AUDIO STEGANOGRAPHY WITH INTENSIFIED SECURITY AND HIDING CAPACITY

A thesis submitted to the Department of Electronics and Communication Engineering in partial fulfillment of the requirements for the degree of Master of Science in Electronics and Communication Engineering

Submitted by
Orora Tasnim Nisha
Student ID: 1602158
Session: 2021

Supervised by
Md. Selim Hossain
Lecturer
Department of ECE, HSTU

Department of Electronics and Communication Engineering

Hajee Mohammad Danesh Science and Technology University (HSTU)

Dinajpur-5200, Bangladesh

2023

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
FACULTY OF POST GRADUATE STUDIES

HAJEE MOHAMMAD DANESH SCIENCE AND TECHNOLOGY UNIVERSITY, DINAJPUR-5200, BANGLADESH

CERTIFICATE

This is to certify that the work entitled **"Audio Steganography with Intensified Security and Hiding Capacity"** has been carried out by Orora Tasnim Nisha under our supervision. To the best of our knowledge, this work is an original one and was not submitted anywhere for a diploma or a degree.

Supervisor

……………………..
Md. Selim Hossain
Lecturer
Department of Electronics and Communication Engineering.
Hajee Mohammad Danesh Science and Technology University, Dinajpur-5200, Bangladesh.

Co-Supervisor

………………………..
Mahfujur Rahman
Lecturer
Department of Electronics and Communication Engineering
Hajee Mohammad Danesh Science and Technology University, Dinajpur-5200, Bangladesh

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
FACULTY OF POST GRADUATE STUDIES

HAJEE MOHAMMAD DANESH SCIENCE AND TECHNOLOGY UNIVERSITY, DINAJPUR-5200, BANGLADESH

DECLARATION

The research work entitled **"Audio Steganography with Intensified Security and Hiding Capacity"** has been carried out in the Department of Electronics and Communication Engineering, at Hajee Mohammad Danesh Science and Technology University. This research work is original and conforms to the regulations of this university. We have published a Scopus Index (Open Access) journal paper with this thesis work. The Publication information is given below. I recommend considering this research work for her/his M.Sc. Degree. We understand the university policy on plagiarism and declare that neither this thesis nor any part of this work has been used or submitted elsewhere for any kind of degree or award.

……………………………
Orora Tasnim Nisha
Student ID: 1602158
Session: 2021-2022

The thesis titled "**Audio Steganography with Intensified Security and Hiding Capacity**" submitted by Orora Tasnim Nisha, Student ID: 1602158 and Session 'January-June' 2023, has been accepted as satisfactory in partial fulfillment of the requirement for the degree of Master of Science in Electronics and Communication Engineering.

BOARD OF THESIS EXAMINERS

Professor Dr. Md. Mahabub Hossain Department of ECE, HSTU, Dinajpur	Chairman and Examiner
Professor Md. Mehedi Islam Department of ECE, HSTU, Dinajpur.	Examiner (Internal)
Md. Abubakar Siddik Assistant Professor Department of ECE, HSTU, Dinajpur	Examiner (Internal)
Professor Dr. Sajjad Waheed Department of ICT, MBSTU, Santosh, Tangail-1902	Examiner (External)
Prof. Dr. Mostofa Kamal Nasir Department of CSE, MBSTU, Santosh Tangail-1902	Examiner (External)

ACKNOWLEDGMENT

"First and foremost, I would like to express my heartfelt gratitude to my understanding supervisor, Lecturer Md. Selim Hossain, for his consistent support, guidance, and direction throughout the initiation and completion of this research project within the designated timeframe. During the research process, he always had an open-door policy, providing me with a platform to share any positive experiment results. His continuous assistance and direction have played a crucial role in steering me in the right direction. Without his invaluable assistance, I would not have been able to complete this thesis.

I would also like to extend my gratitude to Lecturer Mahfujur Rahman for his extensive knowledge of information theory and his valuable insights into my future research and personal development. It has been a privilege to work with him, and his guidance and suggestions have significantly contributed to my growth. I appreciate his support and consider myself fortunate to have had the opportunity to work with such a respected professional.

Lastly, but certainly not least, I would like to express my deep appreciation to my parents and my unwavering family for their constant support and encouragement throughout my life, especially during my years of study. Their unwavering support has played a pivotal role in my achievements, and I attribute this accomplishment to their love and guidance. Without their love and guidance, this achievement would not have been possible.". I am also grateful to the National Science and Technology (NST) fellowship (2022-2023). This research work is supported by the fellowship fund.

ABSTRACT

These days, the web is a secure and crucial vehicle of correspondence, dispersal of data, and network to away individuals. In addition, safeguarding ourselves online is mandatory. In such a manner, steganography is a framework that gives an upgraded correspondence process. It hides the quest for correspondence. Then again, an encryption is provided by cryptography system to create the mystery message decoder. Steganography provides. privacy, confirmation in addition and information uprightness however non-renouncement. Audio steganography has proactively been the subject of numerous studies. The proposed approach yields comparatively better results. This research offers a strategy to disguise data in a sound signal. It represents an improved two-level tied-down correspondence to conceal private data by encoding information utilizing the Genetic Algorithm (Hereditary Calculation). At the sender side, we hide data inside cover audio applying a Genetic algorithm, and that hidden data is extracted at the receiver. For analysis, we use dot wav audio signal files. The cover and stego audio signal strength can be assessed using the SNR (Signal Noise Ratio) value. The resultant Stego audio signal has a higher positive and close to one SNR value. Steganography as the proposed strategy gives a higher got correspondence and concealing limit. Additionally, this method effectively conceals information within the audio signal and is more acoustically transparent. This technique highly secured short-range communication.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER – 1
INTRODUCTION

“Gives a general overview of the study as well as a background and general introduction to the subject, including the purpose and significance of the research”.

INTRODUCTION 1

The rapid development of steganography techniques is discussed in this section. We discussed some audio steganography techniques that embed data in cover audio successfully. We briefly discuss the significance of our models, issues, and this study's goals.

1.1 Introduction

Like a lot of cool words, "steganography" comes from Greece. It is a combination of the Greek words steganos, which meaning "covered," and graphene, this implies "to write," it is used to describe the skill of enabling covert communication by cleverly concealing information from view. An approach to keep information hidden within a sound signal is called audio steganography. The data is altered as it is embedded in the signal. The human ear should be unable to distinguish this modification. Image can also be used as a medium, but audio steganography has more power, a wide range of hearing, and a higher range of audible frequency than image steganography. Cryptography incorporates the encryption of the message. It doesn't try to hide the encrypted message. Steganography does not alter the original message; however, by embedding the message in the chosen medium, the continuation itself is hidden from the intruder. The environments that an audio signal can traverse on its way from an encoder to a decoder are defined by the transmission channel. Computerized start to finish, simple transmission, expanding diminishing resampling, and "over-the-air" conditions are all examples of this.

Digital data is increasingly being transmitted via the Internet for rapid and secure communication. However, maintaining internet security is crucial since people rely on it for secure communication. People employ a variety of techniques to achieve online security on the internet. Cryptography is one approach among many other options. However, steganography masks the existence of secret data. Cryptography, then again, is unable to mask the secret's existence data. Different multimedia files are used by people for communication. The most common method of concealing data inside digital material, such as music, video, and images, is steganography. It is essential to the exchange of communication. Additionally, it guarantees privacy during the communication process. Use a variety of steganographic methods to encrypt the audio signals there to encrypt information. Secret communications for wedding security are concealed using steganography and its analysis [1]. The cover and stego audio cannot be altered by a third party. Unauthorized individuals are kept in the dark regarding the presence of secret communications. An example of a steganographic carrier is an audio file. As VOIP gains popularity daily, audio is being used in more apps as a result. The secret message is concealed using audio steganography technology, which only permits the intended receiver to decipher it. It offers two levels of defense against cryptography. Sound files in WAV, AU, and even MP3 formats can include hidden information thanks to audio steganography. Sound documents are altered in audio steganography, so they include concealed data. This concealment process must be carried out correctly such that the privacy data is kept intact, without degrading audio quality or adding a lot of noise to the original signal.

Data may be concealed in an audio file using a variety of techniques. The genetic algorithm, least significant bit (LSB) coding, parity coding, phase encoding, spread spectrum, and echo data hiding are some of the current techniques for obscuring data inside audio signals. Due to the great transparency and durability of the genetic algorithm technique, we have employed it to conceal data within an audio recording. These procedures come with several dangers. The Least Significant Bit algorithm's (LSB) vulnerability to steganography and lack of stability pose a hazard. The LSB has been modified to operate in a divergent manner to increase stability. Parity coding may fail to detect mistakes. For example, if two data bits are corrupted, it won't detect faults. The principal challenge in section coding is that closed waves in a sine segment interact productively while waves out of phase interfere deadly. Strongness is the dominant obstacle to rehearse concealing. Conversely, however, the challenges associated with executing the hereditary calculation can be computationally costly and difficult to debug. The evolutionary algorithm can provide solutions for a variety of problems that conventional methods cannot solve. Steganography's key advantage is that, unlike encryption, it hides the existence of concealed information [2]. It can effectively address problems with numerous limitations in dot wave audio files. Stego_key + cover media + hidden data = stego_media. As a cover signal, you can use a variety of options, such as an audio signal, a picture, video files, etc. It is more challenging to hide data using a digital audio cover than it is to do so with a digital picture. Using a secret key and a genetic algorithm, the sender may encode data into an audio stream. Dot wave audio coding is the topic of this article [3]. Only the recipient has the secret key needed to decode it. Applied mathematics analysis and aural inspection both make use of two standard steganalysis procedures. The offender compares the concealed message to the original message using statistical analysis to determine the hidden message. The fourth and fifth LSB layers of the LSB algorithm allow for the embedding of data. Genetic algorithms, then again, have an elevated concealing volume [4]. Both Steganography of audio and video makes use of genetic algorithms. principles. Image steganography is distinct from audio and video steganography. With sound and video steganography, veiling is required. Human hearing and sight can detect even the slightest auditory or visual shift. The ability of human-sensitive organs to hide information can be used as a tool for disguising. The main interest groups in the topic of hiding secret information are military and intelligence organizations [5]. The SNR values of the original and stego audio were calculated in this article to examine the audio signal quality and to offer a secure approach with better security. Applying GA has successfully boosted the concealing capacity. The hidden message in the LSB (Least Significant Bit) method is buried in higher LSB Layers [6]. Rather than signal-to-process fluctuation, the LSB algorithm's fundamental flaw is its lack of adaptability. Keeping all of the pixels are present while concealing information within a picture is a dilemma. [7]. There are several ways to hide information using the steganography approach [8]. We require more secure steganographic algorithms to guarantee security. In certain techniques, data is concealed inside the audio signal using secret keys [9]. The payload capacity and visual quality are balanced using the LSB algorithm [10]. Steganography is the finest method for protecting sensitive data from outsiders [11]. When concealing bits, the extraction error can be prevented by combining the lifting wavelet change with the LSB approach [12]. The hereditary calculation, however, offers excellent resilience. It is effective in obscuring sensitive information inside the audio stream. The highest fitness bitstream location is provided by the genetic algorithm. The inserted data must have a higher bit rate for all stago applications. Without using the cover audio bitstream, an intelligent program finds and decodes hidden bits. On the other hand, one of the greatest techniques for encoding concealed data is using genetic algorithms. The most popular technique now for enhancing steganographic-based internet security is audio steganography.

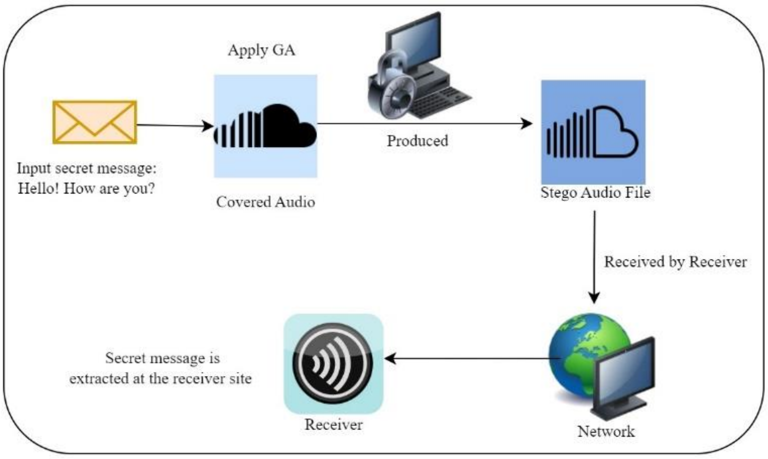


Figure 1.1: The framework of audio steganography using genetic algorithm.

Data may be effectively hidden inside dot wave audio files utilizing this genetic algorithm coding technique while preserving audio quality. Both the noise and the concealment capacity may be improved. The method offers protection for secret internet communication between military and intelligence organizations. It may also be appropriate for brief, private internet communications when some businesses or government organizations want information protection.

1.2 The issue

As researchers strive for high levels of accuracy, the field of object detection has recently received significant attention from the research community. Several approaches have been proposed. Various platforms like MATLAB and Python in the visual studio have been used. This thesis' goal is to put into practice a method applying a genetic algorithm that can hide data efficiently and keep the audio quality high. The genetic algorithm is one of the leading techniques. This method is effective for network security in short-range communication a lot. The methodology will be described in detail in Chapter 4 and was used for the implementation and analysis.

1.3 The study’s objective

Security is an issue in today's communication world. The principal objective of this research Work entails hide confidential information inside an audio file to ensure security. The audio file used as the carrier medium for the embedded data needs to be impenetrable. Neither the human visual nor auditory system nor the carrier file's increased file size should indicate that the carrier is suspicious. The inserted data must remain intact within the conveyance and be simple to remove for the receiving party in the right circumstances.

Digital sound is used to encode secret messages in an audio Steganography system that is based on computers. A sound file's binary sequence is slightly altered to embed the secret message. Messages can be implanted in WAV, AU, and even MP3 sound records using existing audio steganography software. Digital sound signal embedding is typically a more challenging process than implanting data in other forms of media, like advanced pictures. These approaches range from relatively straightforward techniques that submerge information contained in noise in the signal to learn more potent strategies that conceal information by utilizing advanced signal processing techniques. The following are the key objectives of this research work.

