the value of PSNR, the better the quality of Stego

audios. Encryption of data files are done using Steghide tool [26]. This tool is used for the ease of implementation.

3.2 Least Significant Bit (LSB)

Steganography employs a variety of approaches. LSB-based steganography is among the most used ways. This approach is simple to use, and messages may be disguised discreetly. In compared to other techniques, the distortion rate in LSB is quite low. The main idea is to replace the audio file's lowest bits with the message's bits [6].

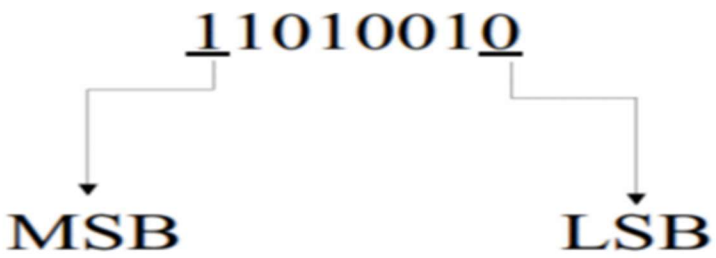

Figure 2: MSB and LSB [6].

As shown above, the 0 bit is the LSB, whereas the 1 bit is the MSB.

Assuming the message is 10 bits long, resulting in multiple bytes consumed = 10 bytes.

00110011 10100010 10100011 00100110
01011001 01101110 10110101 00010101
11100110 11011010

If the binary value of the message is 1110101011, the resulting binary will be:

00110011 10100010 10100011 00100110
01011001 01101110 10110101 00010101
11100110 11011010

According to the notion presented above, the entire message is encoded in the audio.

The LSB algorithm requires two inputs, one of which is the cover audio file and the other is cipher data or text. Once retrieved, the ciphertext must be hidden in an audio file. After completing literature research, it was discovered that the LSB method is the most often used, easiest to implement, and has a very low distortion rate in contrast to other techniques.

3.3 Dataset Used

The dataset used in this study was obtained from IEEE DataPort, a platform built and maintained by IEEE that delivers internationally accessible datasets to academics, data analysts, and the worldwide technical community. The dataset is developed by "State Key Laboratory of Information Security", "Institute of Information Engineering Chinese Academy of Sciences and School of Cyber Security", and "University of Chinese Academy of Sciences" [27] .

Table 1: Dataset Summary

No. of Audio Files	Type of File	Sampling Rate	Duration	Size per audio
1000	WAV	44.1 kHz	10 sec	1.68 MB

One of the objectives of this research is to evaluate the effects of several encryption methods (AES-256, Twofish, Blowfish, and TripleDES) and different data files to be embed (txt, docx, pdf, jpg) on audio steganography. The number of cover audio files from the dataset used in this research is 100. The reason for choosing just 100 from 1000 audios is because all the audio files have exact same properties as can be seen in above table. Also, using all 1000 audio files will results in 16000 stego audio (1000 * 4(types of file) * 4(type of encryption)) which is very high resource intrinsic. The stego audio files in this research is generated using Steghide tool.

Data files used in encryption and embedding are of 4 different types: txt, docx, pdf and jpg. The data in these files is taken from a public domain blog on "What is Steganography" by comptia.org [28]. Details below:

Table 2: Data Files Summary

File Name	Size
Secret-txt.txt	45 KB
Secret-docx.docx	22 KB
Secret-pdf.pdf	37 KB
Secret-jpeg.jpg	42 KB

3.4 Evaluation Metrics

For the evaluation, below metrics are used [29]:

a) **MSE (Mean Square Error)**: The MSE is determined by data comparison of each of the cover audio sample prior to and after insertion. Its numerical result represents the squared difference between the values of the 2 matching samples in the audio cover and the stego audio. The greater the MSE value, the greater the risk of embedding detection if intruders access the stego audio. The formula for computing MSE is:

$$MSE = \frac{1}{N}\sum_{n=1}^{N}(c_i - s_i)^2,$$

where c_i and s_i indicate the i^{th} sample of the audio file cover and the stego audio, respectively, and N represents the total no of samples.

b) **PSNR (Peak Signal to Noise Ratio)**: The quality of a signal's representation is influenced by the ratio of its maximum potential value (power) to the amount of distorting noise. The PSNR is calculated by the comparison of the MSE with the value of sample with the highest value in the original cover audio. This sample value, represented by I_{max}, takes into account the max no. of characters that may be buried inside the audio file. In this case, the I_{max} value is the sampling rate.

$$PSNR = 10\log\left[\frac{I_{max}^2}{MSE}\right].$$

c) **Spectrogram:** A spectrogram is a visual representation of the frequency spectrum of a signal as it changes over time [30].

4 Design Specification

The Design specification part of the research study is intended to depict and expound on the architectural system ‘s viewpoint created by incorporating the algorithms and components covered in the section of methodology. Various diagrams are created in this area for deeper study and a better knowledge of the prototype solution.

4.1 Block Diagram

It is a visual depiction of a system's principal components or operations using blocks. The relationship between the blocks is illustrated by connecting them with lines.

