Login : Jurnal Teknologi Komputer
ISSN : 2302-9692 (print) | 2723-8695 (online)
Vol. 18, No. 01, 2024, pp. 18-23
LOGIN http://login.seaninstitute.org/index.php/Login

Analysis Of The Utilization Of Echo Hiding Algorithm In Hiding Secret Messages

Cahaya Elyzabeth Pangaribuan[1], Ogy Kevinta Surbakti[2], Fera Sihotang [3], Yosafat Tamba [4], Yordan Daniel Ndruru[5], Paskah Marto Hasugian[6]
Universitas Katolik Santo Thomas Medan

Article Info

Keywords:

Steganography, Echo Hiding, Data Embedding, Digital Signal, Audio Quality.

ABSTRACT

Steganography is a technique of hiding information in other media to maintain the confidentiality of the message. One of the challenges in steganography is finding a method that can insert data without being detected while maintaining the quality of the original media. This study discusses the application of the Echo Hiding algorithm in audio steganography, which utilizes acoustic properties to insert information into sound signals. The main objective of this study is to analyze the effectiveness and security of the Echo Hiding algorithm in hiding data in audio signals. To achieve this goal, this study uses a digital signal processing method, which includes the stages of message insertion, hidden message extraction, and audio quality evaluation using objective and subjective parameters. Testing was carried out with various scenarios to assess the capacity of insertion, resistance to attacks, and changes in sound quality. The results showed that the Echo Hiding algorithm was able to store information efficiently with little impact on audio quality. Signal analysis showed that the modifications made were not significant to the listener's perception, thus increasing the security and transparency aspects in audio steganography. Thus, this study contributes to the development of a safe and effective steganography method to maintain the confidentiality of information in sound media.

Corresponding Author:

Cahaya Elyzabeth Pangaribuan,
Universitas Katolik Santo Thomas Medan
Email: cahayaelysabeth@gmail.com

1. INTRODUCTION

Information security is becoming an increasingly important global issue as the need for secure communications and personal data protection increases.(Yel & Nasution, 2022). In the digital age, threats to privacy are increasingly complex, with a variety of attack techniques that can reveal or modify sensitive information.(Al Ihsan & Sekti, 2024). One approach used to protect data is steganography, which allows information to be hidden in other media without attracting the attention of unauthorized parties.(Andika & Darwis, 2020). Steganography has a variety of applications, such as secret communications, copyright protection, and security in digital forensics.(Zen Munawar et al., 2023). However, the main challenge in steganography is maintaining a balance between embedding capacity, resistance to detection (steganalysis), and the quality of the media used.(Baso et al., 2024; Widianto, 2017).

Several studies have explored various steganography methods, including the Least Significant Bit (LSB) technique which is developed in domain transformation.(Permana et al., 2021), statistics based(Wulansari et al., 2019). In the context of audio steganography, the Echo Hiding algorithm

emerges as an effective method because it is able to insert information into a sound signal by exploiting acoustic characteristics that cannot be detected by human hearing.(Purba et al., 2016). This method works by adding a very subtle echo into the original signal, so that the changes that occur are minimal and do not arouse suspicion. Although there have been many studies discussing Echo Hiding, there are still challenges in optimizing parameters such as echo amplitude, delay time, and decay ratio to increase the insertion capacity and resistance to steganalysis attacks.(Albantany, 2021; Rumahorbo & Perangin-angin, 2021).

The existing research gap shows that although Echo Hiding offers high security and minimal distortion, there are not many studies that comprehensively analyze the effectiveness of this method under various signal conditions and steganalysis environments. In addition, optimizing echo parameters to achieve the best balance between audio quality and embedding capacity is still a challenge that needs to be solved.(Octaviany et al., 2021). Therefore, further studies are needed to assess the extent to which this method can be practically applied in various usage scenarios.

This study aims to analyze the working principle of Echo Hiding, evaluate its effectiveness in inserting and extracting information, and examine its impact on audio signal quality. The expected results of this study are an increase in understanding of the optimization of the Echo Hiding algorithm, as well as a contribution to the development of steganography methods that are safer and more efficient in maintaining the confidentiality of information.

