Comparison of the Use of M-Bit Least Significant Bit Steganography Methods on WAV Files in Information Storage

Imelda Imelda*[1] and Mardi Hardjianto[2]

[1,2] Universitas Budi Luhur, Fakultas Teknologi Informasi, Jl. Ciledug Raya, 12260, Indonesia

imelda@budiluhur.ac.id*; mardi.hardjianto@budiluhur.ac.id

Abstract. Audio-based digital steganography involves embedding secret messages within audio content without causing noticeable changes to the original sound. This technique is important to ensure the security of digital audio data distribution in the era of massive information dissemination. The limitations of message storage capacity and audio quality are complicated issues because they can raise suspicions due to changes in sound quality. The urgency of this research is driven by the increasing need for information hiding security in digital communications. Among various steganographic techniques, the Least Significant Bit (LSB) method is a popular technique widely utilized in steganography for data hiding. The m-bit LSB is a variant of the LSB whose m value determines the number of bits used to store information in one byte. This research solution evaluates the audio quality performance by comparing the use of the number of bits in m-bit LSB in WAV files. This method is tested by comparing the payload capacity and audio quality using SNR. The main contribution of this work is an in-depth evaluation of the balance between data capacity and audio quality in m-bit LSB steganography. Experimental results reveal that the 4-bit LSB configuration yields the best compromise, supported by an SNR measurement of 41.61 dB.

Keywords: Steganography, Least Significant Bit, m-bit, WAV file.

1 Introduction

The current era is marked by significant and accelerating developments in science and technology. This progress is evident in the development of information technology, particularly the Internet. The advancement of the Internet has now become a daily necessity for society. The impact of internet advancements is that anyone can access and obtain information easily and quickly, and it can be used to send information to anyone (Mondejar et al., 2021). The flow of information delivery has increased rapidly in recent years.

As information technology advances, criminal techniques also evolve. Sending information from one location to another presents challenges in terms of data security.

N. A. Ishak et al. (eds.), *Proceedings of the International Conference on Cross- Disciplinary Academic Research 2025 - Track 1 Advances in Computing, Electronics, Engineering, and Mathematics (ICAR-T1 2025)*, Advances in Engineering Research 296,
https://doi.org/10.2991/978-94-6239-636-4_7

The protection of information privacy and confidentiality is becoming ever more essential with the advancement of digital communication. Various methods are used to obtain information that does not belong to someone illegally. If the information being sent is confidential, only authorized individuals can read it. Leaked and disseminated confidential information will result in losses for the information owner.

The importance of data confidentiality and security is increasing. Strong security mechanisms are needed to prevent unauthorized access to information (Hakim & Sholikhan, 2024). Various methods are used to secure important data, including cryptography. Cryptography is generally the science and art of maintaining the confidentiality of messages (Saeed & Azadeh, 2024). Although the use of cryptography is quite secure, encrypted information can still be seen (Panigrahi & Padhy, 2025). Other than cryptography, steganography provides a method for data security by embedding secret information in a way that only the sender and receiver are aware of its presence. This information is hidden in a medium or media host and is challenging to detect (G.mohammed, 2023; Senior & Yeboah, 2024; Yalla et al., 2022). The host medium for hidden information, known as the cover object, can consist of various digital formats such as audio, image, or video files. The media host that has been inserted with information is known as a stego object. To increase information security, steganography methods are often combined with cryptography (Firdaus et al., 2025; G.mohammed, 2023; Sultana et al., 2024)Many previous steganography studies have used the LSB method to hide information using only 1 bit of data for each byte of the media host. This results in a small amount of hidden information, which is only 1/8 of the media host size. For example, if the media host size is 80,000 bytes, then the maximum amount of information that can be hidden is only 10,000 bytes. The LSB bit is the least significant bit located on the rightmost bit or the 0th bit of the byte. The location of the LSB bit is shown in Fig. 1.

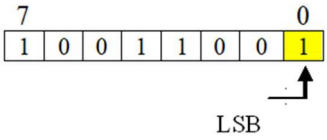


Fig. 1. Least Significant Bit Location

Many studies use the Least Significant Bit (LSB) method, as conducted by these researchers (Abood et al., 2022; Nguyen et al., 2025; Panigrahi & Padhy, 2025; Senior & Yeboah, 2024; Yalla et al., 2022). Previous research has focused mainly on traditional 1-bit LSB methods, which offer minimal impact on the quality of the embedded media host. However, their capacity is unfortunately limited. Some studies have extended to 2-bit or adaptive techniques, but often lack a comparative analysis of several structured m-bit variations.