As steganography and cryptography are employed in the proposed system, it is vital to understand how they function. The block diagrams below depict the fundamental process of symmetric key encryption and steganography.

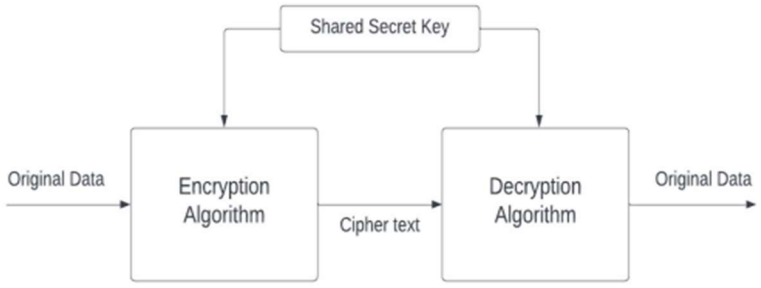

Figure 3: Symmetric Key Encryption Basic Process

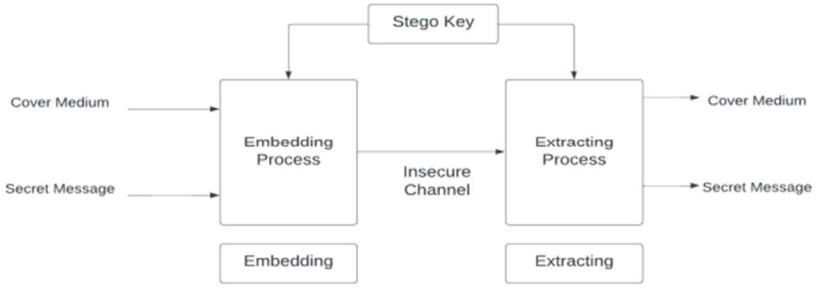

Figure 4: Steganography Basic Process

4.2 Embedding Process

1. Using the LSB approach, the suggested solution embeds the data file within the cover audio. The proposed solution initially takes the secret data file, secret key, and cover audio as input.
2. Using encryption algorithms (AES-256, Twofish, Blowfish, TripleDES), the secret data file (txt, docx, pdf, jpg) is encrypted.
3. Utilising the LSB approach, the cipher data file is embedded within the original audio file.
4. The Stego audio file is generated.
5. The Stego file and Secret key is sent to receiver by some means.

