Audio Steganography with Intensified Security and Hiding Capacity

Orora Tasnim Nisha[1], Md. Selim Hossain[1,*], Mahfujur Rahman[1]

[1]Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science & Technology University, Dinajpur, Bangladesh.

*Email: selim.ece@tch.hstu.ac.bd

Abstract*— Nowadays, the internet is a very powerful and valuable medium of communication, dissemination of information, and connectivity to away people. Moreover, it is very important to keep ourselves secure online. In this regard, steganography is a system providing an enhanced secured communication process. The word steganography originates from the Greek word steganos (which means hidden or covered). It conceals the pursuit of communication. On the other hand, cryptography provides an encryption mechanism to make the secret message decodable. Steganography offers confidentiality, authentication as well as data integrity but non-repudiation. Numerous research has already been done on audio steganography. Among all, this proposed method gives enough good outcomes. This paper proposes a technique to conceal information in an audio signal using the audio-steganography method and presents an enhanced two-level secured communication to hide confidential information by encoding data using the GA (Genetic Algorithm). The SNR (Signal to Noise Ratio) value can calculate to evaluate the quality of both the cover and stego audio signal. The stego audio signal provides a higher SNR value which is positive and near to one. The proposed steganography method provides a higher secured communication and hiding capacity. This method also works efficiently to hide information in the audio signal and is more transparent acoustically.

***Keywords*— *Steganography, audio steganography, genetic algorithm, SNR, hiding capacity*.**

I. INTRODUCTION

Transmission of digital data over the internet is increasing day by day for quick and secure communication. But ensuring security over the internet is a vital issue, as people need secured communication over the internet. People use various ways for the establishment of online security over the internet. Cryptography is one of the ways from the numerous alternatives. But steganography conceals the presence of hidden data. On the other hand, cryptography cannot conceal the presences of secret data. People use a variety of multimedia files for communication purposes. Steganography is the most popular hiding technique that conceals data within a digital media, e.g., audio, video, image. It plays a vital role in communication exchange. As well as ensures confidentiality during the communication exchange. To conceal information inside audio signals there, use various steganographic algorithms. Both Steganography and its analysis are used for hiding secret messages for wed security [1]. The third party cannot make a variation between the cover and stego audio. The existence of secret messages remains hidden from unauthorized people. An audio file is a type of steganographic carrier. As VOIP is becoming more popular day by day, its popularity pushed audio into more applications. Audio steganography technique hides the existence of a secret message and allows it only to decode by the deliberate recipient. It provides two-layer protection against cryptography. Audio steganography can hide messages in WAV, AU, and even MP3 sound files. In audio steganography sound files are changed in a way that they contain hidden data in it. This hiding procedure must be done in such a way that make data secrecy data remain unaltered without adding much noise in the original signal or changing the quality of audio.

There are several methods used for hiding data into an audio file. There are various existing methods for concealing data inside audio signals including Genetic algorithm, Least Significant Bit (LSB) coding, Parity Coding, Phase Encoding, Spread Spectrum, and Echo Data Hiding. We have used Genetic algorithm procedure to hide data into an audio file, because of its high robustness and transparency. There are several risks involved in those methods. The threat in the least Significant Bit algorithm (LSB) is that at risk of steganalysis and is not stable at all. To make it more stable, the LSB has adjusted to work in a divergent method. Parity coding may not catch errors successfully. When two data bits get corrupted for instance, it will not identify the errors. The main issue in phase coding is close sine waves in phase constructively interfere, and out-of-phase waves destructively interfere. Robustness is the main issue in echo hiding. On the other hand, the difficulties in implementing the genetic algorithm are difficult to debug and can be computationally expensive. The genetic algorithm can find solutions to various problems that are more impossible to solve using traditional techniques. The main benefit of steganography is, unlike cryptography, it conceals the existence of hidden information [2]. In dot wave audio files, it can successfully solve problems that have multiple constraints. Cover media + hidden data + stego_key = stego_media. Numerous alternatives can be used as a cover signal i.e., an audio signal, image, video files, etc. Concealing confidential data in a digital audio cover is more difficult than hiding data using digital images as a cover. The sender can embed the data inside the audio signal using the Genetic Algorithm with a secret key. This paper deals

with dot wave audio coding [3]. Only the receiver can decrypt it with an appropriate secret key. Two normal steganalysis techniques are used for auditory inspection and applied mathematics analysis. In statistical analysis, the violator compares the original message and hidden message to extract the secret message. Data can be embedded through the LSB algorithm at the 4th and 5th LSB layers. On the other hand, genetic algorithm offers high hiding capacity [4]. Audio steganography and video steganography conjointly victimize Genetic Algorithmic rule. Audio and video steganography is different from image steganography. The difference is that audio and video steganography need masking. Human eyes and ears are sensitive to any change in audio and video. Disguising can be utilized as the possessions of human's sensitive organs to conceal information unnoticeably. Military and intelligence agencies are the major driving interest in the matter of secret information concealing [5].

