Improved Audio Steganography By Optimizing Non Overlapping Audio Blocks Using Pso

Tabasum kounsar[1] , Er sukhvinder kaur[2]
[1, 2] *Department of Electronics and communication*
Swami Devi Dyal institute of Engineering and technology
Barwala kurukshetra university, kurukshetra, INDIA
E-mail:tabasumkounsar22@gmail.com

Abstract- Steganography is the scheme of concealing confidential data in a cover file. It is the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital audios, images and video. The three most important parameters for audio steganography are imperceptibility, payload (bit rate or capacity), and robustness.Any technique that tries to boost the payload or lustiness ought to preserve physical property. The noise that is introduced due to bit modification would limit payload. This research focuses on audio steganography, particularly with respect to Waveform Audio File Format (WAV) files. In this research different spectrum audios such as as secret audio female, jazz, vlobs and dialogues audio are used. However in cover audio we use Female, dialogues and jazz audio. Every audio frequency and spectrum vary from each other. In this analysis the parameters PSNR, MSE (mean squared Error), SNR and BER are checked. Comparisons of existing, GA based approach and PSO base proposed approach on different cover audio and hidden audio on different optimization like particle swarm optimization and genetic algorithm is done. This research shows that the proposed approach with PSO improve all parameters in different cover audio and secret audio in comparison to Genetic algorithm and without optimization

Keywords*: Particle Swarm Optimization, Signal to Noise Ratio, Human Visual System, Spread Spectrum*

I. INTRODUCTION

Steganography technique is the art and science to hide information in any digital object like image, audio, video only recipient knows of the existence of the information [1, 27]. Precisely steganography is covered message and includes transmitting secret data through the seemingly innocuous files. Steganography is gaining popularity due to growing necessity for security of data [3]. The main objective of steganography is to transfer information from sender to receiver securely in a completely untraceable way and to evade depiction suspicion to the transmission of concealed information [1, 4]. The idea of message hiding in any object is not a novelty; this has been used form centuries all over world under different regimes. It is a technique for hiding information so that it does not even seem to exist. Hiding information in any object has a long history. Greek historian Herodotus writes, Histaeus the Greek ruler wanted to communicate with his son-in-law in Greece. First Histaeus shaved the head of one of his most faith slaves and tattooed the information on the slave’s scalp. After some days slave’s hair grew up again the slave was dispatched with the hidden information. Other historical tricks include tiny pin punctures on selected characters, invisible inks, pencil marks on type written characters and so on.

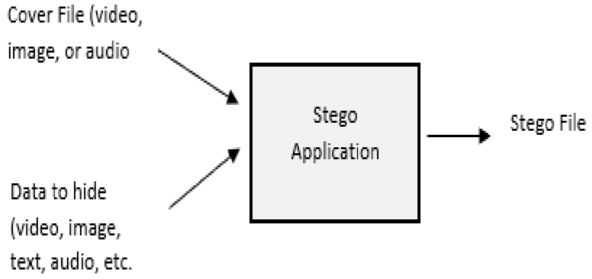
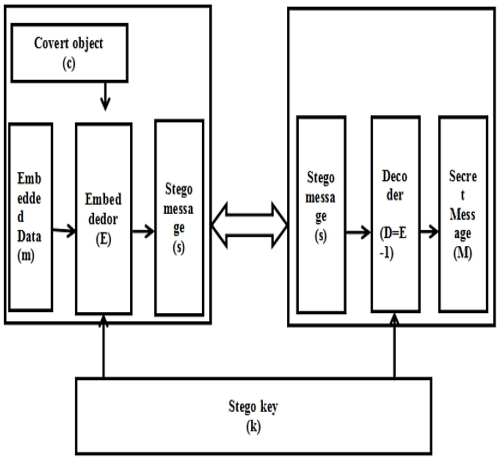

Cover File (video, image, or audio
Data to hide (video, image, text, audio, etc.
Stego Application
Stego File

Figure 1.1: Steganography Application Scenario

Steganography is dissimilar from cryptography. The main goal of cryptography is to secure the communications by modifying the data into a scrambled form but on the other side, steganography methods tend to conceal the existence of the message in any digital object, which makes it very difficult for a spectator to find out where exactly the message is [6, 12]. The message to be hidden in the cover object is known as embedded data. The “stego” object contains both the cover signal and the “embedded” message. The process of hiding information, into the cover digital media object, is known as embedding. The sender hides secret information of any type using a key in a digital cover object to produce a stego file, in such case observer cannot notice the existence of the hidden information. At the receiver end, the receiver extracts the received stego-file to get the hidden message.