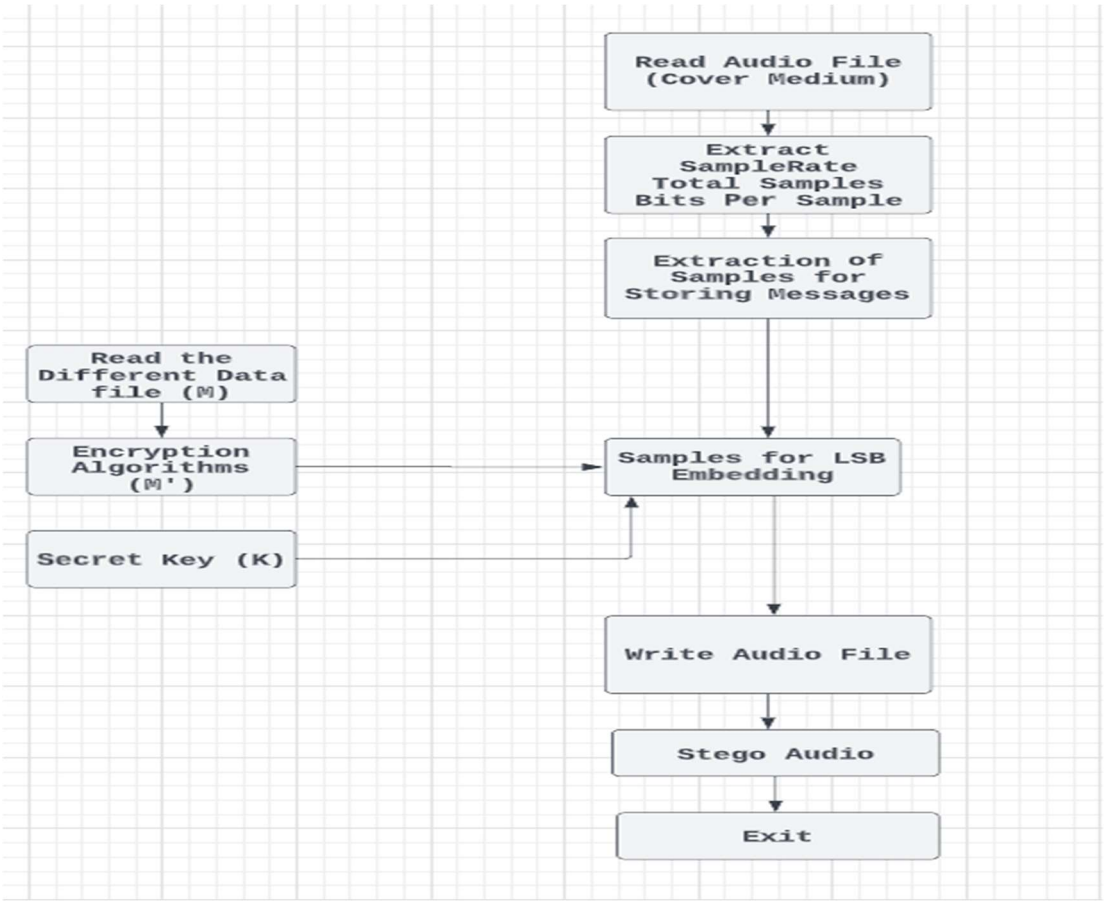

Figure 5: Embedding Process

4.3 Extraction Process

1. The Recipient receives the Secret key and Stego audio file.
2. The Extracted secret key from Samples is matched with User provided secret key.
3. Only if both keys match, the encrypted data file is retrieved from the Stego file.
4. Utilising the same encryption algorithm, the encrypted data file is decrypted.
5. Original data file is taken out from the Stego audio file.

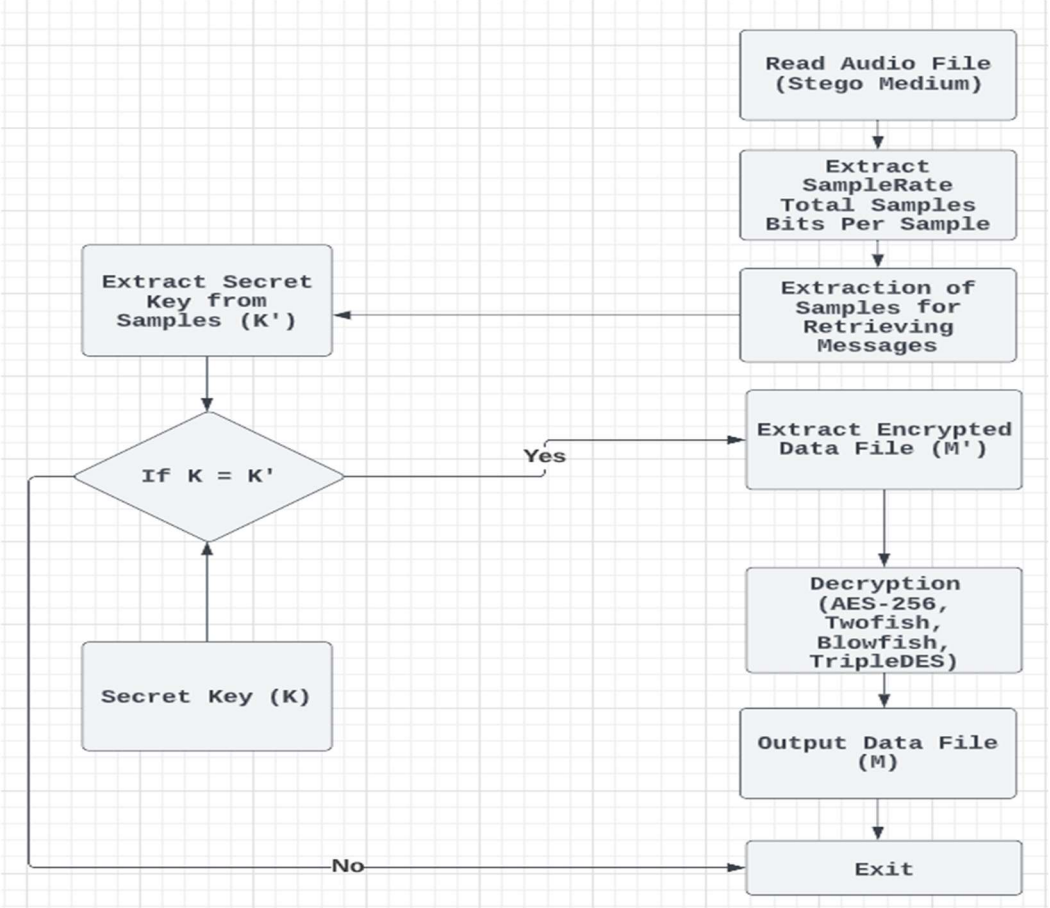

Figure 6: Extraction Process

5 Implementation

The proposed solution is implemented in a Kali Linux VM using Python 3.10.8 coded in Visual Studio to automate the process of retrieving cover files & secret data files, performing encryption & embedding, computing MSE & PSNR values, and finally saving all required data to a CSV file for evaluation. To perform encryption & embedding of data using LSB method Steghide tool is used.

