A COMPARATIVE STUDY OF TEXT AND AUDIO STEGANOGRAPHY FOR CYBERSECURITY

Abstract

Steganography embeds information in digital media for secure communication. This study compares text and audio steganography based on mean squared error and bit error rate to evaluate the better steganography technique for cybersecurity. Experimental results show that audio steganography achieves an average mean squared error of 1.82E-10 and an average bit error rate of 1.22E-02, supporting cybersecure communication. Audio steganography provides improved security and imperceptibility against adversarial analysis compared to text steganography. The higher mean squared error and bit error rate values of 0.022806 in text steganography indicate increased distortion, making the hidden data more detectable. The superior imperceptibility of audio steganography ensures secure communication for cybersecurity applications.

Keywords: Audio Steganography; Text Steganography; Cybersecurity; Least Significant Bit (LSB); Mean Squared Error(MSE); Bit Error Rate (BER).

Authors

K. Revathi
Department of Electronics
and Communication Engineering.
B. S. Abdur Rahman Crescent
Institute of Science and Technology
Vandalur, Chennai, Tamil Nadu
India.
revathivigneswaranphd@gmail.com,

S. Kaja Mohideen
Department of Electronics
and Communication Engineering.
B. S. Abdur Rahman Crescent
Institute of Science and Technology
Vandalur, Chennai, Tamil Nadu
India.
kajamohideen@crescent.education.

I. INTRODUCTION

Advancements in internet technology and the pandemic have increased the demand for a digital world in education, banking, healthcare, government, smart cities, and grid systems. This highlights the need for secure online information transmission and the role of cybersecurity in protecting data and communications. Therefore, data protection, privacy concerns, reliability, availability, and cybersecurity are key considerations in the digital world. Cybersecurity protects individuals, societies, organizations, systems, and technologies from unauthorized activities. As cybersecurity strengthens, cybercriminals continuously develop more sophisticated attacks to bypass security measures, causing an ongoing struggle between security and threats [1-3].

Cybercrime involves various illegal activities that use digital devices or information systems as tools, targets, or both. It includes offenses affecting computer data or systems, often categorized as computer crime, electronic crime, e-crime, high-technology crime, or digital crime. Hence, cybersecurity must protect confidentiality, integrity, and availability (CIA) to protect an organization's systems, computer resources, and network security [1, 4].

Integrating information-hiding techniques with cybersecurity strengthens data protection, reducing the impact of cybercrime on secure communication. Data hiding methods include watermarking, steganography, and cryptography, each with advantages and limitations. Effective data hiding should ensure high capacity, robustness, security, payload, and reliability. The choice of method depends on the required security level and the amount of information embedded in multimedia files. Figure 1 illustrates these techniques [5].

Cryptography encrypts plaintext into ciphertext to ensure confidentiality. The plaintext can be a file, financial data, login credentials, or confidential information. Before encryption, the original data is plaintext, while the encrypted version is ciphertext. The fundamental components of cryptography include plaintext, a key, ciphertext, and encryption and decryption algorithms. The encryption algorithm transforms plaintext into ciphertext, while the decryption algorithm reverses the process, restoring the original plaintext. The cryptographic keys are symmetric and public keys. Symmetric key cryptography employs a single key for encryption and decryption. Public key cryptography uses a key pair, with the public key for encryption and the private key for decryption[5].