Different types of Covers can be used like image, video, audio, text, and IP datagram. Video and Image build steganography rely on the limited HVS (Human Visual System) in observing luminance difference at levels greater than 1 in 240 in constant gray levels or 1 in 30 of random patterns. Though, audio steganography feats the masking affects property of HAS (Human Auditory System), numerous features impact on the quality of audio steganographic technique. The significance and the impact of all features rely on the transmission conditions and the application. Most significant properties or valuables of audio steganography are robustness to noise and to signal manipulation, concealing-capacity of embedded message and security. Robustness requirement is firmly linked to the application and is the most stimulating to satisfy in a steganographic system. In audio steganography system, secure information is embedded in digital audio object [3, 6]. The binary sequence of a cover audio object is utmost altered by adding secret information in it. The digital audio file formats used in audio steganography technique are AU, WAV and MP3 sound files. The altered audio file should not be made identified to the human hearing senses.



1.1.1 Structures of steganography

Given the expanded general consideration over steganography strategies and practices, few basic phrasings that the majority of the application have in like manner has been examined and determined [20, 22]. The things conceded to:

- **Embedded(m):** Some data information or signal to be hidden, in other media.
- **Stego Message(s):** The output of the steganography procedure which is the signal, record or information that has the installed message hidden in it.
- **Cover Object(c):** The contribution to the data concealing procedure which speaks to the blameless transporter flag or document.
- **Stegokey (k):** This is extra unembedded mystery information which might be required in the data concealing procedure. Specifically, this key is regularly expected to extricate the installed message again in the last goal.

1.1.2 Methods of Hiding

1. Substitution-Based: In substitution we can supplant those slightest critical odds for majority of the data that makes the significant substance of the spread record for new information which makes those less measure from claiming twisting. In this the blanket record evaluate doesn’t transform following the execution of the figuring. Confined measure for data could conceal for this approach.

2. Insertion-Based: In this sort we can store the data that we need to hide in those segments of a document which are disregarded by handling application. Because of this we abstain from adjusting those document bits that are significant to an end-client. To instance, for a couple records there is an EOF alternately end-of-file marker. Stowed away information might afterward have the ability to be inserted after the EOF marker. Those end-client might not comprehend that the record holds additional disguised information. We can utilize an infusion strategy which changes record measure with measure of information covered up in document and if the record estimate expansive, it might stimulate doubt.

3. Generation-Based: This kind doesn't require any current blanket archive. In this it makes a cover record to those sole inspirations behind hiding those messages. The standard disservice of the consideration is that examination of the stego record with any former copy of the blanket report (which ought to make A comparative record) furthermore find contrasts between the both.

The Steganography method used should have:

- **Imperceptibility:** The audio with information and unique information source ought to be perceptually indistinguishable
- **Robustness:** The inserted information ought to survive any preparing operation the host signal experiences and safeguard its devotion.
- **Capacity:** Maximum information implanting rate.
- **Secrecy:** Extraction of hidden data from the audio must not occur without earlier authorization of expected client having secret word.
- **Accuracy:** The extraction of the hidden information from the medium ought to be precise and solid.

1.1.2 Steganography Measures

a) **Payload:** It indicates the measure for mystery information that can have a chance to be embedded in the cover audio. The implanting rate may be provided for over aggregate estimation, for example, those periods of the secret message.

b) **Imperceptibility:** A steganographic system will be ambiguous when mankind's eye can't remember the disguise picture and the stego picture.

c) **Security:**Security of a steganographic framework are characterized regarding imperceptibility, which is guaranteed when the statistical tests can't recognize the cover and the stego-picture.

d) **Measurable Attacks:** The approach to uprooting the secret information starting with the stego protest may be known as measurable assault. The algorithm used for steganography must be robust to measurable strike.

e) **Perceptual Quality:** Expanding the payload debase the nature of the audio so approach ought to be utilized to such an extent that the quality ought to stay in place to maintain a strategic distance from it from getting in locate.

f) **Computational Cost:** Information hiding and Data recovery are the two parameters used to figure computational cost of any stegnography approach.