- To develop a steganography technique to provide secure communication.
- To implement the technique with Genetic algorithm.
- To achieve a better quality of audio signal and hiding capacity of steganographic technique.
- To practice modern user experiences

1.4 Significance and motivation of the research

1.4.1 Advantages:

- Steganography based on audio has the potential to conceal additional information.
- Audio steganography has a huge potential for power because of its flexibility: Why Images are usually smaller than audio files.
- Our hearing is readily deceived. Large amounts of information can be saved by making small amplitude modifications.
- The discussed methods make the technology more accessible to everyone and give users a lot of options.
- A party that desires to impart can rank the significance of elements, for example, information transmission rate, data transfer capacity, vigor, and clamor discernibility, and afterward select the technique that best accommodates their details.

- For instance, the straightforward LSB coding method could be utilized by two individuals who only wish to exchange brief secret messages with one another. On the other hand, a more advanced strategy like phase coding, SS, or echo hiding may be considered by a large company that wishes to safeguard its intellectual property from "digital pirates."
- The use of stooges will continue to gain significance as a safeguard as more and more attention is paid to surveillance, privacy, and copyright protection.
- Sound Steganography specifically resolves major questions achieved by the MP3 design, P2P programming, and the requirement for a protected telecom conspire that can keep up with the mystery of the sent data, in any event, while going through unreliable stations.
- The variety of sources and types complicates statistical analysis and Security.
- It is possible to embed greater amounts of secret data without any audible degradation.
- Numerous malicious attacks on image steganography algorithms (such as spatial scaling and mathematical contortions) against sound Steganography plans, cannot be used. Because of this, embedding information into audio appears to be more secure because there are fewer strategies for steganalysis attacks on audio.

Audio Steganography's ability to combine with existing cryptography technologies is another attractive feature. Users no longer must rely solely on one approach. Information can be disguised completely as well as encrypted.

1.4.2 Disadvantages

- Because the HAS dynamically dominates the human visual framework, installing extra data into sound sequences is a more laborious process than inserting information into images.
- Stain resistance: If a criminal discovers that copyright marks are concealed by substitution, they could be changed or destroyed in audio samples easily.
- The disadvantages of commercial audio steganography include the fact that Hidden messages are simple to find. seen and that just certain sizes of data can be concealed.
- The hidden message will be lost when an audio file is compressed using lossy compression because the file's structure will be altered.

- In addition, by eliminating all unheard frequencies, some lossy compression algorithms take advantage of limitations within the human ear.
- Furthermore, this will eliminate any frequencies in that spectrum that a steganography system uses to conceal data.

1.5 Motivation

Encrypting important information before sharing it is an extremely important task in the modern era to prevent misuse. Steganography is the most effective method for encrypting data, hiding it in a carrier audio or image file, securely sharing the data between two parties, and minimizing file size. Techniques for audio Steganography addresses problems with comfort and conceal the integrity of statistics, particularly in voice technology. From our perspective, the variety and comprehensiveness of current audio steganography strategies increases software opportunities. The advantage of using one method over another is determined by the software's limitations, which include the need for masking capability, embedded data protection, and encountered assault resistance. The creation of a robust and dependable algorithm that can withstand steganalysis may be the subject of future research.

1.6 A summary of the study

There are six chapters in the thesis.

Chapter 1: Gives a general overview of the study as well as a background and general introduction to the subject, including the purpose and significance of the research.

Chapter 2: Discusses previous related research on audio steganography, including its methods and outcomes.

Chapter 3: Focuses on the theory and related formulas of audio steganography techniques.

Chapter 4: Explains the model and applied genetic algorithm used in the thesis in detail, including their underlying formulas.

Chapter 5: Discusses and presents the findings.

Chapter 6: Makes suggestions for enhancing the research topic in the future.

CHAPTER – 2
LITERATURE REVIEW

" Examines methods and results from previous associated research."

LITERATURE REVIEW 2

Related work of audio steganography

This writing survey part will give a thorough comprehension of the present status of the field of sound steganography, including the different techniques and their proficiency. It has also demonstrated that those models make use of a variety of algorithms. The literature review highlights the significance of audio steganography and the potential for further improvement. These models have produced remarkable results. The chapter will be a useful resource for those working in the field as researchers and practitioners.

2.1 Overview of relevant literature

Cryptography allows individuals to send secret messages to each other without the oversight of an outside party. A form of cryptography known as steganography involves encasing a secret message within a digital image. Steganography focuses on shielding such messages from detection by concealing their very existence, whereas cryptography is concerned with protecting the contents of a message or information. The first important part of steganography is the data's compression or embedding, and the second is the data's decompression or extraction. Steganography, derived from the Greek word steganographic, which means "covered writing," is now used to describe the concealment of information within other information. Naturally, these methods have been around for a long time, with the primary use being the transportation of information during wartime. Steganography is closely linked to the term "watermarking." A piece of data that is indistinctly and securely incorporated into the host data and can't be taken out is known as a digital watermark. Information concerning the host data's beginning, status, or beneficiary is typically included in a watermark. Quite possibly of the most crucial aspects of the safety of communications and information is steganography. Reversible and nonreversible data-hiding techniques are the two most common types [13]. Multi-access radio communication systems typically employ direct spread spectrum technology, such as CDMA principles, worldwide satellite route frameworks, Wi-Fi network remote conventions, and so on. It guarantees that the transfer of information is highly reliable and secure. Additionally, spread spectrum technology obscures the messages' semantic content by giving the communicated signals a commotion like appearance [14]. Steganography is a useful technique for allowing complete local access control of digital works shared over the internet. The information or data is hidden in access control frameworks for computerized content wholesalers, but the page's content is not. Anyone who visits the page sends an access request to the owner. The owner can then develop an entrance key to clients who wish to read the page's content. using a digital image, video, or audio file with a text message to conceal information [15]. The information conveyed can be found in a variety of formats and utilized in numerous applications. In many of these applications, it desires that communication take place behind closed doors. Examples of such secret communication include bank transfers, corporate communications, credit card purchases, as well as a significant portion of everyday emails [16]. In genetic computation, message pieces are inserted into many, dubious, and higher layers of LSB, resulting in increased power. Durability would be strengthened against both deliberate attacks that attempt to expose the covert message as well as accidental attacks like noise addition [17].

The PSNR security and hiding capacity capabilities of the audio's media noted information were tested as part of the authentication verification study using LSB 3 models (1-LSB, 2-LSB, and 3-LSB). It's encouraging research revealed comprehensive repercussions of data dependency, highlighting real and compelling opportunity to contribute [18]. The LSB calculation's principal idea is watermark inserting with insignificant installing mutilation that the host sound. The two-step process embeds the LSB layers with higher watermark bits, enhancing their resistance to noise addition and MPEG compression. The method's perceptual quality of watermarked audio was found to be superior to that of the standard LSB method in listening tests [19]. Inserting technique of secret information in sound files is extra difficult than inserting information bits in different forms, such as images. Different algorithms are used in audio steganography, but the least significant bit (LSB) is used in this paper. The user-selected audio size and message length determine the sound quality. [20]. An application has been developed to improve email security for personal information transfers. By encasing info in high-quality pictures, the application makes it possible to communicate secretly. This method allows the safe mailing of the hidden data to the target. Authentication of images and tamper-proofing, which stops unauthorized copying and alteration of images, is another use for image steganography. Image tamper proofing has been made possible by several new methods. Like movie subtitles, in-band-captioning involves the incorporation of textual data into digital images. Digital steganography is used in revision tracking. Text steganography is less common than the other methods of steganography. This is because text files contain less unnecessary information than other types of files. Again, the structural analysis that text files are relatively simple, and the missing hidden message when the unrevealed document is reformatted. Still, secret communication is carried out through text steganography. To send private text messages in secret, A text steganography security model is suggested. Steganography's ability to conceal sensitive data within a cover media ensures that no one will ever be able to suspect that any data is hidden. However, sensitive data can be discovered if anyone notices a change in the cover media. Before concealing the sensitive data in the cover media, it is, therefore, preferable to employ another method, such as cryptography, to encrypt it. Because of this, even if the embedded text is found, no one will be able to determine its contents because it is encrypted. Therefore, we can benefit from combining the two methods for increased security to ensure that secret data are not damaged or misused even in the face of extremely challenging security breakthroughs [21].

There are two types of steganography techniques: Both adaptive and non-adaptive range tables are used in PVD [22]. It makes good use of research in psychoacoustics and has significantly better results than Low Bit Encoding, like phase encoding. Dealing with audio formats like WAV is substantially more expensive than dealing while comparing "file size to storage capacity" with bitmap graphics, as is the case with all sound file codecs. Audio files are far less common than image files to be delivered via email or the internet, making them much more suspect. It offers greater robustness and a higher data transfer rate than noise-generating techniques [23]. Each of these techniques also includes theft of service, whether from a customer or the phone carrier; as a result, this is one instance in which the police's interest in signals intelligence and the consumer's interest in robust authentication overlap. Nevertheless, authentication is insufficient on its own. As a result of the strong authentication mechanisms [24]. Copyright protection, data monitoring, and data tracking are all applications [25]. Numerous recent applications necessitate the creation of systems that integrate a single signal, also known as a "embedded signal" or "watermark," included in another signal, also known as a "host signal." The embedded signal needs to be "hidden" throughout the embedding process," meaning that it does not significantly affect the host. In addition, When the host signal occurs, the watermark must remain intact is degraded, so embedding needs to be resistant to typical watermarked signal degradations [26]. The development of alterations that are largely indiscernible to the reader while still being consistently decodable (even in the presence of noise) is the objective in the design of coding methods. Reliable decoding and minimal visible change appear to be contradictory criteria; The difficulty in developing document marking strategies lies here [27]. Digital watermarking dominated early research in the field, driven by the significant financial interest in copyright protection applications of data hiding. Concerns that steganography might be used for terrorist or other criminal purposes fueled interest in steganography and steganalysis as watermarking developed into an established field. Steganography is now a well-established field that is piquing the interest of signal, communication, and network security researchers as well as practitioners [28]. Watermarking digital speech is a useful method of concealing and protect data during transmissions, like audio and video, from being changed in any way, either intentionally or unintentionally. Digital speech signals differ from audio, music, and other signals in some respects, such as bandwidth, voice/non-voice, and production model. While there are several review papers on digital speech watermarking, there aren't many on image, audio, or video watermarking. As a result, the overview of this article discusses imperceptibility, capacity, and robustness. of digital speech watermarking [29].

Most schemes make use of the fact that digital media contain seemingly insignificant parts that can be altered or replaced to incorporate copyright protection. The authors of [30] proposed a novel solution to the issues with approaches for audio steganography substitution. The first issue is that they are less resistant to intentional attacks that attempt to reveal hidden messages, and the second issue is that they are less resistant to unintentional attacks. The algorithm will alter other bits to reduce error and hide the message in accordance with the proposed solution (in deeper layers of audio samples). The method currently employs two bits per audio sample byte. This will make progress toward increasing robustness and capacity. This study examined a variety of audio steganography techniques employing various algorithms, such as the genetic algorithm approach and the LSB approach, in-depth. Authors [31] examined these techniques in detail. It has attempted a few methods that aid in audio steganography. It is both an art and a science to create concealed messages in a way that only the sender and recipient are aware of their presence. There have been several studies in recent years that use image and video steganography, but none that use audio as a carrier. It has long been known the auditory system of the human, or HAS, than the human visual system, is more sensitive. Audio messaging with the help of a variety of chat applications presents privacy and confidentiality issues because of the increased information exchange, opening the door to research in the field of audio steganography. The audio data's redundant nature makes it suitable for steganography practice. Steganography is used to conceal accuracy of the information insecure channels. Because of this, the information must be safely transmitted and received using a medium by the authority known as a file or a carrier. Currently, many kinds of digital files are employed as defense confidential data; nevertheless, multimedia files, data are regularly employed due to their widespread distribution across via the internet, where millions of them are regularly shared by users. Depending on the number of words or the properties of the sentences, several methods can be used to encrypt a secret message and store it in a text file. In steganography, this is the first technique employed. Due to the text file's low redundancy and consequently low hiding capacity, this kind of using steganography is challenging with huge amounts of secret data.

Most data hiding methods as much data as you can into the host without harming its file's perceived quality degradation. In the process of developing algorithms for hiding data, it is one of the most crucial aspects. a visual similarity between the cover file and the stego-cover is typically used to describe the fidelity of the steganography algorithm. Nonetheless, the disparities ought to be minimal. Most of the time, an objective quality measure or a subjective test is used to evaluate imperceptibility. Some steganography techniques fall into the category of high-transparency techniques. The capacity is the volume of data that a successful information-hiding method can conceal without causing perceptional distortion. It shows how many details regarding the size of the host cover are concealed. How to incorporate secret data as much as feasible while retaining host cover quality is the issue at hand. For audio steganography, it is measured in bits per second, while for image steganography, it is measured in bits per pixel. To increase the cover file's capacity, numerous algorithms were developed. Security keeps unauthorized people from accessing the hidden data, and robustness ensures that the hidden message cannot be changed or removed. The stego-cover may be affected by one of two types of attacks: intentional attacks that seek unintentional assaults and that seek to alter or destroy the stego-cover (such as compression, rotation, blurring, and other filtering techniques) in order to remove the stego-cover and reveal the concealed information. Typically, robustness and capacity must be sacrificed to work together in the same steganographic system. For watermarking and copyright protection, robustness is a crucial factor. applications, whereas steganography applications place a greater emphasis on imperceptibility and high hiding capacity because the objective is to conceal as much data as possible while maintaining the cover file's quality. Depending on the complexity of the algorithm, the hide/de-hide process takes time with hiding algorithms. To deliver streaming data that is hiding in real time over the network, Secret information should be rapidly integrated or extracted from the host file.

2.2 Methods for audio steganography

In this section, describes about some common audio steganography techniques.

2.2.1 LSB Coding

The simplest way to incorporate data into a digital audio file is with the least significant bit (LSB) coding, as demonstrated in this section. LSB coding lets you encode a lot of data by using a binary message to replace the least significant bit of each sampling point. In shrewd, the Most un-Critical Piece (LSB) is the piece position in an extremely parallel whole number providing the unit's value, whereby, to control whether the amount is even or odd. It is comparable in the direction a decimal integer's one (right-most) digit, which is also its least significant digit.