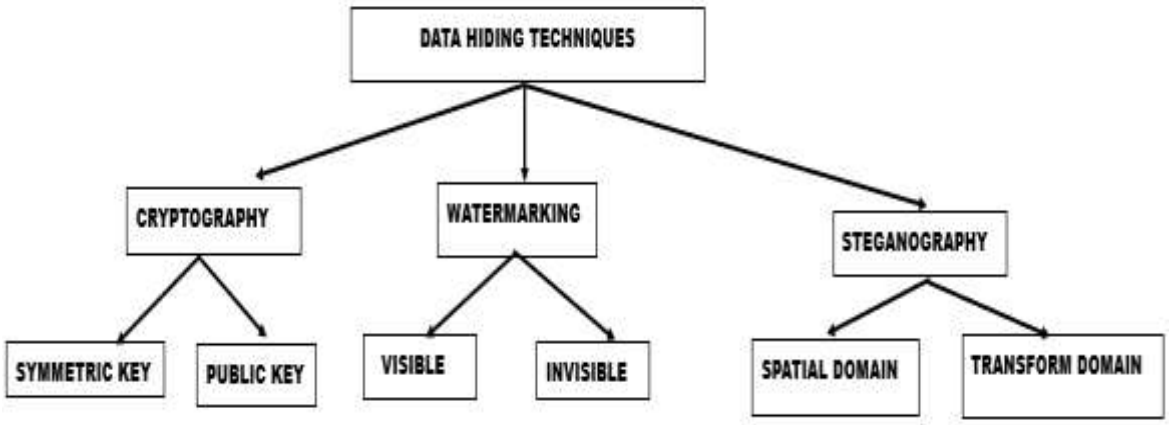


Figure 1: Data hiding techniques

Watermarking is a data security technique for authentication and copyright protection with digital data embedded into multimedia files. It is classified into visible watermarking, which includes logos or text, and invisible watermarking, which remains imperceptible while ensuring protection. This method prevents unauthorized duplication and false ownership claims, enabling users to place an indelible mark on digital content. Watermarking ensures robustness, security, and efficiency in safeguarding intellectual property [5, 6].

Steganography embeds confidential data in a cover file such as text, audio, image, or video. It secures messages by concealing data within media, unlike cryptography, which converts data into ciphertext. While cryptography ensures security through encryption, steganography enhances protection by keeping data hidden. In cryptography, security is compromised if the encrypted data is accessed. In contrast, steganography strengthens security by concealing the existence of communication [6]. Steganography is categorized based on the type of cover object used, including image, network, video, audio, and text steganography. Image steganography, the most common method, uses an image as the cover object. Network steganography conceals data within network protocols such as TCP, IP, and UDP. Video steganography embeds secret data within video files, while audio steganography hides information within audio files. Text steganography involves embedding data in a text file, producing a stego text as the output [5]. This study aims to identify the best steganography method between text and audio for cybersecurity communication. The framework is illustrated in Figure 2.

The rest of the chapter is structured as follows: Section II briefs about audio and text steganography. Section III discusses the LSB technique. Section IV details the simulated experiments, evaluates the results, and discusses the most suitable steganography approach for cybersecurity. Section V concludes the paper with future scope.

II. AUDIO AND TEXT STEGANOGRAPHY

In ideal steganography ensures secure communication without prior key exchange. Secret key steganography uses a stego key for the secure embedding and extraction of messages.

Public key steganography uses a public key for embedding and a private key for retrieval to enhance security through asymmetric encryption. In all cases, the cover file should be large enough to embed the message for accurate retrieval. The similarity between the cover and stego audio files minimizes distortion, ensuring secure communication with a similarity value close to one [7].

Audio steganography is the process of embedding secret data in the cover audio file. Figure 3[8] illustrates the embedding and extraction process. Embedding data in audio files is more challenging than in images due to the higher sensitivity of the human auditory system. However, the larger size, high redundancy, and high data transmission rate make audio files more suitable as host files [9].

An audio steganographic system should maintain the trade-off between capacity, robustness, and imperceptibility to provide cybersecurity. Capacity is a percentage of hidden messages in cover audio files. Robustness is the strength of audio-steganographic communication resisting attacks. Imperceptibility is the similarity in the cover audio file before and after embedding the hidden messages [10].

