Message Security Enhanced By Bit Cycling Encryption and Bi-LSB Technique

Gera, Anju
Banasthali University

Vyas, Vaibhav
Banasthali University

https://doi.org/10.5109/4843115

出版情報：Evergreen. 9 (3), pp.845-852, 2022-09. 九州大学グリーンテクノロジー研究教育センター
バージョン：

Message Security Enhanced By Bit Cycling Encryption and Bi-LSB Technique

Anju Gera[1, 2*], Vaibhav Vyas[1]

[1]Banasthali University, Jaipur, India

[2]GLBITM, Greater Noida, Uttar Pradesh, India,

*Author to whom correspondence should be addressed:

E-mail:anju.gera@gmail.com

(Received May 23, 2022; Revised July 25, 2022; accepted July 25, 2022).

Abstract: Steganography is a powerful and effective data-hiding technique that has received great interest in recent years due to its effectiveness in maintaining the security of data transferred over the internet. To provide safe data transfer, various steganography technologies have lately been presented and developed. Steganography and encryption are basic methods of securing data exchange. A new algorithm is encrypted based on text messages and exchanges the bit positions around a key point using the Bi-LSB (Bi-Least Significant Bit) method. After adding the hidden message, the changed audio file appears to be the original carrier file. In comparison to previous experiments, the suggested approach increases hiding capacity by 30% while maintaining an acceptable stego. The Signal to noise (SNR) is 69.2 DB.

Keywords: Audio Steganography, LSB, Bit Cycling Encryption and Audio Security

1. Introduction

As the need for security grows, encryption requires a more secure method of concealing confidential information. Thus, cryptography is the process of converting plain text to cipher text. Using cryptography, it is possible to encrypt highly secure data. This method aids in the conversion of data in such a way that it cannot be understood. Steganography is a form of encryption that is used in addition to encryption. It is not intended to be a replacement for encryption. However, combining steganography and encryption increases data security. “The objective of audio steganography is to hide the information contained within the audio files”) [1]. The Internet, in digital form, allows people all over the world to share information (Fricker & Schonlau, 2002)[1, 2, 3]. The security of digital data against any type of access, attack, or theft is the key issue. The major difficulty is coming up with a way to secure data and assure its security while it is being transmitted. Confidentiality, integrity, and availability are three components of information security. This could be accomplished using information concealment techniques such as cryptography and steganography (Lenti, 2000)[4, 5]. The act of encrypting and decrypting digital data is referred to as cryptography. (Katzenbeisser & Petitcolas, 2000)[6, 7, 8] One of the major flaws in such techniques is that the message remains unencrypted even after it has been encrypted. “Steganography is the practice of hiding information within the cover file. The study of the concealing information within primary data without impacting the size of the data or the cause of any form of perceived distortion"[9]. “Matthews (2003)[9, 10] Watermarking, on the other hand, is a second technique for embedding a watermark into the host cover to protect the copyright of the hosts. Steganography is commonly used to create point-to-point data security. (Bilal, R. Kumar, M. S. Roj, and P. K. Mishra, 2014)” [12] During transmission, the steganographic technique's ability to secure data in the carrier media against intrusions or manipulation is limited. (Katzenbeisser & Petitcolas, 2000)[9], in most circumstances, steganography and watermarking are used to embed information in host material in a transparent manner. El-Khamy, S. E., Korany, N. O., & El-Sherif, M. H (2017)[15].To implement cryptography, a new algorithm has been developed, which is based on cycling bits around a hidden point. The user identifies that hidden location as a crucial point. It is a symmetric approach that is inexpensive in cost, straightforward to implement, and secure since the bits after and before the key point are exchanged with each other. Hariri, M., Karimi, R., & Nosrati, M. (2011)[16] according to this paper for further security, a steganogram is incorporated. Audio steganography is an effective technique for transferring embedded data over the internet. Unfortunately, neither the compressed text message approach nor the LSB methodology focuses on steganography before encoding a secret message.

Research Objectives

An Enhanced Bi-Least Significant Bit MP3 audio steganography approach has been developed to tackle the security challenges related to LSB approach. How can a modern steganalysis method that relies on the LSB approach be designed to resolve security concerns? [17-19].This is the key research subject.