2. METHOD

This study uses an experimental approach with quantitative analysis methods to evaluate the effectiveness of the Echo Hiding algorithm in audio steganography. The selection of this method is based on the need to measure the robustness, embedding capacity, and impact of the algorithm on the quality of the audio signal. This approach also allows comparison with other steganography methods to assess the advantages of Echo Hiding in various scenarios with the following work process:

1. Media Identification
   Selecting the media to be used to hide the data, such as audio or images. Reviewing the characteristics of each media and how they can affect the final result.
2. Algorithm Implementation
   Develop and implement Echo Hiding algorithms in selected contexts. Use relevant software to test and validate the effectiveness of these methods in hiding data.
3. Security Analysis
   Perform security analysis to evaluate how well the hidden data can withstand detection attempts. Use various analysis techniques to measure the resistance of this method to attacks.
4. Performance Evaluation
   Evaluate the performance of the algorithm in terms of hiding capacity, quality of affected media, and processing time. Compare the results with other steganography methods to determine strengths and weaknesses.
5. Case study
   Using case studies to demonstrate practical applications of the Echo Hiding algorithm in real situations, such as in confidential communications or sensitive data protection.

3. RESULTS AND DISCUSSION

Research result

This section presents the results of research related to the implementation of the Echo Hiding algorithm in audio steganography, as well as an analysis of its effectiveness, security, and impact on signal quality. The results obtained include an evaluation of the embedding capacity, resistance to detection, and a comparison with other steganography methods. The discussion is carried out by analyzing the extent to which Echo Hiding is able to hide information without being detected by the listener or steganalysis method. In addition, the audio quality after data embedding is tested using objective and subjective methods to ensure that changes due to embedding do not significantly affect the listener's experience. Further analysis also includes the effectiveness of the algorithm in various

scenarios, including differences in the echo parameters used and how this affects the security and embedding capacity. The results of this study are expected to provide deeper insight into the application of Echo Hiding as a safe and efficient steganography technique in secret communications and sensitive data protection.

1. Convert Message to Binary

The first step in the steganography process is usingEcho Hiding Algorithmis to convert the message to be inserted into binary form. Each character in the text message is converted into a binary representation usingASCII codeorUnicode, depending on the system requirements in this study, text insertion was carried out as "I" with the following representation.

Representation Table

Character	Ascii	Binary
S	83	01010011
A	65	01000001
Y	89	01011001
A	65	01000001

From table 1, the Binary representation of My Text is merged into 01010011010000010101100101000001

2. Defining Insertion Parameters

Once the message is converted into binary format, the next step in the algorithmEcho Hiding is to determine the embedding parameters to be used in the embedding process. These parameters play an important role in maintaining a balance between embedding capacity, security, and the quality of the resulting audio signal. In this study, the two main parameters used aredelayAndamplification**.**Delayrefers to the distance between samples in the audio signal where the message bits will be inserted, whereasamplificationdetermines how much the signal amplitude changes due to data insertion. The selection of this parameter is based on psychoacoustic considerations, where the signal modifications made must be small enough to be undetectable by the listener but still allow for message extraction with high accuracy. In this study, useddelay of 2 samples Andamplification of 0.5, which aims to maintain a balance between resistance to detection and optimal audio quality.

3. Insert a message

After defining the insertion parameters, the next step is to insert a binary message into the audio signal usingEcho Hiding Algorithm. At this stage, each bit of the binary message is inserted into an audio signal by utilizing the effectechogenerated based on previously determined delay and amplification parameters with valuesThe original audio amplitude is [1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000] then the process is carried out for the first insertion, which is 0.

a. Echo position for bit 0 (position 1 x delay = 2) with Audio modification is 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, while Audio modification in position 2: 1000 – (0.5 * 32767) = 1000 – 16383.5 (negative values will be limited)
b. Echo position for bit 1 (position 2 x delay 4) with Modified Audio at position 4: 1000 + 16383.5 = 17383.5, limited to 32767 to avoid clipping. With a result of 32767, the process is carried out in the same way until all bits are processed, creating modified audio according to the binary bits of the message.