II. RELATED WORK

Inas Jawad Kadhim, et.al [1] provided a thorough review of existing types of image steganography and the recent contributions in each category in multiple modalities. The article also provides a complete overview of image steganography including general operation, requirements, different aspects, different types and their performance evaluations. Different performance analysis measures for evaluating steganographic system are also discussed here. Moreover, this paper also discussed the strategy to select different cover media for different applications and a few state-of-the-art steganalysis systems.

Shilpi Mishra, et.al [2] studied the overall standards concealing mystery facts in sound document utilizing sound information concealing systems, and conveys an outline of present strategies and capacities furthermore talks about favourable circumstances and disservices of diverse sorts of audio steganography method.

Mustafa Sabah Taha et.al [3] reviewed several ways of combining steganography and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganography techniques were presented as well.

Shashikant Singh, et.al [4] proposed a new image steganography method based on spatial domain using least significant bit (LSB) steganography. The colour image is divided into four equal parts and the secret data is also divided into four equal parts and those divided data was hidden in the image segments using least significant bit steganography. In this paper the researchers have critically analysed various stenographic techniques and also have covered steganography overview its major types, classification, applications.

Alaknanda S. Patil, et.al [5] reviewed the steganography as the embedding process of the secret message in other carrier message. It carries the security, transparency and authenticity. The type of steganography is depending on the cover message used, if cover message used is audio to hide any type of data, it is audio steganography. The secret data hidden behind the audio can be image, audio or text. Audio steganography is more preferable because of the lots of redundancy. The different domains and methodologies are in exist for secret data embedding in audio signal. This paper gives the variety of algorithms to study the Audio Steganography.

Pratiksha Sethi, et.al [6] For appealing the defence of data thrashing and communication over network, the anticipated system uses cryptographic algorithm along with Steganography. In the anticipated system, the file which we want to make protected was firstly compressed to shrink in size and then the compressed data is transformed into cipher text by using AES cryptographic algorithm and then the encrypted data is concealed in the image. Genetic Algorithm was used for pixel assortment of image where data was to be concealed so that detection of clandestine information become multifarious.

Mahmoud Mustafa Mohammed Mahmoud [7] presented a model which consists of three stages, the text is first compressed using the Huffman algorithm then encrypted using AES algorithm and finally hide using the novel LSB-Block algorithm. A novel proposed mechanism, Binaries of Message Size Encoding (BMSE), were performed before the hiding process to produce a key, which is used in the hiding process in the proposed enhanced LSB-Block algorithm. The model was applied using the MATLAB program and tested using the Mean Error Square (MSE) operators and the Peak Signal to Noise Ratio (PSNR). Different comparisons were made and the results verified the efficiency and effectiveness of the proposed model.

Kamred Udham Singh [8] surveyed the overall principles of hiding secret data in audio file using audio data hiding techniques, and deliver an overview of present techniques and functions and also discuss the advantages and disadvantages of different types of audio stenographic methods. This work presents a review on audio steganography techniques and approaches and we also discussed their strengths and weaknesses. In general aim of temporal domain techniques are to maximize the embedding capacity, while in transform domain techniques exploit the masking properties in order to make the noise produced by hidden data undetectable. This survey presented that the frequency domain is preferred over the temporal domain and music signals are better covers for data embedding in terms of capacity, inaudibility and Detectability. The flexible nature of audio file formats and signals makes them good and practical medium for steganography.

Harish Kumar, et.al [9] invented a new strategy in Steganography to get the minimum effect in audio which is used to hide data into it. In this paper, the authors have presented a Steganography method of embedding text data in an audio file. The basic approach behind this paper is to provide a good, well-organized method for hiding the data and sent to the destination in safer manner. In the proposed technique first the audio file is sampled and then appropriate bit is modified. In selected sample one bit was modified at least significant bit. The remaining bits may be used but it may be cause noise. The authors have attempted to provide an overview, theoretical framework about audio Steganography techniques and a novel approach to hide data in an audio using least significant bit (LSB).