Research Gap analysis

- Due to the extraordinary sensitivity of the human auditory system, it is difficult to hide concealed data in audio files.
- Increasing hiding capacity reduces the resilience of the hidden message of the stego file. It is difficult to strike a balance between these aspects.

The rest of the paper is organized as follows: Section 2 described the previous work on steganographic audio techniques. In Section 3 the metrics of data steganography are discussed. Section 4 introduces the proposed model, as well as its phases and dataset. The results of the experiment, as well as the ensuing discussion, are described in Section 5. In Section 6 conclusion is demonstrated.

2. Literature Review

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021)[29] The method may raise the level of the embedding layer without reducing signal transparency, according to the results of the tests.[20-29] The maximum number of bits that may be used in LSB audio steganography without having a noticeable influence on the host audio stream is 4 LSBs. Experiments demonstrate that employing this novel data embedding approach with 7 LSBs instead of the LSB standard algorithm with 4 LSBs increases carrier audio data concealing capacity by 35 to 55 percent.

El-Khamy, N. O. Korany, and M. H. El-Sherif (2017)[15] proposed a steganography method using the Discrete Wavelet Transform (DWT) domain. This approach encrypts an original picture component using RSA and then embeds cipher bits in the audio signal's detailed components using a predefined threshold value. Panyavaraporn and Horkaew (2018)[23] proposed an efficient method for an undetectable digital watermarking technique using discrete Cosine Transform and discrete Wavelet Transform domains. According to the experimental results of the suggested technique, the PSNR values of watermarked movies can reach about 37 dB with the optimal watermarking strength. (High Efficiency Video Coding) HEVC stream compression resistance has been demonstrated for the suggested approach.

A. Wahab, A. A. Khalaf, A. I. Hussein, and H. F. Hamed (2021)[31]. In the proposed work, a hybrid data compression methodology enhances the input data so that it can be encrypted using the RSA cryptographic method to improve security. Ali and J. M. Kadhim (2021)[4]. The submitted study proposed a text-hiding mechanism for encrypting confidential texts using Unicode characters. The glyphs' similarity gave invisibility and boosted the ability to hide. Finally, employing the Huffman compression technique on an unlimited text length, the proposed method proved successful in safeguarding secret data and obtaining high payload capacity. Furthermore, by hiding the changes to the original data, the procedure complies with cognitive transparency. The approach presented in this work increases security by using the Advanced Encryption Standard algorithm to encrypt a secret message before embedding it in the cover text. Karthik, S. M. Satapathy, and A. K. Dwivedi (2022)[21] "The LSB algorithm is used to encrypt messages in images, and the Steganography method encrypts data in a data carrier in such a way that an outsider cannot identify that a message has been encoded. The existence of the watermark is frequently broadcast totally over the image, making any communication or message clandestine or discrete impossible" [21]. The main topic of our paper is the essence of data security and measures to protect it.

2. 1 Related Studies

Embedding in Before All Frames: Karthik. (2022)22) proposes a new way to build before all frames (BAF). The text message is embedded in an MP3 audio file in this way. The text message is disguised using the RSA technique to strengthen the security of the secret message. When the encryption algorithm is not used, around 30 KB of space is required for an MP3 file; otherwise, about 15 KB is required. Although this method has a chance of revealing hidden information, the benefits outweigh the disadvantages. Message Integrity was used to develop a mechanism for audio steganography. According to Atoum, Ibrahim, Sulong, and Zamani (2013)[5], the Steganography technique's designer employed a simple paradigm for extracting and embedding the hidden information. Some of them used the same key to extract hidden messages as well as embed messages in the host signal. The initial steganography paradigm used actual information for the hidden message buried in the cover medium, resulting in a stego-object that included both the cover and the secret message [32, 33]. The possibilities of attackers damaging and reading the secret message, on the other hand, have increased. It's possible that if the attacker discovers the secret message, it will be changed or deleted [22]. The proposed approach offers two options: first, scrambling the secret message before embedding it; and second, encrypting the secret message after it has been inserted. Furthermore, the random selection offers higher security than sequential selection.

[25, 26] demonstrates a novel method for embedding the secret message in audio files using M16MA and M4M.