4. Running the Insertion Process

With the specified modification steps, after inserting all 32 bits of the message “I”, a modified audio signal with an encoded message will be obtained. The result of this process is an audio file that can be played, but at that time there was a hidden message in it.

5. Extracting Messages

When the extract message function is applied to the modified audio, the program will re-read the same bit positions used for insertion. With the same delay (e.g. every 2 samples), the program checks the amplitude value and determines the corresponding bit. If the amplitude is greater than a certain limit (e.g. threshold value), it is considered as a '1' bit and If the amplitude is less than that limit, it is considered as a '0' bit. In this way, it will take back the encoded binary and convert it back to text characters, getting the original message “I”.

Frequency Analysis

After the message insertion process usingEcho Hiding Algorithm, the next step isfrequency analysisto evaluate the changes that occur in the audio signal spectrum due to data insertion. This analysis aims to ensure that the modifications made do not cause significant distortion that can be detected by the technique.steganalysisor significantly reduce the audio quality. Analysis of the Original Audio Waveform in Figure 1.

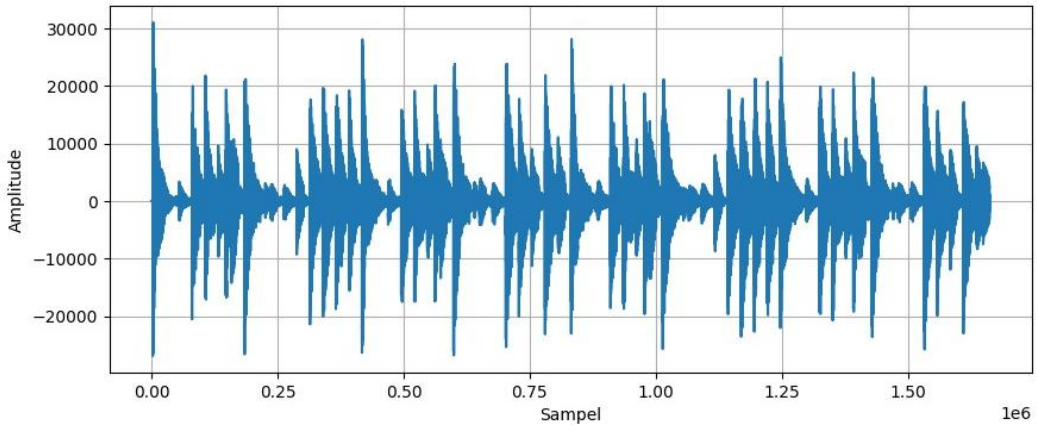


Figure 1. Original Audio Waveform

Figure 1. shows an audio waveform graph titled “Original Audio Waveform,” which represents the amplitude of the audio signal versus the number of samples in the recording. The horizontal (X) axis is labeled “Samples,” indicating the number of samples in the audio signal, which is about 1.6 million, while the vertical (Y) axis shows “Amplitude,” ranging from about -30,000 to 30,000. The waveform pattern in this graph shows typical amplitude fluctuations, with repeated peaks and valleys, reflecting variations in the intensity of the sound in the recording. The amplitude appears stronger in some parts and weaker in others, possibly indicating changes in volume or dynamics in the audio signal. This visualization provides an idea of how a digital audio signal is represented in a time waveform. Figure 2. Is a visualization after embedding.