In this study, we use a variant of the traditional LSB steganography method, namely m-bit LSB, to hide information. The media host used to hide information is an audio file with a bit-depth of 24 bits. The m-bit LSB method utilizes more than 1 bit of data from each byte of the media host. If the usual LSB only uses the last 1 bit, then the m-bit LSB uses the last m bits. For example, 4-bit LSB means inserting 4 bits per byte

(bits 0 to 3). Using more than one bit will increase the media host's capacity to hide information, but at the expense of reduced audio quality. The purpose of this study is to determine how many bits can be used to hide secret information while maintaining good audio quality so that the media host capacity can be optimally utilized. The quality of audio that has been inserted with secret information is still considered good if the Signal-to-Noise Ratio (SNR) value is above 30dB (Nguyen et al., 2025).

This research contributes through an extensive evaluation of the m-bit LSB method and presents experimental evidence determining the most suitable bit depth for concealing data within audio media. This study supports practitioners and researchers in selecting effective parameters for secure and undetectable audio steganography.

2 Research Methodology

The research steps used to describe the general sequence of activities are shown in Fig. 2.

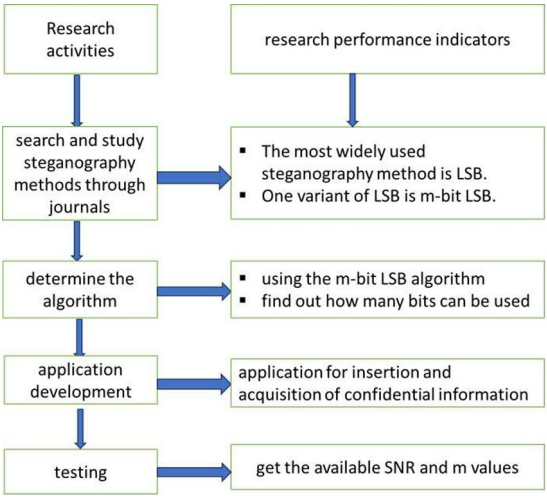


Fig. 2. Research Steps

In the initial stages of our research, we searched for and studied steganography methods through previous research journals. Many researchers use the LSB method to embed secret information because it is relatively easy to implement. The media host used is primarily an image. In general, the steganography process using an audio media host is shown in Fig. 3. Messages or information are embedded into the cover audio to become stego audio. This process is called encoding. The process of retrieving the information is called decoding, which is the process of extracting the hidden information from the stego audio.

Fig. 3. Steganography Process

The resulting Stego Audio quality should not differ significantly from the Cover Audio. This result is to avoid suspicion for steganologists. Stego Audio quality is still good if the Signal-to-Noise Ratio is more than 30dB. The calculation for finding the PSNR is shown in Eqs (1).

$$SNR = 10 \bullet Log_{10}\left(\frac{\sum_{n=0}^{N-1} x[n]^2}{\sum_{n=0}^{N-1}(x[n]-y[n])^2}\right) \quad (1)$$

Where
SNR = Signal-to-Noise Ratio
x[n] = original signal at time n
y[n] = stego signal at time n
N = total samples

2.1 Cover Object

A cover object is the original medium or media host used to store confidential information in the steganography process. In this study, the cover object used is a .WAV audio file with a mono channel, 16-bit bit depth, 44100 Hz frame rate, 470,000 total frames, and a duration of 10.66 s. We use the term cover audio in this study. The cover audio used is shown in Fig. 4.