This paper proposed a secure technique with enhanced security and analyzed the audio signal quality by calculating SNR value of the original and stego audio. The hiding capacity has been successfully increased by applying GA. In LSB (Least Significant Bit) algorithm, the secret message is embedded into higher LSB Layers [6]. The main drawback in the LSB algorithm is the low agility as opposed to signal-to-process variation. It creates a problem to keep each of the pixels unaltered while hiding data inside an image. [7]. The steganography technique has multiple information-hiding methods [8]. To ensure security, we need more secure steganographic algorithms. Some algorithms use secret keys to hide data inside the audio signal [9]. The LSB algorithm has a balance between the payload capacity and visual quality [10]. To keep confidential information, secured from intruders' steganography is the best option [11]. The extraction error can be avoided during hiding bits by using lifting wavelet transform combined with the LSB method [12]. However, the genetic algorithm provides high robustness. It can hide confidential data inside the audio signal efficiently. The genetic algorithm provides the highest fitness bitstream position. All the stego-applications need a higher bit rate of the inserted data. An intelligent algorithm determines and deciphers secret bits without access to the cover audio bitstream. In contrast, genetic algorithms are one of the best methods for embedding the hidden data. To improve online security based on the steganographic methods, audio steganography is the leading procedure in today's era.

This implemented method with genetic algorithm coding using the python platform successfully hides data inside dot wave audio files by maintaining the audio quality. The hiding capacity can be enhanced, and the noise can be reduced. The technique provides security in confidential online communication like military and intelligence agencies. It also can be suitable for short-range confidential online communication where some companies or agencies need information security.

II. GENETIC ALGORITHM FOR AUDIO STEGANOGRAPHY

The genetic algorithm is a technique for deciphering both the inhibited and the uninhibited escalation difficulties that construct on the logical selection, the method that operates the biological development. The genetic algorithm persistently alters an inhabitant of single solutions. This method hides messages inside an audio file by applying the Genetic algorithm of that audio with the bits of message to be kept that secret. The genetic algorithm works on three operators: manipulate chromosome/ solutions or Selection operator, Mutation operator, and Crossover operator. Procedure to selecting two or more parents from the inhabitants for crossing. The motive of selection is to point up filter discrete in the inhabitants in desires that their off springs have soaring fitness. Methods of selection: Roulette wheel selection, Boltzmann selection, tournament selection, rank selection. Generally, apply Roulette wheel selection method.

III. METHODOLOGY

III. (i) Proposed Algorithm to improve all the creatures:

Maximization of the function f(x) = x^2 with x in interval [0, 31] i.e., x= 0,1, ……30, 31.

Algorithm: hiding message inside audio signal

//Number of individuals in each generation

Population_Size = ()

// Valid genes

// Target string to be generated

Target = "Hello! How are you?"

representing individual in population

//mating and produce new offspring

//create new Individual

//generated chromosome for offspring
return Individual(child chromosome)

Generating initial population at random. Those are chromosomes or genotypes,
Example, 01110 (14), 11001 (25), 01001 (9), 10100 (20).
Calculating fitness,

(a) Decoding into integer (called phenotypes). 01110 = 14, 11001 = 25, 01001 = 9, 10100 = 20.
(b) Evaluating fitness, f(x) = x^2. 14 = 196, 25 = 625, 9 = 81, 20 = 400.

Select parents (two individuals) constructed on their fitness is p: pi = $fi/(\sum_{f=i}^{n}$ Fj)
Where, Fi = Fitness for the string i in inhabitants.
Pi = Probability of the string i is selected.
n = Number of individuals in the inhabitants. n*pi expected count.

Crossover operator: It can be either one-point or two-point crossovers. In the one-point crossover, at any random position, the selected pairs of strings can cut. Then the segment was swapped to form new string pairs. Whenever In the two-point crossover, there will be a breakpoint.

Mutation operator: Mutation can apply to each child individually. After crossovers, Binary bits are altered from 0 to 1 or from 1 to 0 at an arbitrarily selected position of an unevenly chosen string. An uneven mutation occurs. Then 0 muted to 1, and 1 muted to 0. The GA can improve the fitness of all the individuals. And here is the better result after applying Genetic algorithm.

A. Proposed secure communication procedure with the Genetic algorithm.

An algorithm design for communication networks using Genetic Algorithm (GA) to create a faster steganography process, as well as robust and highly secure. Genetic algorithms exist in the vast group of evolutionary algorithms (EA), which solve optimization problems using procedures inspired by natural evolution.