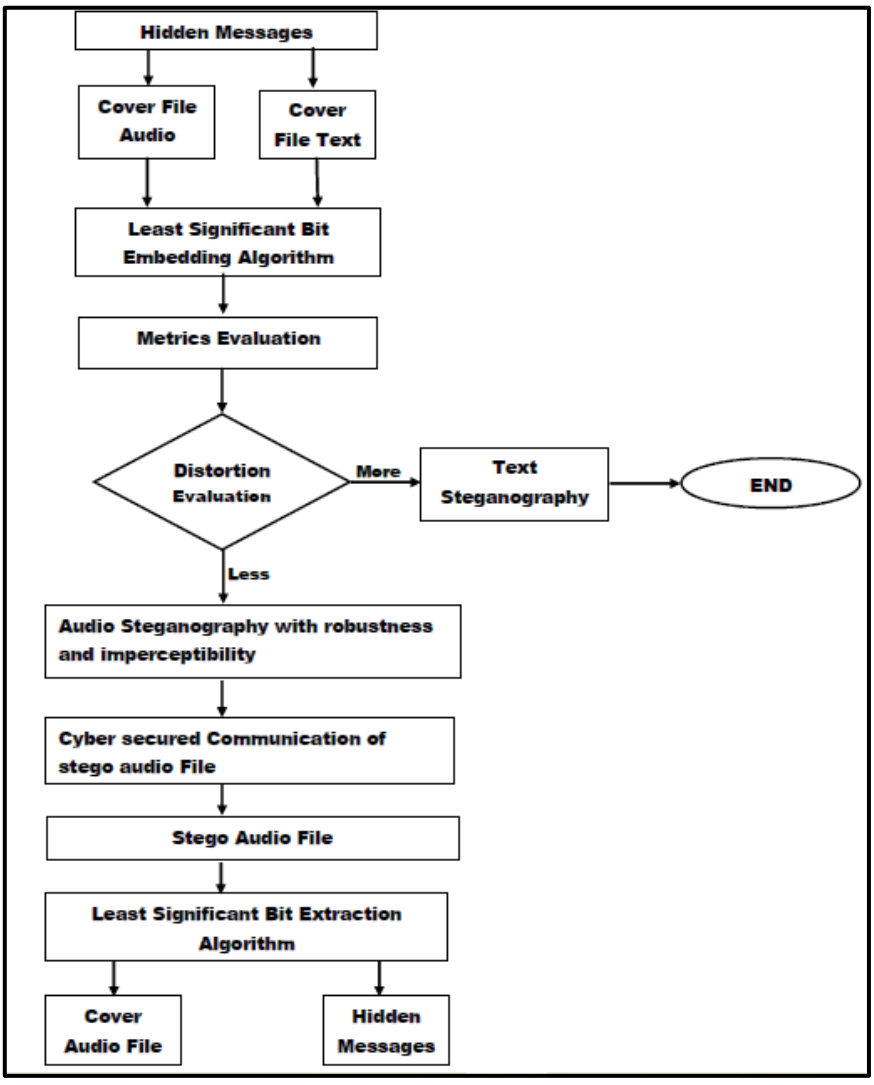


Figure 2: The Framework of the chapter

The least significant bit algorithm is a basic and efficient steganography method for embedding and extracting hidden messages in audio steganography. Figures 5 and 6[11] illustrate the LSB algorithm in audio steganography. The algorithm's efficiency resulted in indistinguishability between the cover and stego audio files [11]. Audio steganography is applied in Cybersecurity, Healthcare, Media and Entertainment, Government and Defence, E-commerce, and Intellectual Property Protection for secure communication and data storage. In the medical domain, it embeds Electronic Health Records (EHRs) and diagnostic data in audio signals to ensure confidentiality. In Government and Defence applications, it enables covert transmission of operational information. In multimedia and industrial applications, production data, control parameters, and copyright information are embedded in audio signals to protect intellectual property and prevent unauthorized access. Steganographic techniques protect data from cyber threats for information security companies [7,12].

Text steganography is the natural language steganography that hides the message in the medium of text. The two main groups in natural language steganography are linguistic steganography and text steganography. Linguistic steganography preserves linguistic structure while embedding the hidden message, whereas text steganography manipulates cover text elements to conceal data. Text steganography hides messages within text by modifying text components such as words, spaces, and lines, making the presence of the message undetectable.