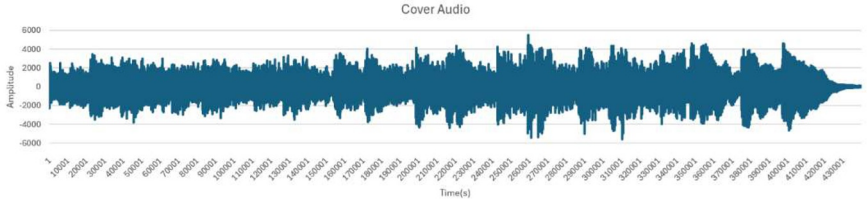


Fig. 4. Audio Cover

2.2 Insertion Process

The embedding process begins by reading the audio file. The data read is the amplitude of the sound, which will later be used to store confidential information. The process of inserting confidential information into the audio cover is carried out in increments of 1 bit to 7 bits. This embedding process is to determine up to what m-bit the audio quality is still considered good. Insertion of 8 bits and beyond is not performed because it is estimated that the audio quality is no longer as good as the original due to the influence of noise. The m-bit LSB embedding model is shown in Fig. 5. In Fig. 5(a), there are

two images of the initial state of the audio cover and confidential information. Fig. 5(b) insertion using 1 bit (m=1) of secret information into the audio cover. Fig. 5(c) insertion is done per two bits, and Fig. 5(d) insertion using 3 bits. And so on for the values m=4, 5, 6, and 7.

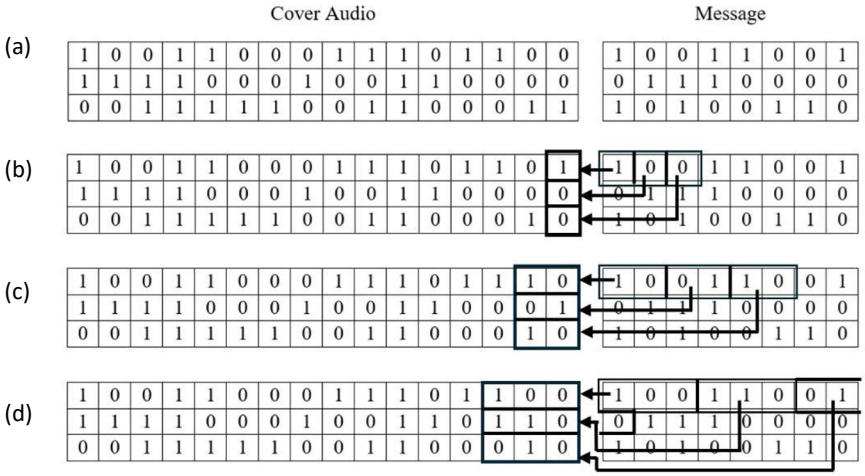


Fig. 5. Insertion of Confidential Information into Audio Cover

2.3 Testing

This research includes two experimental tests. In the initial test, the audio cover was altered by inverting its bit values, where bit 0 was changed to bit 1 and vice versa. This change is made on m with values 1 to 7. At m = 1, the rightmost bit is changed. At m = 2, the two rightmost bits are changed, and so on until m = 7. This test is done to determine how many bits can be used in the worst case, namely, the insertion process changes all used bits. An example of a bit change is shown in Fig. 6.

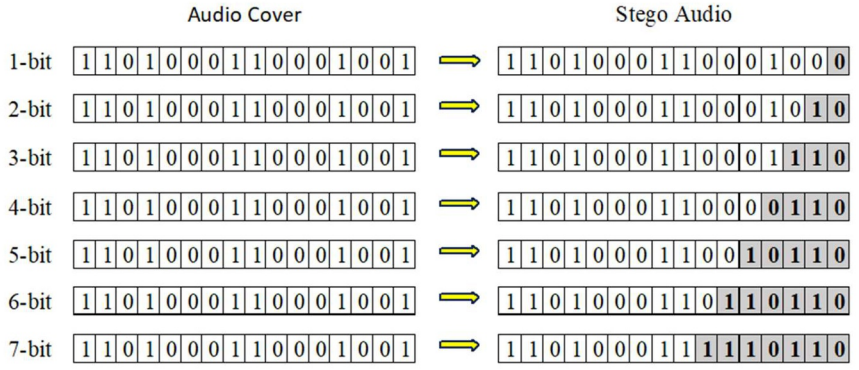


Fig. 6. Bit Changes At m=1, 2, 3, 4, 5, 6 and 7

The second test was conducted using several files of varying sizes as secret information. The files used for the second test are shown in Table 1. The Document1.txt file will be inserted into the audio cover using m = 1. Document2.txt will be inserted using m = 2, Document3.txt will be inserted using m = 3, and so on. The purpose of the second test is to determine how many bits can be used so that the stego audio still has good quality when using the real file.