B. Embedding and extracting process of the secret message

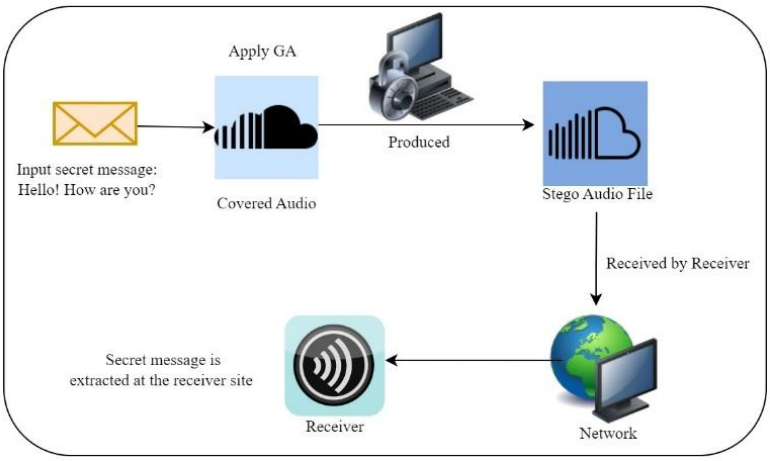


Fig 1. The framework of the proposed method

C. The proposed scheme

Fig.1 presents the detail of this technique in this section. Its aim is to enhance the security of communication and improve the hiding capacity of the audio. The proposed framework was implemented using the python code in the visual studio platform.

D. Embedding Process

This process was run on the sender's side. The secret message was loaded into the covered audio. Each audio sample such as dot wav audio file had different sizes. The Sizes of audio files were, 868kb, 3318kb, 1Mb, 2.52Mb, 10Mb, 21Mb, 45Mb.The covered

audio sample partitioned into bitstream. Application of the genetic algorithm improves all the individual fitness of the bitstream. Because of its simplicity and requiring less computation time, the genetic algorithm is best. The secret message was encoded in the covered sample's highest fitness bitstream position which was modified for hiding the secret message bits.

E. Extraction Process

This process was run on the receiver's side. Through this process, the receiver will collect the stego audio file. Reproduce the original message in the same order we must gather the embedded bits of the selected stego-file samples. The retrieved highest fitness bitstream position reconstructed the original secret message.

F. Modification during embedding

Transparency is simply the difference between the original sample and the modified one. This proposed method modifies and adjusts more bits and samples than some previous ones. Let assume, Sample bits are: 01110 (14). Target layer is 5 and message bit is 1. Without adjusting: 11110 (30), the difference is 16**.** After adjusting: 10000 (16), the difference will be 2 for 1 bit embedding. Again, Samples bits are: 11001(25). Target layers are 2 and 3, and the message bits are 11. Without adjusting: 11111(31), the difference is 6. After adjusting: 10110(22), the difference will be 3 for 2 bits embedding. Genetic algorithms are intelligent enough to produce the optimal solutions.

G. Mathematics

To measure the induced noise during the embedding of the secret message in the cover audio the proposed method used the SNR. The technique clarifies that if SNR is positive and higher then it is suitable for efficient communication. After the embedding process, the stego audio is produced. In this experiment, the SNR was calculated for both the covered audio and the stego audio files. Positive and higher SNR value were best for efficient communication over the internet.

H. Signal to Noise Ratio (SNR)

The signal-to-noise ratio (SNR) is the estimate operated in communication engineering that differentiates the magnitude of an impulse signal to the magnitude of its surround noise. In communication engineering during the analog and the digital signal processing, a signal-to-noise ratio, usually written as S/N, is an estimate of the robustness of the impulse signal relative to the surround noise (unwanted signal). The SNR in decibel define as,

$$SNR = 10 \log_{10} (S/N) \quad \text{.....(1)}$$

Where, S = Signal Power, and N = Noise Power. The audio samples are presented using 8 bits per sample, this is 255. The SNR is a measure of the quality of an estimator— in efficient communication it is always non-negative, and better values become closer to one. From equation (1), signal noise can be calculated by measuring the variation between the original signal strength and noise signal strength by subtracting the noise value from the cover signal strength value.

Equation (1) formula used in the python platform. In python code to calculate SNR. We use a signal-to-noise ratio function to calculate the SNR of both cover and stego audio. In the python platform, the SciPy library has a sub-package that contains a signal-to-noise ratio () function.