Code in Figure 7, fetch cover audio files and secret data files from respective folders for performing encryption and embedding.

```
coverFiles = []
secretFiles = []
for i in os.listdir('/home/kali/Desktop/Coverfiles/'):
    coverFiles.append(i)
# print(coverFiles)

for i in os.listdir('/home/kali/Desktop/Secret-message/'):
    secretFiles.append(i)
# print(secretFiles)
```

Figure 7: Reading Cover audio files and Secret data files

Code in Figure 8, perform 4 types of encryptions (AES-256, Twofish, Blowfish, TripleDES) on 4 different type of secret data file (txt, pdf, docx, jpg), embedded these encrypted data file into cover audios and save resulting stego audio into a folder.

```
cmd = 'steghide embed -cf /home/kali/Desktop/Coverfiles/'+cvFile+' -ef /home/kali/Desktop/Secret-message/'+sctFile+' -p Pass@123@ -e '+ency+' -sf /home/kali/Desktop/Embedfiles

print(subprocess.getoutput(cmd))
```

Figure 8: Steghide command for Encryption & Embedding

Code in Figure 9, compute MSE and PSNR for purpose of evaluation.

```
def PSNR(original, compressed):
    signal1, sr1 = sf.read(original,dtype='float32')
    signal2, sr2 = sf.read(compressed,dtype='float32')
    err = np.mean((signal1 - signal2) ** 2)
    mse = sqrt(err)
    if(mse == 0):  # MSE is zero means no noise is present in the signal .
                   # Therefore PSNR have no importance.
        return 100
    max_pixel = 65536
    psnr = 20 * log10(max_pixel / mse)
    result=[psnr,mse]
    return result
```

Figure 9: PSNR & MSE Calculation

Code in Figure 10, take all the relevant data fields and their values and saves them into a CSV file.

```
import csv
with open('thesisOutput.csv', 'w') as csvfile:
    fieldnames = ['CoverFile', 'CoverFile_size','SecretFile','SecretFile_size','Encryption','outputFile','PSNR','MSE']
    writer = csv.DictWriter(csvfile, fieldnames=fieldnames)
    writer.writeheader()
    for i in csvData:
        writer.writerow(i)
```

Figure 10: Data saving in CSV

The resultant CSV looks like below.

CoverFile	CoverFile_size	SecretFile	SecretFile_size	Encryption	outputFile	PSNR	MSE
wav10s20221214_00033.wav	1.682327271	Secret-jpeg.jpg	0.040212631	rijndael-256	wav10s20221214_00033_Secret-jpeg_rijndael-256.wav	96.72780354	1.39E-05
wav10s20221214_00033.wav	1.682327271	Secret-jpeg.jpg	0.040212631	twofish	wav10s20221214_00033_Secret-jpeg_twofish.wav	96.72792187	1.39E-05
wav10s20221214_00033.wav	1.682327271	Secret-jpeg.jpg	0.040212631	blowfish	wav10s20221214_00033_Secret-jpeg_blowfish.wav	96.7565866	1.38E-05
wav10s20221214_00033.wav	1.682327271	Secret-jpeg.jpg	0.040212631	tripledes	wav10s20221214_00033_Secret-jpeg_tripledes.wav	96.72406854	1.39E-05
wav10s20221214_00033.wav	1.682327271	Secret-docx.docx	0.021067619	rijndael-256	wav10s20221214_00033_Secret-docx_rijndael-256.wav	98.0608508	1.02E-05
wav10s20221214_00033.wav	1.682327271	Secret-docx.docx	0.021067619	twofish	wav10s20221214_00033_Secret-docx_twofish.wav	98.18329543	9.96E-06
wav10s20221214_00033.wav	1.682327271	Secret-docx.docx	0.021067619	blowfish	wav10s20221214_00033_Secret-docx_blowfish.wav	98.09973116	1.02E-05

Figure 11: Resultant CSV

6 Evaluation

The quality of steganography used is defined by the Stego audio quality. The quality of an audio file can be determined using a variety of characteristics; in this research study, PSNR and MSE are utilised to assess the stego-audio quality.

100 WAV audio files were chosen at random from a dataset of 1000 WAV audio files for audio steganography implementation and data concealing efficiency research. At the first stage, the secret data files of 4 different file types (txt, docx, pdf, jpg) were encrypted using 4 well-known encryption algorithms (AES-256, Twofish, Blowfish, TripleDES). After encryption, these cipher data files were embedding into 100 cover audio files. This test is carried out to investigate the effect of different file formats and encryption techniques on the PSNR value. Variations in PSNR provide information into the concealing efficacy of the used steganography technology.

6.1 PSNR and MSE Results

Table 3 shows Mean, Standard Deviation, and Ranges of the PSNR for various types of encryption algorithms. As shown in below table, Encryption algorithms doesn't seem to have a major impact on PSNR values. All 4 of them have similar PSNR ranges which lies between 95.50 to 101.90.

Table 3: RANGES OF PSNR VALUES FOR DIFFERENT ENCRYPTION ALGORITHMS

Encryption Algorithm	PSNR Range	Mean	Std. Deviation
Rijndael-256	95.66 to 101.65	97.154	1.034
Twofish	95.59 to 101.47	97.156	1.036
Blowfish	95.53 to 101.82	97.157	1.036
TripleDES	95.50 to 101.47	97.158	1.037

Table 4 shows Mean, Standard Deviation, and Ranges of the PSNR for various types of file types. As shown in below table, File types have a noticeable effect on PSNR values. All 4 of them have noticeable difference in PSNR ranges. Text file has the most difference while JPEG file has the least difference in PSNR range.

