AUDIO STEGANOGRAPHY USING LEAST SIGNIFICANT BIT METHOD FOR CONFIDENTIAL DATA EMBEDDING

Muhd Izzul Haziq Rahim, Nazirah Abd Hamid[1], Siti Dhalila Mohd Satar, Mohd Fadzil Abdul Kadir, Ahmad Faisal Amri Abidin @ Bharun, Mohamad Afendee Mohamed and Mumtazimah Mohamad

Faculty of Informatic and Computing, Tembila Campus, Besut, Terengganu

ABSTRACT

As the demand for secure communication increases, traditional encryption techniques, though effective, often expose the presence of sensitive information, making them vulnerable to detection. Audio steganography offers a more discreet alternative by embedding hidden data within audio signals, preserving the secrecy of the communication. Among existing methods, the Least Significant Bit (LSB) technique is widely used due to its simplicity and high imperceptibility. However, conventional LSB methods face limitations in embedding capacity, robustness, and decoding reliability, particularly when handling large datasets. This study proposes a modified LSB approach that addresses these issues by introducing a compact binary encoding scheme and a fixed End-of-File (EOF) marker to improve efficiency and accuracy. The method involves embedding custom binary representations of secret data into 8-bit audio samples, with extraction aided by the EOF marker. Results demonstrate that the waveform and spectrogram comparisons confirmed the imperceptibility of the modifications, with a 100% similarity score between original and stego-audio. While the technique is lightweight and effective, it is still susceptible to audio compression and signal manipulation. Future enhancements may include adaptive EOF patterns and integrated encryption to increase resistance to tampering. Overall, this research contributes a practical and efficient advancement to audio steganography, offering improved security for embedded data in digital audio communication.

KEYWORDS

Audio Steganography, Least Significant Bit (LSB), Data Embedding, wave and spectrogram

1. INTRODUCTION

The word 'steganography' is derived from the Greek words for 'covered' or 'concealed' ('steganos') and 'to write' ('graphein'), which reflects its core purpose: to communicate in secret without anyone noticing [1]. Steganography provides an additional layer of security by embedding information into another medium, such audio, enabling secret communication [2][3]. without drawing attention to yourself in the face of growing threats to data privacy and security Audio steganography is particularly effective because the human ear is relatively insensitive to slight changes in audio, especially in certain frequencies or phase components. Information can be embedded in an audio signal without significantly changing the audio quality by changing small aspects of the signal, such as the phase of sound waves or the least significant bits (LSB) of each audio sample [4].

Despite the effectiveness of the LSB technique, it suffers from low robustness and limited capacity when embedding large datasets. Existing research does not adequately address these

limitations or provide enhanced LSB variants that improve performance while maintaining audio quality. This paper aims to bridge this gap by introducing a modified LSB approach with enhancements in binary encoding and message delimitation. This paper is structured as follows: Section 2 reviews related works in audio steganography. Section 3 introduces the Least Significant Bit (LSB) method. Section 4 presents the proposed methodology. Section 5 discusses enhancements to the standard LSB technique using custom binary encoding and an End-of-File (EOF) marker. Section 6 evaluates the results through waveform and spectrogram analysis and finally, Section 7 concludes the study and outlines potential directions for future research.

2. RELATED WORKS

Audio steganography has been the focus of extensive research, with numerous techniques developed to conceal data within audio signals. This section reviews key methods—particularly the Least Significant Bit (LSB) approach—and compares their strengths, limitations, and applicability to secure data embedding.

2.1. Audio Steganography Techniques

Researchers have explored various audio steganography methods that hide secret messages within audio files, carefully using the limitations of human hearing to keep these messages undetectable. Various algorithms and approaches have been proposed to achieve this. One common method is Least Significant Bit (LSB), where data is hidden in the least significant bits of audio samples, making the modifications nearly imperceptible [5][6]. Another technique, Phase Coding, embeds information by modifying the phase of the audio signal, ensuring minimal distortion. Spread Spectrum is another approach that distributes the secret message across the entire audio spectrum, making detection and removal more challenging. Additionally, Echo Hiding involves embedding data by introducing inaudible echoes into the original audio signal, further enhancing the stealth of the hidden message [7][8]. These techniques, among others, play a crucial role in secure data communication through audio steganography.

2.2. Least Significant Bit

The Least Significant Bit (LSB) technique is widely used for hiding information in digital media, such as audio, video, and images, without significantly altering the content [9][10]. This approach embeds secret data into the least significant bits of the cover medium, which typically contribute the least to the overall visual or auditory quality of the content. Over time, this technique has been extensively investigated, and a substantial body of research has been dedicated to understanding its characteristics, limitations, and potential applications [9][10].