IV. Result And Discussion

This method claimed that if a secret message is hided using the genetic algorithm, then the amount of noise in the covered audio file would get decreased enormously which will create difficulties in extracting the actual information from the covered audio file by the third parties, which will increase the robustness and transparency of this proposed method. In case of an audio signal, if the calculated SNR is high, then it signifies that the induced noise in that covered audio signal is very less. From the experiment, it can be observed that the stego audio provides higher SNR compared to the covered audio that enhanced the communication security. Audio files have an elevated level of redundancy and a higher data transmission rate. So that Audio files can be a convenient host file. Here, from the data analysis table-1 and table-2, it can assume that the algorithm efficiently hides large size text in audio files. The algorithm hides text within an audio file and provides higher SNR which was near to one. This technique can decrease the noise power efficiently in case of hiding the text of small size but in case of large data, the noise power decreased to a certain level which was also suitable for efficient communication.

A. Genetic algorithm for optimal and suboptimal solution

Genetic Algorithm (GA) is a search-dependent optimization procedure supported by the crucial of Genetics and Natural Selection. It is habitually used to create solutions to optimization issues in research and machine learning. Genetic algorithms produce solutions by selection, recombination, and mutation until the better ones are obtained. It works efficiently for productive building block hypotheses that can recover in some other deficient solutions.

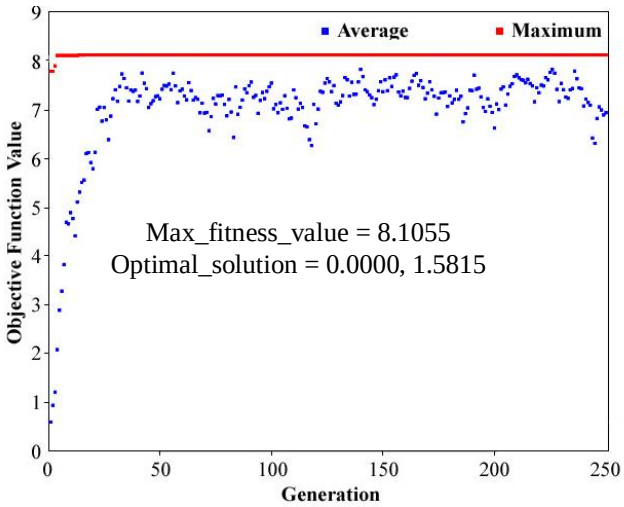


Fig 2. Genetic algorithm for finding optimal solution.

In Figure 2, the graph shows that the genetic algorithm repeatedly modifies a population of individual solutions. Over successive generations, the population 'evolves' towards an optimal solution. During each generation, the chromosome was evaluated using some measures of fitness. Here, blue indicates the average values and red indicates the maximum values of generation vs objective function value.

A new generation can form by selecting fitness values. To keep the population size constant, we have chosen some parents and offspring and rejected others. Fitter chromosomes have higher probabilities of being selected. After multiple generations, the algorithm converged to the best chromosome.

When evaluating the fitness of this process, we must ensure that no signal is missed and that less noise is induced. To check this, we compare the SNR value between the cover and the encoded audio signal. Genetic algorithms are intelligent enough to reduce that amount of noise. So further recovery is not needed.

B. Analyze the method with a different text file.

Here the audio file size is 1Mb. Hiding various sizes of text content in the audio file, we analyze the audio quality as well as hiding capacity by measuring the SNR value of the audio. The negligible difference between stego and cover audio shows a large hiding capacity.

TABLE I. THE SNR VALUES FOR DIFFERENT SIZE OF TEXT CONTENT WITH THE SAME 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

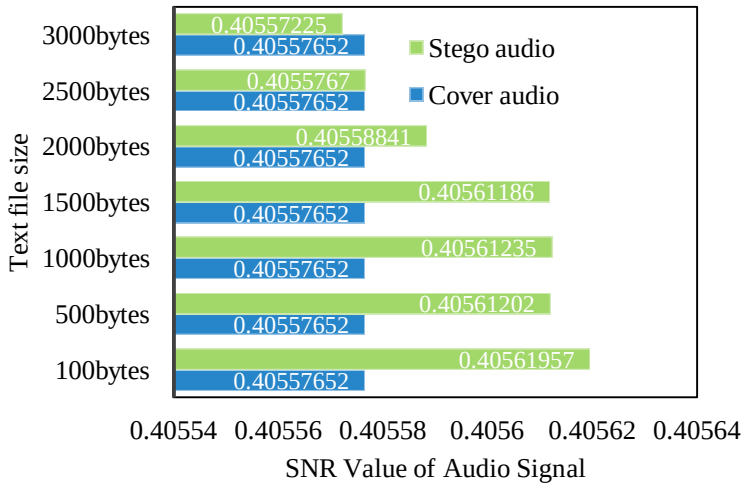


Fig 3. SNR values of an audio file (1Mb) after hiding distinct size of the text files.