Table 4: RANGES OF PSNR VALUES FOR DIFFERENT TYPES OF SECRET DATA FILE

File Type	PSNR Range	Mean	Std. Deviation
Text file (.txt)	95.59 to 101.82	97.157	1.039
Document file (.docx)	95.91 to 98.52	97.154	1.036
Adobe Reader file (.pdf)	95.50 to 97.18	97.152	1.035
JPEG file (.jpg)	95.53 to 96.93	97.151	1.035

Examples of the experiment results are in Table 6 and Table 7.

Table 5: PSNR and MSE values for different encryption and file types for the cover file wav10s20221214_00001.wav

CoverFile	CoverFile_size	SecretFile	SecretFile_size	Encryption	PSNR	MSE
wav10s20221214_00001.wav	1.68 MB	Secret-jpeg.jpg	0.040212631 MB	rijndael-256	96.78293953	1.37E-05
				twofish	96.80835114	1.37E-05
				blowfish	96.81069723	1.37E-05
				tripledes	96.81526170	1.36E-05
		Secret-docx.docx	0.021067619 MB	rijndael-256	98.29757478	9.70E-06
				twofish	98.27080640	9.76E-06
				blowfish	98.34994903	9.58E-06
				tripledes	98.24795841	9.81E-06
		Secret-pdf.pdf	0.035646439 MB	rijndael-256	97.03740870	1.30E-05
				twofish	97.07475484	1.29E-05
				blowfish	97.04651395	1.29E-05
				tripledes	97.03009474	1.30E-05
		Secret-txt.txt	0.043862343	rijndael-256	100.6239373	5.68E-06

			MB	twofish	99.6437907	7.11E-06
				blowfish	100.7321121	5.54E-06
				tripledes	99.9706852	6.60E-06

Table 6: PSNR and MSE values for different encryption and file types for the cover file wav10s20221214_00052.wav

CoverFile	CoverFile_size	SecretFile	SecretFile_size	Encryption	PSNR	MSE
wav10s20221214_00052.wav	1.68 MB	Secret-jpeg.jpg	0.040212631 MB	rijndael-256	96.75675456	1.38E-05
				twofish	96.75462152	1.38E-05
				blowfish	96.7505292	1.38E-05
				tripledes	96.73690809	1.39E-05
		Secret-docx.docx	0.021067619 MB	rijndael-256	98.13002634	1.01E-05
				twofish	98.20390486	9.91E-06
				blowfish	98.15188847	1.00E-05
				tripledes	98.08978501	1.02E-05
		Secret-pdf.pdf	0.035646439 MB	rijndael-256	97.03255724	1.30E-05
				twofish	97.03231216	1.30E-05
				blowfish	97.04143697	1.30E-05
				tripledes	97.06206439	1.29E-05
		Secret-txt.txt	0.043862343 MB	rijndael-256	99.36167773	7.59E-06
				twofish	99.71724125	6.99E-06
				blowfish	101.0284705	5.17E-06
				tripledes	100.7006303	5.58E-06

As seen in the above tables, the created system delivers high-quality encryption and steganography. PSNR levels are high according to the statistical study. However, MSE is more in a few cases. The preceding tables also illustrate that steganalysis techniques cannot easily discover text files and documents since they have higher PSNR value as compared to PDF and JPEG files.

6.2 Spectrogram Results

For visual evaluation of the experiment spectrogram is used. Spectrogram computes a signal's short-time Fourier transform. Below is the original audio file spectrogram (wav10s20221214_00001.wav).

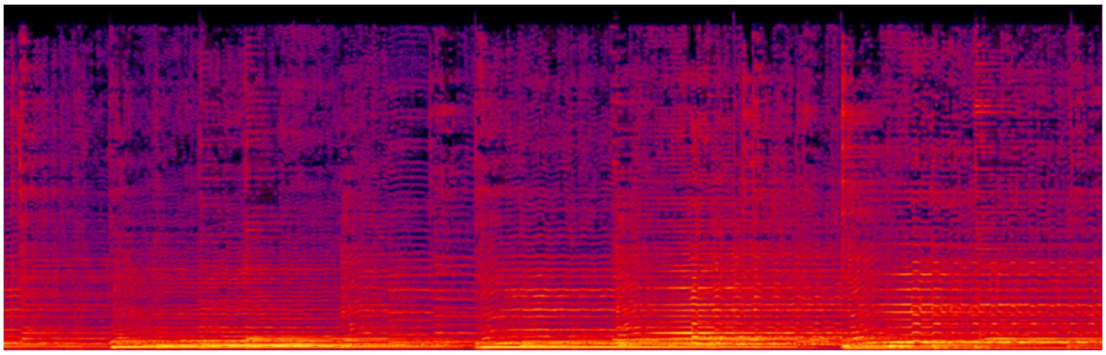

Figure 12: Original Audio File Spectrogram

6.2.1 Case Study 1

A 45 KB text file is encrypted using AES-256 and then inserted in the original cover audio file. The resultant spectrogram is shown below. MSE and PSNR values are 5.68E-06 and 100.62 respectively. The PSNR value is quite high which shows that the quality of compressed audio is quite high. There is no noticeable difference between the produced spectrogram and the original spectrogram.