For example, the following digital signal values are, LSB-Steganography is a steganography approach in which we cover messages internally in a sound record by changing the least significant bit of that audio and the fragments of secret information to be stored.

00110011 10100010 10100011 00100110 01011001 01101110 10110101
00010101 11100110 11011010

The audio file's newly added message,

00110011 10100011 10100011 00100110 01011001 01101110 10110101
00010100 11100111 11011011

To insert the character in this instance, only three bits must be changed, fortunately. On a median, only 1/2 of the bits in an exceedingly digital audio signal ought to be changed to hide a secret message exploiting the greatest cover size. The consequence modifications that make the smallest significant bits are not large enough to be stated via the human visual system, so the secret information can successfully conceal. The algorithm's low computational complexity is the LSB coding method's primary benefit, while its major drawback is: If more LSBs are used during LSB coding or the depth of the modified LSB layer grows, there is a greater chance that the encoded message will become statistically detectable and there will be less perceptual transparency for stego objects. Low Bit Encoding is a poor option as a result because it doesn't satisfy the condition of Steganography to be undetectable.

2.2.2 Phase Coding

Phase coding tends to the inconveniences of the commotion initiating techniques for sound Steganography. The foundation phase components of sound are not as noticeable to the human ear as noise, which is a disadvantage of phase coding. In terms of the signal-to-perceived noise ratio, the method encodes the data bits as the phase changes in a digital signal's phase spectrum rather than introducing perturbations. The sound file has been divided into N chunks using the phase coding technique. To create a phase and magnitude matrix, each segment is subjected to a Discrete Fourier Transform (DFT). The first phase (s0) has a synthetic absolute fragment of p0 created, and all different fragments have freshly created segment frames. After then, each segment's phase difference is determined. The new segment, Sn., is created by combining both the new phase and the initial magnitude. The encoded output is made by concatenating these new segments, and the frequency is maintained. To disentangle the secret data the collector should know the length of the fragments and the information stretch utilized. If The first segment, which is either a 0 or a 1, marks the start of the message.

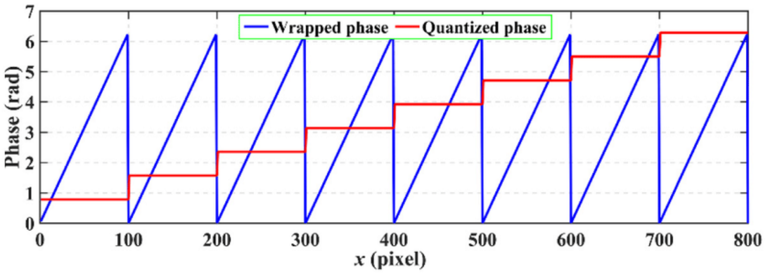


Figure 2.1: Phase coding.[32]

Compared to Low Bit Encoding, this method has many advantages, the most significant of which is that it is imperceptible to human hearing. However, it still lacks robustness to changes in the audio data, like all the techniques described thus far. The information would be distorted and unable to be retrieved by any single sound operation or data modification.

2.2.3 Echo Hiding

By echoing the original audio, echo hiding embeds data. This Artificial Echo is used to mask the embedded data by varying its delay, decay rate, and beginning amplitude. The human ear becomes more and more unable to differentiate between the echo and the source audio as the delay between the two decreases, to the point where the echo of a created carrier sound is simply perceived as additional resonance. Additionally, the binary message is represented by varying the offset. A binary one is represented by one offset value, and a binary zero is represented by two offset values. One bit of data could only be encoded. if the initial signal produced only one echo. As a result, the initial signal is divided into blocks before the beginning of the encrypting process. The final signal is created by re-concatenating the blocks after the encoding procedure is complete.

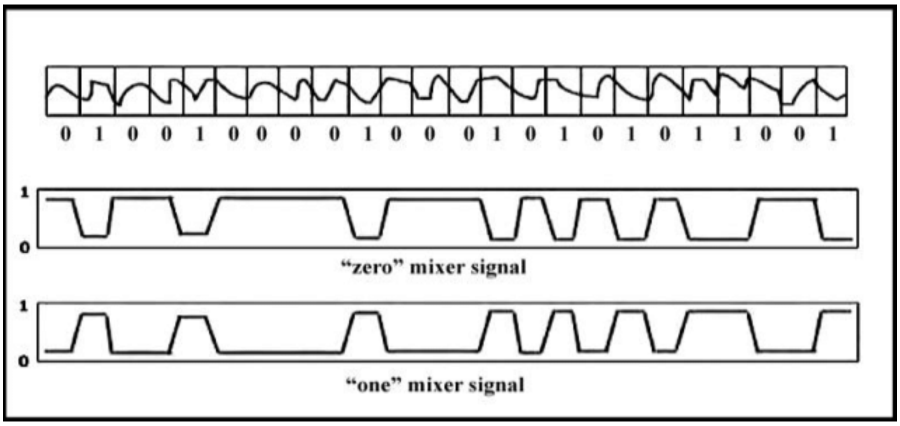


Figure 2.2: Echo hiding.[33]

The final signal is produced by recombining the blocks. After that, the mixer signal multiplies the mixer signal multiplies the "zero" echo signal by the "one" echo signal. When the two findings are combined, the final signal is generated. Compared to the signal that was acquired from the original application of echo hiding, the final signal is less abrupt. This is because each signal makes use of ramp transitions, and the two mixer echoes are complementary to one another. The mixer signals' two characteristics result in smoother echoes-to-echoes transitions. The signal must be split into the same block sequence by the receiver as it was during encoding to extract the secret message from the stego-signal. Since it exhibits a spike at each echo time offset, the auto-correlation function of the signal's spectrum—the Forward Fourier Transform of the signal's frequency spectrum—can then be used to decode the message, making it possible to reassemble the message. This effectively utilizes the research that has been completed to date in psychoacoustics and has significantly better results than Low Bit Encoding, like phase encoding. When it comes to the ratio of "file size to storage capacity", working with audio formats like WAV is significantly more expensive than working with bitmap images, as is the case with all sound file encoding. Audio files sent via email, or the internet are much less common than image files, making them greater suspicion. Compared to noise-generating methods, it offers superior robustness and a high data transmission rate.

2.2.4 Spread Spectrum

Data is encoded by spread spectrum systems as a noise-like binary sequence. When the proper key is used, the receiver can recognize it. Since the 1940s, the army has used this technique due to the fact the indicators are challenging to jam or intercept due to the fact they are lost in the heritage noise. By matching the medium's large bandwidth to the embedded data's narrow bandwidth, spread spectrum techniques can be utilized for watermarking. Audio steganography can use either one of two versions of SS: the frequency-hopping and direct-sequence schemes. The secret message is presented in direct-sequence SS is modulated by a pseudorandom signal and stretched by a consistent known as rate of chips. The cover signal then interrupts it. The frequency spectrum of the audio file has been altered to produce frequency-hopping SS, which includes quick frequency flipping. There is a lot of promise for secure commercial and military communications with spread spectrum steganography. Spread spectrum and audio steganography together could provide more layers of protection. Spread spectrum encoding is the safest way to transmit secret messages through audio, but it increases the likelihood of data loss because it can introduce random noise into the audio. They have a good level of resilience against removal procedures and provide a moderate data transmission rate.

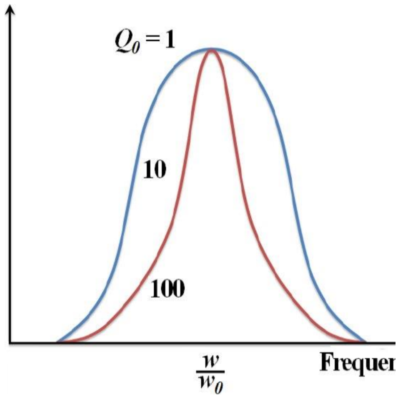


Figure 2.3: Spread spectrum.[34]

If used appropriately, along with using cryptography approaches to protect the embedded data before inserting it into a cover media, several of the above-described data-hiding techniques have the potential to become effective instruments for transferring undetected and dependable communication. The encoded information is spread as widely as possible throughout the frequency range. The signal is spread in Direct Sequence Spread Spectrum by dividing it by a certain chip, or maximal length pseudorandom sequence. The chip cost for coding is the host signal's sampling cost.

2.2.5 Genetic Algorithm

The genetic algorithm runs faster than any other algorithm currently in use. It outperforms other widely used LSB algorithms in terms of hiding capacity by improving each bitstream's fitness. With less unwanted signal (noise) and better audio quality, efficient hiding capacity is possible. The genetic algorithm outperforms other audio steganography algorithms in terms of network security and hiding power.

Message bits are introduced through an evolutionary process into a few fuzzy, higher LSB levels, boosting robustness against both deliberate assaults that aim to reveal the concealed message and accidental threats such as noise addition. based on the survival and reproduction laws of Darwin. Chromosome populations (individuals) are processed by the GA, which sequentially replaces one population with another. The GA frequently holds the chromosome in parallel encoding. The chromosomes each include a potential a finding in the search area. To give each chromosome in the present population a score (fitness), the GA normally need a fitness component. The GA begins by guessing the initial population of people. Generations are how individuals develop over time. The fitness function is used to evaluate each individual in each generation. To produce a subsequent generation of individuals, genetic operators are applied to individuals in the population. The procedure continues until some kind of criterion is met, such as a certain level of fitness.

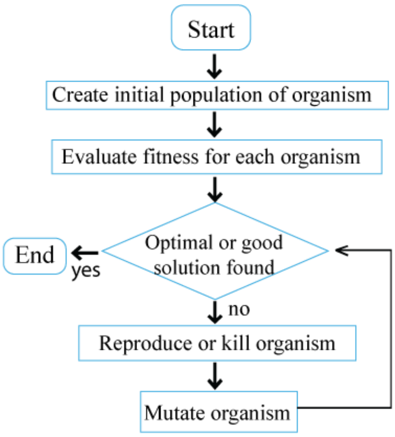

Start
Create initial population of organism
Evaluate fitness for each organism
Optimal or good solution found
End
yes
no
Reproduce or kill organism
Mutate organism

Figure 2.4: Flow chart of genetic algorithm

Alteration: In the initial step, samples' target bits take the place of message bits. The bits that are placed at the layer that we wish to alter are referred to as target bits. This is accomplished through a straightforward substitution without the need to measure the result's adjustability.

Modification: The most fundamental and important stage of the algorithm is actually this one, according to the modification. This stage is necessary for the fulfillment of all anticipated outcomes. Here, sophisticated, and useful algorithms are helpful. The algorithm's current goals are to increase accuracy and reduce opaqueness. Two distinct algorithms will be used for this stage.

Verification: In truth, this process controls quality. The algorithm has finished working; therefore, the result now must be checked. The new sample will be used if the discrepancy between the old and new samples is reasonable and acceptable; else, the old sample will be used to construct the new audio file.

Reconstruction: The final step in the reconstruction process is to create a brand-new audio file (a stego file). This is done one sample at a time. The input for this step consists of two states. The input sample may be either a modified sample or the original sample that corresponds to the host audio file. This allows us to claim that not all known samples are altered by the algorithm. This implies that the choice of sample will be made based on the decision of the intelligent algorithm and the state of the samples (Environment).

2.3 Relevance and constrain in the literature.

Audio steganography has the capability of concealing additional data. Audio steganography has a lot of potential power because it is so adaptable. numerous malicious attacks on the image steganography algorithm, including spatial scaling, geometrical distortion, and others. cannot be used to combat audio steganography plans. Consequently, less steganalysis techniques attacking audio suggests that embedding information within audio is more secure.

When compared to ships and submarines that employ conventional technology, they provide pilots and crews with a degree of safety that is somewhat superior because they are virtually undetectable.

The study’s constraints:

Steganography doesn't come without its drawbacks. The algorithms keep the information confidential, so this method is useless if the algorithms are known. Unauthorized access to data can be caused by password leakage. The technique can be extremely risky for everyone in the wrong hands, such as hackers. However, these can be fixed, and once it is carried out, it can enhance the steganography components.

CHAPTER – 3
GENETIC ALGORITHM

“Focuses on genetic algorithm method, including the theory, method statistics.”

3.1 Genetic Algorithm

- 3.1.1 Genetic algorithm encoding procedure.
- 3.1.2 Selection Operator
- 3.1.3 Crossover Operator
- 3.1.4 Mutation Operator

3.2 Criteria of the genetic algorithm

GENETIC ALGORITHM 3

Hereditary calculations are considered a pursuit cycle utilized in processing to track down definite or rough answers for improvement and search issues. Global search heuristics are another name for these features. These procedures are roused by developmental science, for example, legacy transformation, choice, and get-over. These calculations give a method to program to further develop their boundaries consequently. This paper is a presentation of the hereditary calculation approach including different applications and depicted the coordination of hereditary calculation with object-situated programming draws near.

3.1 Genetic Algorithm (GA)

A genetic algorithm uses methods stimulated by evolutionary biologists like choice, transformation, legacy, and recombination to remedy an issue. The majority employed technique in genetic algorithm creates a crew of persons from a given populace. The humans accordingly shaped evaluate with the assistance of the comparison feature furnished using the programmer. Individuals are furnished with a rating. which does not directly highlight the health of the given situation. The excellent two humans are then used to create one or greater offspring, after which random mutations are accomplished on the offspring. Depending on the wants of the application, the method continues till an ideal answer is derived or till a positive wide variety of generations have passed.

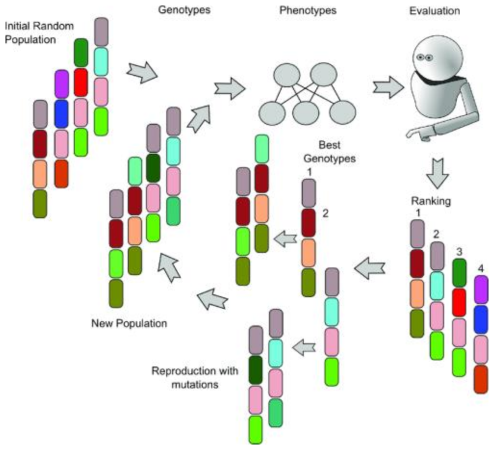


Figure 3.1: Genetic Algorithm. [35]

A derivative-based optimization method differs from a genetic algorithm in two respects.