Because of M16M, these algorithms were created in the form of images. The M4M, a mathematical function, precisely embeds two bits of the secret message in a random process by mapping two bits of the hidden message into the necessary slot using a pseudo-random integer. The algorithm, which is the optimum technique of insertion, functions in such a way that the nature of the data is decided ahead of time to be disguised. "The M16MA was also upgraded in terms of determining the embedding location. In the year 2021, researchers created a technique for embedding text in audio steganography utilizing Advanced Encryption Standard, Spread Spectrum Techniques, and text Compression in Mp3 and Mp4 File Formats"[28]. Encryption and compression of plain text, audio signal breakdown and mixed-signal synthesis are all employed in the embedding module. Timothy, A. O., Adebayo, A[30], "To secure the plaintext secret message from attackers, it is encrypted with a public key and a private key. This prevents unauthorized access to the content. This work used the Advanced Encryption Standard)"[30]. Abood, E. W., Abdullah, A. M., Al Sibahe, M. A., Nyangaresi, V. O., &Kalafy, S. A. A. (2022)[1] A robust hybrid security stego-system was created by combining steganography and cryptography. To begin with, a text message is encrypted using a novel approach that generates cipher text via a bit-cycling mechanism.

3. Data Steganography Metrics

- **SNR**

"The fidelity error of two input and output is tested using SNR. SNR is denoted as" [31].

$$SNR = 10log10 \sum_{i=1}^{N} s1(i)^2 / \sum_{i=1}^{N} (s1(i) - s2(i))^2 \quad (1)$$

- **Mean square error**

"It is the ordinary size of input-output differences and is denoted by"[31].

$$MSE = 1/N \sum_{i=1}^{N} (s1(i) - s2(i))^2 \quad (2)$$

- **Hiding Capacity**

HC, which is the key component for measuring any approach in steganography[31].

$$HC = (hidden\ file\ size\ /\ cover\ file\ size * 100) \quad (3)$$

4. Proposed System

The proposed method comprises two stages (see Fig.1). In this work, to encrypt a text message, a bits-cycling method is used, which exchanges the bits' position around a key point. After that, hide the message inside the cover file using the Bi-LSB method. For increased security, a steganography technique is included with the use of the MATLAB programme and by introducing Bi-Least Significant Bit MP3 audio steganography technology has been modified to overcome the security issue with traditional LSB approaches and give a more secure way to hide audio data

