BIOS: Jurnal Informatika dan Sains
Volume 4 Number 01, 2026, DOI 10.54209/bios.v4i01
E.SSN 2988-6910(Online)
https://seaninstitute.or.id/bersinar/index.php/bios/index

Implementation of the Echo Hiding Steganography Method for Embedding Secret Messages in Audio Media

Kevin Marcho Nainggolan[1], Kasih Delayana Marpaung[2], Wetina Hulu[3]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas

Article Info
Corresponding Author:
Kevin Marcho Nainggolan

ABSTRACT

The development of digital technology and audio communication has increased the intensity of information exchange through online media, but it also raises the risk of data leakage and misuse by unauthorized parties. Therefore, information security techniques are needed that not only protect the content of messages but also conceal the existence of the messages themselves. Steganography is an information security technique that embeds secret messages into a carrier medium without raising suspicion. Audio media is chosen because it has high tolerance for small changes in sound signals. This study discusses the implementation of the Echo Hiding steganography method for embedding secret messages in digital audio media. The Echo Hiding method works by adding an echo to the audio signal using specific delay time and amplitude parameters so that it does not significantly degrade audio quality. The research stages include audio data preparation, message embedding process, message extraction process, and evaluation of the stego audio quality. The expected results of this study show that the Echo Hiding method is capable of embedding and extracting messages accurately while maintaining audio quality. Thus, this method can be used as an alternative for audio-based steganographic information security.
Keywords: Steganography, Echo Hiding, Secret Message Embedding, Audio Media

INTRODUCTION

The development of digital technology and audio communication has increased the intensity of information exchange through online media. However, this condition also increases the risk of data leakage and information misuse by unauthorized parties. Data security has become a crucial aspect, especially in maintaining the confidentiality of messages transmitted through open networks. In addition to cryptographic techniques, steganography emerges as an alternative solution that not only protects the content of a message but also conceals the existence of the message itself to avoid suspicion.

Audio steganography utilizes the characteristics of sound signals, which have high tolerance to small modifications, allowing secret messages to be embedded without significantly affecting audio quality. One effective audio steganography method is Echo Hiding, a technique that embeds messages by adding echoes to the audio signal using specific parameters such as delay time and echo amplitude. This method is designed so that the resulting changes are imperceptible to human hearing, thereby maintaining message

invisibility and providing better resistance to signal analysis compared to conventional methods such as Least Significant Bit (LSB).

Based on these conditions, this study focuses on the implementation of the Echo Hiding method for embedding secret messages in digital audio media. This research aims to analyze the ability of the Echo Hiding method to embed and extract messages accurately and to evaluate the quality of the resulting stego audio. It is expected that the results of this study will contribute to the development of audio-based steganographic security techniques and serve as a reference for future research in digital data protection.

The objective of this study is to implement the Echo Hiding steganography method on digital audio media in WAV format as a means of embedding secret messages. In addition, this study aims to analyze the process of message embedding and extraction in stego audio, as well as to evaluate the effectiveness of the Echo Hiding method in maintaining audio quality and successful message retrieval without significant distortion.

LITERATURE REVIEW AND PROBLEM STATEMENT

Although the Echo Hiding method has advantages in maintaining audio quality and improving message security, its implementation still requires further analysis to ensure the accuracy of message embedding and extraction. In addition, an evaluation of the stego audio quality is necessary to ensure that the embedding process does not significantly degrade audio performance.

Based on this, the problem addressed in this study is how the Echo Hiding method is implemented in embedding secret messages into digital audio media and to what extent the method is able to maintain audio quality and extraction accuracy. This study is expected to provide a clear understanding of the effectiveness of the Echo Hiding method as an audio-based steganographic information security technique.

RESEARCH METHODOLOGY

The research method used in this study is an experimental method, which involves the design and implementation of an audio steganography application using the Echo Hiding method. The implementation is carried out directly on digital audio media through a system interface that has been developed. This research consists of several interconnected stages, starting from data preparation, message embedding process, message extraction process, and result evaluation.

Data Preparation

The data preparation stage is carried out through the Echo Hiding Audio Steganography system interface. At this stage, the user uploads a digital audio file using the *Upload Audio* WAV feature. The WAV format is chosen because it is uncompressed, ensuring that audio quality is preserved and suitable for steganographic processing.

After the audio is uploaded, the system displays audio information such as duration, embedding capacity, and sample rate. Next, the user enters a secret message in text form through the *Secret Message* field. The text message is then processed by the system by converting it into binary form so that it can be embedded into the audio signal.