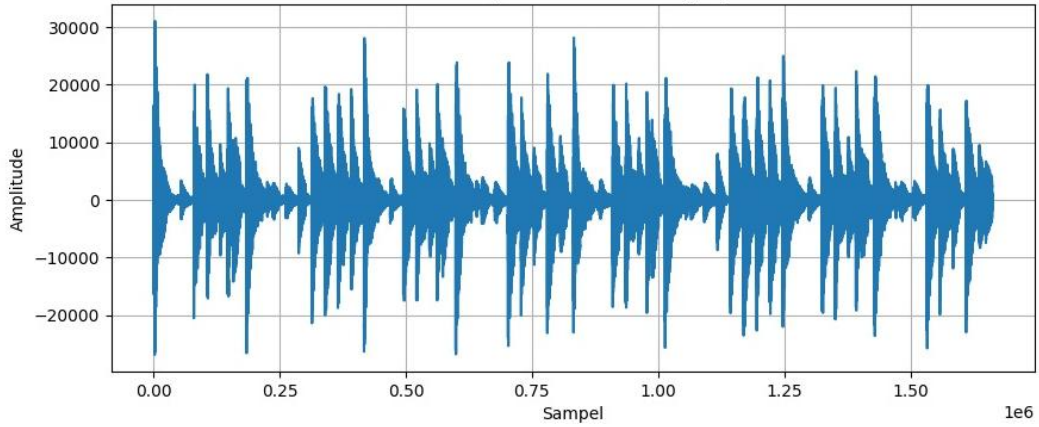
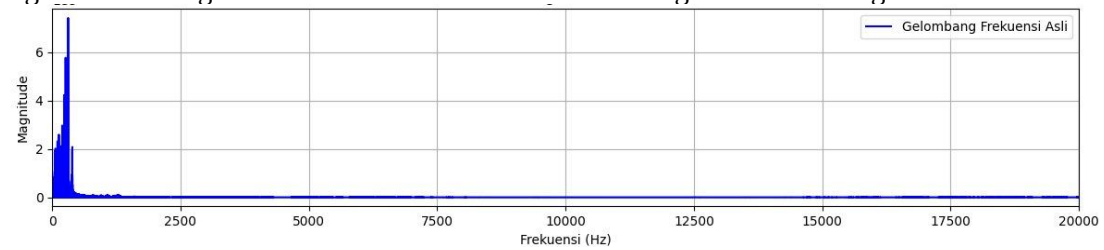
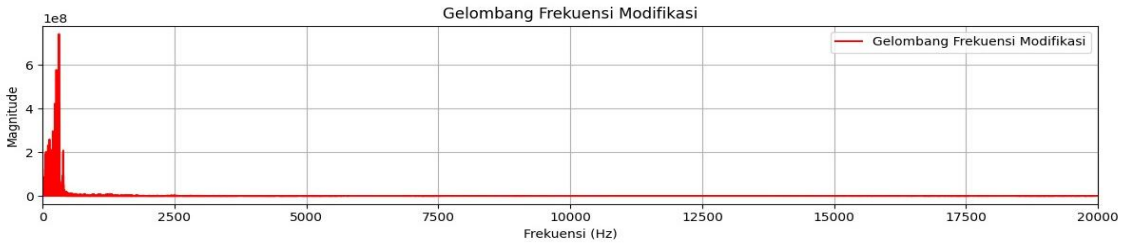


Figure 2. Audio Waveform After Insertion

This figure shows an audio waveform graph titled "Audio Waveform After Insertion", which represents the amplitude of the audio signal against the number of samples after undergoing a modification or data insertion process. The horizontal (X) axis shows the number of samples in the audio signal, with a range of about 1.6 million samples, while the vertical (Y) axis shows the amplitude with a range of about -30,000 to 30,000. Visually, this waveform looks similar to the original audio waveform, showing a pattern of amplitude fluctuations that are maintained with similar peaks and valleys. This indicates that the insertion process that was carried out did not change the waveform significantly, or the changes that occurred were subtle and not immediately visible from this graph. Thus, the resulting audio waveform still maintains its original characteristics even though it has undergone modifications before and after being described in Figure 3 below:



(a) Original Frequency Wave



(b) Modified Frequency Wave

Figure 3. Frequency Waves (a) Original and (b) Modified

Figure 3 shows two frequency spectrum graphs of an audio signal before and after modification. The first graph, titled “Original Frequency Waveform,” shows the frequency spectrum of the original audio signal, depicted in blue. In this graph, it can be seen that most of the signal energy is concentrated at low frequencies, with high magnitudes at the beginning of the spectrum and gradually decreasing to near zero at higher frequencies. This graph shows that the original audio signal has frequency components dominated by low frequencies, which is common in sound recordings. Meanwhile, the second graph, titled “Modified Frequency Waveform,” shows the frequency spectrum after modification in red. In general, the shape of this spectrum is still similar to the original spectrum, with energy dominated at low frequencies and magnitudes gradually decreasing at high frequencies. However, upon closer inspection, there may be slight changes in the magnitude distribution or the presence of additional frequency components that were not present in the original signal, indicating that the modification process has caused slight changes in the frequency domain. The similarity in the shape of the spectrum between the two graphs suggests that the modification has not drastically changed the main characteristics of the audio signal in the frequency domain, although there is the potential for information insertion or subtle changes in the amplitude of certain frequencies.

4. CONCLUSION

This study examines the application of the Echo Hiding algorithm in audio steganography to embed data securely without reducing the quality of the original signal. The experimental results show that this method has high effectiveness in maintaining a balance between embedding capacity, resistance to detection, and audio quality. By utilizing parameters such as delay and amplification, Echo Hiding is able to hide information with minimal distortion that is undetectable by the listener. Evaluation through objective and subjective testing proves that changes due to data embedding are not significant to the listener's perception, thus increasing the security and transparency aspects.

Thus, this study contributes to the development of more optimal audio steganography methods in confidential communication and sensitive data protection.

REFERENCE

Al Ihsan, R., & Sekti, B. A. (2024). Pentingnya Keamanan Data Dalam Era Digital: Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia. *Prosiding SISFOTEK*, *8*(1), 7–11.

Albantany, A. Q. (2021). *Text Steganography Pada Media Audio Format M4A Dengan Menggunakan Metode Least Significant Bit*. Universitas Islam Negeri Sumatera Utara.

Andika, D., & Darwis, D. (2020). Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi. *Jurnal Ilmiah Infrastruktur Teknologi Informasi*, *1*(2), 19–23.

Baso, F., Rais, N. A., Hatima, H., & Nur, P. A. A. (2024). Steganografi Berbasis Kecerdasan Buatan untuk Mengatasi Ancaman Terbaru dalam Keamanan Data. *Jurnal MediaTIK*, 145–149.

Octaviany, A. S., Suprayogi, S., & Fitriani, N. (2021). Optimasi Geometri Bahan Peredam Untuk Ruang Anti Gema Suara. *EProceedings of Engineering*, *8*(5).

Permana, D. A., Fauzi, R., & Mulyana, R. (2021). Perancangan Tata Kelola Teknologi Informasi untuk Transformasi Digital di Industri Perbankan Menggunakan Framework COBIT 2019 Domain Align, Plan, and Organise: Studi Kasus di Bank XYZ. *EProceedings of Engineering*, *8*(5).

Purba, Y. S., Budiman, G., & Ramatryana, I. N. A. (2016). Audio Watermarking Dengan Metode Discrete Wavelet Transform Dan Echo Hiding Pada Ambient Mode. *EProceedings of Engineering*, *3*(3).

Rumahorbo, B., & Perangin-angin, R. (2021). OPTIMASI KETAHANAN WATERMARKING AUDIO DIGITAL MENGGUNAKAN ALGORITMA RSA DAN MSB. *METHODIKA: Jurnal Teknik Informatika Dan Sistem Informasi*, *7*(1), 45–49.

Widianto, S. R. (2017). Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK. *Jurnal Multinetics*, *3*(2), 32–37.

Wulansari, T., Putra, A., Rusliah, N., & Habibi, M. (2019). Pengaruh model pembelajaran berbasis masalah pada materi statistika terhadap kemampuan penalaran statistik siswa. *AKSIOMA: Jurnal Matematika Dan Pendidikan Matematika*, *10*(1), 35–47.

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101.

Zen Munawar, S. T., Kom, S., Kom, M., Putri, N. I., Kharisma, I. L., Kom, M., Insany, G. P., ST, S., Kom, M., & Nurhadi, S. (2023). *Keamanan Sistem Informasi: Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep*. Kaizen Media Publishing.