Gunjan Nehru, et.al [10] introduced a robust method of imperceptible audio data hiding. This system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Thus, it concludes that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection.

Swati Malviya, et.al [11] reviewed the technique of Information hiding as a new kind of secret communication technology. Steganography has been proposed as a new alternative technique to enforce data security. A perfect audio Stenographic technique aims at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. Hence the main challenge in digital audio steganography is to obtain robust high capacity stenographic systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques. In this paper, the authors have presented a current state of art literature on audio steganographic techniques and how it’s performed.

Soumyendu Das, et.al [12] focussed on Steganography i.e. often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. In this article, the researchers have tried to elucidate the different approaches towards implementation of steganography using 'multimedia' file (text, static image, audio and video) and Network IP datagram as cover. Also, some methods of steganalysis will be discussed.

III. THE PROPOSED METHOD

3.1 Proposed Framework

Step1 : PREPROCESSING

Pre-processing under the embedding phase consists of the following two main tasks. Construct blocks and compute mean and variance This sub process is responsible for constructing the cover and secret blocks. Moreover, the mean and variance for all cover and secret blocks are also computed in this sub process.

Step2: Generate Non Overlapping Blocks

Generate chaotic indexes process:- Chaotic indexes are generated, and these indexes will be used in selecting the cover samples instead of the sequential manner in the traditional LSB. In this proposed model, two secret keys which are the initial parameters of the chaotic map are considered as a secret key provided in sender and receiver sides. In the process, the secret and cover blocks are considered as the range and domain pools, respectively. The IFS coefficients consist of the index, scale, symmetry, and the mean of the secret blocks. The total number of bits of the IFS for all secret blocks is less compared with the number of bits required to hide the actual secret samples. The binary sequences of IFS are used in the embedding sub process. These blocks are optimized by particle swarm optimization, which find the embedded area of optimization

Step3: Generate stego audio

In this step optimize embedded spectrum of audio which converge by particle swarm optimization and mix the audio. This audio contains cover audio embedded with hiding audio. This audio is called stego audio.

STEP4: Reconstruct audio

Extraction process:- The LSB bits of the stego audio samples are collected in the same chaotic way as in the embedding process by using the secret key that retrieves the IFS coefficients. The retrieved coefficients are then used to reconstruct the secret blocks that are later used in the decoding process to reconstruct the secret audio.

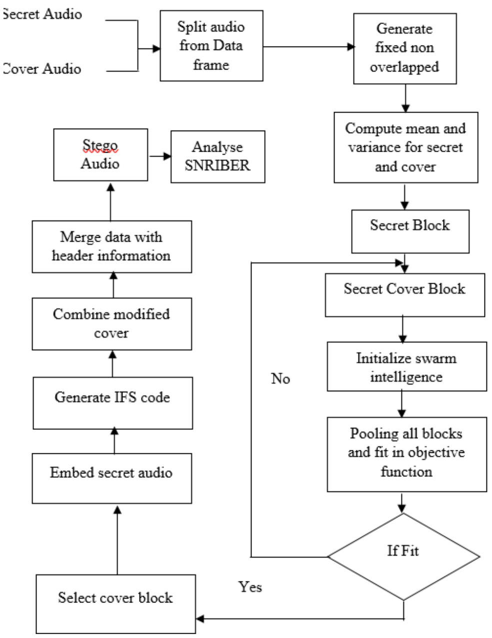

Secret Audio
Cover Audio
Split audio from Data frame
Generate fixed non overlapped
Compute mean and variance for secret and cover
Secret Block
Secret Cover Block
Initialize swarm intelligence
Pooling all blocks and fit in objective function
If Fit
No
Yes
Select cover block
Embed secret audio
Generate IFS code
Combine modified cover
Merge data with header information
Stego Audio
Analyse SNRIBER