- In contrast to a classical algorithm, which only produces a single factor at each iteration, a genetic algorithm generates a population of factors in each iteration.
- A classical algorithm chooses the next factor by deterministic computing, whereas a genetic algorithm chooses the next population through computation using random number generators.

A genetic algorithm has many advantages over conventional artificial intelligence. It is more durable, but it can break down if the inputs change even slightly or there is noise. When scanning over vast state spaces, multi-modular state spaces, or n-layered surfaces, a hereditary calculation can give preferable and more critical outcomes over other improvement procedures like praxis, linear programming, heuristic, to start with, or broadness first. Numerous fields employ genetic algorithms, including engineering design, computer-aided molecular design, optimized telecommunications routing, robotics, and automotive design.

3.1.1 Genetic algorithm encoding procedure.

This algorithm has three encoding operators. Encoding can take place in various ways. Binary, octal, Hexadecimal, permutation, value, and tree encoding are a few examples. The operators are,

1. Selection operator
2. Mutation operator
3. Crossover operator

The encoding scheme—that is, the process of converting into a particular form—plays a significant role in the majority of computational problems. A specific bit string needs to be used to encode the given information. The problem domain is used to distinguish the encoding schemes. The most well-known encoding techniques include binary, octal, hexadecimal, permutation, value-based, and tree. Binary encoding is the most popular type of encoding. For each gene or chromosome, a string of one or zero is employed as a representation. The solution's characteristics are represented by each bit in binary encoding. It makes it simpler to employ the crossover and mutation operators. However, converting it into binary requires additional effort, and the algorithm's accuracy is dependent on the binary conversion. The problem determines the modification of the bit stream. Because of epistasis and natural representation, the binary encoding scheme is not suitable for solving some engineering design issues. In the octal encoding scheme, the gene or chromosome is represented by octal numbers (0–7). Hexadecimal numbers (0–9, A–F) are used in the hexadecimal encoding scheme to indicate the gene or chromosome. Permutation encoding is usually used for ordering problems. The gene or chromosome is represented in this encoding scheme by a string of integers that corresponds to a place in a sequence. These values can be characters, real, or an integer number. When it comes to resolving issues involving the use of more complex values, this encoding scheme may be of assistance. because such issues may fail binary encoding. It is mostly used to find the best weights in neural networks.

A tree of functions or commands is used to represent the gene or chromosome in tree encoding. Any programming language can be associated with these commands and functions. This is particularly like the portrayal of suppression in tree design. Expressions or programs that are constantly changing typically employ this type of encoding.

3.1.2 Selection Operator

In genetic algorithms, selection is a crucial step that determines whether a particular string will participate in reproduction. The reproduction operator is another name for the selection step. The selection pressure influences the GA convergence rate. Roulette wheel, rank, tournament, Boltzmann, and stochastic universal sampling are the most well-known methods of selection. The process of selecting a roulette wheel involves mapping each of the possible strings onto a wheel, with a portion of the wheel allotted to each string based on its fitness value. After that, this wheel is turned at random to pick specific solutions that will help form the next generation. However, it has a lot of issues, like errors brought on by its stochastic nature. By introducing the idea of determinism into the selection procedure, De Jong and Brindle altered the roulette wheel selection method to eliminate errors. The modified version of the Roulette wheel selection is rank selection. Instead of fitness value, it uses ranks. Each person has a chance of being selected based on their ranks, which are assigned to them based on their fitness benefits. The likelihood of the arrangement prematurely converging to a local minimum is reduced using the rank selection method. The idea is to give people with high fitness scores preference and let them pass on their genes to future generations. Within the search area, the population of individuals is maintained. In the search space for a given problem, everyone represents a solution. Everyone is encoded as a component vector of finite length, analogous to a chromosome. Genes are comparable to these variable components. As a result, a person's chromosome is made up of several genes, or variable components.

Table 3.1: Selection operator of genetic algorithm

String no.	Initial population	X value	Fitness(Fj) F(x) = x.x	pi	Expected count no. Of probability
1	01101	13	169	0.14	0.58
2	11000	24	576	0.49	1.97
3	01000	8	64	0.06	0.22
4	10011	19	361	0.31	1.23
Sum			1170	1.00	4.00
Average			293	0.25	1.00
Maximum			576	0.49	1.97

3.1.3 Crossover Operator

The offspring are produced by combining the genetic information of two or more parents using crossover operators. Single-point, two-point, k-point, uniform, to some extent coordinated, request, priority safeguarding hybrid, mix, decreased proxy, and cycle are notable hybrid administrators. A random crossover point is chosen in a single-point crossover. Two parents' genetic information that is beyond that point will be exchanged with one another. It supplanted the tail exhibit pieces of both the guardians to get the new posterity.

Table 3.2: Crossover operator of genetic algorithm

String no	Mating pool	Crossover point	offspring	X value	Fitness F(x)= x.x
1	0110| 1	4	01100	12	144
2	1100| 0	4	11001	25	625
2	11| 000	2	11011	27	729
4	10| 011	2	10000	16	256
sum					1925
average					439
max					729

Parents cannot be broken down into segments during a uniform crossover. Each gene can be treated separately from the parent. We choose at random whether the gene on a different chromosome should be swapped. Individuals swapping across crossover tables under uniform crossover operation. A somewhat paired hybrid is the most often utilized hybrid administrator. It is a crossover operator that outperforms the majority of the others. D. Goldberg and R. Lingle came up with the idea for the partially matched (mapped) crossover. For mating, two parents are chosen. A portion of the child's genetic material is donated by one parent, and the other parent shares that portion. The missing alleles are copied from the second parent after this step is finished.

Davis proposed order crossover (OX) in 1985. From the selected cut-points, OX copies one or more portions of the parent to the offspring and fills the remaining space with values that are not included in the copied section. Different researchers have proposed OX variants for a variety of issues. OX is useful for problems with the order. However, the Travelling Salesman Problem reveals that OX is less effective. Precedence preserving crossover (PPX) keeps the order of individual solutions in the parent of offspring as it was before crossover was used. The offspring is set up with a string of random 1s and 0s that tells whether the children from both parents should be chosen. To lessen the bias that is caused by other crossover methods. To ensure that the crossover point does not introduce bias into the crossover, it shuffles the values of a particular solution before the crossover and then unshuffled them following the crossover operation. Be that as it may, the use of this hybrid is exceptionally restricted in the new year. If the parents have the same gene sequence, reduced surrogate crossover reduces the number of unnecessary crossovers for solution representations. RCX is based on the idea that if the parents have enough genetic diversity, GA will produce better offspring. However, RCX cannot produce better offspring for parents with identical genetics. Olive proposed a cycle crossover. It tries to produce offspring by using parents, with each component referring to the position of their parents. It borrows some components from the first parent during the first cycle.

Crossover techniques are compared in Table Crossover. From Table crossover, single and k-point crossover methods are simple to use. Large subsets can benefit from uniform crossover. The exploration provided by order and cycle crossovers is superior to that of the other crossover methods. Exploration is improved by using partially matched crossover. Partially matched crossover outperforms the other crossover methods in terms of performance. Premature convergence affects cycle and reduces surrogate crossovers.

3.1.4 Mutation Operator

Mutation, an operator, preserves genetic diversity from one population to the next. Well-known mutational operators include displacement, simple inversion, and scramble mutation. Within one unique solution, a substring is moved using the displacement mutation (DM) operator. The position is chosen at random from the provided substring for displacement to guarantee that the solution and the random displacement mutation are both legitimate.

Two DM variations are the insertion mutation and the exchange mutation. Using the Exchange mutation and Insertion mutation operators, two components from a single solution are either exchanged for one another or inserted at a different place. Using the SIM (simple inversion mutation operator), the substring between any two given points in a single solution is inverted. The random string is placed in a random spot and is reversed by the inversion operator SIM. The scramble mutation (SM) operator randomly places the elements within a predetermined range of the individual solution to test whether the fitness value of the freshly generated solution has increased or decreased. The Mutation Table contrasts the different mutation techniques.

Table 3.3: Mutation operator of genetic algorithm

String no	Mating pool	Crossover point	offspring	X value	Fitness F(x)= x.x
1	01100	4	11100	26	676
2	11001	4	11001	25	625
2	11011	2	11011	27	729
4	10000	2	10100	18	324
sum					2354
average					588.5
max					729

The primary concept is to introduce random genes into the offspring to maintain the diversity of the population and avoid premature convergence. The key thought is to embed irregular qualities in posterity to keep up with the variety in the populace to stay away from untimely combinations.

For example: 100 1 11101

101 1 01011

Offspring: 10001011

10111101

Two point: 100 1 11 1 101

101 1 01 1 011

Offspring: 10001 101

10111 011

The algorithm can be summarized as follows:

1) Randomly initialize populations p

2) Determine population fitness

3) Repeat until convergence:

- Choose parents from the population.
- Crossover and create a new population.
- Perform mutation on the new population.
- Calculate fitness for the new population.

GA is a useful metaheuristic for resolving operation management (OM) issues like the facility layout problem (FLP), the design of supply networks, scheduling, forecasting, and inventory control.

3.2 Criteria of the genetic algorithm

Genetic Algorithm has some outstanding criteria. Those criteria are the main reason for choosing this algorithm.

- Genetic algorithms work faster than another existing algorithm.
- By improving all the individual fitness of bitstream
- Efficient hiding capacity allows better audio quality.
- Genetic algorithms ensure higher network security.

CHAPTER – 4
METHODOLOGY

"Explains in detail, including their underlying formulas, the genetic algorithm and implementation platform used in the thesis."

4.1 Research Implementation Procedure

4.1.1 Implement GA in Visual Studio Platform with Python

4.2 Methodology of This Process

4.2.1 Encoding at the sender side

4.2.2 Decoding at the receiver side

4.3 Determine the Audio Quality

4.4 Data Collection Methods

4.5 Proposed Calculation to work on every one of the creatures.

METHODOLOGY 4

Data collecting, technique analysis, major behavior construction, and classification based on similarity make up the review approach for this work.

Discussing the three primary needs of audio steganography and current trade-offs is essential to comprehending the methods examined in this research as well as the motivations behind such a level of variation. Each audio steganography technique's performance improvement is still largely dependent on one of the three key criteria, namely capacity, perceptual transparency, and robustness.

4.1 Implementation Procedure

Genes can be represented in a variety of ways, including binary, decimal, integer, and other formats. The treatment of each type is different. Bit flip, swap, inverse, uniform, non-uniform, Gaussian, shrink, and other mutations are just a few examples. Additionally, there are various types of crossover, including uniform, blend, one-point, and two-point, among others. This procedure will only put one type of each GA step into action, not all of them. Genes, one-point crossover, and uniform mutation are represented using decimals.

4.1.1 Implement GA in Visual Studio Platform with Python

The process begins with the presentation of the equation that we will use. The condition is displayed underneath:

The equation has six inputs (x1 to x6) and six weights (w1 to w6), as shown, and the input values are (x1,x2,x3,x4,x5,x6)=(4,-2,7,5,11,1). Y = w1 x 1 + w2 x 2 + w3 x 3 + w4 x 4 + w5 x 5 + w6 x 6, We are looking for the parameters (weights) that contribute the most to this equation. Maximizing such an equation seems straightforward. The positive input must be multiplied by the largest positive number and the negative input by the smallest negative number. However, the idea that we want to put into action is how to make GA decide for itself whether positive inputs and positive weights are preferable to negative loads with negative data sources. Let's begin putting GA into action.

The following stage is to characterize the underlying populace. Each solution or individual chromosome in the population will unquestionably contain six characteristics, one for each weight. In any case, the inquiry is what number of arrangements per populace? We can choose the value that best addresses our issue because there is no set amount. However, we could leave it as-is so that the code can modify it. The number of solutions per population, the size of the population, and the actual initial population are all held in variables that are created next. We can use the NumPy random uniform function to randomly generate the initial population after importing the NumPy library. It will have a shape that matches the parameters that were chosen (8, 6). Each of the eight chromosomes contains six genes, one for each weight.

We will select the best individuals from the current population to be the parents for mating after preparing the population using the fitness function. The next step is to use the GA variants (crossover and mutation) to produce the next generation's offspring, adding both parents and offspring to the population and repeating this process for several iterations or generations.

Utilizing the ***ga.cal_pop_fitness*** function, the first step is to determine the fitness value of each population solution. The GA module's implementation of this function. In addition to the population, the fitness function considers both the values of the equation's inputs (x1 to x6). As per our capability, the wellness esteem is determined as the amount of the item (SOP) between each info and its related quality's weight. There will be several SOPs in light of the quantity of arrangements per populace. As we recently set the number of answers for 8 in the variable named ***sol_per_population*** After computing the wellness values for all arrangements, next is to choose the best of them as guardians in the mating pool as per the following capability ***ga.select_mating_pool***. The population, fitness values, and the required number of parents are all accepted by this function. It returns to the chosen parents. The next step is to mate with these chosen parents to produce children. Using the ***ga. crossover*** function, the crossover procedure initiates mating. The size of the parents and the offspring are accepted by this function. It determines the number of children to produce from these parents based on the size of the offspring. The ***ga. mutation*** function within the GA module is used to apply the second GA variant, mutation, to the crossover results stored in the offspring variable. After applying uniform mutation, this purpose returns the hybrid posterity.

The function recurs these results succeeding in adding them to the ***offspring_crossover*** variable. We have effectively created four children from the four chosen ancestors at this point, and we are prepared to raise the advanced generation's inhabitants. Keep in mind that GA is an optimization method based on randomness. It attempts to improve the ongoing arrangements by introducing a few haphazard modifications. We are uncertain that such random changes will result in better solutions. As a result, it is preferable to incorporate the prior best solutions—parents—into the new population. We will continue to use these parents even if, in the worst case, all the new offspring are worse than their parents. Consequently, we guarantee that the subsequent generation will not worsen the previous generation's achievements. The previous parents will provide the new populace with its initial four arrangements.