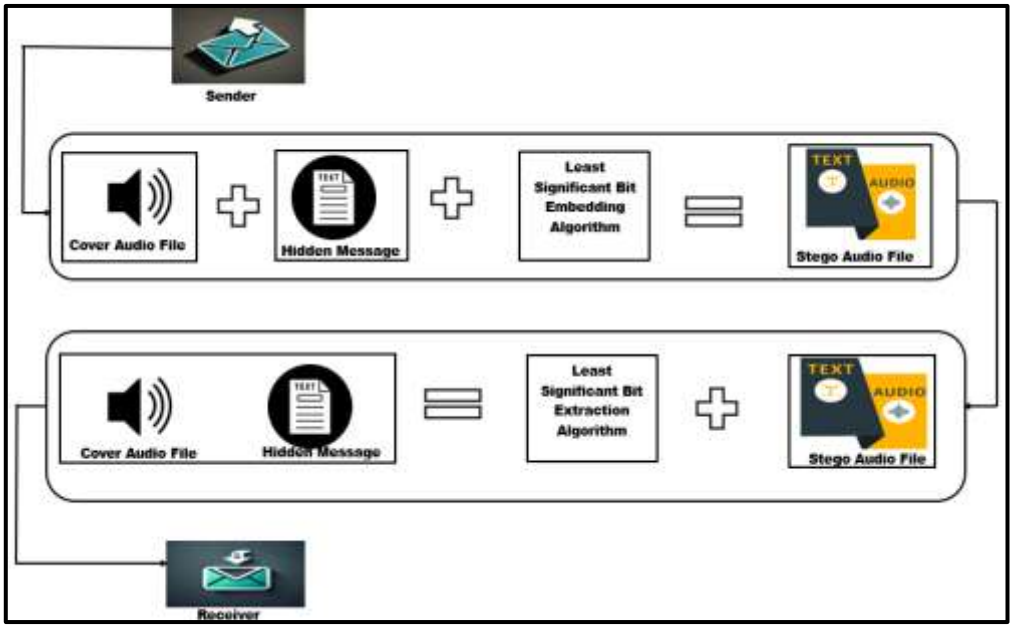


Figure 3: Audio steganographic process

Text steganography methods are further divided into word-rule-based and feature-based approaches. Word-rule-based methods embed hidden messages by modifying text alignment. Line-shift coding alters vertical line positions, encoding binary values by shifting lines up or down. Word-shift coding horizontally adjusts word positions within lines to conceal information. Feature-based methods manipulate text features such as letter shape, size, and position to hide data by exploiting the unique structure of the cover text [13].

The text steganography in this study, where both cover and hidden messages are text files, is shown in Figure 4[8].The cover file with the hidden message is a stego file. The LSB method is a simple steganography technique that embeds hidden messages in cover text files. Figures 5 and 7[11] illustrate the LSB embedding and extraction algorithm in text steganography. The algorithm demonstrates efficiency by increasing the percentage of hidden messages in cover text files, maintaining uniqueness between cover and stego text files, and ensuring undetectable communication of stego files. The main challenge in text steganography is its low hiding capacity due to the insufficient redundant data in textual documents compared to digital media such as images, audio, and video files [6].

Text steganography has several technical applications, including hidden communication, network covert channels, and unauthorized access detection. Hidden communication involves embedding secret data within ordinary text files or messages transmitted over public networks, such as SMS and social media. Intelligence agencies, journalists, or individuals under strict regulations can use these hidden messages to exchange sensitive information securely. Network covert channels utilize text steganography to establish undetectable communication paths within network protocols. These channels covertly transmit malware or bypass internet restrictions. Additionally, text steganography aids in detecting unauthorized access to sensitive documents by embedding identifiers within confidential files, allowing traceability without the recipient's awareness [14].

III. LEAST SIGNIFICANT BIT ALGORITHM

The least significant bit (LSB) algorithm is one of the earliest methods of information-hiding techniques. In the LSB embedding algorithm, there is a 50% probability that the least significant bit of the cover file will remain unchanged when embedding a bit from the hidden message, which helps minimize distortion.

The LSB of a cover file must be modified carefully to preserve its quality, ensuring that the hidden message before steganography and the stego message after steganography retain the same characteristics. In the LSB extraction algorithm, the least significant bits are extracted from the stego file, and eight bits are grouped to reconstruct the hidden message. Figure 5[15] presents the flow chart for the LSB embedding and extraction algorithm.