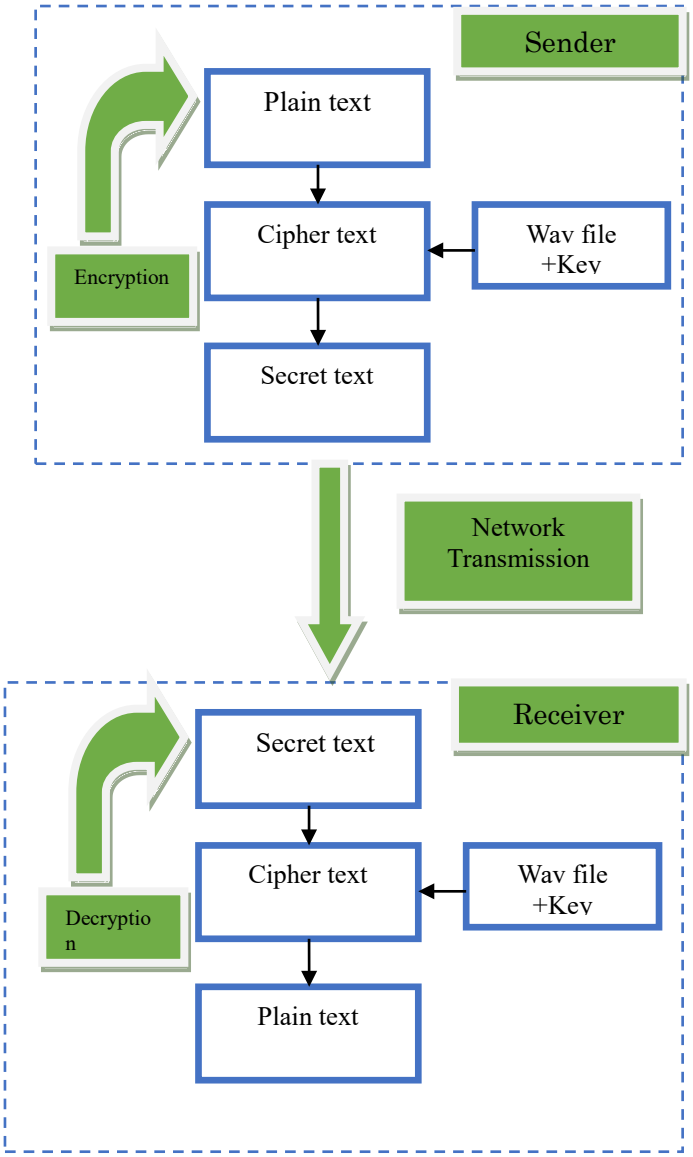

Fig.1: General system Diagram

To evaluate the suggested Bi-LSB approach's performance, this includes SNR and MSE values for various message sizes embedded in an audio cover file.

4. 1 Embedding Phase

The embedding and extraction processes are the two key processes in this phase. The secret message is handled via bit cycling with turns and keys to produce encrypted data throughout the embedding process. Using the Bi-LSB approach, the secret message is then inserted into the cover, resulting in compressed stego data.

4.2 Extraction Phase

The stego file is then opened to reveal the hidden file. The retrieval of stego-data will be aided by decrypting the message using bit cycling from each pixel. The Bi-Least significant Bit technique is used to retrieve the cover's hidden file.