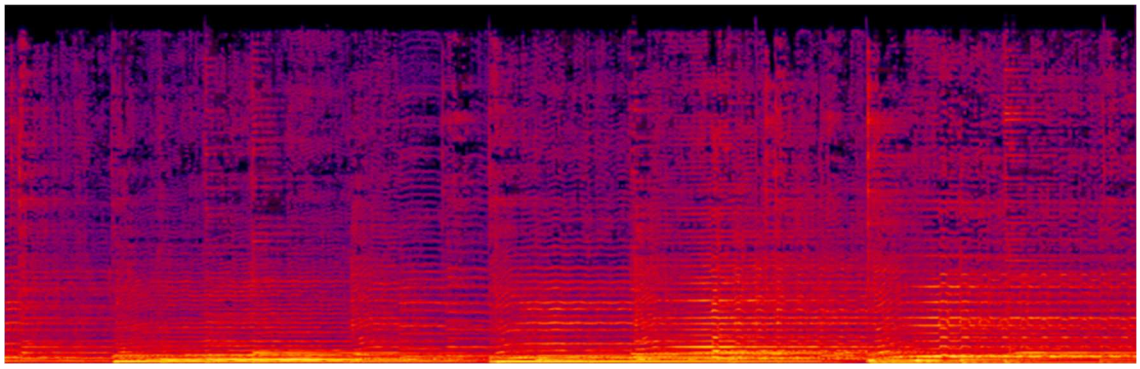

Figure 13: Spectrogram in Case 1

6.2.2 Case Study 2

A 22 KB docx file is encrypted using AES-256 and then placed in the original cover audio file. The resultant spectrogram is shown below. MSE and PSNR values are 9.70E-06 and 98.29 respectively. The difference between resulting spectrogram and the original spectrogram can’t be noticed because of high PSNR value.

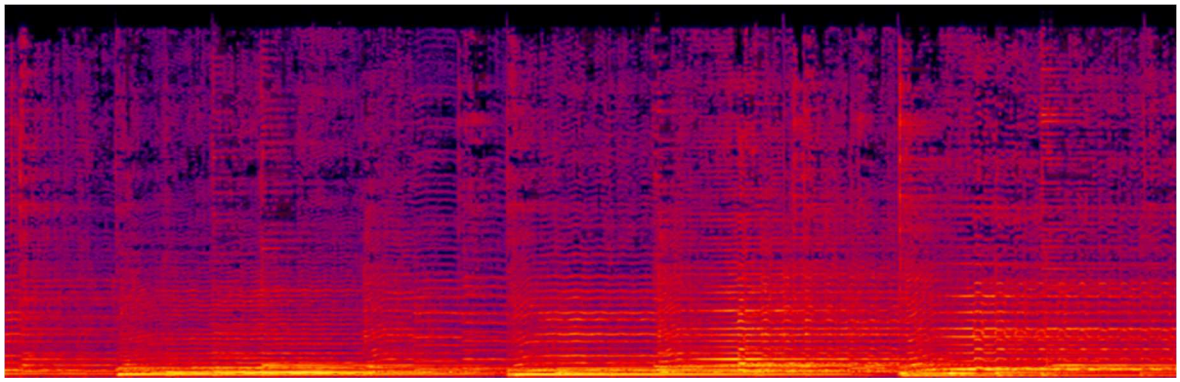

Figure 14: Spectrogram in Case 2

6.2.3 Case Study 3

A 37 KB PDF file is encrypted using AES-256 and then inserted in the original cover audio file. The resultant spectrogram is shown below. MSE and PSNR values are 1.30E-05 and 97.03 respectively. The difference between resulting spectrogram and the original spectrogram can't be noticed because of high PSNR value.