Message Embedding Process (Embedding)

The message embedding process is performed when the user clicks the *Embed Message* button in the system. At this stage, the system applies the Echo Hiding method by adding an echo to the original audio signal.

Message embedding is carried out by adjusting echo parameters such as delay time and echo amplitude, which differ to represent bit values 0 and 1. With these differences in echo characteristics, each bit of the secret message can be embedded into the audio without significantly affecting sound quality.

The result of this process is a stego audio file, which sounds almost identical to the original audio but contains a hidden message. The system also displays a waveform visualization of the audio to show the signal changes before and after embedding.

Message Extraction Process

The message extraction process is performed using the *Extract Message* button in the application. At this stage, the stego audio is analyzed by the system to detect the previously embedded echo parameters.

The system analyzes the audio signal to identify differences in delay and echo characteristics that represent the message bits. These bits are then converted from binary form back into text and displayed in the *Hidden Message* tab. This process ensures that the secret message can be accurately extracted in accordance with the originally embedded message.

Evaluation and Analysis

The evaluation stage is conducted by comparing the original audio and the stego audio in terms of sound quality and message extraction success. Audio quality evaluation is carried out both subjectively through listening and visually through waveform comparison displayed in the system.

In addition, the success of the Echo Hiding method is evaluated based on the accuracy level of the extracted message. The evaluation results are used to assess the effectiveness of the Echo Hiding method in embedding secret messages into digital audio media without significantly degrading audio quality.

RESULTS AND DISCUSSION

The testing of the audio steganography system using the Echo Hiding method was conducted by running the developed application. This testing aims to evaluate the system's performance in performing secret message embedding and extraction processes in digital audio media in WAV format. The test results were obtained from program execution outputs, which include the system interface display, audio waveform visualization, and successfully extracted secret messages.

Furthermore, the program execution results are presented and analyzed to explain the processes occurring at each stage, starting from audio uploading, secret message embedding, to message extraction. This explanation is used to evaluate the success of the Echo Hiding method implementation and its impact on the resulting audio quality.

Initial Display of the Echo Hiding Audio Steganography System

When the Echo Hiding Audio Steganography application is launched, the user uploads a WAV audio file through the *Upload Audio WAV* button. The system then displays audio information such as duration, capacity, sample rate, and waveform visualization.

Next, the user enters a secret message in text form and presses the *Embed Message* button to perform the embedding process using the Echo Hiding method by adding an echo to the audio signal. After the embedding process is completed, a stego audio file is generated without significant changes in sound quality. To retrieve the hidden message, the user presses

the *Extract Message* button, allowing the system to analyze the echo characteristics and display the secret message back in text form.

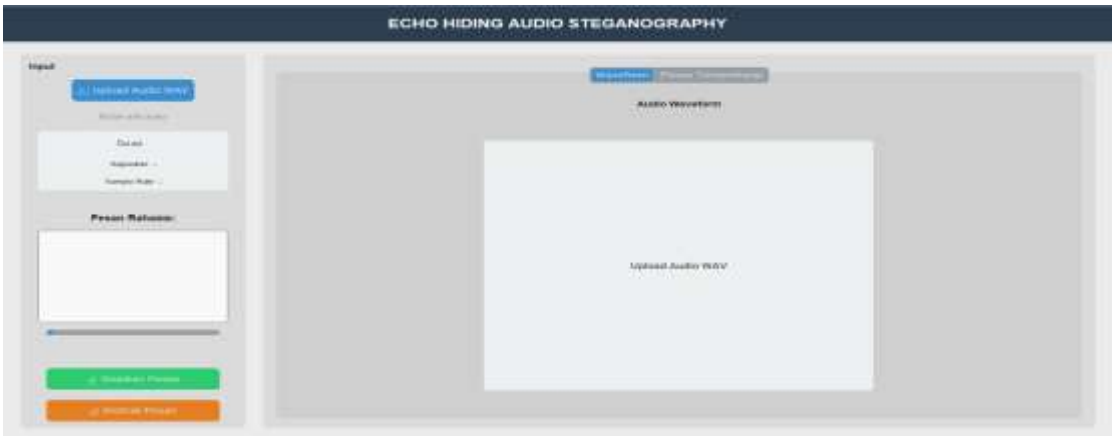

Figure 1. Initial Interface of the Echo Hiding Audio Steganography System

WAV Audio File Selection Interface

After the user clicks the *Upload Audio WAV* button, the system displays a file selection window used to choose the audio media. At this stage, the user can only select audio files in WAV format as a primary requirement for the steganography process. The WAV format is chosen because it is uncompressed, ensuring that the audio quality remains preserved and suitable for the message embedding process using the Echo Hiding method.