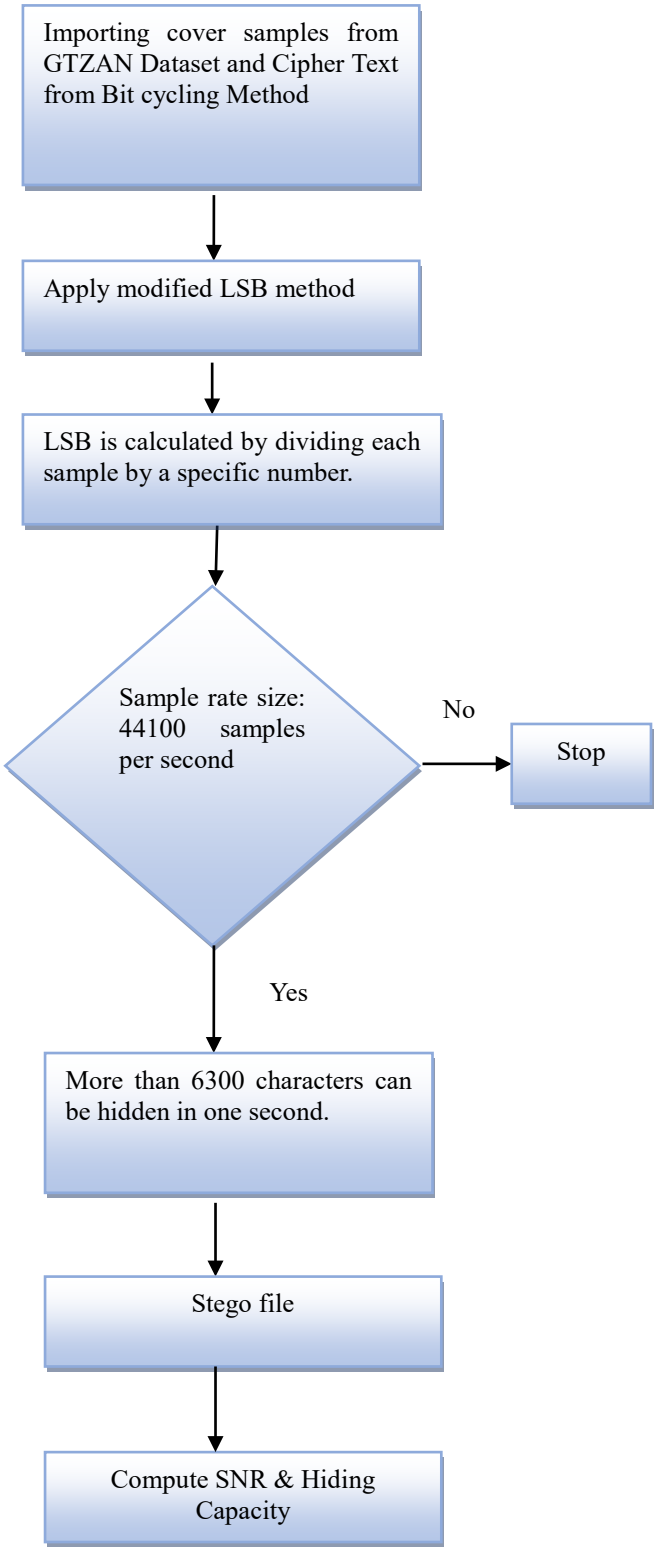

Fig: 2 proposed flow Diagram

The capacity of hiding messages and the length of the plain text varies depending on the wav files sampling rate (See Fig. 2). The text character takes a 7-bit binary representation. A sampling rate of 44100 samples per second means that more than 6300 characters may be hidden in 1 second.

4.3 Datasets

GTZAN dataset is easily accessible to use embedding and extraction algorithms for securing confidential audio files. "Free Audio Converter to convert each genre from wav to MP3 format in order to produce MP3 files" [31].

4.4 System Development

The proposal system was created with MATLAB. The developed system imports the audio file from the MP3 into MATLAB.

4.5. Encryption technique

Encrypting plain text messages with a recommended method that uses plain text to produce a cipher text was the original security solution. To represent each readable letter in the computer in the recommended manner, 7 bits are required (C6 - - - C0). To create a new character, the arrangement of these bits was modified. The encryption algorithm is depicted in fig 1.

Sender side algorithm:

a. Use an encryption key that is a number between 1 and 6, such as M=3, as a cycling point.

b. Remove the portions that come after point M and put them at the start of the new text. (C6 C5 C4 C3 / C2 C1 C0) A= (C6 C5 C4 C3 / C2 C1 C0) B = (- - - C6 C5 C4 C3).

c. The remaining pieces of A are added to the beginning of the new character: B = (C2 C1 C0 C6 C5 C4 C3) The ASCII code for the character 'c', for example, is 99, while the binary code is (1100/011). The new binary is ('011/1100'), which is 60 for the letter ',' if the key is 3. The procedure is performed for each character in the message to obtain the encrypted message.

d. The recipient receives the encrypted message, which is concealed in a sound file (as stated in the following part).

e. end

Receiver side algorithm:

After the recipient gets the audio message, the ecryption key is used to recover the encrypted text message from the cover file.

Encryption key+1: Decryption key=Encryption key: cipher character B= (b2 b1 b0 / b6 b5 b4 b3)

Plain character A= (b6 b5 b4 b3 / b2 b1 b0)

The binary code is then converted to an ASCII code, which is then converted into plain text message characters.

4.6 Steganography Technique - Applying the Embedding Process

Starting at GR Generation Randomly, a message embedding for-loop is started, and using a mod (i, 100) step, the hidden message is inserted in the cover audio, by initializing two values k, w which is used in the LSB method. In the classical technique, the chosen byte is updated using the following logic in each of the cycle iterations:

- If the 4-LSB is employed, the secret message's second to fifth bits are replaced with the first four bits available.
- The secret message's bits 2nd to 3rd are substituted with the first available 2 bits if the 2-LSB is used.
- Only the second bit of the secret message is substituted with the first bit when utilizing the 1-LSB. Bits are concealed as follows in each of the cycle rounds for the enhanced Bi-LSB technique:

Hiding bits in Bi-LSB as follows:

- In the first byte - 1 bit hiding
- In the second byte - 2 bits hiding
- In the third byte - 2 bits hiding
- In the fourth byte - 1 bit hiding and repeat

K counter is modified on chosen Bi-LSB method in each one of the iterations.

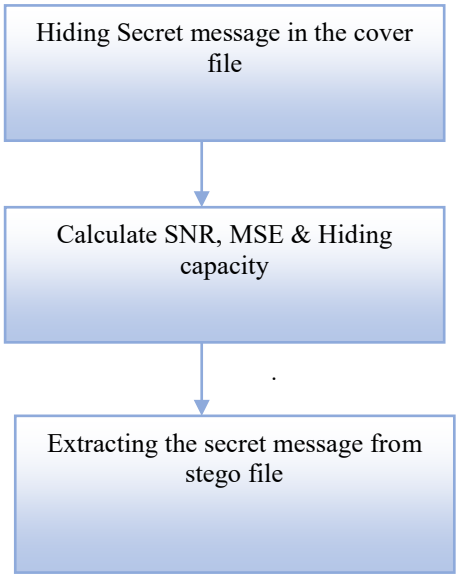

Fig. 3: Stages of simulation

Table 1. Cover, Hidden and Stego data

Cover Data	Hidden Data	Stego	
		MSE	SNR
Voice	welcome	0.42	69.2
Jazz	welcome	0.43	65.2
Male	welcome	0.42	65.2
Female	welcome	0.41	69..2