4.2 Methodology of This Process

The method used and procedure proposed for implementation. Our objective is to successfully conceal secret messages within cover audio. We encode secret messages using a genetic algorithm and conceal them on the receiver side. To embed secret data, we select a cover audio file (.wav format). In this instance, we must work to maintain the highest possible audio quality and increase the hiding capacity. We successfully decrypted secret messages for the receiver. This is a safe and effective method of communication.

4.2.1 Encoding at the sender side

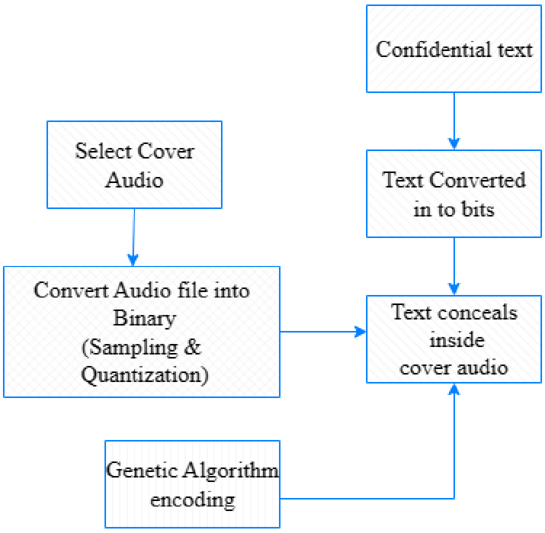

Confidential text
Select Cover Audio
Text Converted in to bits
Convert Audio file into Binary (Sampling & Quantization)
Text conceals inside cover audio
Genetic Algorithm encoding

Figure 4.1: Block diagram of encoding procedure

Sender side encryption

1. Select any size secret text message.
2. Convert each secret message symbol into a binary-like bit.
3. Receive the cover audio signal.
4. Utilize sampling and quantization to convert the selected cover audio file into binary format.
5. Utilize the Genetic algorithm to transform the binary bit of the cover audio into the binary bit of the secret message.

4.2.2 Decoding at the receiver side

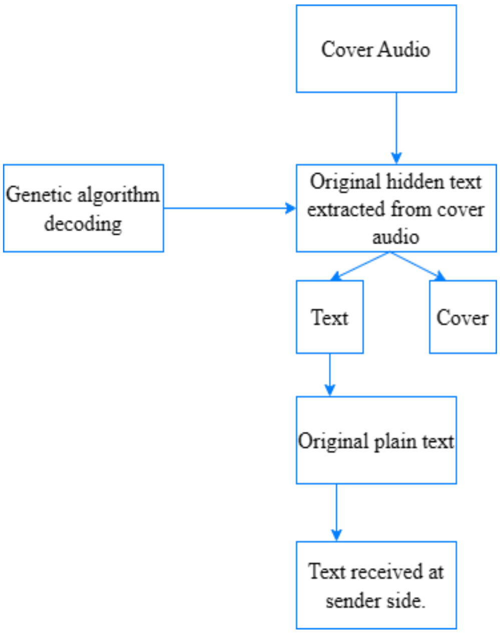

Cover Audio
Genetic algorithm decoding
Original hidden text extracted from cover audio
Text
Cover
Original plain text
Text received at sender side.

Figure 4.2: Block diagram of decoding procedure

Decryption on the first receiver side

1. Utilizing the genetic algorithm decoding method, decode the concealed text message from the carrier audio signal.

2. After decompression, retrieve the original text from the receiver.

Both Figures 3.1 and 3.2: demonstrate the genetic algorithm-based encoding and decoding of secret data in an audio file using a block diagram. Through sampling and quantization, the analog host message (cover audio) is transformed into binary. The binary bit of the contracted hidden message takes the place of the GA in the cover audio for each sample. The replacement operation was carried out by us using the GA coding method. We used the GA decoding method to get the hidden message from the cover audio file.

4.3 Determine the Audio Quality

After hiding, we try to maintain high audio quality. Noise causes the audio signal to become distorted when message bits are inserted into it. A distorted signal makes it easier for hackers to determine which signal carries a secret message bit, and extra bits add noise, which lowers audio quality. So that no third party can detect the signal, it is essential to maintain the highest possible sound signal quality. Additionally, the hiding capacity must be sufficient and high.

The SNR value of both the carrier audio and the Stego audio is how we determine the audio quality.

$$SNR = 10 \log(S/N) \ldots\ldots\ldots\ldots\ldots\ldots. (1)$$

The proposed technique made use of the SNR to assess the triggered commotion caused by the implantation of the mystery message in the cover sound. It is clear from the method that good and greater signal-to-noise ratios (SNR) are necessary for efficient communication. The stego audio is produced using the embedding procedure. The SNR for both the covered audio signal and the stego audio signal files was calculated in this experiment. The best SNR values for efficient internet communication were positive and higher.

where N is the power of noise and S is the power of the signal. 8 bits per sample, or 255, are used to present the audio samples. An estimator's quality is measured by its SNR, which is always positive in effective communication and moves closer to one as the value increases. From condition (1), sound signal clamor can be ascertained by estimating the variety between the first sign strength and commotion signal strength by deducting the clamor esteem from the cover signal strength esteem. Condition (1) recipe utilized in the Python stage. SNR can be calculated with Python code. The SNR of both cover and stego audio is determined with the help of a signal-to-noise ratio function. A signal-to-noise ratio () function is included in a subpackage of the SciPy library for the Python platform.

4.4 Data Collection Methods

SNR value of cover audio and stego audio will be collected.

- Data will be collected from every sound example, for example, dot wav sound document. Various sizes of sound document will be taken. Size of audio will, 868kb, 3318kb, 1Mb, 2.52Mb, 10Mb, 21Mb, 45Mb……
- Secret text will hide inside those audio files. This proposed Method will be implemented in such a way that it will be able to hide different size of text file even a large size text file. Size of text will, 100bytes, 500bytes, 1000bytes, 1500kbytes, 2000bytes, 2500bytes, 3000bytes…………
- To measure audio quality after hide text, SNR of the original audio and stego audio will be calculated. This technique must keep the SNR value positive and near to 1.

4.5 Proposed Calculation to work on every one of the creatures:

Boost of the capability f(x) = x^2 with x in stretch [0, 31] i.e., x= 0,1, ………….30, 31.

1. Randomly generating the initial population. Genotypes or chromosomes are those,
   Example, 01110 (14), 11001 (25), 01001 (9), 10100 (20).
2. determining fitness,
   (a) Decoding into number (called aggregates). 01110 = 14, 11001 = 25, 01001 = 9, 10100 = 20.
   (b) Evaluating wellness, f(x) = x^2. 14 = 196, 25 = 625, 9 = 81, 20 = 400.
3. Two select parents were chosen based on their fitness is p: pi = $fi/(\sum_{f=i}^{n} Fj)$

Where, Fi is the population's suitability for the string i.

Pi is the chance that the string i will be chosen.
n is the quantity of people in the population. expected number, n*pi.

Operator of crossovers: One-point or two-point crossovers are possible. The selected strings can be cut in the one-point hybrid at any arbitrary orientation. After that, new string pairs were created by swapping the segment. There will be a breakpoint at every stage of the two-point crossover.

The operator of the mutation: Each child's mutation may be unique. Binary bits change from 0 to 1 or from 1 to 0 at any position on an unevenly chosen string after crossovers. There is an uneven mutation. After that, 1 was muted to 0 and 0 to 1. All the people's fitness can be improved by the GA. And the superior outcome here after utilizing the genetic algorithm. Protocol for secure communication with the genetic algorithm that has been proposed. A Genetic Algorithm (GA)-based algorithm design for communication networks that is both robust and highly secure while also speeding up the steganography process. Hereditary calculations exist in the huge gathering of developmental calculations (EA), which take care of advancement issues utilizing techniques propelled by regular development.

Embedding Procedure: This procedure was carried out by the sender. The covert audio contained the secret message. The sizes of each sample of audio, such as a dot wav sound signal file, varied. 868kb, 3318kb, 1Mb, 2.52Mb, 10Mb, 21Mb, and 45Mb were the audio file sizes. Bitstream was formed by partitioning the covered audio sample. The bitstream's fitness is improved when the genetic algorithm is used. The genetic algorithm is superior due to its simplicity and speed of computation. The mystery message was encoded in the covered example's most noteworthy wellness bitstream position which was adjusted for concealing the mystery message bits.

Extraction Interaction: This cycle utilised the beneficiary's side. Through this cycle, the recipient will gather the stego sound record. Recreate the same order as the original message in which the selected stego-file samples' embedded bits must be gathered. The original secret message was reconstructed using the highest fitness bitstream position that was obtained. During inserting straight forwardness, modification is merely the distinct between the indigenous and altered sample. More bits and samples are modified and adjusted with this proposed method than with other methods. Let's assume the following: 01110 (14). The message bit is 1 and the target layer is 5. Without modification: 16 is the difference between 11110 (30). After changing: 10000, the difference will be 2 for embedding with one bit. Once more, the sample bits are 11001(25). The message bits are 11 and the target layers are 2 and 3. Without changing: 11111(31), the thing that matters is 6. After changing: 10110(22), the difference will be three for embedding with two bits. The genetic algorithm is smart enough to come up with the best solutions.

CHAPTER – 5

RESULT AND ANALYSIS

"Shows the results and analysis them."

RESULT AND ANALYSIS 5

According to this approach, if a secret message were to be concealed using a genetic algorithm, how much commotion in the covered sound document would significantly reduce, making it more challenging for outsiders to decode the covered audio file's content. This would increase the method’s transparency and robustness. In the case of an audio signal, a highly calculated SNR indicates that the covered audio signal has very little induced noise. The experiment reveals that the stego audio has a higher SNR than the covered audio, which increased Securing communications. Audio files transmit data at a faster rate and have a high level of redundancy. for audio files to function as useful host files.

5.1 Outcomes

Genetic algorithm for finding the best and worst solution: An optimization that depends on search method backed by the fundamentals of natural selection and genetics is the Genetic Algorithm (GA). In research and machine learning, it is frequently used to come up with solutions to problems related to optimization. Through selection, recombination, and mutation, genetic algorithms come up with solutions until the best ones are found. It works well for useful building block speculations that can overcome other subpar answers.

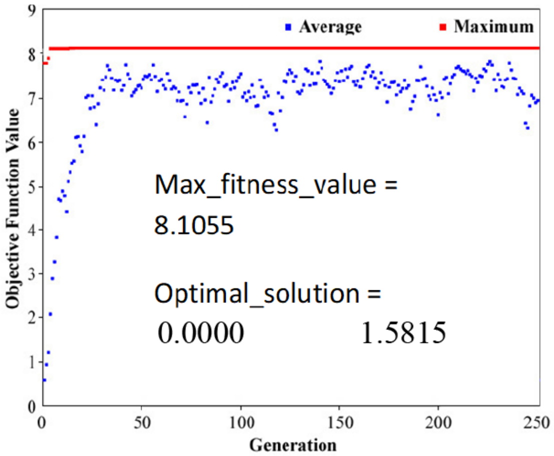


Figure 5.1: Genetic algorithm for finding optimal solution.

The graph in Figure 2 demonstrates that the genetic algorithm alters a population of distinct solutions repeatedly. The populace "develops" toward the best possible solution over time. Several fitness measures were used to evaluate the chromosome after each generation. The generation vs. objective function value values are shown in this figure in blue, while the maximum values are shown in red. By choosing fitness values, a new generation can be formed. Some parents and children have been selected, while others have been rejected. to maintain a constant population size. It is more likely that chromosomes that are more fitting will be chosen. The best chromosome was found by the algorithm after multiple generations.

5.1.1 Data analysis and interpretation with different text files.

Dissect the strategy with an alternate text document:

Here the sound record size is 1Mb. Concealing different sizes of text content in the sound document, we break down the sound quality as well as the concealing limit by estimating the SNR worth of the sound. Stego and cover audio differ only insignificantly, indicating a substantial hiding capacity.

Table 5.1: The SNR values for various text sizes within a single audio file

Audio File Size 1 MB			
File Name	**Text File Size (bytes)**	**SNR Value of Audio File**	
		Cover audio	**Stego audio**
Text 1	100	0.40557652	0.40561957
Text 2	500	0.40557652	0.40561202
Text 3	1000	0.40557652	0.40561235
Text 4	1500	0.40557652	0.40561186
Text 5	2000	0.40557652	0.40558841
Text 6	2500	0.40557652	0.4055767
Text 7	3000	0.40557652	0.40557225

Represents the above table in a graph:

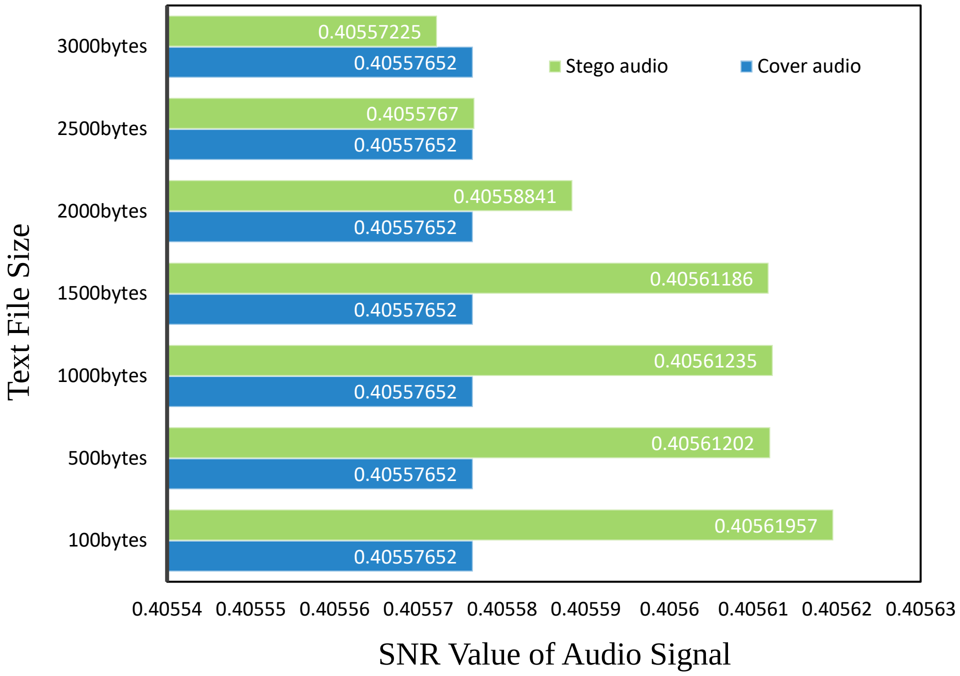


Figure 5.2: Different text file vs SNR value of audio signals.