Table 1 Table File for the Second Test

No.	File Name	File Size (Bytes)
1.	Document1.txt	58,750
2.	Document2.txt	117,500
3.	Document3.txt	176,250
4.	Document4.txt	235,000
5.	Document5.txt	293,750

3 Results And Discussion

3.1 First Test

In the first test, we made changes to the bit values as in Figure 6 to form stego audio. After the stego audio was formed, we performed Signal-to-Noise Ratio calculations from 1-bit to 7-bit. The SNR calculation results were still above 30 dB, meaning the stego audio quality was still considered good. However, noise was present at 5-, 6-, and 7-bit changes. The results of this first test are shown in Fig. 7.

When viewed in Fig. 7, from 1-bit to 7-bit, the graphics are the same with almost no difference. We tried to display the first 40 frames of each graph in Fig. 7. The first 40 frames are shown in Fig. 8. Figure 8(a) is an audio cover that does not include confidential information. Fig. 8(b) – 8(h) is a stego audio graph that has had its bits changed from 1 to 7 bits. The graph appears less smooth, indicating the emergence of noise as shown in Fig. 8(e).

3.2 Testing Second

In the second test, a text file of the appropriate size for the audio cover was used. The audio cover used had 470,000 frames, so the capacity of the audio cover can be calculated using the Eqs (2).

$$Capacity = Number\ of\ Frames * m / 8 \quad (2)$$

Where

Capacity = Size of message that can be inserted (in bytes)

Number of Frames = Number of frames of the audio file
m = number of bits used for information insertion

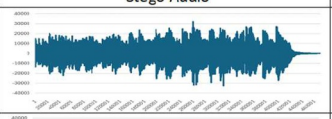
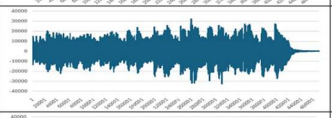
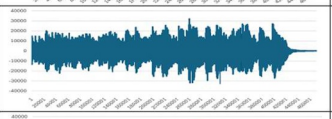
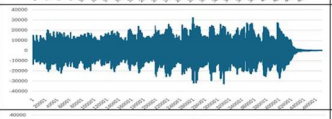
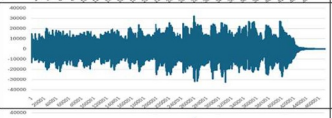
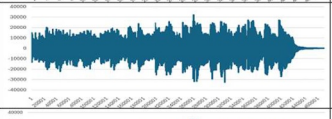
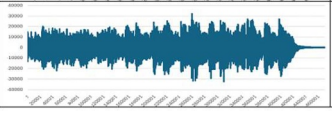
m	Stego Audio	SNR (dB)
1-bit		75.82
2-bit		68.83
3-bit		62.63
4-bit		56.54
5-bit		50.50
6-bit		44.46
7-bit		38.41

Fig. 7. First Test Results

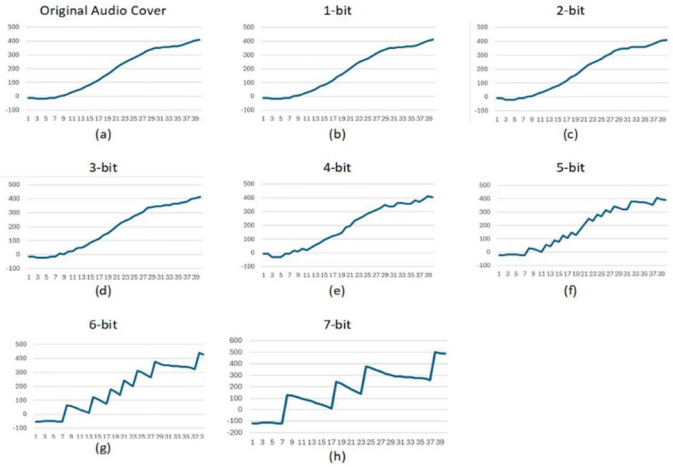


Fig. 8. Amplitude Graph of the First 40 Frames

The message capacity that can be inserted with m values, one to seven, is shown in Table 2.