Table 2. Hiding Capacity

Cover Secret	Cover samples	Secret sample	Block size samples	Hiding Capacity%
Voice	2,20,500	44,100 1,75,300	7 27	20 80
Jazz		2,20,500	34	100
Voice	2,20,500	44,100 1,75,300	7 27	20 80
Voice		2,20,500	34	100
Female	2,20,500	44,100 1,75,300	7 27	20 80
jazz		2,20,500	34	100

5. Evaluation and Results

The text message is encrypted within a cover sound file using a modified LSB approach and then hidden using a unique methodology based on exchanging bit positions around a key point. Fig. 3 shows the stages of the simulation. The extraction method is the inverse of the embedding method. Above Table 1 depicts the cover data, hidden data, and stego audio, as well as the SNR, while Table 2 shows the cover samples 220,500 for Voice, Jazz, Female and Secret samples are not fixed. When Block size is increased, then hiding capacity is increased and thereby decreasing the stego SNR. Using Eq. (3) hiding capacity is measured and SNR is measured by using Eq.(1) of 69.2 dB. Block size are used by ((L2/L1)*IFS) +1), where IFS stands for iteration function system and IFS= {(i), 1<=I<+L2}.The cover audio is shown in Fig. 4 and stego audio is shown in Fig. 5 and retrieved audio is shown in Fig. 6. Table 3 shows the audio specifications that are used in the experimental results

Table 3 Audio parameters

Specifications	
(BPS)Bit per sample	sixteen
(SR)Sample rate	44,100
Medium	Mono
Audio_Type	Speech
Duration(Sec)	One to Nine

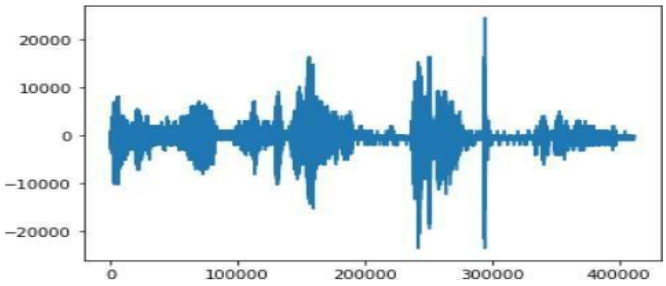

Fig.4: Cover audio

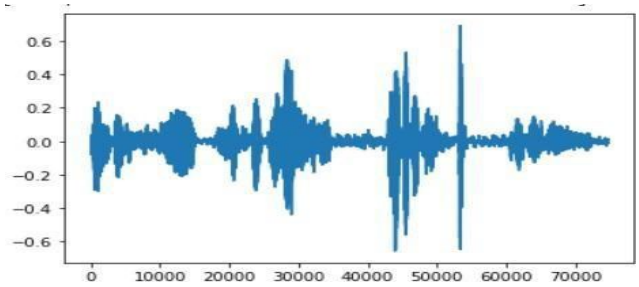

Fig.5: Stego audio

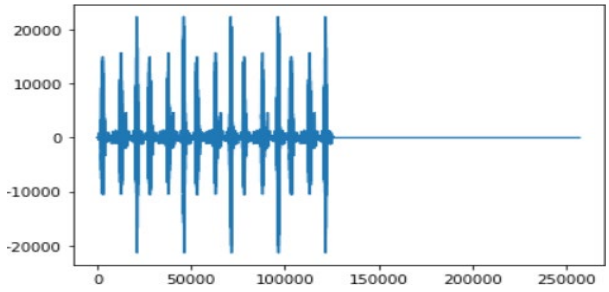

Fig.6: Retrieved hidden data

The performance of the cover Audio, Stego Audio, and retrieved hidden Audio is evaluated and displayed in Figures 4–6. On the receiving end, the hidden data will be extracted by following just the LSB bits of the message.