Digital audio files are represented as a sequence of samples, each with a specific value. For example:

- In an 8-bit audio file, each sample is represented by 8 bits (e.g., 10110110).
- In a 16-bit audio file, each sample is represented by 16 bits (e.g., 1011011010110110).

The least significant bit is the rightmost bit in this binary representation. Modifying this bit changes the sample value slightly, but this change is usually inaudible to humans. In an 8-bit sample (e.g., 10110110), the last bit can be altered without perceptible change. For example, modifying samples to encode binary "1010" results in minor, inaudible changes. Although effective for small data payloads, traditional LSB methods struggle with capacity and detection resistance.

Example input:

Audio samples (8-bit):
11001100, 10010101, 11100001, 10101010
Secret message in binary:
1010
Embedding:
Replace LSB of each sample with each message bit:
11001100 → 11001101 (message bit: 1)
10010101 → 10010100 (message bit: 0)
11100001 → 11100001 (message bit: 1)
10101010 → 10101010 (message bit: 0)

Output:

Modified audio samples:
11001101, 10010100, 11100001, 10101010

2.3. Audio Steganography

Several audio steganography methods have been explored, including Phase Coding, Echo Hiding, and Spread Spectrum. Table 1 summarizes key recent works:

Table 1. Comparative analysis of audio steganography methods.

Author(s) & Year	Method	Advantages	Limitations
Abood et al. (2022) [11]	Enhanced LSB + Bit Cycling	Increased robustness; includes encryption features	Higher complexity; reduced speed
Sayed & Wahbi (2024) [12]	Phase Coding	High imperceptibility and minimal audible changes	Lower capacity; more complex implementation
Aslantas & Hanilci (2022) [7]	Comparative Study of Multiple Methods	Broad evaluation of LSB, Echo, Spectrum techniques	Does not propose a new technique; only comparative

3. METHODOLOGY

In audio steganography, the methodology involves carefully embedding confidential data into an audio signal in a way that ensures the data is secure, robust, and remains undetectable to unintended listeners. Usually, the procedure is picking a suitable audio file (cover audio), choosing on an embedding method, encoding the secret data, and then retrieving it when required [11]. Evaluation metrics like wave and spectrogram are used to assess the effectiveness of the steganographic method. A well-defined methodology in audio steganography ensures that the embedded data remains undetectable to unintended listeners while being reliably extracted by authorized recipients. This study follows a structured process:

1. Select appropriate WAV audio files (16-bit PCM, 44.1kHz).
2. Convert the secret message into a custom binary format.
3. Embed binary into LSBs of each 8-bit sample.
4. Append an EOF marker (11111111) to signal message termination.
5. Evaluate the stego-audio using waveform and spectrogram analysis.

3.1. Framework

In this section, we introduce the framework used in the audio steganography process, focusing on how the confidential data is embedded into the audio signal. We break down the process into two main components: the sender's role in embedding the secret data into the audio file, and the receiver's role in extracting that data accurately.

3.1.1. Sender Part

Figure 1 demonstrates how sender part works. The user need to insert the secret message and sound carrier before both input goes to binary converter. After that, embedding process happen where every binary in secret message will be embedded into a Least Significant Bit of every 8-bit frame in sound carrier and produce Audio Steganography. This output will be sent through communication medium.

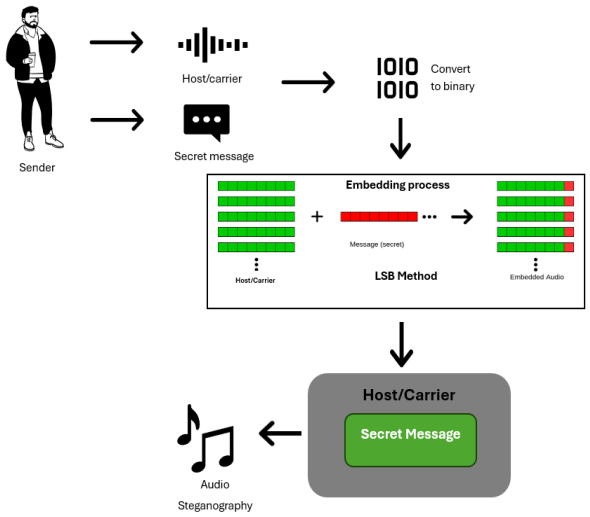

Figure 1. Framework of a sender

3.1.2. Receiver Part

Figure 2 demonstrates how receiver part works after the Audio steganography file arrived at intended receiver. Audio steganography file will be converted to binary before extraction happens. At extraction process, the system will take Least significant bits from sound carrier and combine it together after finish. This process will produce secret messages and the original sound carrier.