.

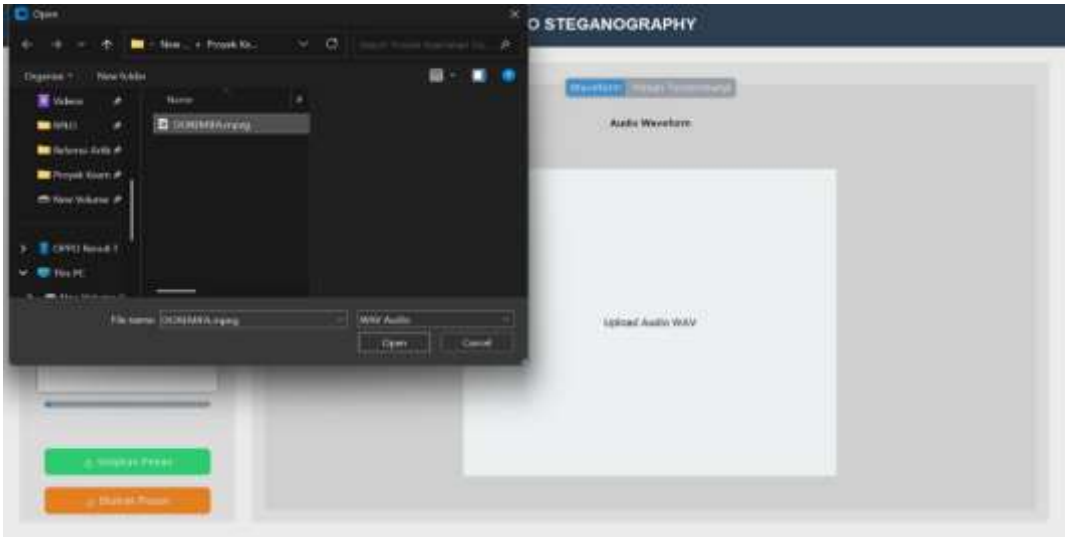

Figure 2. WAV Audio File Selection Interface

Audio Upload Result and Waveform Visualization Interface

After the user successfully selects a WAV audio file, the system displays the uploaded audio file name along with audio information such as duration, message embedding capacity, and sample rate. In addition, the system also presents a waveform visualization in the display area as a representation of the audio signal that will be used in the steganography process. This visualization serves to show the characteristics of the audio signal before the secret message embedding process using the Echo Hiding method is performed.

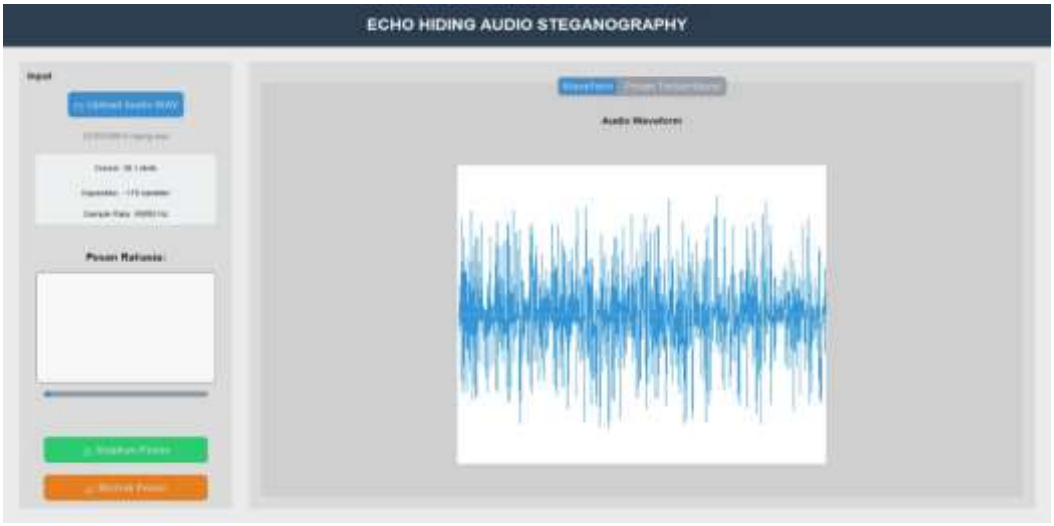

Figure 3. Audio Upload Result and Waveform Visualization Interface

Secret Message Input Interface

At this stage, the user enters a secret message into the *Secret Message* field provided in the application. The input message is in text form, which will then be processed by the system and converted into binary form before the embedding process is carried out. After the secret message is entered, the system is ready to perform the embedding process using the Echo Hiding method by clicking the *Embed Message* button.