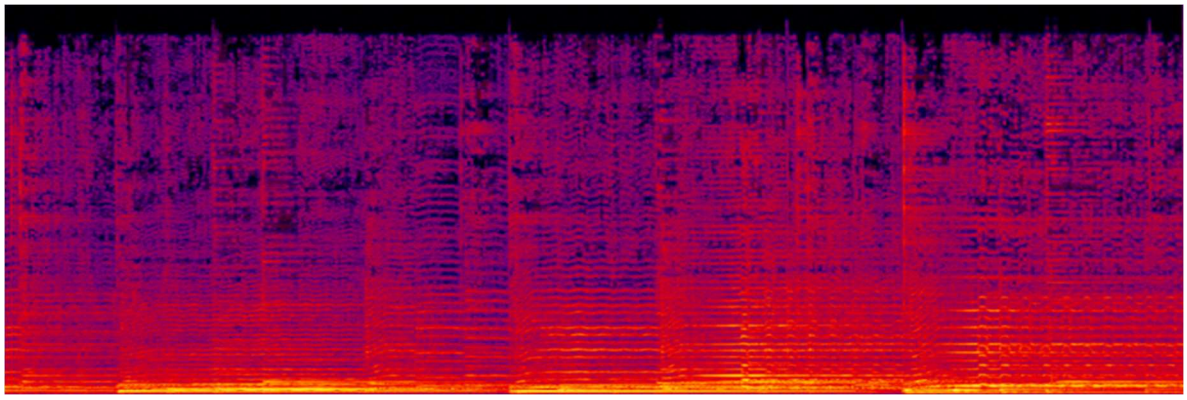

Figure 15: Spectrogram in Case 3

6.2.4 Case Study 4

A 42 KB JPEG image is encrypted using AES-256 and then placed in the original cover music file. The resultant spectrogram is shown below. MSE and PSNR values are 1.37E-05 and 96.78 respectively. The difference between resulting spectrogram and the original spectrogram can't be noticed because of high PSNR value.

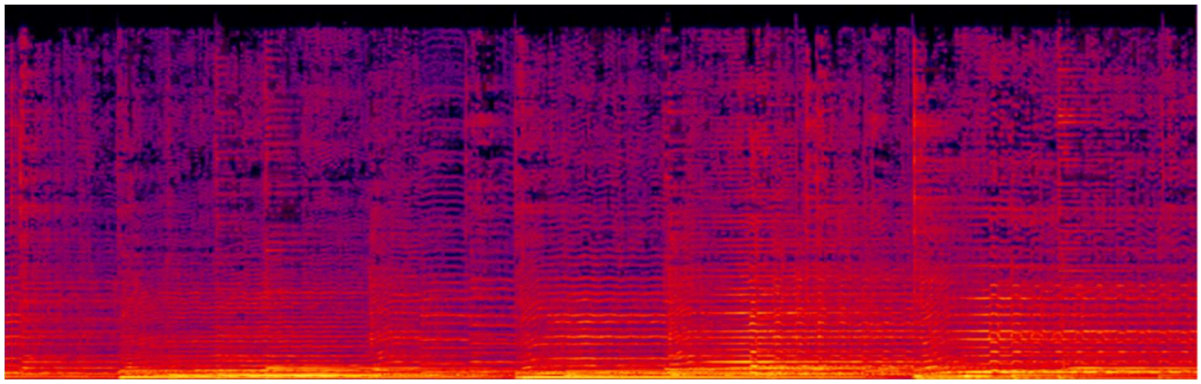

Figure 16: Spectrogram in Case 4

7 Conclusion and Future Work

An intruder can intercept simple text messages transferred over the internet, compromising confidentiality. This research successfully demonstrated a way for encrypting data files using encryption algorithms and masking the cipher data file produced using the LSB algorithm in a cover audio file. This study report also demonstrated the effect of many well-known encryption techniques, as well as varied file types and sizes, on the PSNR value. In the evaluation section, table 3 and 4 answer our research question as they shows that different file types have a major impact on PSNR values whereas that is not the case with different encryption algorithms. There are several ways offered for steganography and encryption, each with its own set of pros and downsides. Steganography fails when the malicious user discovers that it has been used, hence it is critical to keep the steganography secret. To preserve the steganography hidden, there ought to be no obvious distinction between the quality of the source and Stego-audio files. The proposed method produces high-quality steganography with no visible changes in the cover file after steganography. As proven by spectrograms, PSNR, and MSE values, the proposed approach hides the cypher data in the cover audio recording with minimal changes and without harming the quality. If the attacker/intruder succeeds in breaking the steganography, he won't be able to access the ciphertext since the message is encrypted first before steganography is performed. The suggested technique effectively offers secrecy to the given basic text.

In the proposed solution, only wav audio file type is used, in the future different audio file formats can be used as cover audio to embed data. Different file types such as video can be utilised as the cover file to efficiently disguise the encrypted message or data. Several combinations of encryption and steganography technologies might be explored to provide confidentiality to the input data.

8 References

[1] "Cryptography and its Types," *GeeksforGeeks*, Jul. 08, 2019. https://www.geeksforgeeks.org/cryptography-and-its-types/ (accessed Dec. 15, 2022).

[2] "What is Steganography? A Complete Guide with Types & Examples," *Simplilearn.com*, Oct. 25, 2021. https://www.simplilearn.com/what-is-steganography-article (accessed Dec. 15, 2022).

[3] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, no. 1, p. 25, Oct. 2012, doi: 10.1186/1687-4722-2012-25.

[4] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," in *International Conference on Computer Networks and Information Technology*, Jul. 2011, pp. 143–147. doi: 10.1109/ICCNIT.2011.6020921.

[5] K. Gopalan, "Audio steganography using bit modification," in *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03).*, Apr. 2003, vol. 2, p. II–421. doi: 10.1109/ICASSP.2003.1202390.

[6] Lindawati and R. Siburian, "Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio," in *2017 3rd International Conference on Wireless and Telematics (ICWT)*, Jul. 2017, pp. 170–174. doi: 10.1109/ICWT.2017.8284161.