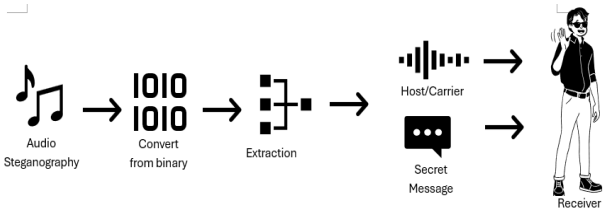

Figure 2. Framework of a receiver

4. MODIFIED LEAST SIGNIFICANT BITS TECHNIQUES

In this section, we explore enhanced techniques for embedding confidential data using the Least Significant Bit (LSB) method. While traditional LSB methods have proven effective, they have limitations in terms of capacity and robustness. To address these challenges, we propose modifications to the standard LSB technique. These modifications, including the use of custom binary encoding and End-of-File (EOF) markers, aim to improve both the efficiency and security of the data embedding process.

4.1. Custom Binary

The custom binary technique converts characters into compact binary sequences, with each type of character—such as digits and letters—being represented by unique markers. Each character is encoded with a prefix marker: digits (0), uppercase (10), lowercase (11). This reduces space and identifies character type. This technique only takes 'fix bit' instead of whole 8 bit and assign marker bit in front of character bit.

For example, Table 2, number (0-9) have a constant first four bit '0000' and the rest four bit is fix based on value. So, we take the fix bit and then we assign marker bit '0' at front of character binary to uniquely identify it was a number.

Marker Bit = '0'
Example : 9
Normal : 00001001
Propose technique : '0' + 1001 **= 01001**

Table 2. Number binary.

Number

Number	Binary							
0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	0	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	0	0	0	0	0	1	0	1
6	0	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	0	0	0	0	1	0	0	1

For alphabetical, there is only 5 bit which the value is fix while order 3 bit from most significant bit (MSB) is constant. For marker bit we assign '10' for uppercase and '11' for lowercase to uniquely identify them. We can see the example for uppercase letter in Table 3.
Marker Bit = '10'
Example : C
Normal : 01000011
Propose technique : '10' + 00011 = **1000011**

Table 3. Uppercase binary.

Uppercase

Letter	Binary							
A	0	1	0	0	0	0	0	1
B	0	1	0	0	0	0	1	0
C	0	1	0	0	0	0	1	1
D	0	1	0	0	0	1	0	0
E	0	1	0	0	0	1	0	1
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
W	0	1	0	1	0	1	1	1
X	0	1	0	1	0	0	0	0
Y	0	1	0	1	1	0	0	1
Z	0	1	0	1	1	0	1	0

4.2. End-of-File (EOF)

An EOF marker (11111111) signals the end of the embedded message, improving decoding accuracy. Its purpose is to avoid the decoder incorrectly interpreting random bits in the file as part of the message, it makes sure the decoder knows when the message finishes. The EOF marker is added to the end of the binary sequence once the secret message has been converted into its unique binary representation. The binary data is read during the decoding process until it reaches the EOF marker, at which point it ends.

5. Results and Discussion

The results of applying the proposed LSB technique were evaluated based on factors like sound quality, efficiency, stealthiness, and capacity, with a focus on how well the hidden data remained imperceptible. A comparison with the others LSB technique is also conducted to highlight improvements and potential limitations. The waveform comparison between the original and steganographic audio files as in Figure 3 shows that the LSB-based audio steganography technique successfully hides the secret data without causing noticeable distortions. The waveforms are almost identical, which means that the changes made to the audio were minimal and didn't affect the overall sound quality.

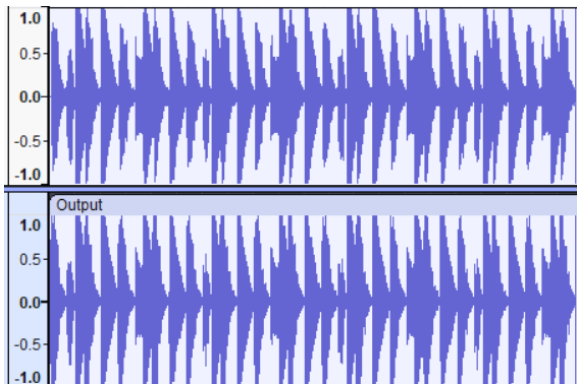

Figure 3. Wave comparison

Figure 4 shows the spectrogram for both original and steganography audio by showing that the frequency content of both the original and the steganographic audio is nearly identical. The spectrogram is a visual representation of how the frequency energy is distributed over time, and

the fact that there are no significant differences between the two spectrograms indicates that the LSB embedding did not introduce any distortion or noise into the frequency spectrum.