The various sizes of the text files that will be hidden within a 1Mb audio file are depicted on the Y-axis of this graph. The audio file's corresponding SNR values are shown on the X-axis. Here, it can expect that stego sound possesses higher SNR esteem contrasted with cover sound. This graph shows that the SNR upsides of stego sound continue to decrease in comparison to cover audio when the data size is large (2000 bytes, a text file). This means that this method can successfully hide a 1Mb audio file up to 2000 bytes. When compared to the size of an audio file, this technique offers a huge concealing limit. The procedure keeps the nature of sound signal stable by keeping up with the sign-to-commotion proportion of the sound signal. The cover audio signal has less induced noise because the stego audio signal has a higher SNR. The security of communication is successfully enhanced by this method.

5.1.2 Data analysis and interpretation with different audio files

Utilize a different audio file to examine the method.

The text here is 1500 bytes in size. Concealing this text size in every sound record, we break down the sound quality by estimating the SNR worth of every sound.

Table 5.2: The SNR values for distinct size of audio files with same size text content

File Name	**Audio File Size**	**SNR Value of Audio File**	
		Cover audio	**Stego audio**
Audio 1	868 kilobytes	0.36886518	0.36927474
Audio 2	3318 kilobytes	0.66604743	0.666081511
Audio 3	1 Megabytes	0.40557652	0.40560117
Audio 4	2.52 Megabytes	0.62930035	0.63029749
Audio 5	10 Megabytes	0.40959791	0.40965664
Audio 6	21 Megabytes	0.33539042	0.33657810
Audio 7	45 Megabytes	0.38839123	0.38864556

Represents the above table in a graph:

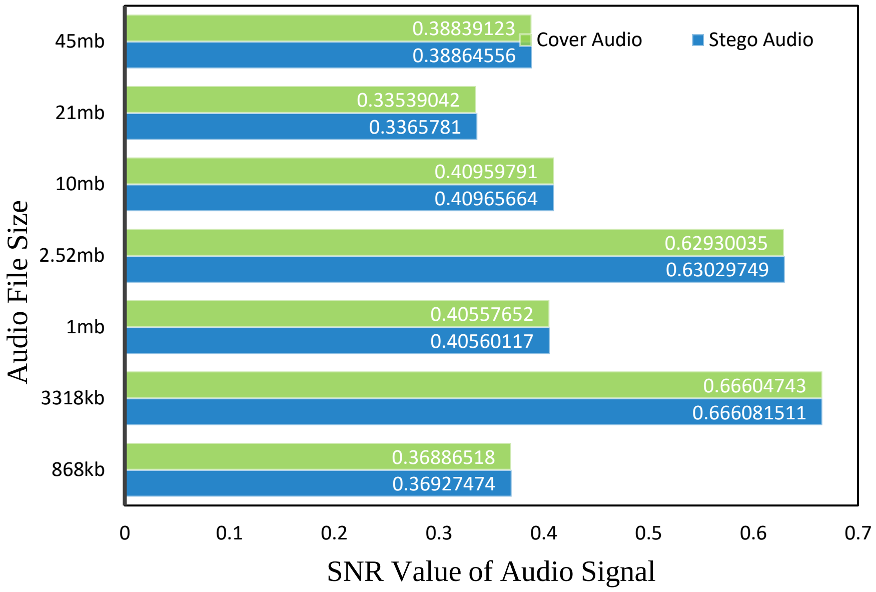


Figure 5.3: Different audio files vs SNR value of audio signals.

Figure 5.3 shows the SNR values for audio files of various sizes with the same amount of content (1500 bytes).This method was examined by concealing a similar size of mystery text inside various sound records, the concealing limit was adequate for huge sizes of sound documents, for example, 10mb, 21mb, 45mb, and so on. By keeping the audio's quality, the larger audio files effectively concealed the hidden message. Compared to the covered audio, those gave a positive and higher SNR esteem (close to 1) for the stego audio. In contrast, these proved unable effectively enhance the audio quality of Stego for smaller audio files, such as 868 kilobytes or 1 megabyte. Even though the stego audio has lower SNR than the covered sound, the thing that matters is as well small to be considered significant. As a result, the audio signal's quality is preserved while large amounts of data are successfully hidden using this strategy. This approach promises to improve safe internet communication. When comparing text files of different sizes included in the same audio signal (1 MB), the covered audio SNR is 0.40557652 and the stego audio SNR is 0.40557225. The gap in this instance is 4.27e-6. Additionally, the covered audio SNR for 2500 bytes of data is 0.40557652, while the stego audio SNR is 0.4055767. The difference is 1.8e-7 in this case. These distinctions are too minute to be easily overlooked. Then again, while dissecting various sizes of sound documents with a similar substance (1500bytes), in the event of 45mb sound, the covered sound SNR is 0.38864556, and the stego sound SNR is 0.38839132. This variation is 0.00025424. Furthermore, the covered audio SNR for 21 MB audio is 0.3365781, while the stego audio SNR is 0.33539042. 0.00118768 is the difference in this case. In this instance, the differences are also too minor to be easily overlooked.

The various audio files' potential for concealing information has risen, and audio quality has improved, as can be seen in Table 5.1, Table 5.2, Figure 5.2, and Figure 5.3 Despite the content's relatively small size, the audio quality improved (the SNR value increased) by encasing secret texts of varying sizes within the same audio file. The quality was comparable to the audio that was covered when there was a lot of data. At the point when the text content was extended to 3000bytes, which was a significant quantity of data, the audio quality marginally declined. To improve audio quality, noise must be reduced, and the SNR value must be increased. It functions.

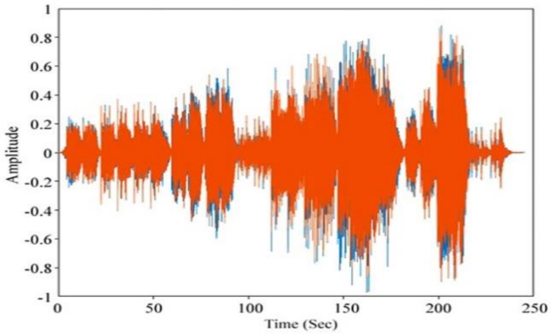
5.1.3 MATLAB - Amplitude vs. time plots:

effectively for secret data contents of a small and medium sizes.

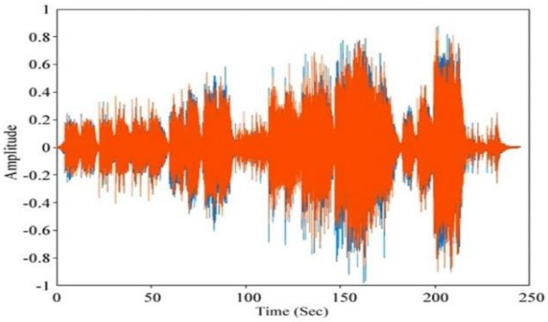
Using MATLAB code, plot wav sound files onto a graph for analysis of cover dot. wav sound records and stego dot. wav sound records.