Table 2. Information Capacity on Audio Covers

m	Capacity
1	470,000 * 1 / 8 = 58,750 Bytes
2	470,000 * 2 / 8 = 117,500 Bytes
3	470,000 * 3 / 8 = 176,250 Bytes
4	470,000 * 4 / 8 = 235,000 Bytes
5	470,000 * 5 / 8 = 293,750 Bytes
6	470,000 * 6 / 8 = 352,500 Bytes
7	470,000 * 7 / 8 = 411,250 Bytes

Table 3 shows the findings obtained from the second test.

Table 3. Experimental Results of the Second Test

M	SNR (dB)
1	78.84
2	72.37
3	65.80
4	59.96
5	53.68
6	48.04
7	41.61

The lowest SNR value, 41.61 dB, for information embedding using 7-bit data, indicates that the stego audio quality is still good. When each stego audio is played, the music can still be heard clearly. However, at m values of 5, 6, and 7, noise is also quite audible. This result is the same as in the first test.

4 Conclusion

From the test results, it can be concluded that the m-bit LSB method can be used well up to an m value of four on sound-type cover objects. Using m-bit LSB with m value of 4, the cover object capacity increases up to four times, and the stego audio quality remains quite good. Using m value more than four will produce noise in the stego audio, even though the SNR is still above 30dB. This value will raise suspicion for steganologists.

References

Abood, E. W., Abdullah, A. M., Al Sibahee, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Kalafy, S. A. A., & Ghrabta, M. J. J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics, 11(1), 185–194. https://doi.org/10.11591/eei.v11i1.3279

Firdaus, D. T., Croix, N. J. D. La, Ahmad, T., Mukanyiligira, D., & Sibomana, L. (2025). Steganographic model to conceal the secret data in audio files utilizing a fourfold paradigm: Interpolation, multi-layering, optimized sample space, and smoothing. Journal of Safety Science and Resilience, 6(2), 138–149. https://doi.org/10.1016/j.jnlssr.2024.09.004

G.mohammed, S. (2023). A survey on Rijndael based LSB Audio Steganography techniques. Wasit Journal for Pure Sciences, 2(4), 80–87. https://doi.org/10.31185/wjps.245

Hakim, F. N., & Sholikhan, M. (2024). Enhancing Data Security through Digital Image Steganography: An Implementation of the Two Least Significant Bits (2LSB) Method. International Journal of Graphic Design, 2(2), 222–235. https://doi.org/10.51903/ijgd.v2i2.2124

Mondejar, M. E., Avtar, R., Diaz, H. L. B., Dubey, R. K., Esteban, J., Gómez-Morales, A., Hallam, B., Mbungu, N. T., Okolo, C. C., Prasad, K. A., She, Q., & Garcia-Segura, S. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. Science of the Total Environment, 794(June). https://doi.org/10.1016/j.scitotenv.2021.148539

Nguyen, D. D., Gupta, R., Gunjawate, D. R., Holik, J., Jin, C., & Madill, C. (2025). Speech-to-Noise Ratio and Voice-to-Noise Ratio of Voice Databases With Implications for Acoustic Voice Analysis. Journal of Voice, 1–15. https://doi.org/10.1016/j.jvoice.2025.05.029

Panigrahi, R., & Padhy, N. (2025). An effective steganographic technique for hiding the image data using the LSB technique. Cyber Security and Applications, 3(August 2024). https://doi.org/10.1016/j.csa.2024.100069

Saeed, B. F., & Azadeh, I. R. (2024). When cryptography stops data science: Strategies for resolving the conflicts between data scientists and cryptographers. Data Science and Management, 7(3), 238–255. https://doi.org/10.1016/j.dsm.2024.03.001

Senior, I. A., & Yeboah, C. (2024). Critical Review of Video , Audio , Image and Text Steganalysis Technique for Digital Forensics. 7081–7095.

Sultana, H., Kamal, A. H. M., Apon, T. S., & Alam, M. G. R. (2024). Increasing embedding capacity of stego images by exploiting edge pixels in prediction error space. Cyber Security and Applications, 2(August 2023). https://doi.org/10.1016/j.csa.2023.100028

Yalla, S. P., Uriti, A., & Sethy, A. (2022). GUI Implementation of Modified and Secure Image Steganography Using Least Significant Bit Substitution. International Journal of Safety and Security Engineering, 12(5), 639–643. https://doi.org/10.18280/ijsse.120513