In this graph, Y-axis shows the different sizes of text files that are to be hidden inside 1Mb audio file. X-axis shows the corresponding SNR values of audio file. Here, it can assume that stego audio occupies higher SNR value compared to cover audio. In case of large data size (2500 bytes, 3000bytes text file) this graph indicates that the SNR values of stego audio keep decreasing compared to cover audio. That means the hiding capacity of this technique successfully works up to 2000bytes for 1Mb audio file. This method offers large hiding capacity compared to audio file size (1Mb). The technique keeps the quality of audio signal stable by maintaining the signal to noise ratio of the audio signal. The stego audio signal's SNR is higher, that means, induced noise in the cover audio signal is less. This method successfully enhances communication security.

C. Analyze the method with different audio files.

Here the text content size is 1500bytes. Hiding this text size in each audio file, we analyze the audio quality by measuring the SNR value of each audio.

TABLE II. THE SNR VALUES FOR DISTINCT SIZE OF AUDIO FILE 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

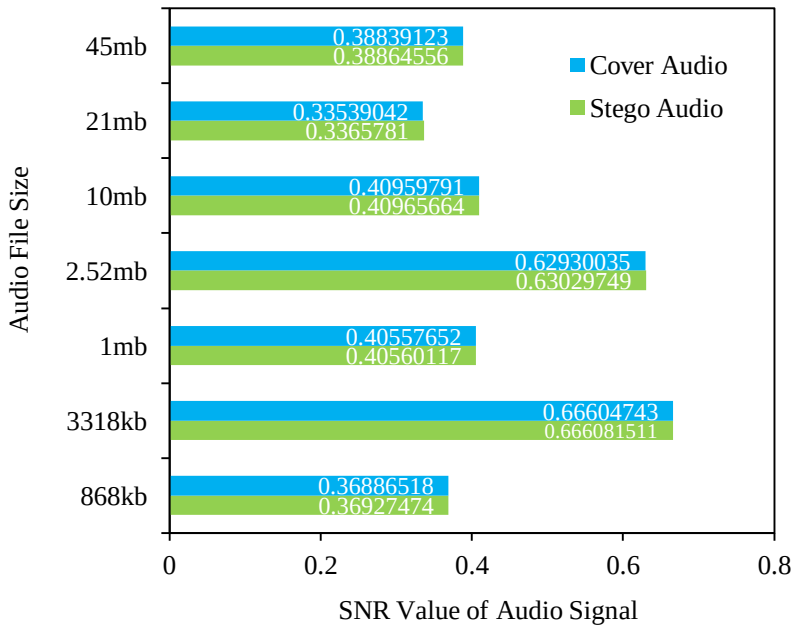


Fig 4. SNR values for distinct size of audio files with the same of the content size (1500bytes)

This technique was analyzed by hiding the same size of secret text inside different audio files, the hiding capacity was good enough for large sizes of audio files, such as 10mb, 21mb, 45mb etc. The larger audio files hid the secret message efficiently by maintaining the quality of the audio. Those provided positive and higher SNR value (which is near to 1) of the stego audio compared to the covered audio. Oppositely, in the case of the smaller audio file, such as 868kb, 1mb, these could not improve the stego audio quality efficiently. Though the SNR of the stego audio is lower compared to the covered audio, the difference between them is too little that it can be ignored. Thus, this method successfully hides data even in large sizes and maintains the quality of the audio signal. This method offers to enhance secure communication over the internet. While analyzing with different sizes of text files within the same audio signal (1mb), in case of 3000bytes data, the covered audio SNR is 0.40557652, and the stego audio SNR is 0.40557225. Here the difference is 4.27e-6. And for 2500bytes data, the covered audio SNR is 0.40557652, and the stego audio SNR is 0.4055767. Here the difference is 1.8e-7. Those differences are too small and can be easily neglected. On the other hand, while analyzing with different sizes of audio files with the same content (1500bytes), in case of 45mb audio, the covered audio SNR is 0.38864556, and the stego audio SNR is 0.38839132. Here the difference is 0.00025424. And for 21mb audio, the covered audio SNR is 0.3365781, and the stego audio SNR is 0.33539042. Here the difference is 0.00118768. Here the differences are also too small that can easily neglect.