[7] S. P. Rajput, K. P. Adhiya, and G. K. Patnaik, "An Efficient Audio Steganography Technique to Hide Text in Audio," in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Aug. 2017, pp. 1–6. doi: 10.1109/ICCUBEA.2017.8463948.

[8] M. Nosrati, R. Karimi, and M. Hariri, "Audio Steganography: A Survey on Recent Approaches," *World Applied Programming*, vol. 2, Mar. 2012.

[9] J. M. Ahmed and Z. Ali, "Information Hiding using LSB technique," 2011.

[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. doi: 10.1109/ICCICT.2012.6398182.

[11] B. Datta, P. Pal, and S. K. Bandyopadhyay, "Robust multi layer audio steganography," in *2015 Annual IEEE India Conference (INDICON)*, Dec. 2015, pp. 1–6. doi: 10.1109/INDICON.2015.7443342.

[12] S. V. Jadhav and A. M. Rawate, "A New Audio Steganography with Enhanced Security based on Location Selection Scheme," 2016.

[13] C. C. Sobin and V. M. Manikandan, "A Secure Audio Steganography Scheme using Genetic Algorithm," in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, Nov. 2019, pp. 403–407. doi: 10.1109/ICIIP47207.2019.8985689.

[14] J. Mohajon, Z. Ahammed, and K. Hasan Talukder, "An Improved Approach in Audio Steganography Using Genetic Algorithm with K-Bit Symmetric Security Key," in *2018 21st International Conference of Computer and Information Technology (ICCIT)*, Dec. 2018, pp. 1–6. doi: 10.1109/ICCITECHN.2018.8631918.

[15] M. Anwar, M. Sarosa, and E. Rohadi, "Audio Steganography Using Lifting Wavelet Transform and Dynamic Key," in *2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT)*, Mar. 2019, pp. 133–137. doi: 10.1109/ICAIIT.2019.8834579.

[16] K.-C. Choi, C.-M. Pun, and C. L. P. Chen, "Application of a generalized difference expansion based reversible audio data hiding algorithm," *Multimed Tools Appl*, vol. 74, no. 6, pp. 1961–1982, Mar. 2015, doi: 10.1007/s11042-013-1732-1.
[17] A. H. Ali, L. E. George, A. A. Zaidan, and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," *Multimed Tools Appl*, vol. 77, no. 23, pp. 31487–31516, Dec. 2018, doi: 10.1007/s11042-018-6213-0.
[18] M. H. A. Al-Hooti, S. Djanali, and T. Ahmad, "Audio Data Hiding Based on Sample Value Modification Using Modulus Function," *Journal of Information Processing Systems*, vol. 12, no. 3, pp. 525–537, Sep. 2016.
[19] B. Geethavani, E. V. Prasad, and R. Roopa, "A new approach for secure data transfer in audio signals using DWT," in *2013 15th International Conference on Advanced Computing Technologies (ICACT)*, Sep. 2013, pp. 1–6. doi: 10.1109/ICACT.2013.6710492.
[20] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," *International Journal of Advanced Computer Science and Applications (ijacsa)*, vol. 7, no. 6, Art. no. 6, 32/01 2016, doi: 10.14569/IJACSA.2016.070651.
[21] S. D. Torvi, K. B. ShivaKumar, and R. Das, "An unique data security using text steganography," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, Mar. 2016, pp. 3834–3838.
[22] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *IJSRP*, vol. 8, no. 7, Jul. 2018, doi: 10.29322/IJSRP.8.7.2018.p7978.
[23] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, Sep. 2017, pp. 1–7. doi: 10.1109/ICACCAF.2017.8344738.
[24] J. Hashim, A. Hameed, M. J. Abbas, M. Awais, H. A. Qazi, and S. Abbas, "LSB Modification based Audio Steganography using Advanced Encryption Standard (AES-256) Technique," in *2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Nov. 2018, pp. 1–6. doi: 10.1109/MACS.2018.8628458.
[25] "Visual Studio Code - Code Editing. Redefined." https://code.visualstudio.com/ (accessed Dec. 15, 2022).
[26] "Steghide." https://steghide.sourceforge.net/ (accessed Dec. 15, 2022).
[27] yuntao wang, "Audio Steganalysis Dataset." IEEE, Feb. 14, 2019. Accessed: Dec. 15, 2022. [Online]. Available: https://ieee-dataport.org/documents/audio-steganalysis-dataset
[28] "The Ancient Practice of Steganography: What is it, How is it Used and Why Do Cybersecurity Pros Need to Understand it?," *Default*. https://www.comptia.org/blog/what-is-steganography (accessed Dec. 15, 2022).
[29] "lahiri-2016-ijca-909223.pdf." Accessed: Dec. 15, 2022. [Online]. Available: https://www.ijcaonline.org/research/volume140/number2/lahiri-2016-ijca-909223.pdf
[30] "Spectrogram Image - Audioalter." https://audioalter.com/spectrogram (accessed Dec. 15, 2022).