5.1 Scheme Comparison

The performance of the suggested method is assessed to the other strategies offered in the relevant work, resulting in improved audio steganography hiding capacity. Table 4 shows the literature survey along with the proposed scheme. Gera, A., & Vyas, V. (2022)[31] proposed a method for hiding text. The results show that the SNR value is 72.2 dB with an SDG rate of 4.8. Altinbaş (2021)[17] implemented and proposed a Bit reduction technique with less distortion in the audio file. Alsabhany (2020)[26] proposed an efficient technique to improve the capacity of hiding by 70%. MohammedJ(2020)[5])proposed a model for hiding data in mp3 files. Hussein(2019)[32]The proposed techniques are more suitable and cable for hiding text and measured SNR and PSNR values. Kapoor et.al (2019)[30] used a combination of cryptography and steganography for securing text using echo hiding. And the proposed method shows the result superior to the existing methods.

Table 4. Comparison to related methods

Methods	Hiding Capacity %	Stego SNR dB	PSNR dB
(2022)Gera, A	100	72.2	
(2021)Altinbaş		65.4	45
(2020)Alsabhany	40	40	
(2020)Mohammd J. Alhaddad	97		
(2019)Hussein			74.2
(2019)Kapoor, Kapil		47.7	59.93
Proposed model	100	69.2	

6. Conclusion and Future Work

This study shows how audio steganography may be used to hide encrypted text. In comparison to previous experiments, the suggested approach increases concealing ability by 30% while maintaining an acceptable stego. Audio quality is rated at 69.2 dB SNR. The new model, which is 30% more powerful than the prior system, generates 100% hiding capacity. In the future, more efficient techniques to further increase embedding capabilities should be considered, and the video stream should be used for embedding. In the future, this work might be enhanced by merging it into the hiding of new hidden messages and the inclusion of various types of noises.

References

1) Abood, E. W., Abdullah, A. M., Al Sibahe, M. A., Nyangaresi, V. O., &Kalafy, S. A. “A, Audio steganography with enhanced LSB method for securing encrypted text with bit cycling”, Bulletin of Electrical Engineering, and Informatics, 11(1) (2022). (https://doi.org/10.11591/eei.v11i1.3279.
2) Shaiden, Affiq SM, Shayla Islam, and Kasthuri Subramaniam. "Android based Digital Steganography Application using LSB and PSNR Algorithm in Mobile Environment." (2021): 421-427.
3) S. Choudhary, A. Sharma, S. Gupta, H. Purohit, S. Sachan, "Use of RSM Technology for the Optimization of Received Signal Strength for LTE Signals Under the Influence of Varying Atmospheric Conditions", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol 07, Issue 04, pp 00-00, December 2020
4) Ali, R. H., & Kadhim, J. M.,“Text-based Steganography using Huffman Compression and AES Encryption Algorithm”. Iraqi Journal of Science, 4110-4120.(2021).
5) Alhaddad, M. J., Alkinani, M. H., Atoum, M. S., &Alarood, A. A.). “Evolutionary detection accuracy of secret data in audio steganography for securing

5G-enabled internet of things". *Symmetry*, *12*(12), 2020.