Before encoding **After encoding**

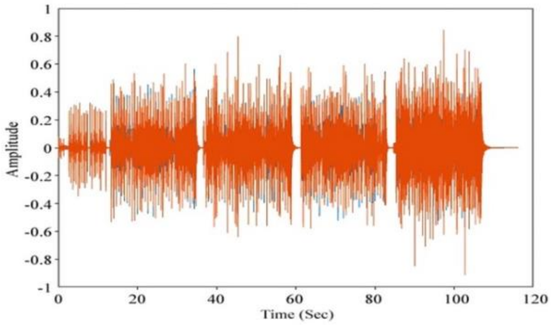
(a) 45 Mb cover audio



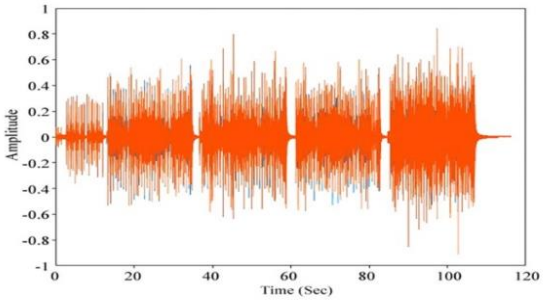
(b) 45 Mb stego audio



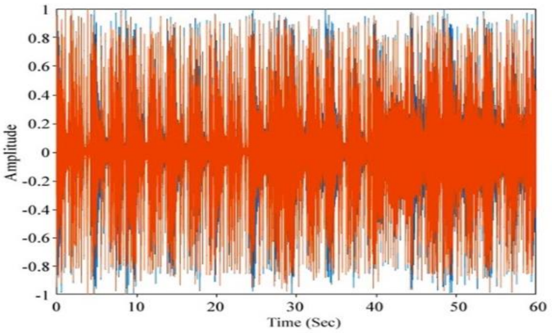
(c)21 Mb cover audio



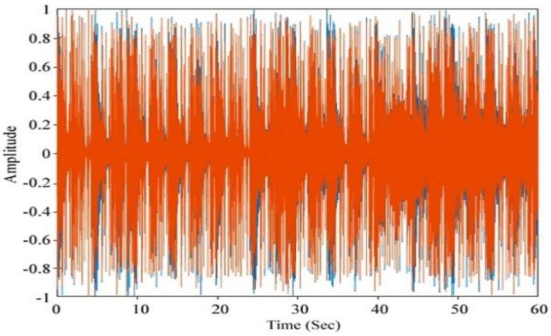
(d) 21 Mb stego audio



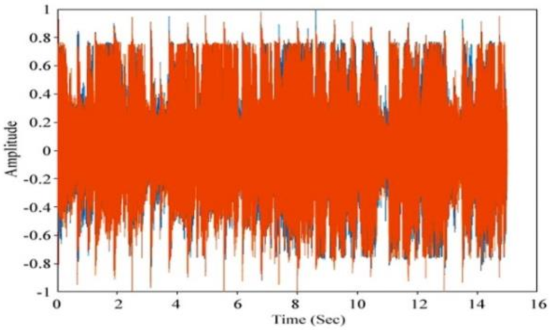
(e)10 Mb cover audio



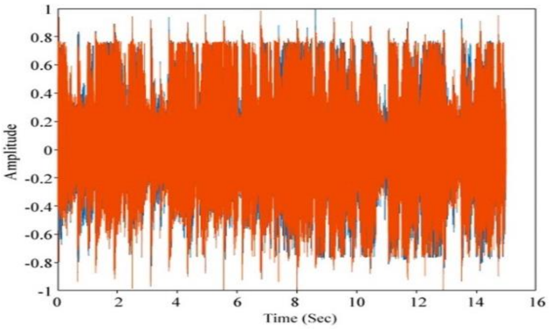
(f) 10 Mb stego audio

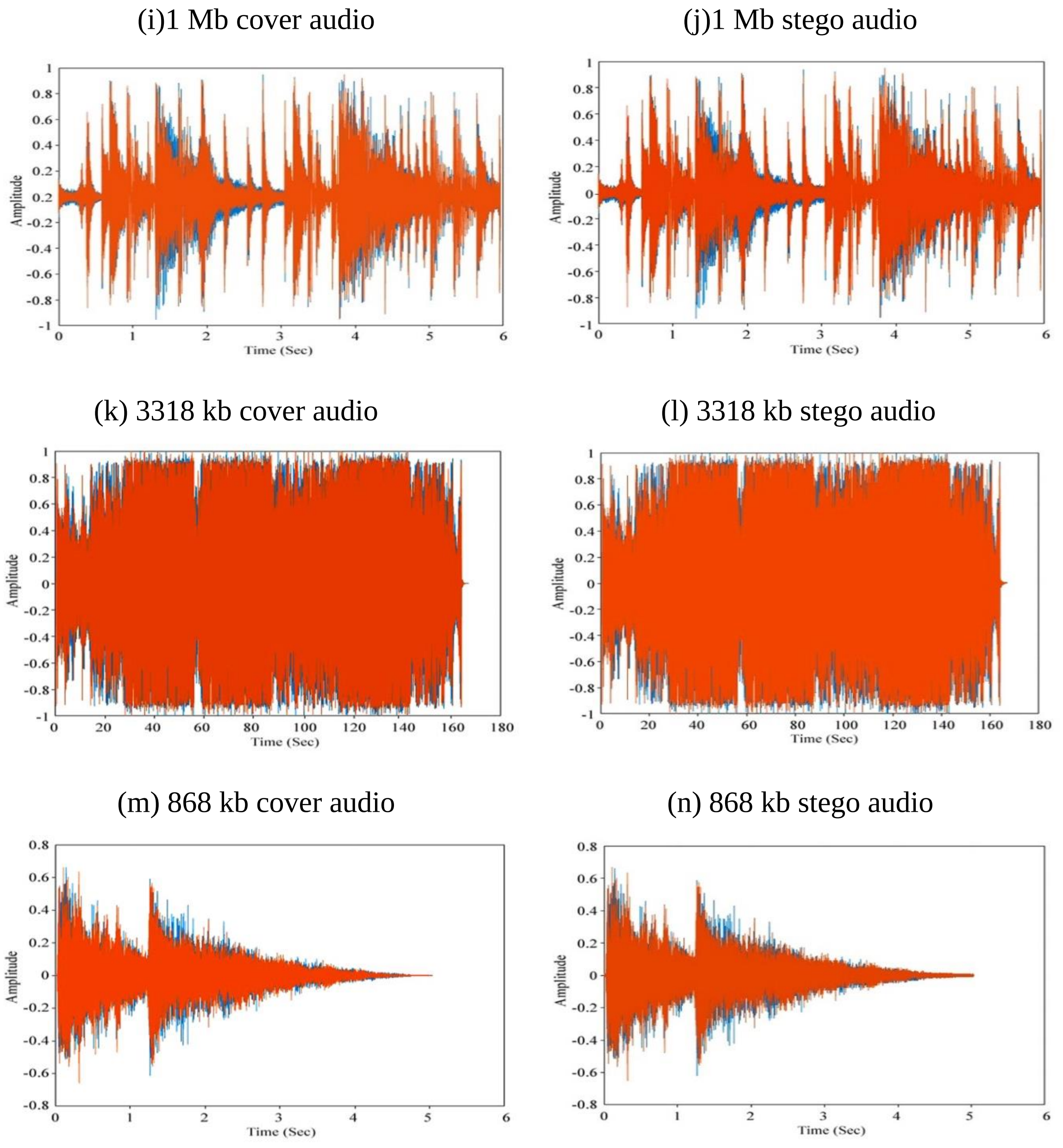


(g) 2.52 Mb cover audio



(h) 2.52 Mb stego audio





(i)1 Mb cover audio

(j)1 Mb stego audio

(k) 3318 kb cover audio

(l) 3318 kb stego audio

(m) 868 kb cover audio

(n) 868 kb stego audio

Figure 5.4: Amplitude vs. time plots

Sound steganography is an additional step for stowing away or safeguarding classified information. A secret message written into a dot wave file adds unwanted signals. The Python platform's genetic algorithm-based method can effectively conceal data with very little When encoding, noise (unwanted signals) is added. A gatecrasher never recognizes the progressions between a cover sound and a stego sound. After encoding the dab wave sound signs show no visual changes. In the hereditary calculation, message pieces can implant into a few more profound layers to accomplish higher limits and strength. To improve the SNR and conceal a hidden message in wav files, efficient coding methods are required. The outsider necessities to disentangle correspondence codes to interpret the secret message. Third parties find this action challenging. Any two pairs' amplitude and time scale values do not change in the amplitude vs. time plot signal. The comparison of cover audio and stego audio files is depicted in Figure 5.4 Before encoding, all cover audio files are identified by (a), (c), (e), (g), (i), (k), and (m). In contrast, all stego audio files are identified by (b), (d), (f), (h), (j), (l), and (n) after being encoded. Figure 5 suggests that after encoding, all stego audio signals maintain their original structure. This productive technique adds an irrelevant measure of commotion so that after encoding the sign shape doesn't change discernibly. Compared to the 45Mb cover audio, the 45Mb stego audio remains unchanged after encoding. Too for 21Mb, 10Mb, 2.52Mb, 1Mb, 3318Kb, and 868Kb cover sound records their particular stego sound documents stay unaltered discernibly. Audio steganography aims to conceal the secret message when detecting the wave by taking advantage of human visual redundancy to embed it in the original cover audio. This strategy has adaptability. It doesn't change anything, so it keeps more information hidden. Audio steganography prevents the implementation of numerous malicious attacks. As a result, it appears that all cover audio files remain unchanged after encoding when MATLAB graphs are created. Figure 5.4 shows that less noise is added to a large audio file than a small audio file, effectively masking the same data. By zooming in on the audio signal, it can justify itself. The signal shape of smaller audio files becomes thicker after encoding than that of larger audio files. This indicates that audio files smaller than 2.52Mb, 1Mb, and 868Kb have a lower hiding capacity than files larger than 45Mb, 21Mb, and 10Mb. Small audio files add more noise than large audio files, just like text of the same size does. Notwithstanding, the progressions are too little to even think about distinguishing, as encoded diagrams convey a similar time and plentifulness scale for their particular cover sound. The hidden message that is contained within an audio signal cannot be decoded by various malicious attacks, such as geometrical distortions and spatial scaling. Because there are fewer steganalysis techniques for attacking audio, encoded audio appears to be more secure. There is no difference between the original and encoded dot pairs as seen by the common eye. wav signals in each of the seven instances.

This method offers stability after encoding. That is the main achievement of this technique.

5.2 Analysis of the Findings Concerning the research question

According to our aim, we successfully hide secret information, and we can keep audio quality high by keeping the SNR value positive. We also efficiently increase the hiding capacity. We must ensure that less noise is generated and that no signals are missed when evaluating this process's fitness. We check this by comparing the cover's SNR value to that of the encrypted audio signal. knowledgeable enough to minimize that much noise is a genetic algorithm. so that additional recovery is unnecessary to secure communication. Based on the data analysis tables 5.1.1 and 5.1. 2, it is reasonable to assume that the algorithm successfully conceals large amounts of text in audio files. The algorithm provides near-zero SNR and conceals text within an audio file. In the case of hiding text of small size, this method can effectively reduce the noise power; however, when dealing with enormous amounts of information, the clamor power dropped to a point that was likewise appropriate for clear interaction.

5.3 Functional Application

The process provides excellent security. Because there is no discernible contrast between the original and the encoded signals, any third party that receives the signal will never be able to decipher the concealed information. The technique has useful uses in cyber security. The technique offers defense industry and transportation system protection, as well as critical infrastructure protection. Systems for tracking and communication are part of transportation. This method can maintain the security of the transportation network. Communication over the internet is the economy’s engine. It is the gateway to new resources and opportunities. It connects users in the economy, encourages their chat, and keeps them posted on their plans. Communication through social networks such as Facebook, YouTube, and WhatsApp are economical and the most popular platforms. Keeping secure communication over those platforms is a vital issue. Cybersecurity is important for the government and other organizations like the military, and special detective branch, which has a direct relation with nations or the world. This proposed method aim is to create safe functioning of cyberspace against the threats of cyber-attacks. Therefore, this technique has a large importance in communication in socio-economic development.

CHAPTER – 6
DISCUSSION

“We discuss the result and studies.”

6.1 Interpretation of Results

6.2 Applications and significance of the findings

6.2.1 For confidential information security

6.2.2 For video processing

6.2.3 For medical imaging

6.2.4 For image processing

6.2.5 In Wireless Networking

6.3 Limitations of the Study

6.3.1 Choosing the initial population.

6.3.2 Premature convergence

6.3.3 Selecting effective fitness functions.

6.3.4 Degree of mutation and crossover Operators

DISCUSSION 6

In our proposed strategy, that's what we guaranteed if we pack the mystery message before concealing than a measure of commotion in the cover sound record would be diminished tremendously which will make hardships in extricating the genuine data from the cover sound the document by the outsiders, which will build the vigor and straightforwardness of our proposed strategy. If the calculated SNR for an audio signal is positive, it indicates that the cover audio signal has very little induced noise.

6.1 Interpretation of Results

Audio files are an excellent host file for hiding because of their high level of redundancy and high data transfer rate, as well as their size relative to other multimedia files. The data analysis tables indicate that our method conceals text more successfully in larger audio files than in smaller ones.

For audio signals, this is a high-capacity method for hiding data. Any size of audio signal can be used with the presented algorithm. It offered more space for audio files of larger sizes. It maintained the audio quality while improving security. It became more difficult by incorporating the method into large texts, but it also provided improved security measures that can provide stipple security. To conceal the availability of data utilizing a carrier file, two authorized parties must communicate secretly. This is a channel-based better steganography method where secret pieces are inserted by the hereditary calculation of the covered sound. Our planned methodology is typically put to the SNR test using this approach. We can see from the values above that the covered audio had a significant increase in its capacity to conceal new information without affecting the audio output from the host perceptual transparency, that can lessen noise. Increased online security is provided by the implemented method. In addition, it offers effective confidentiality and a large capacity for concealment. The result of this method's implementation is a tiny difference between stego and the original audio. The difference between 300-byte text data and 45 MB audio is 0.00118768, and the variance is 1.8e-7. It is simple to avoid those minute values.

A third party cannot distinguish between the stego and the original audio. This indicates that not at all, the signal change following the message is hidden. The strategy can be used for reliable and private interaction that is both secure and effective. However, for this method to be effective with audio files of any size, further development is required. Therefore, additional research on this restriction will be required in the future.

Table 6.1: Comparison with Existing Literature

Authors	Capacity	SNR	OUTPUT
Mazdak Zamani 1, Azizah A. Manaf [17]	greater strength and capacity	-	Effectively conceal confidential data
Padmashree G, Venugopala P S [18]	-	Less than zero	Efficiently hide secret data
Nedeljko Cvejic, Tapio Seppänen [19]	-	-	Increase the resilience of the stego audio transmission and conceal a secret message.
Mazhar B. Tayel, Ahmed Gamal Abdalatife [20]	-	-	Measure the PSNR of the stego audio signal while hiding secret info. The method's results have greater PSNR values and, in comparison, lower MSE values.
Proposed	Obtain a good hiding place. This method can hide up to 10,000 bytes.	SNR value is close to 1 and positive.	Easily conceal sensitive information inside audio signals while preserving audio quality. The approach is secure, has a high SNR value, and has a sizable hiding capacity.

6.2 Applications and significance of the findings

Numerous NP-hard problems have been solved with high accuracy using genetic algorithms. There are a few areas of application where GAs have been utilized successfully.

6.2.1 For confidential information security

Images, videos, and audio are transferred over the Internet because of advancements in multimedia applications. The transmission of images is found to be more prone to error, according to research. As a result, image security measures like watermarking, encryption, and cryptography are required. The input parameters are required for encryption by the traditional image encryption methods. Encryption results will be inadequate if the input parameters are not selected correctly. The right control parameters have been chosen using GA and its variants. A genetic algorithm with multiple goals was created by Kaur and Kumar to improve the control parameters of a chaotic map. The beta chaotic map was used to produce the secret key. The image was encrypted with the generated key. In addition, the image was encrypted with parallel GAs.

6.2.2 For video processing

Pattern recognition and computer vision have both made extensive use of video segmentation. Video segmentation is associated with several significant issues. These are what differentiate the object from the background and establish precise boundaries. These problems can be fixed with the help of GA. GAs have been successfully used for gesture recognition. used GA to recognize gestures. They used GAs and found that robot vision was 95 percent accurate. They said that compared to the current method, which has an accuracy of 79%, their improved recognition rate was 85 percent. Face recognition, in addition to gesture recognition, plays a crucial role in the identification of criminals, unmanned vehicles, surveillance, and robots. The occlusion, orientations, expressions, pose, and lighting conditions can all be addressed by GA.

6.2.3 For medical imaging

In medical imaging, genetic algorithms have been used to detect pulmonary nodules in a CT scan image and edges in an MRI. a GA-based template matching method for CT image nodule detection. detecting the brain tumor using a region-growing technique based on GA. GAs have been utilized for pathological subject-captured medical prediction problems. In biomechanics, GA was used to solve problems that arose. During the examination, it is used to predict pathologies. utilized cellular automata and sequential GA to model the COVID-19 data for modeling. GAs can be used to find rules in biological datasets in parallel. a parallel GA that evaluates the fitness of each solution in parallel and divides the process into smaller sub-generations. In medicine and other related fields, genetic algorithms are used to evaluate a drug's side effects using a genetic algorithm.

6.2.4 For image processing

Preprocessing, segmentation, object detection, denoising, and recognition are the primary image processing operations. A crucial step in resolving issues with image processing is image segmentation. A lot of computational power is needed to decompose or partition an image. GA is used to solve this issue due to its superior search capabilities. An approach to enhancing an image's contrast and quality is called enhancement. To analyze the given image, better image quality is required. GAs have been used to magnify images and increase natural contrast. To combine the noise and color attributes, some researchers are working on hybridizing a rough set using an adaptive genetic algorithm. The noise in the given image was removed using GAs. To remove noise from the noisy image, GA can be combined with fuzzy logic. Haze, fog, and smog can all be removed from the given image using a restoration technique based on GA. In a real-world problem, object detection and recognition are a challenging issue. During the process of detection and recognition, the performance of the Gaussian mixture model is superior. GA is used to make the control parameters work better.

6.2.5 In Wireless Networking

GA has been utilized to resolve a variety of wireless networking issues because of its adaptability, scalability, and ease of implementation. Routing, quality of service, load balancing, localization, bandwidth allocation, and channel assignment are the primary issues of wireless networking. To solve the routing issues, GA has been combined with other metaheuristics. Hybrid GA is used for load balancing in addition to producing effective routes between pairs of nodes.

6.3 Limitation of the study

Despite the various benefits, there are provokes that should be settled for future headways and further development of hereditary calculations. The following are major obstacles:

6.3.1 Choosing the initial population.

The performance of genetic algorithms is always influenced by the initial population. The quality of the solution is also influenced by population size. The researchers argue that the algorithm takes longer to compute if a large population is considered. However, the small number of people may result in a poor solution. As a result, determining the ideal population size is always a challenging problem. The population was studied using the self-adaptation method. used two strategies, including (1) self-adaptation before algorithm execution, in which the population size remains unchanged, and (2) self-adaptation during algorithm execution, in which the population size is affected by the fitness function.

6.3.2 Premature convergence

GA frequently encounters this issue. It may result in the loss of alleles, making gene identification challenging. Premature convergence states that if the optimization problem coincides too early, the result will be suboptimal. Some researchers suggested that diversity should be used to avoid this problem. Diversity should be increased through selection pressure. Selection pressure is a level that favors the best people in the first group of GAs. The population using SP1 should be larger than the population using SP2, as SP1 has a higher selection pressure than SP2. Population diversity can be reduced because of the increased selection pressure, which may result in premature convergence.

6.3.3 Selecting effective fitness functions.

The fitness function is the driving force behind the selection of the fittest person in each algorithm iteration. A costly fitness function can be modified if the number of iterations is small. The computational cost may rise as the number of iterations increases. The fitness function to choose is determined not only by their suitability but also by their computational cost. utilized the Davies-Bouldin index for document classification.

6.3.4 Degree of mutation and crossover Operators

For mutation and crossover are essential components of GAs. There will be no new information for evolution if the mutation is not considered during the process. The algorithm may produce local optima if the crossover is not considered during evolution. GA performance is significantly influenced by the degree of these operators. To guarantee global optima, these operators must strike a healthy balance. The probabilistic nature can't decide the specific degree for a viable and ideal arrangement.

CHAPTER – 7
CONCLUSION

"Gives proposals for future improvement of the examination subject and summary of exploration work."

7.1 Summary of key findings

7.2 Contribution to the field

7.3 Conclusion

7.4 Recommendations for future research

CONCLUSION 7

The Outcome and Conversation section fills in as a basic piece of the review, this part centers on the show and conversation about the outcomes got from the trials done in the review. The steganalysis and forensics that mitigate them must also become more sophisticated as stego tools become more advanced. There is currently no global screening method for steganography, but several projects are underway to create algorithms in this vein. Traffic detection and mitigation can currently be achieved in some measure by scanning systems with application-aware controls and firewalls.