Fig 3.1 proposed flow chart

IV RESULT ANALYSIS

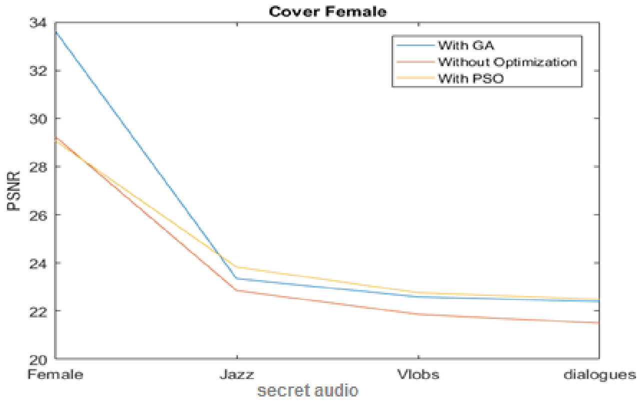


Fig 4.1Comparison of Proposed (PSO) and Existing approach PSNR parameter on different Cover and hidden audio

In fig4.1 comparison of existing, GA based approach and PSO based proposed approach on different cover audio and hidden audio on different optimization like particle swarm optimization and genetic algorithm. In fig 4.1 x-axis show the secret or hidden audio and cover audio. In Y-axis show the PSNR .In different secret audio Proposed approach PSNR averagely increase from other approaches.

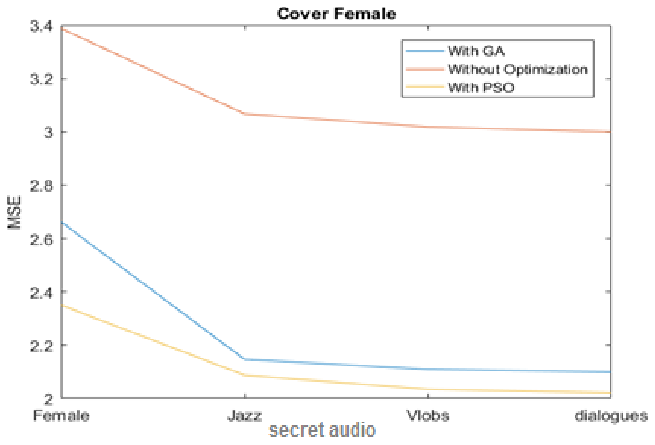


Fig 4.2 Comparison of Proposed (PSO) and Existing approach MSE parameter on different Cover and hidden audio

In fig4.2comparisons of existing, GA based approach and PSO base proposed approach on different cover audio and hidden audio on different optimization like particle swarm optimization and genetic algorithm. In fig 4.2 x-axis show the secret or hidden audio and cover audio. In Y-axis show the MSE. In different secret audio Proposed approach MSE averagely reduce from other approaches.

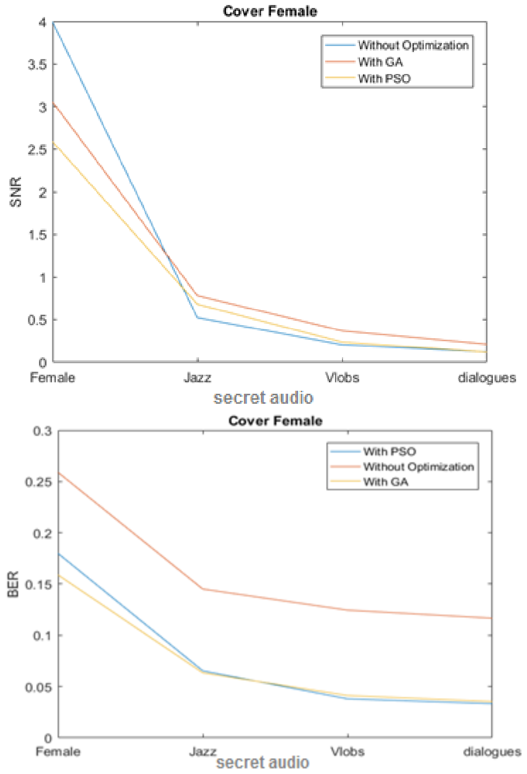


Fig 4.3 Comparison of Proposed (PSO) and Existing approach SNR-BER parameter on different Cover and hidden audio

In fig4.3comparisons of existing, GA based approach and PSO based proposed approach on different cover audio and hidden audio on different optimization like particle swarm optimization and genetic algorithm. In fig 5.10 x-axis show the secret or hidden audio and cover audio. In Y-axis show the SNR-BER. In different secret audio Proposed approach SNR-BER average difference reduce from other approaches. It show BER reduce in proposed approach