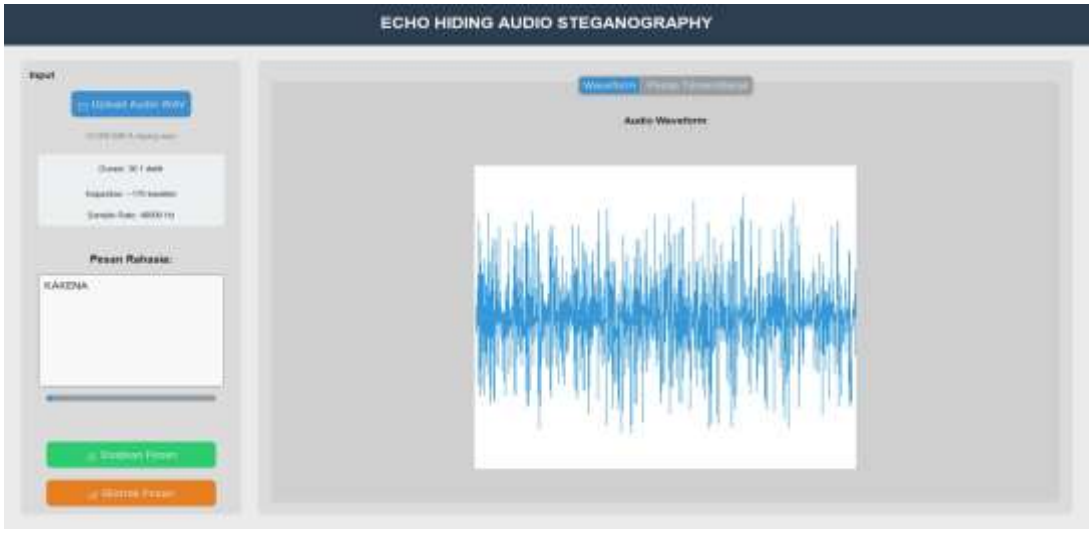

Figure 4. Secret Message Input Interface

Secret Message Embedding Process and Audio Saving Interface

After the secret message is entered, the user clicks the *Embed Message* button to start the embedding process using the Echo Hiding method. The system then displays a *Save As* dialog window, which is used to save the new audio file in WAV format. This audio file is the result of the steganography process and already contains the embedded secret message.

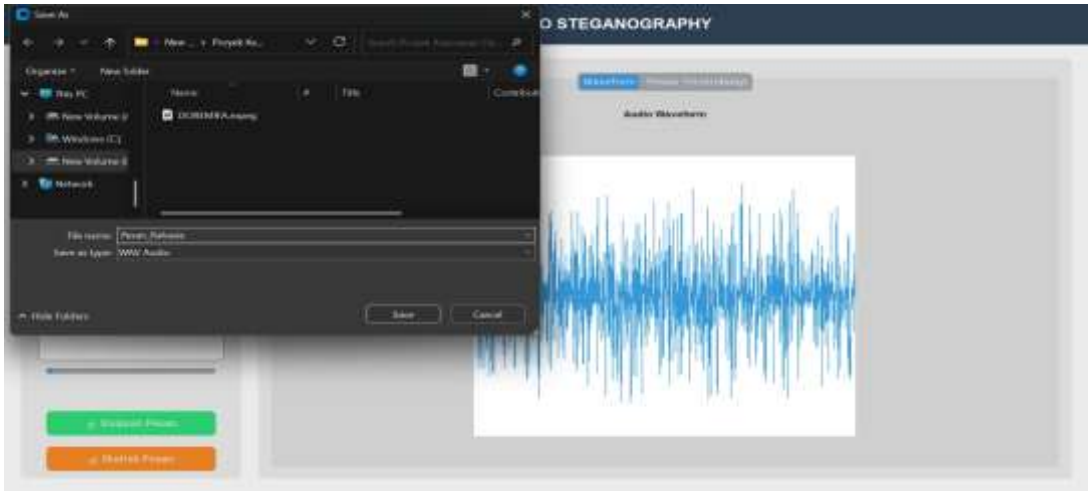

Figure 5. Secret Message Embedding Process and Audio Saving Interface

Success Notification Display

The system displays a notification indicating that the message embedding process has been successfully completed, along with brief information about the stego audio file and the embedded secret message.

