BIOS: Jurnal Informatika dan Sains
Volume 3 Number 01, 2025, DOI 10.54209/bios.v3i01
E.SSN 2988-6910(Online)
https://seaninstitute.or.id/bersinar/index.php/bios/index

Implementation of an Audio Steganography Method for Embedding Secret Messages in Audio Media

Setia Mangiring Marpaung[1], Rani Rosalinda[2], Jusnan Pangabean[3]
Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas

Article Info
Corresponding Author:
Setia Mangiring Marpaung

ABSTRACT
The rapid development of information technology demands the existence of data security systems capable of protecting confidential information from unauthorized parties. One technique that can be used to maintain information confidentiality is steganography. Steganography is a technique of hiding secret messages within a cover medium so that the existence of the message cannot be directly detected. This study aims to implement an audio steganography method for embedding secret messages into digital audio media. The method used is the Least Significant Bit (LSB), in which the secret message is embedded in the lowest bits of the audio data without significantly altering the audio quality. The research process includes the stages of audio data preparation, secret message embedding, and message extraction. The test results show that the secret message can be successfully embedded and extracted without causing significant changes in audio quality. Therefore, the LSB-based audio steganography method can be used as an effective alternative for data security.
Keywords: Steganography, Audio, Least Significant Bit, Data Security.

INTRODUCTION

Information security is one of the most important aspects in today's digital era. Confidential information such as personal data, important documents, and secret messages requires protection to prevent unauthorized access. One common issue that frequently occurs is data interception or theft during the transmission of information through digital media.

In addition to cryptography, steganography is also a widely used method for maintaining information confidentiality. Unlike cryptography, which obscures the content of a message, steganography hides the message within another medium such as images, text, or audio, making the existence of the message undetectable.

Audio media has an advantage because small changes in audio signals are difficult for the human ear to detect. Therefore, audio steganography is an appropriate choice for embedding secret messages covertly. Based on this, this study focuses on the implementation of an audio steganography method for embedding secret messages in audio media.

The increasing complexity of digital communication technologies has also heightened risks to data security, particularly in the exchange of information over open networks. Threats such as interception, data manipulation, and unauthorized access pose serious

challenges that must be addressed. Therefore, a security method is required that not only protects the content of the message but also conceals its existence to avoid suspicion.

Steganography emerges as an effective alternative solution because it can hide messages within other media without significantly altering the appearance or main characteristics of the medium. Unlike cryptographic methods that focus on scrambling message content, steganography emphasizes hiding the message so that it remains undetected. This makes steganography highly relevant in modern information security systems.

The use of audio media as a steganographic medium offers its own advantages due to the limited sensitivity of human hearing to slight changes in sound signals. By leveraging this characteristic, secret messages can be embedded into audio files without creating significant differences between the original audio and the modified audio. This technique becomes even more effective when combined with appropriate embedding methods, such as the Least Significant Bit (LSB).

Furthermore, to enhance security, the steganography process can be combined with encryption techniques such as the Advanced Encryption Standard (AES). With encryption applied before embedding, the hidden message is not only difficult to detect but also remains secure even if it is extracted by unauthorized parties. This combination provides an additional layer of security that is essential for protecting confidential digital information.

THEORETICAL BACKGROUND

Steganography

Steganography originates from the Greek words *steganos*, meaning hidden or concealed, and *graphein*, meaning writing. Steganography is the science and art of hiding secret messages within other media in such a way that the existence of the message cannot be detected by others. The main objective of steganography is to conceal the existence of the secret communication itself, not just the content of the message. Media that can be used for steganography are very diverse, including text, images, audio, video, and network protocols. In this study, the medium used is an audio file in WAV (Waveform Audio File Format).

Least Significant Bit (LSB) Method

The Least Significant Bit (LSB) is the simplest and most widely used steganography method. This method works by replacing the last bit (the least significant bit) of each byte of media data with bits from the message to be hidden.