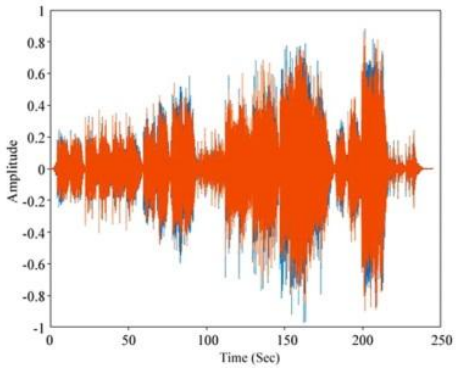
From Table 1 and Table 2, and Figure 3 and Figure 4, it can observe that the audio quality became improved, and the hiding capacity of the different audio files become large. After hiding different sizes of secret texts inside the same audio, the quality of the audio became high enough (the SNR value was higher) in case of the small amount the size of the content. In case of large data, the quality was same compared to the covered audio. When the text content was increased up to 3000bytes, which was very large in the size of the data content, the audio quality decreased little bit. So, the proposed technique can improve audio quality by removing the noise and enhancing the SNR value. It works efficiently in the case of the small and the medium size of secret data contents.

D. MATLAB - Amplitude vs. time plots:

Analyze cover wav sound files and stego wav sound files by plotting wav sound files onto a graph using MATLAB code.