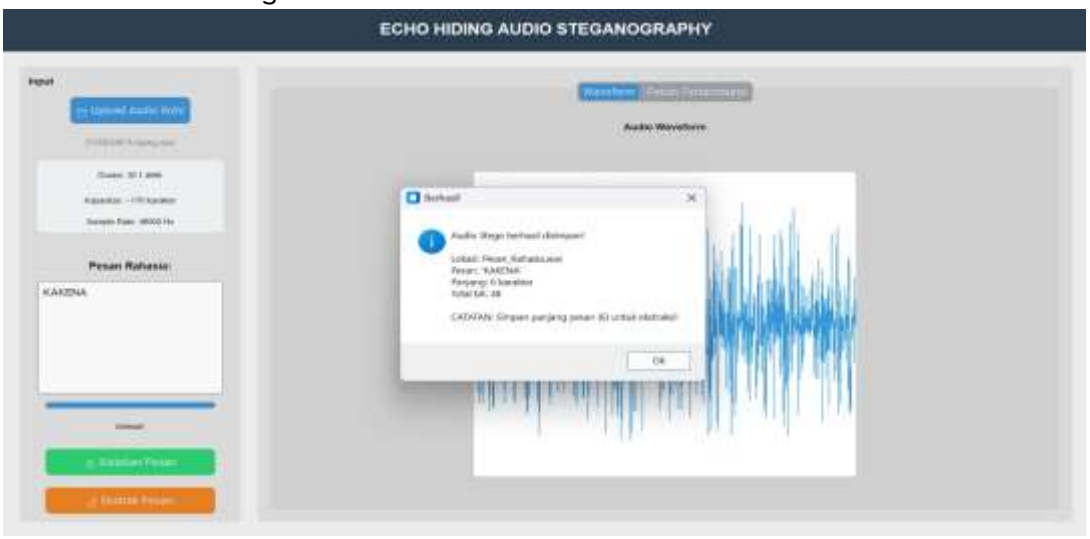

Figure 6. Success Notification Display

Audio Selection Process for Message Extraction

To extract the secret message, the user clicks the *Extract Message* button and selects the previously created stego audio file. The selected file is then processed by the system to retrieve the hidden message embedded within it.

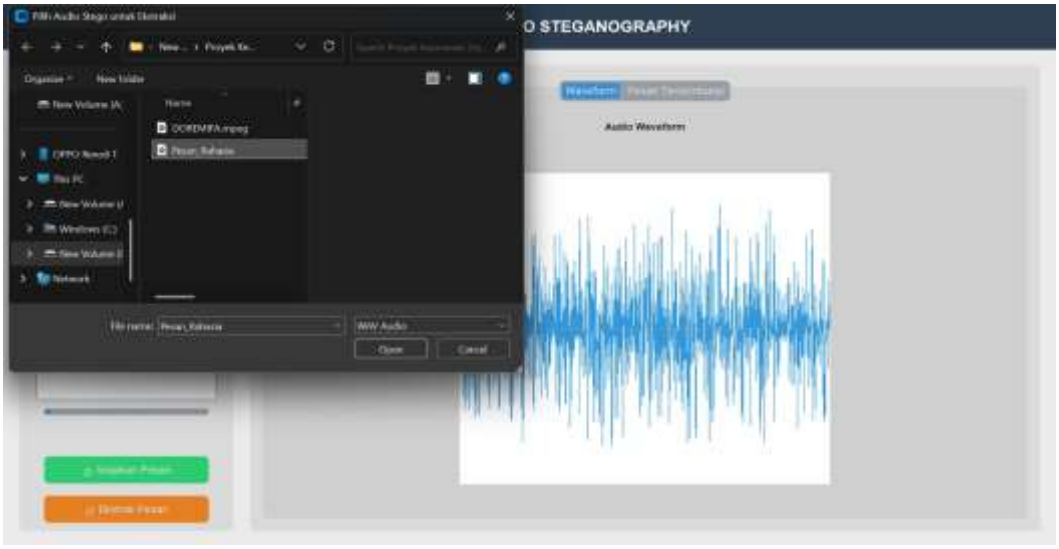

Figure 7. Audio Selection Process for Message Extraction

Secret Message Extraction Result Display

After the stego audio file is selected, the system successfully extracts the secret message and displays it directly on the screen, indicating that the message extraction process using the Echo Hiding method has been successfully executed.