In audio files, each audio sample is typically represented using 16-bit or 24-bit data. By replacing the LSB of each sample, the change in audio amplitude is very small and almost inaudible to the human ear. This makes the LSB method highly suitable for audio steganography because it does not significantly affect audio quality.

Example of bit embedding using the LSB method:

1. Original audio sample: 10110110 (182 in decimal)
2. Message bit to be embedded: 1
3. Modified audio sample: 10110111 (183 in decimal)

The change from 182 to 183 is very small and does not significantly affect the resulting audio quality.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm adopted by the National Institute of Standards and Technology (NIST) in 2001 as the standard for securing sensitive information. AES replaced the Data Encryption Standard (DES), which is no longer considered secure.

AES uses encryption keys with lengths of 128, 192, or 256 bits. The longer the key, the higher the level of security. However, AES-128 is already considered highly secure for most applications. AES uses a substitution-permutation network structure and operates on 128-bit data blocks. The AES encryption process consists of several rounds involving four main transformations:

1. SubBytes: Non-linear byte substitution using an S-box.
2. ShiftRows: Cyclic shifting of rows.
3. MixColumns: Column mixing using mathematical operations.
4. AddRoundKey: Addition of the round key (XOR with the key).

The number of rounds depends on the key length: 10 rounds for AES-128, 12 rounds for AES-192, and 14 rounds for AES-256.

Combination of AES and LSB

The combination of AES encryption and LSB steganography produces a multi-layer security system. First, the plaintext message is encrypted using AES to produce ciphertext. Then, the ciphertext is embedded into an audio file using the LSB method. The advantages of this approach are:

1. The existence of the message is hidden within the audio (steganography).
2. The message content remains secure even if it is successfully extracted (AES encryption).
3. Minimal changes to audio quality (LSB method).

Procedure

This study is divided into two main processes: encoding (message embedding) and decoding (message extraction).

Encoding Process (Message Embedding)

1. Preparation: Prepare the text message to be hidden and a WAV audio file as the medium.
2. AES Encryption: Encrypt the message using AES-128 with a predefined key. The result is ciphertext in byte form.
3. Bit Conversion: Convert the ciphertext into binary representation (bits).
4. Read Audio File: Read the WAV audio file and extract the audio samples into an array.
5. LSB Embedding: Replace the LSB of each audio sample sequentially with bits from the ciphertext.
6. Save File: Save the modified audio samples as a new audio file.

Decoding Process (Message Extraction)

1. Read Audio File: Read the audio file containing the embedded message.
2. LSB Extraction: Extract the LSB from each audio sample to obtain ciphertext bits.
3. Byte Conversion: Convert the extracted bits into bytes to reconstruct the ciphertext.