6) N. Yu, W. Tomoaki, "Social Factors Affecting Innovation Cycle of Liquid Crystal Technologies: A Japanese Case Study", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 04, Issue 04, pp. 8-15, December 2017.
7) Fachransjah, T. Y. M. Zagloel, A. Romadhani, "Discrete-Event Simulation and Optimization of Spare Parts Inventory and Preventive Maintenance Integration Model Considering Cooling Down and Machine Dismantling Time Factor", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 07, Issue 01, p 79-85, March2020.
8) D. A. Wulandari, M. Akmal, Y. Gunawan, Nasruddin, "Cooling Improvement of the IT Rack by Layout Rearrangement of the A2 Class Data Center Room: A Simulation Study", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 07, Issue 04, December 2020
9) Rully, L. Yusuf, "Conceptual Framework of Development of Quality Culture in Indonesian Construction Company", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 07, Issue 01, pp 144-149, March 2020.
10) Atoum, M.S., Ibrahim, S., Sulong, G. & Zamani, M. "A New Method for Audio Steganography Using Message Integrity". Journal of Convergence Information Technology. 8. 35- 4. (2013).
11) Gera, A., Dixit, A., & Saini, S., "Elliptic curve cryptography with secure text-based cryptosystem". International Journal of Management, IT and Engineering, 1(7), 167-176.(2011).
12) Bilal, R. Kumar, M. S. Roj, and P. K. Mishra, "Recent advancement in audio steganography," Proc. 2014 3rd Int. Conf. Parallel, Distrib. Grid Comput. PDGC 2014, pp. 402–405, 2015, DOI: 10.1109/PDGC.2014.7030779.
13) Bobade, S., &Goudar, R., Secure data communication using protocol steganography in IPv6. In 2015 International Conference on Computing Communication Control and Automation (pp. 275-279). IEEE2015.
14) El-Khamy, S. E., Korany, N. O., & El-Sherif, M. H. "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption". Multimedia Tools and Applications, 76(22), 24091-24106.2017.
15) Hariri, M., Karimi, R., & Nosrati, M." An introduction to steganography methods". World Applied Programming, 1(3), 191-195.2011.
16) Hemalatha, S. A," Robust MP3 Audio Steganography with Improved Capacity". In 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA) (pp. 640-645). IEEE. 2020, October
17) Altinbaş, Ali Erdem, and Yildiray Yalman. "Bit Reduction Based Audio Steganography Algorithm." *2021 6th International Conference on Computer Science and Engineering (UBMK)*. IEEE, 2021.
18) Jayasankar, U., Thirumal, V., &Ponnurangam, D.,"A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications". Journal of King Saud University-Computer and Information Sciences, 33(2), 119-140.2021.
19) Karthik, C., Satapathy, S. M., & Dwivedi, A. K. "Message Encryption in Images Using LSB Steganography Sequence to Sequence Architecture". In Advances in Distributed Computing and Machine Learning (pp. 104-113). Springer, Singapore.2022.
20) Kotha, H. D., Tummanapally, M., & Upadhyay, V. K."Review on lossless compression techniques". In Journal of Physics: Conference Series (Vol. 1228, No. 1, p. 012007). IOP Publishing.(2019, May)
21) Mitali, V. K., & Sharma, A. "A survey on various cryptography techniques". International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(4), 307-312.(2014).
22) Panyavaraporn, J., & Horkaew, P. "DWT/DCT-based invisible digital watermarking scheme for video stream". In 2018 10th International Conference on Knowledge and Smart Technology (KST) (pp. 154-157). IEEE.(2018, August).
23) Patil, K. A. S. A., &Adhiya, K. P." Hiding text in audio using LSB based steganography". In Information and Knowledge Management (Vol. 2, No. 3, pp. 8-15).(2012).
24) Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. "Video steganography: a comprehensive review". Multimedia tools and applications, 74(17), 7063-7094.(2015).
25) Saravanan, K., Purusothaman, T., Velmurugan, T., & Kavitha, K. V. N." Design and performance analysis of diverse generic data hiding algorithms in cryptography". ARPN J. Eng. Appl. Sci, 12, 6423-6429.(2017).
26) Alsabhany, Ahmed A., Farida Ridzuan, and A. H. Azni. "The progressive multilevel embedding method for audio steganography." In *Journal of physics: conference series*, vol. 1551, no. 1, p. 012011. IOP Publishing, 2020.
27) Sheikhan M, Asadollahi K, Shahnazi R "Improvement of Embedding Capacity and Quality of DWTBased Audio Steganography Systems". World Applied Sciences Journal 13(3):507–516. (2011)
28) Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). "Image steganography: A review of the recent advances". IEEE Access
29) Timothy, A. O., Adebayo, A., & Junior, G. A., (2021) "Embedding Text in Audio Steganography System using Advanced Encryption Standard, Text Compression and Spread Spectrum Techniques in

Mp3 and Mp4 File Formats". International Journal of Computer Applications, 975, 8887.

30) Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. "Hiding data using an efficient combination of RSA cryptography, and compression steganography techniques". IEEE Access, 9, 31805-31815.(2021).
31) Gera, A., & Vyas, V. (2022). Hiding Capacity and Audio Steganography Model Based on LSB in Temporal Domain. *Recent Patents on Engineering*, *16*(2), 65-74.
32) Hussein, Reem, and Wassim Alexan. "Secure message embedding in audio." In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6. IEEE, 2019.