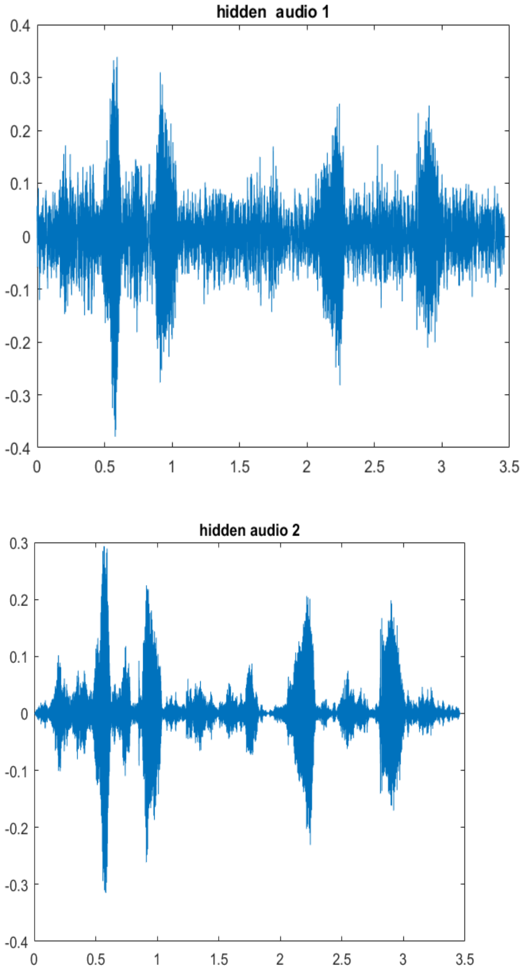


Fig 4.4Comparison of Proposed (PSO) and Existing approach SNR-BER parameter on different Cover and hidden audio

In fig4.4show the screenshot of cover audio and different hidden audio. these results are derived by particle swarm optimization.

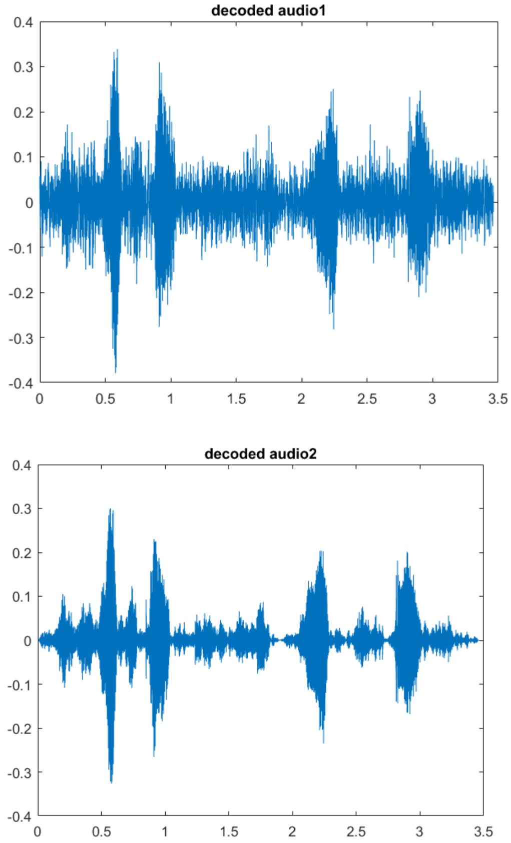


Fig 4.5Comparison of Proposed (PSO) and Existing approach SNR-BER parameter on different Cover and hidden audio

In fig4.5show the screenshot of decoded audio and different hidden audio. these results come by particle swarm optimization.

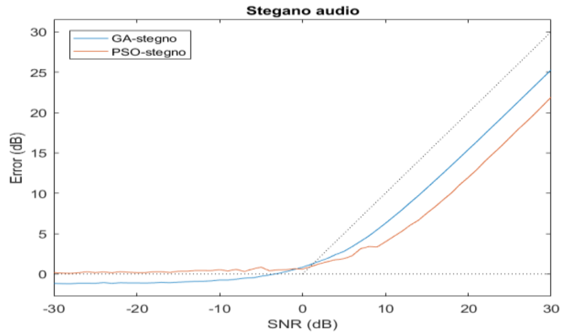


Fig 4.6 Comparison of Proposed (PSO) and Existing approach SNR-BER parameter on different Cover and hidden audio

In fig4.6 show the screenshot of decoded audio and different hidden audio. these results come by particle swarm optimization.