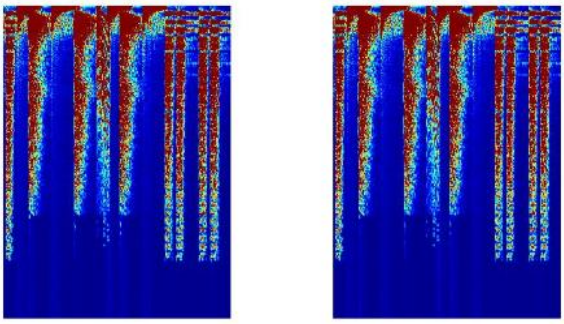

Figure 4. Spectrogram comparison

One of the key advantages of the proposed modified LSB technique lies in its straightforward design, which makes it well-suited for environments where system resources are limited. The use of least significant bit embedding, paired with a compact binary encoding strategy, ensures that the changes made to the audio file are subtle and generally imperceptible to the human ear. Furthermore, incorporating an End-of-File (EOF) marker helps streamline the retrieval process by clearly indicating where the hidden message ends, thereby reducing potential extraction errors. However, there are limitations that should be acknowledged. The method, like other time-domain approaches, is sensitive to standard audio processing operations such as compression or filtering. These operations may distort or erase the embedded data, compromising the integrity of the hidden message. In addition, the fixed nature of the EOF marker may become a weakness if an attacker is familiar with the pattern, as it could make the embedded data easier to detect or manipulate. These aspects point to possible future improvements, such as adopting a more dynamic EOF mechanism or integrating basic encryption to enhance security.

6. CONCLUSION

This study has explored the use of audio steganography through a modified Least Significant Bit (LSB) method to securely embed confidential data within audio signals. Traditional LSB techniques, while widely used for their simplicity and imperceptibility, are often limited by their embedding capacity and vulnerability to signal manipulation. To address these shortcomings, a custom binary encoding scheme and an End-of-File (EOF) marker were introduced in this work, aiming to improve both the efficiency and accuracy of the data embedding and extraction processes. The proposed technique demonstrated several advantages. First, it maintains the perceptual quality of the audio, as confirmed by waveform and spectrogram analyses that showed no significant distortion. Second, the incorporation of a fixed EOF marker helped enhance the reliability of data retrieval by clearly signalling the end of the embedded message, thereby reducing decoding errors.

However, certain limitations must be acknowledged. The technique remains susceptible to common audio processing operations such as compression, filtering, or resampling, which could compromise the integrity of the hidden data. Additionally, the fixed nature of the EOF marker, while effective in controlled scenarios, may be predictable in adversarial contexts. Future work may focus on enhancing robustness by integrating lightweight encryption or adaptive EOF schemes that vary dynamically to avoid pattern detection. Exploration of hybrid methods combining time- and frequency-domain embedding could further improve resistance to signal degradation. Overall, this research contributes a practical, efficient advancement to the field of

audio steganography and opens the door to more secure and scalable methods for covert communication.

REFERENCES

[1] J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, "Video steganography: recent advances and challenges," Apr. 04, 2023, Springer Science+Business Media. doi: 10.1007/s11042-023-14844-w.

[2] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, and M. Mamat, "A New Model for Hiding Text in an Image Using Logical Connective," Jun. 30, 2015, Global Vision Press. doi: 10.14257/ijmue.2015.10.6.20.

[3] A.H. Lone, A. W. Lone and M. Uddin, "A novel scheme for image authentication and secret data sharing," 2016. https://doi.org/10.5815/ijcnis.2016.09.02.

[4] T. N. Aruna, L. R. Nandika, C. I. Sneha, T. J. Xavier, and T. M. George, "Text, Image and Audio Steganography." Apr. 2023.

[5] R. Shanthakumari, E. M. R. Devi, R. Rajadevi, and B. Bharaneeshwar, "Information Hiding in Audio Steganography using LSB Matching Revisited," May 01, 2021, IOP Publishing. doi: 10.1088/1742-6596/1911/1/012027.

[6] M. B. Begum and Y. Venkataramani, "LSB Based Audio Steganography Based On Text Compression," Jan. 01, 2012, Elsevier BV. doi: 10.1016/j.proeng.2012.01.917.