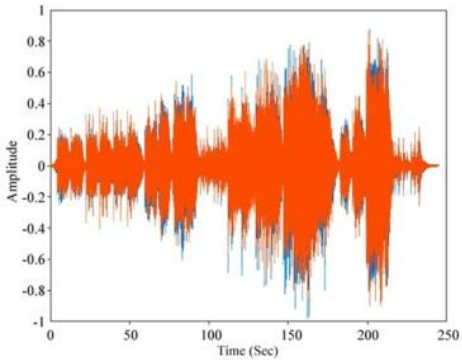
Before encoding

(a) 45 Mb cover audio

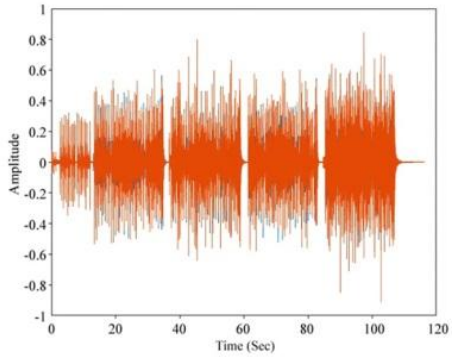


After encoding

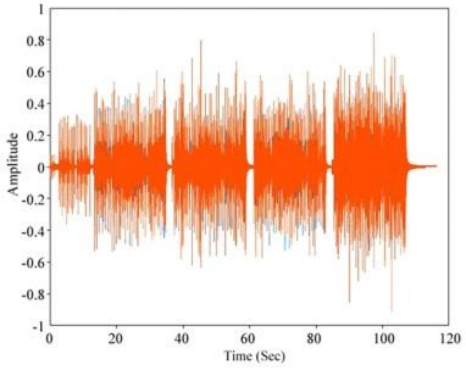
(b) 45 Mb stego audio



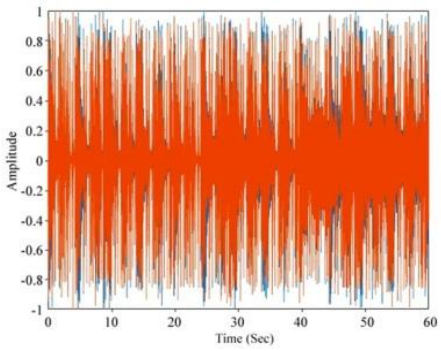
(c)21 Mb cover audio



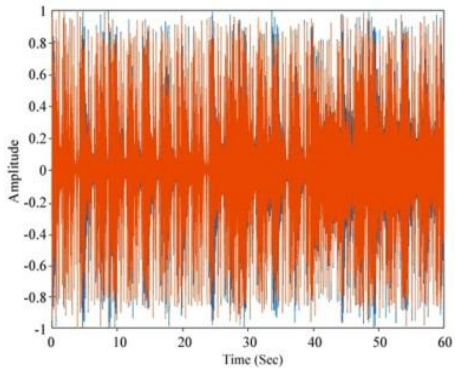
(d) 21 Mb stego audio



(e)10 Mb cover audio

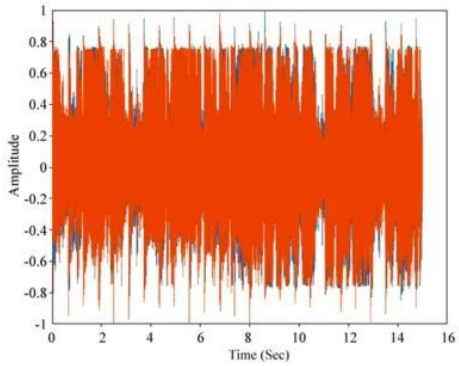


(f) 10 Mb stego audio

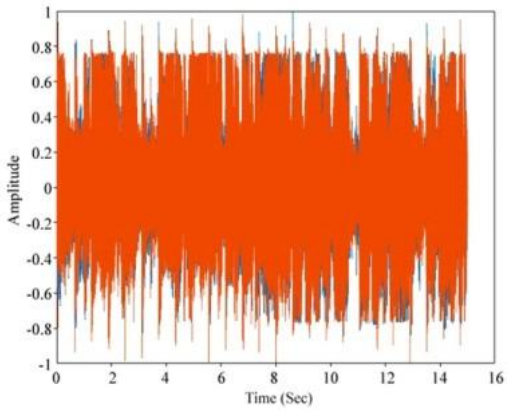


(g) 2.52 Mb cover audio

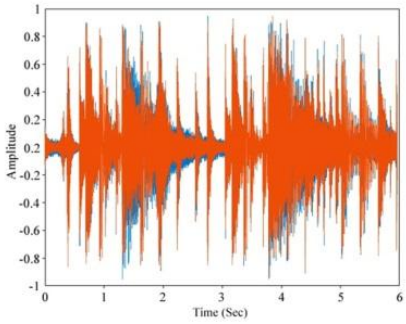
(h) 2.52 Mb stego audio



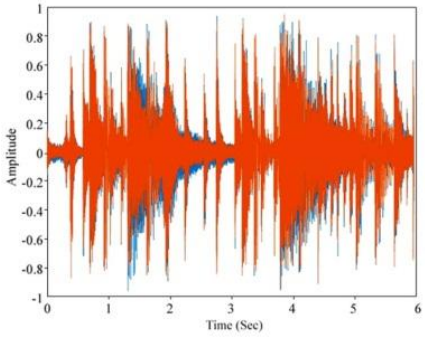
(i)1 Mb cover audio



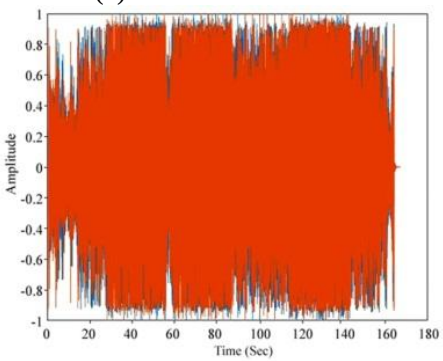
(j)1 Mb stego audio



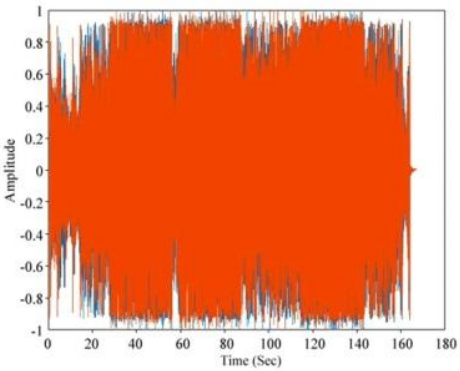
(k) 3318 kb cover audio



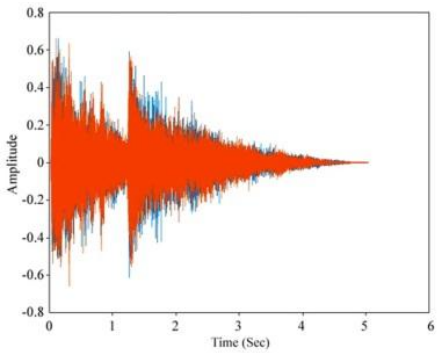
(l) 3318 kb stego audio



(m) 868 kb cover audio



(n) 868 kb stego audio



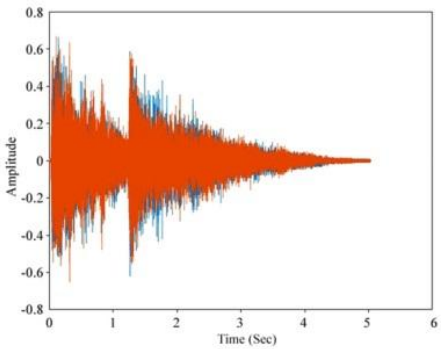


Fig 5. Dot wav files plot (amplitude vs. time)

Audio steganography is an extra step for hiding or protecting confidential data. Writing a secret message inside a dot wave file causes unwanted signal addition. The implemented method with genetic algorithm in the python platform can efficiently hide data that a negligible amount of noise (unwanted signals) adds during the encoding process. An intruder never detects the changes between a cover audio and a stego audio. After encoding the dot wave sound signals show no visual changes. In the genetic algorithm, message bits can embed into several and deeper layers to achieve higher capacity and robustness. Efficient coding techniques are needed to hide a hidden message in wav files and improve the SNR. The third-party needs to decode communication codes to decipher the hidden message. This action is difficult for third parties. The amplitude vs. time plot signal of any two pairs shows no changes in the amplitude and time scale value.