.

IV CONCLUSION

growing use of Internet among public masses and the abundant availability of public and private digital data has driven industry professionals and researchers to pay a particular attention to data protection. Currently, three main methods are being used: cryptography, watermarking, and steganography. Novel and versatile audio steganography methods have been proposed. The goal of steganography systems is to obtain secure and robust way to conceal high rate of secret data. We focus in this paper on digital audio steganography, which has emerged as a prominent source of data hiding across novel telecommunication technologies such as covered voice-over-IP, audio conferencing, etc. The multitude of steganography criteria has led to a great diversity in these system design techniques. In this paper, we review current digital audio steganography techniques and evaluate their performance In proposed approach using PSO effects on non-overlapping block and improve the different spectrum audio embedding. PSO improve optimization because its optimize local and global blocks. In fig 4.6 and fig 4.9 analysis the PSNR, MSE ,SNR and BER parameters on different cover and hidden audio are analysed. In fig 4.1 analysis of PSNR is done. In cover audio female PSNR is highest 34 and less in cover audio jazz 22. In fig 4.2 analysis of MSE is done .MSE reduce when cover audios use dialogues and Jazz. In cover audio female MSE is lowest 0.2 and highest in cover audio jazz 2.2.

V REFERENCES

1. Kadhim, Inas Jawad, Prashan Premaratne, Peter James Vial, and Brendan Halloran. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research." *Neurocomputing* 335 (2019): 299-326.

2. Mishra, Shilpi, Virendra Kumar Yadav, Munesh Chandra Trivedi, and Tarun Shrimali. "Audio Steganography Techniques: A Survey." In *Advances in Computer and Computational Sciences*, pp. 581-589. Springer, Singapore, 2018.

3. Taha, Mustafa Sabah, Mohd Shafry Mohd Rahim, Sameer Abdulsattar Lafta, Mohammed Mahdi Hashim, and Hassanain Mahdi Alzuabidi. "Combination of Steganography and Cryptography: A short Survey." In *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, p. 052003. IOP Publishing, 2019.

4. Singh, Shashikant, Seema Yadav, Ankur Raj, and Priya Gupta. "A Survey Paper on Different Steganography Techniques." In *Proceedings on International Conference on Emerg*, vol. 2, pp. 103-108. 2018.
5. Patil, Alaknanda S., and G. Sundari. "An Embedding of Secret Message in Audio Signal." In *2018 3rd International Conference for Convergence in Technology (I2CT)*, pp. 1-3. IEEE, 2018.
6. Sethi, Pratiksha, and V. Kapoor. "A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography." *Procedia Computer Science* 87 (2016): 61-66.
7. M. Mustafa, M. Mahmoud, H. Tagelsir, and I. Elshoush, "A Novel Enhanced LSB Algorithm for High Secure AudioStegnography" *2018 10th Comput Sci Electron Eng. Conf. CEEC 2018-PROC.,PP. 125-130,2019.*
8. Singh, Kamred Udham. "A survey on audio steganography approaches." *International Journal of Computer Applications* 95, no. 14 (2014).
9. Kumar, Harish. "Enhanced LSB technique for audio steganography." In *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, pp. 1-4. IEEE, 2012.
10. Nehru, Gunjan, and Puja Dhar. "A detailed look of audio steganography techniques using LSB and genetic algorithm approach." *International Journal of Computer Science Issues (IJCSI)* 9, no. 1 (2012): 402.
11. Malviya, Swati, Manish Saxena, and Dr Anubhuti Khare. "Audio steganography by different methods." *Int. J. Emerg. Technol. Adv. Eng* 2, no. 7 (2012): 371-375.
12. Das, Soumyendu, Subhendu Das, Bijoy Bandyopadhyay, and Sugata Sanyal. "Steganography and Steganalysis: different approaches." *arXiv preprint arXiv:1111.3758* (2011).