[7] F. Aslantaş and C. Hanilçi, "Comparative Analysis Of Audio Steganography Methods," Jan. 22, 2022. doi: 10.38088/jise.932549.

[8] S. Dussan, A. S. Henao, M. M. Silva, and S. A. Donado, "Audio Steganography Algorithm Based On Phase Coding," Nov. 03, 2023, Research Square (United States). doi: 10.21203/rs.3.rs-3504599/v1.

[9] D. Verma and P. Singh, "Performance Analysis of Audio Steganography using Modified LSB Technique." Jan. 2017.

[10] K. P. Adhiya and S. A. Patil, "Hiding Text in Audio Using LSB Based Steganography," Jun. 08, 2012. Accessed: Oct. 2024. [Online]. Available: http://pakacademicsearch.com/pdf-files/eng/510/8-14%20Vol%202,%20No%203%20(2012).pdf.

[11] E. W. Abood et al., "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," Jan. 22, 2022, Institute of Advanced Engineering and Science (IAES). doi: 10.11591/eei.v11i1.3279.

[12] M. H. Sayed and T. M. Wahbi, "Information Security for Audio Steganography Using a Phase Coding Method," Jan. 01, 2024. doi: 10.59324/ejtas.2024.2(1).55.

AUTHORS

Nazirah Abd Hamid is a senior lecturer in University Sultan Zainal Abidin, Terengganu, Malaysia. She holds a degree in Bachelor of Information Technology from University Utara Malaysia (UUM), in 2004, M. Sc. Com. (Information Security) from University Teknologi Malaysia (UTM), in 2011 and PhD in Computer Science from Universiti Teknikal Malaysia Melaka (UTeM), in 2023. Her research interests are Information Security, Cyber Security, Pattern Recognition and Data Mining.

Siti Dhalila Mohd Satar received her Ph.D. from Universiti Putra Malaysia in 2024 and her M.Sc. from Universiti Teknologi Malaysia in 2012. She is a Lecturer at Universiti Sultan Zainal Abidin, specializing in access control security systems, security services—including digital forensics, steganography, network security, and biometrics—and data security. Her research contributions focus on advancing security mechanisms to protect digital ecosystems.

Mohd Fadzil Abdul Kadir received a Ph.D. in engineering (system engineering) from the Mie University, Mie, Japan, in 2012. Since 2006, he has been with the Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, where he is currently a Senior Lecturer. His main areas of research interest are digital image processing, pattern recognition, information security, and cryptography. He is also a member of the Malaysia Board of Technologists. He can be contacted at email: fadzil@unisza.edu.my.

Ahmad Faisal Amri Abidin @ Bharun received his M. Sc. Com from Universiti Putra Malaysia in 2008. He is a senior lecturer specializing in Security Services (Digital Forensic, Steganography, Network Security, Public Key Infrastructure and Biometrics). He has almost 15 years of experience in cybersecurity. In addition, he has led various cybersecurity workshops.

Mohamad Afendee Mohamed received his Ph.D. in Mathematical Cryptography from Universiti Putra Malaysia in 2011. Upon completion, he served the university for three years as a senior lecturer. In 2014, he moved to Universiti Sultan Zainal Abidin and later assumed an associate professor position. His current research interests include both theoretical and application issues in the domain of data security and mobile and wireless networking. He has authored more than 100 articles that have appeared in various journals, book chapters, and conference proceedings. He can be contacted at email:

Mumtazimah Mohamad was born in Terengganu, Malaysia. She received a bachelor's degree in information technology from Universiti Kebangsaan Malaysia, in 2000, an M.Sc. degree in computer science from Universiti Putra Malaysia, and a Ph.D. degree in computer science from Universiti Malaysia Terengganu in 2014. She was a Junior Lecturer in 2000. Currently, she is an Associate Professor with the Department of Computer Science, Faculty of Informatics and Computing (FIK), Universiti Sultan Zainal Abidin, Terengganu, Malaysia. She has published over 50 research articles in peer-reviewed journals, book chapters, and proceedings. She has been appointed as a reviewer and technical committee for numerous conferences and journals and has worked as a researcher in several nationally funded Research and Development projects. Her research interests include pattern recognition, machine learning, artificial intelligence, and parallel processing.

Muhammad Izzul Haziq Bin Rahim is Final Year Student in University Sultan Zainal Abidin, Terengganu, Malaysia. He currently pursue his study in B.Sc Computer Network Security focusing on Network Architecture, Cyber Defence, Cyber Attack and Digital Forensic. He also have experience with IoT device while participate in many trainee workshops and involvement in R&D related to IoT projects.