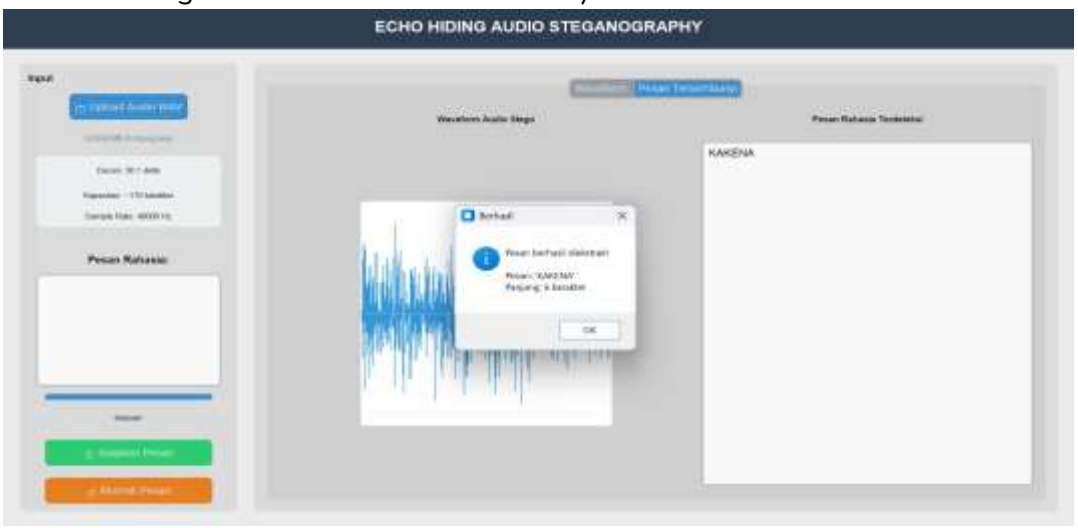

Figure 8. Secret Message Extraction Result Display

Result Analysis

Based on the test results conducted, the audio steganography system using the Echo Hiding method is able to successfully embed secret messages into WAV audio media. The extraction results show that the retrieved message matches the originally embedded message, indicating that both the embedding and decoding processes work correctly.

In addition, the stego audio quality does not experience significant changes compared to the original audio, both subjectively through listening and visually through waveform analysis. This indicates that the Echo Hiding method is effective in maintaining message invisibility without degrading audio quality.

CONCLUSION

Based on the results of implementation and testing conducted, it can be concluded that the Echo Hiding steganography method has been successfully applied to digital audio media in WAV format. The developed system is able to embed secret messages into audio signals

by utilizing echo effects so that the presence of the message cannot be directly perceived by human hearing. In addition, the system is also capable of accurately and consistently extracting the embedded secret messages. The test results show that the steganography process does not cause significant changes to audio quality, allowing the stego audio to still be used in the same way as the original audio. Therefore, the Echo Hiding method can be considered an effective alternative for maintaining information security and confidentiality in digital audio media.

REFERENCES

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). *Techniques for data hiding*. IBM Systems Journal, 35(3–4), 313–336.

Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*. Artech House.

Cvejic, N., & Seppänen, T. (2002). *Increasing robustness of audio steganography using echo hiding*. Proceedings of the IEEE International Conference on Multimedia and Expo (ICME).

Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information hiding: Steganography and watermarking—attacks and countermeasures*. Springer.

Sharma, R., & Bansal, S. (2013). *Audio steganography using echo hiding technique*. International Journal of Computer Applications, 74(6), 1–5.

Aly, H. A., & Al-Qahtani, M. S. (2014). *Audio steganography using phase coding and echo hiding techniques*. International Journal of Computer Science and Network Security, 14(1).

Hassan, M. M., & Saleh, A. A. (2016). *Secure audio steganography based on echo hiding and encryption*. Journal of Information Security, 7(3), 173–182.

Mazurczyk, W., & Kotulski, Z. (2006). *New security and control protocol for VoIP based on steganography*. Computer Communications, 29(15), 3221–3232.

Kekre, H. B., & Athawale, A. A. (2010). *Information hiding in audio signals*. International Journal of Computer Applications, 7(2), 14–19.

Cvejic, N. (2004). *Algorithms for audio watermarking and steganography*. Oulu University Press.