4. AES Decryption: Decrypt the ciphertext using the same AES key to retrieve the original message.

RESULTS AND DISCUSSION

Initial Display

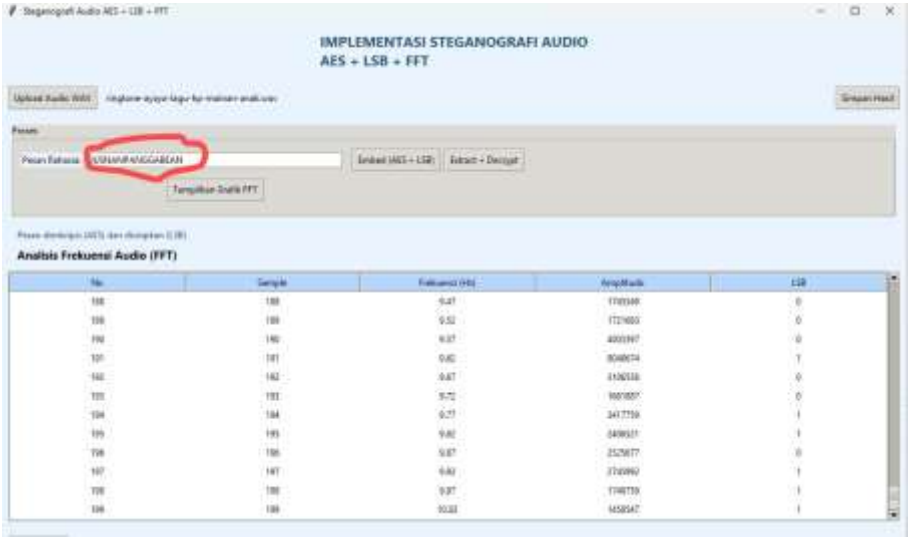

Figure 1. Secret Message Embedding Process

The figure shows the process of embedding a secret message in an audio steganography application. A WAV audio file is successfully uploaded and used as the carrier medium for the message. The secret message “JUSNANPANGGABEAN” is entered in its original text form (plaintext).

Through the Embed (AES + LSB) button, the message is encrypted using the AES algorithm, and then the encrypted result is embedded into the audio using the Least Significant Bit (LSB) method. The success of the process is indicated by a notification stating that the message has been successfully encrypted and embedded.

The Show FFT Graph button and the Audio Frequency Analysis Table (FFT) are used to analyze the frequency characteristics of the audio after message embedding. The LSB column shows the last bit of the audio samples, which is utilized as the storage medium for the message. Overall, the figure demonstrates that the encryption and message embedding processes run successfully, and the audio is ready for the extraction stage.

Second Display

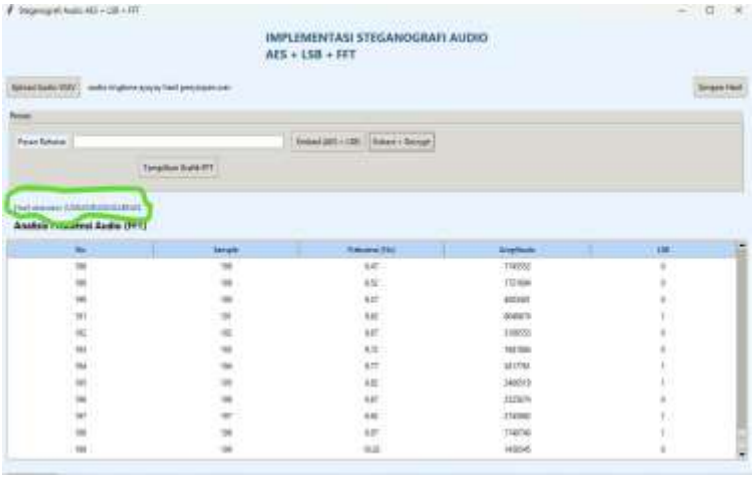

Figure 2. Embedding and Extracting Secret Messages

The figure shows the application for the implementation of Audio Steganography using AES + LSB + FFT, which is used to embed and extract secret messages in WAV audio files. The audio file is successfully uploaded through the Upload Audio WAV button, indicating that the file is ready to be processed.

In the Process section, the system provides the Embed (AES + LSB) feature to encrypt the message using AES and embed it into the audio using the LSB method, as well as the Extract + Decrypt feature to retrieve and decrypt the message from the audio. The displayed extraction results indicate that the secret message has been successfully recovered correctly.

The Show FFT Graph button and the Audio Frequency Analysis Table (FFT) are used to analyze the frequency characteristics of the audio. The LSB column shows the last bit of the audio samples, which is utilized as the storage medium for the message. Overall, this interface demonstrates that the audio steganography system operates according to the design and functions properly.