Figure 5 shows the analysis between cover audio and stego audio files. All cover audio files before encoding signify by (a), (c), (e), (g), (i), (k), (m). On the other hand, after encoding all stego audio files signify by (b), (d), (f), (h), (j), (l), (n). From Figure 5, it can assume that the signal shape of all stego audio remains unchanged after encoding. This efficient method adds a negligible amount of noise so that after encoding the signal shape doesn't change noticeably. The 45Mb stego audio after encoding remains unchanged as compared with the 45Mb cover audio. As well for 21Mb, 10Mb, 2.52Mb, 1Mb, 3318Kb, and 868Kb cover audio files their respective stego audio files stay unchanged noticeably. Audio steganography aims to exploit human visual redundancy to embed the secret message into the original cover audio without raising suspicion when detecting the wave. This method has flexibility. It conceals more information without any alteration. Various malicious attacks cannot be implemented against audio steganography. Consequently, creating MATLAB graphs seems all cover audio files remain unaltered after encoding. From Figure 5, it can identify that a large audio file hides the same data efficiently by adding less noise compared to a small audio file. It can be justified by zooming the audio signal. After encoding, the smaller audio files' signal shape becomes thicker than larger audio files. That means the hiding capacity of small audio files such as 2.52Mb, 1Mb, and 868Kb is lower than large files like 45Mb, 21Mb, and 10Mb. As with the same size text content, small audio files add more noise compared to large audio files. However, the changes are too small to identify, as encoded graphs carry the same time and amplitude scale for their respective cover audio. Various malicious attacks (e.g., geometrical distortions, spatial scaling) cannot detect and decode the hidden message inside an audio signal. Encoded audio seems more secure due to fewer steganalysis techniques for attacking audio. From the ordinary eye's view, there is no variation between any two pairs of original and encoded dot. wav signals in all seven examples.

The method offers high security. If any third party gets the encoded signal will never guess about the hidden message because there is no markable change between the original and the encoded signal. The method has valuable applications in cyber-security. The method provides critical infrastructure protection, including the defense sector and transportation system. Transportation systems include tracking and communication systems. The technique can keep the transportation system safe.

TABLE III. COMPARISON OF CAPACITY, SNR AND OUTPUT

Authors	Capacity	SNR	OUTPUT
Mazdak Zamani 1, Azizah A. Manaf [17]	Higher capacity and robustness	-	Efficiently hide secret data
Padmashree G, Venugopala P S [18]	-	Less than zero	Efficiently hide secret data
Nedeljko Cvejic, Tapio Seppänen [19]	-	-	Hide secret message and enhance the robustness of stego audio signal
Mazhar B. Tayel, Ahmed Gamal Abdalatife [20]	-	-	Conceals secret data and measure stego audio signal quality with PSNR. The result of the applied method contains higher PSNR value and comparatively less MSE values.

Proposed	Obtain high hiding capacity.	SNR value is positive which is near to 1.	Efficiently hide secret data inside audio signal and maintain the quality of audio. The output offers a secure method with high SNR value and comparatively large hiding capacity.

V. CONCLUSION

This is a high-capacity data-hiding technique for audio signals. The presented algorithm is suitable for any size of audio signal. It gave more capacity for larger sizes of audio. It enhanced security and preserved the audio quality. By inserting the technique into the generous sized texts, it became complicated, but provided with better security measures, which can provide stipple security. Secret communication between two authorized parties is necessary for hiding the existence of information using a carrier file. This is a filter based improved steganography technique where hidden bits are embedded according to the genetic algorithm of the covered audio. This method tends to test our planned methodology by the SNR. From the above-observed values, we can notice that there was a remarkable increase in the capacity of the covered audio for hiding additional data without affecting the perceptual transparency of the host audio signal which can reduce the amount of noise. The implemented method provides higher online security. It also offers a large hiding capacity as well as provides efficient confidentiality. The result of this implemented method represents a negligible distinction between stego and original audio. In the case of 300bytes text data, the variance is 1.8e-7 and in the case of 45 Mb audio, the distinction is 0.00118768. Those minuscule values can easily be avoided.

Third party cannot make difference between the original and the stego audios. That means, the signal does not distort after hiding the message. The method is applicable for effective and secure communication which provides reliability and confidentiality. Nevertheless, this method needs further improvement to work efficiently on any size of audio file. So, in the future, further work will be needed on this limitation.

VI. ACKNOWLEDGEMENT

The work is a part of the steganography research for the master's degree in Electronics and Communication Engineering in Hajee Mohammad Danesh Science and Technology university. The research work has been supported by the National Science and Technology (NST) fellowship (2022-2023).

VI. 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