7.1 Summary of key findings

In our research work we implemented a highly secure communication method.

- We hide secret data inside audio files.
- Keep audio signal unaltered and high.
- Increase hiding capacity.

7.2 Contribution to the field

We develop the method. After hiding we can increase the audio quality compared to other research work as well as increase the hiding capacity.

Hereditary calculations are an amazing asset for improving complex cycles, and sound steganography is no exemption. We can greatly improve the process's efficiency and accuracy by employing genetic algorithms to encode and decode hidden audio file messages.

Using genetic algorithms for audio steganography has a number of advantages, one of which is that they make it possible for us to choose from a wide range of options. This is particularly valuable when managing enormous sound documents or complex encoding plans, where manual improvement would be illogical or inconceivable. Genetic algorithms offer a high degree of adaptability and flexibility in addition to their efficiency. They are simple to adapt to accommodate various audio file types, encoding schemes, and even alphabets or languages. Consider the following scenario as an illustration of the power of genetic algorithms in audio steganography: A genetic algorithm was used by a group of researchers to improve the process of hiding messages in audio files. They had the option to make a progress pace of more than 95%, contrasted with only 60% with customary techniques. By and large, hereditary calculations offer a strong and adaptable way to deal with sound steganography that can significantly work on the proficiency and exactness of the interaction. We can anticipate even more exciting applications of this technology in the future as the field continues to develop. All in all, we have investigated the captivating universe of sound steganography and hereditary calculation. We have perceived how these two ideas can cooperate to make an integral asset for concealing mystery messages in sound records. By utilizing hereditary calculation to improve the interaction, we can accomplish more prominent proficiency and precision than at any other time. The utilizations of sound steganography with hereditary calculation are immense and changed. This technology has the potential to change the way we protect our information in the digital age, from secure communication to digital watermarking. As the field keeps on developing, we urge you to remain informed and engage in this thrilling area of exploration.

7.3 Conclusion

The structured and explained perspective of genetic algorithms is presented in this paper. With the application, GA and its variants have been discussed. Genetic operators for specific applications are discussed. Some genetic operators are meant to be interpreted. However, research domains do not apply to them. A lot of research has been done on how genetic operators like crossover, mutation, and selection can reduce premature convergence. It has been discussed how GA and its variants can be used in various research fields. This paper focused primarily on wireless network applications and multimedia. The difficulties and issues discussed in this paper will be of assistance to practitioners in conducting their research. In addition to metaheuristic algorithms, using GAs in other areas of research has numerous benefits. The purpose of this paper is to provide information about each component of GA as well as the source of recent research in GAs. It will inspire the researchers to comprehend the fundamentals of GA and apply this understanding to their research problems.

7.4 Recommendations for future research

Future Research

GAs have been used in a variety of fields by modifying their fundamental structure for future research directions.

The current obstacles can be overcome to improve the optimality of a GA-derived solution. The following are some possibilities for GA in the future:

1) The appropriate degree of crossover and mutation operators ought to be selectable in some way. The crossover and mutation operators, for instance, are adapted by Self-Organizing GA following the problem at hand. By saving time, it can hasten computation.

2) Premature convergence can also be reduced through future research. This is where some researchers are working. To address the premature convergence issue, however, it is suggested that novel crossover and mutation techniques are required.

3) Genetic algorithms imitate the process of natural evolution. The responses of the human immune system and virus mutations, for example, may lend themselves to the simulation of natural evolution.

4) The mapping of genotype to phenotype in real-world problems is complicated. In this instance, either the problem lacks readily apparent building blocks, or the building blocks are not adjacent gene groups. As a result, novel encoding schemes for a variety of problems with varying degrees of difficulty are within reach.

The method will be super-efficient then. In the future, the method will be much more secure than before after the above development of the algorithm.

REFERENCES

[1] Karampidis, Konstantinos and Kavallieratou, Ergina and Papadourakis, Giorgos, “A review of image steganalysis techniques for digital forensics”, Elsevier-Journal of information security and applications, vol. 40, pp. 217-235, 2018

[2] Y. K. Lee and L. H. chen, “High-capacity image steganographic model”, IEEE proceedings - vision, image, and signal processing, vol. 147, no. 3, pp. 288–294, 2000.

[3] P. Bassia, I. Pitas, and N. Nikolaidis, “Robust audio watermarking in the time domain”, IEEE. Transactions on Multimedia, vol. 3, no. 2, pp. 232–241, 2001.

[4] Bhowal Krishna, Bhattacharyya Debnath, Pal Anindya Jyoti, and Kim Tai-Hoon, “A GA based audio steganography with enhanced security”, Springer. Journal of Telecommunication Systems, vol. 52, no. 4, pp. 2197-2204, 2013.

[5] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding—A Survey”, IEEE proceedings, vol. 87, no. 7, pp. 1062-1078, 1999.

[6] N. Cvejic and T. Seppanen, “Increasing the capacity of LSB based audio steganography”, IEEE International Workshop on Multimedia Signal Processing (7810062), St. Thomas, VI, USA, pp. 336-338, 2002.

[7] Ravi Kumar B. and Dr. Murti P. R. K., “Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology”, International Journal on Computer Science and Engineering (IJCSE), vol. 3, no. 7, pp. 2818-2827, 2011.

[8] Stefan Katzenbeisser and Fabien A.P. Petitcolas, “Information hiding techniques for steganography and digital watermarking”, Artech House, Rolf Oppliger, 2000.

[9] A. Westfeld and A. Pitzmann, Booktitle- “International workshop on information hiding”, Springer, Berlin, Heidelberg, Andreas Pfitzmann, Title- “Attacks on Steganographic Systems”, Lecture Notes in Computer Science, vol. 1768, pp. 61-76, 2000.

[10] Bandyopadhyay and Samir Kumar, "Genetic algorithm-based substitution technique of image steganography", Journal of Global Research in Computer Science, vol. 1, no.5, pp. 62-69, 2010.

[11]Johnson, Neil F, Jajodia, and Sushil, "Steganalysis: The investigation of hidden information",IEEE. International Conference on Information Technology (6047761), Syracuse, NY, USA, pp. 113-116, 1998.

[12] Pooyan Mohammed and Delforouzi Ahmed, "LSB based steganography method based on lifting Wavelet Transform", IEEE. International Conference on signal processing and information technology (4458198), Giza, Egypt, pp. 600-603, 2007.

[13] A. Al-Hooti, M. Hatem, 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, 2016.

[14] P. Zhang, Y. Li, X. Ma, Y. Fan, and X. Chen, "Efficient audio data hiding via parallel combinatory spread spectrum", IEEE. International Conference on Image and Signal Processing (CISP) (15790782), Shenyang, China, pp. 814-818, 2015.

[15] Thangadurai K. and Sudha Devi G., "An analysis of LSB based image steganography techniques", IEEE. International Conference on Computer Communication and Informatics (14684379), Coimbatore, India, pp. 1-4, 2014.

[16] Sara, Khosravi and Mashallah, Abbasi Dezfouli, "A New Method to Steganography whit Processing Picture in Three Colors (RGB)", International Journal of Computer Tech. and Applications, vol. 2, no. 2, pp. 274-279, 2011.

[17] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, "A genetic-algorithm-based approach for audio steganography", International Journal of Computer and Information Engineering, vol. 3, no. 6, pp. 1562-1565, 2009.

[18] Padmashree G and Venugopala PS, "Audio Steganography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers", International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, no. 4, pp. 177-181, 2012.

[19] N. Cvejic and T. Seppanen, “Increasing robustness of LSB audio steganography using a novel embedding method”, IEEE. International conference on Information Technology: Coding and computing (8126928), Las Vegas, NV, USA, vol. 2, pp. 533-537, 2004.

[20] Mazhar Tayel, Ahmed Gamal, and Hamed Shawky, “A proposed implantation method of an audio steganoghraphy technique”, IEEE. International Conference on advance communication technology (15824048), PyeongChang, Korea (South), PP. 180-184, 2016.

[21] Deshmukh R, Deshmukh P, “4 Layer enhanced security for audio signals using steganography by modified lsb algorithm and strong encryption key”, International Journal of Advanced Research in Computer Science, vol. 2, no. 2, pp. 492-495, 2011.

[22] Swain, Gandharba, “Adaptive and Non-adaptive PVD steganography using overlapped pixel blocks”, Arabian Journal of Science and Engineering, vol. 43, no. 12, pp. 7549-7562, 2018.

[23] Gutub, Adnan and Al-Qurashi, Adel, “Secure shares generation via mblocks partitioning for counting-based secret sharing”, Journal of Engineering Research, vol.8, no.3, pp. 91-117, 2020.

[24] R. J. Anderson and F. A. Petitcolas, “On the limits of steganography”, IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 474–481, 1998.

[25] F. Hartung and M. Kutter, “Multimedia watermarking techniques”, Proceedings of the IEEE, vol. 87, no. 7, pp. 1079–1107,1999.

[26] B. Chen and G. W. Wornell, “Quantization index modulation: a class of provably good methods for digital watermarking and information embedding”, IEEE Trans. On Information Theory, vol. 47, no. 4, pp.1423–1443, 2001.

[27] M. Hariri, K. Ronak, and M. Nosrati, “An introduction to steganography methods”, World Applied Programming, vol. 1, no. 3, pp. 191–195, 2011.

[28] M. Barni, “Steganography in digital media: Principles, algorithms and applications (fridrich, j. 2010)[book reviews]”, IEEE Signal Processing Magazine, vol. 28, no. 5, pp. 142–144, 2011.

[29] M. A. Nematollahi and S. Al-Haddad, “An overview of digital speech watermarking”, International Journal of Speech Technology, vol. 16, no. 4, pp. 471–488, 2013

[30] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, “Robust audio watermarking using perceptual masking”, Signal processing, vol. 66, no. 3, pp. 337–355, 1998.

[31] N. Kundu and A. Kaur, “Audio steganography for secure data trans-mission”, International Journal of Computer Sciences and Engineering, vol. 5, no. 2, pp. 124–129, 2017.

[32] Chen, Xiangcheng and Wang, Yuwei and Wang, Yajun and Ma, Mengchao and Zeng, Chunnian, “Quantized phase coding and connected region labeling for absolute phase retrieval”, Optics Express, vol. 24, no. 25, pp. 28613—28624, 2016.

[33] Bhattacharyya, Souvik and Sanyal, Gautam, “Feature based audio steganalysis(FAS)”, International Journal of Computer Network and Information Security, vol. 4, no. 11, pp. 62, 2012.

[34] Goo, Eun Hoe and Lee, Jae Seung and Kim, Moon Jib and Kweon, Dae Cheol and Dong, Kyung Rae and Chung, Woon Kwan and Lee, Jin Kook and Jang, Keun Jo and Lim, Jong-Deuk, “A Study on Development of Phase Array Coil for MRI of Mouse in the 3.0 T High Magnetic Field”, Journal of the Korean Physical Society, vol. 59, no. 4, pp. 2855—2860, 2011.

[35] Pacella, Daniela and Ponticorvo, Michela and Gigliotta, Onofrio and Miglino, Orazio, “Basic emotions and adaptation. A computational and evolutionary model”, PLoS one, vol.12, no. 11, pp. e0187463, 2017.

PUBLICATION DETAILS:

Orora Tasnim Nisha[1], Md. Selim Hossain[1*,] Mahfujur Rahman[1], “Audio Steganography with Intensified Security and Hiding Capacity”, European Chemical Bulletin, 12(10):162-173, 2023, doi: 10.48047/ecb/2023.12.10.013.

APPENDIX

Source code of the System

```
import wave

def em_audio(af, string, output):
    print ("Please wait...")
    waveaudio = wave.open(af, mode='rb')
    frame_bytes = bytearray(list(waveaudio.readframes(waveaudio.getnframes())))
    string = string + int((len(frame_bytes)-(len(string)*8*8))/8) *'#'
    bits = list(map(int, ".join([bin(ord(i)).lstrip('0b').rjust(8,'0') for i in string])))
    for i, bit in enumerate(bits):
      frame_bytes[i] = (frame_bytes[i] & 254) | bit
    frame_modified = bytes(frame_bytes)
    with wave.open(output, 'wb') as fd:
      fd.setparams(waveaudio.getparams())
      fd.writeframes(frame_modified)
    waveaudio.close()
    print ("Done...")

try:
  af = input("Enter audio file name: ")
  string = input("Enter message: ")
  em_audio(af, string, "output.wav")
except:
  print ("Something went wrong!! try again")
  quit(")
import wave

def ex_msg(af):
    print("Please wait...")
    waveaudio = wave.open(af, mode='rb')
    frame_bytes = bytearray(list(waveaudio.readframes(waveaudio.getnframes())))
    extracted = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
    string = "".join(chr(
        int("".join(map(str, extracted[i:i+8])), 2)) for i in range(0, len(extracted), 8))
    msg = string.split("###")[0]
    print("Your Secret Message is: \033[1;91m"+msg+"\033[0m")
    waveaudio.close()

try:
    af = input("Enter file name: ")
    ex_msg(af)
except:
    print("Something went wrong!! try again")
    quit('')
```

Calculate the SNR of cover and stego audio

```
import scipy.io.wavfile as wavfile
import numpy as np
import os.path

def signaltonoise_dB(a, axis=0, ddof=0):

    mx = np.amax(a)
    a = np.divide(a,mx)
    a = np.square(a)
    a = np.asanyarray(a)
    m = a.mean(axis)
    sd = a.std(axis=axis, ddof=ddof)
    return 20*np.log10(abs(np.where(sd == 0, 0, m/sd)))


def snr(file):
    if (os.path.isfile(file)):
        data = wavfile.read(file)[1]
        signalchannel= data


    try:
        singleChannel = np.sum(data, axis=1)
    except:
        pass

    norm = singleChannel / \
        (max(np.amax(singleChannel), -1 * np.amin(singleChannel)))

    return (signaltonoise(norm))

inp1 = input("Enter your 1st file name: ")
inp2 = input("Enter your 2nd file name: ")


print(snr(inp1))
print(snr(inp2))
```