Third Display

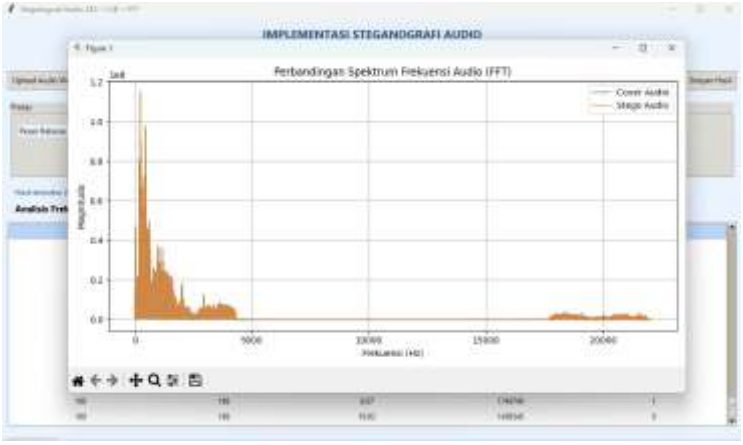

Figure 3. Comparison of Frequency Characteristics

The Frequency Spectrum Comparison Graph (FFT) is used to compare the frequency characteristics between the cover audio (original audio) and the stego audio (audio after message embedding). The X-axis represents frequency (Hz), while the Y-axis represents the magnitude or amplitude of the audio signal.

The graph results show that the frequency spectra of the cover audio and stego audio almost overlap, both in the low, mid, and high-frequency ranges. No new frequency spikes or significant changes are observed after the message embedding process.

This indicates that the LSB method is able to embed messages without significantly affecting audio quality, while AES only serves to secure the message and does not affect the audio signal. Thus, the stego audio has frequency characteristics that are nearly identical to the cover audio.

Fourth Display

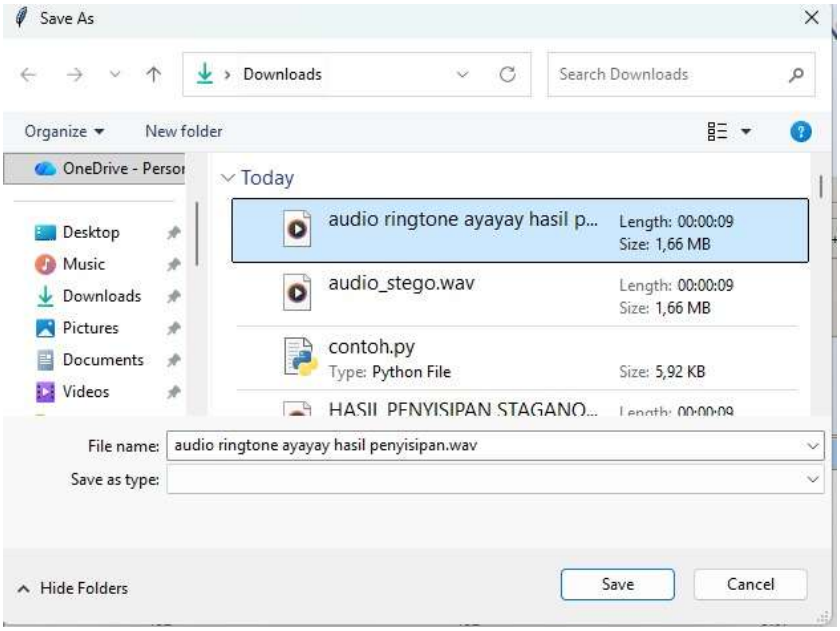

Figure 4. Stego Audio Saving Process

The figure shows the process of saving the stego audio, which is the audio file resulting from the secret message embedding process. The file is saved through a Save As window with the name “audio ringtone ayayay hasil penyisipan.wav” in the Downloads folder.

The audio has been encrypted using AES and embedded with a secret message using the LSB method, without any significant changes in file size or duration. This indicates that the message embedding process was successful and the audio is ready to be used or distributed.

Discussion

The implementation results show that the message embedding process using the LSB method works very well, where the message can be inserted into the audio file without causing significant changes in audio quality. This proves that the LSB method has a high level of transparency, as it does not produce differences that can be directly detected by human hearing.

In addition, the use of the AES algorithm prior to the embedding process provides an important additional layer of security. The encrypted message becomes meaningless before the decryption process is performed, so even if an unauthorized party successfully extracts the data from the audio, the message content cannot be understood without the appropriate key. This demonstrates the effectiveness of a multi-layer security approach in the developed system.

Analysis using the Fast Fourier Transform (FFT) also strengthens the research findings, where the frequency spectrum between the original audio and the stego audio shows very small differences. The resulting graphs indicate that both spectra are almost identical, leading to the conclusion that the embedding process does not significantly damage the audio signal structure. This serves as an important indicator that the media quality is well preserved.

Overall, the developed system not only successfully embeds and extracts messages accurately, but also maintains audio quality and ensures information security. This shows

that the combination of LSB and AES methods is an effective and efficient solution for audio steganography implementation and has strong potential for application in various digital data security needs.

CONCLUSION

Based on the implementation and testing results, it can be concluded that the audio steganography method using a combination of the Advanced Encryption Standard (AES) and Least Significant Bit (LSB) has been successfully implemented to embed secret messages into WAV audio media. The AES encryption process is able to maintain the confidentiality of the message content, while the LSB method enables the embedding of messages into the least significant bits of audio samples without causing significant changes in sound quality. The extraction results show that the secret message can be fully recovered and matches the original message, indicating that the system works as designed. Frequency spectrum analysis using the Fast Fourier Transform (FFT) shows that the difference between the cover audio and stego audio is very small and almost negligible. This proves that message embedding using the LSB method does not significantly affect the audio frequency characteristics, making it difficult to detect by human hearing. Therefore, the combination of AES and LSB in audio steganography can be considered an effective, secure, and efficient data protection solution for hiding secret messages in digital audio media.

REFERENCES

Darwis, D. (2015). Implementasi Steganografi pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding. *Expert*, *5*(1), 346079.

Kusuma, P., & Prayudi, Y. (2025). Implementasi Steganografi Dengan Menggunakan Metode Masking And Filtering Untuk Menyisipkan Pesan Ke Dalam Spectrogram Audio: Indonesia. *AJIE (Asian Journal of Innovation and Entrepreneurship)*, 1-15.

Sianturi, T. N., & Hutagaol, R. G. (2019). Penyisipan Pesan Rahasia Kedalam Audio Menggunakan Algoritma F5. In *Prosiding Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*.

Baskara, T. (2007). Studi dan Implementasi Steganografi pada MP3 dengan Teknik Spread Spectrum. *Diakses dari http://rasta-shared. blogspot. com/p/dan-lain2. html*.

Ashari, I. F., & SUGIHARTO, A. (2015). *Aplikasi steganografi pesan teks pada media audio mp3 menggunakan metode penyisipan least significant bit dan advanced encryption standard skripsi* (Doctoral dissertation, Universitas Diponegoro).

Chalid, I. R. (2012). Aplikasi Audio Steganografi untuk Melindungi Data Menggunakan Bahasa Pemrograman Java.

Akbar, Z., Nafis, M., El Hakim, D., & Faqih, M. I. (2026). Implementasi Algoritma Least Significant Bit (LSB) untuk Penyembunyian Pesan Teks pada Media Citra Digital dan Audio Berbasis Python. *JIKUM: Jurnal Ilmu Komputer*, *2*(2), 294-300.

Akmal, R. A., & Furqan, M. (2023). Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital. *G-Tech: Jurnal Teknologi Terapan*, *7*(2), 543-553.

Hendrata, A. D., & Prihanto, A. (2021). Analisis Kualitas Suara Stego Audio Penyisipan Informasi Tersembunyi dengan Metode Least Significant Bit. *Journal of Informatics and Computer Science (JINACS)*, *2*(03), 178-184.

SIBURIAN, R. (2017). *IMPLEMENTASI STEGANOGRAFI AUDIO MP3 DAN WAV PADA SMARTPHONE ANDROID DENGAN MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT)* (Doctoral dissertation, POLITEKNIK NEGERI SRIWIJAYA).

Madawara, V. N. (2014). *Perancangan dan Implementasi Teknik Steganografi Menggunakan Metode Enhanced Audio Steganography (EAS) dengan Algoritma Columnar Transposition* (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW).

Dharmawan, D. (2024). Penerapan Three Sided Side Match Method Untuk Penyisipan Pesan Pada Audio. *Journal of Computing and Informatics Research*, *4*(1), 261-270.