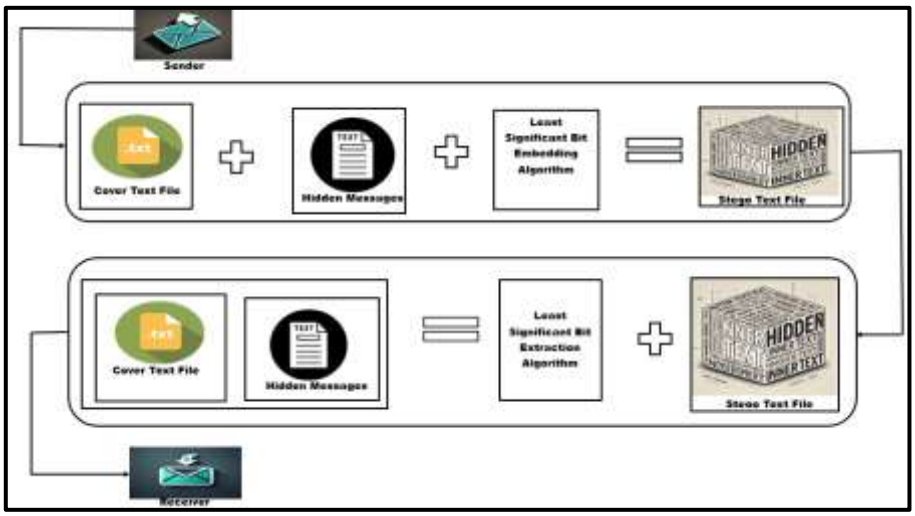


Figure 4: Text steganography process

The hidden message is a text file (.txt), while the cover file can be either a text file or an audio file. Embedding one byte requires eight one-byte text characters in a text cover file. Similarly, embedding one byte of a text file into an audio file requires eight one-byte audio samples. The LSB algorithm increases embedding capacity, achieving an embedding rate of 8 kbps in cover audio files at 8 kHz [11].

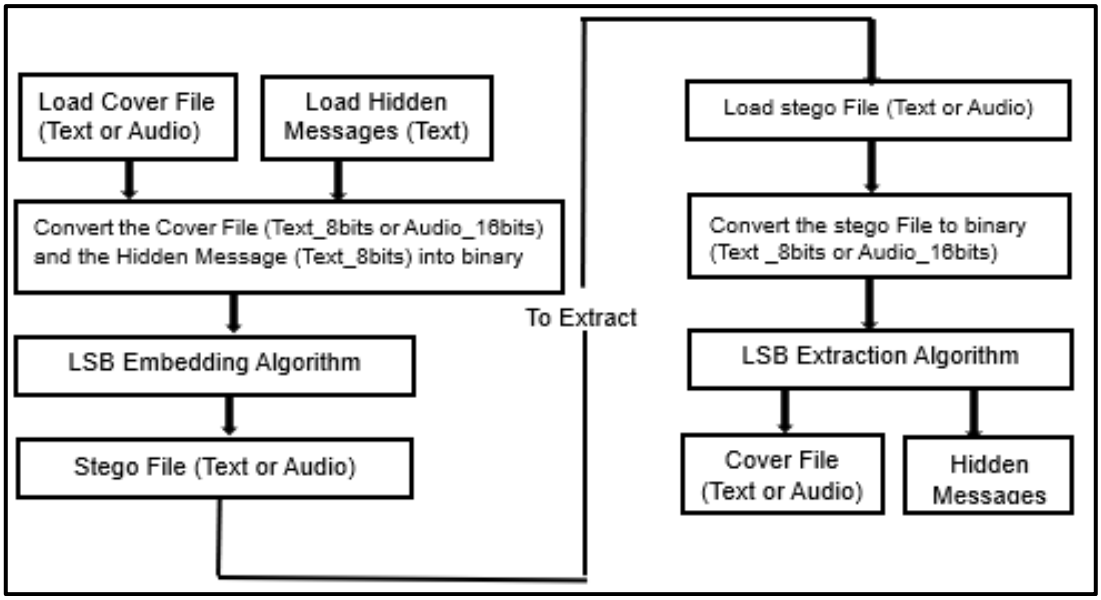


Figure 5: The flowchart of the LSB algorithm

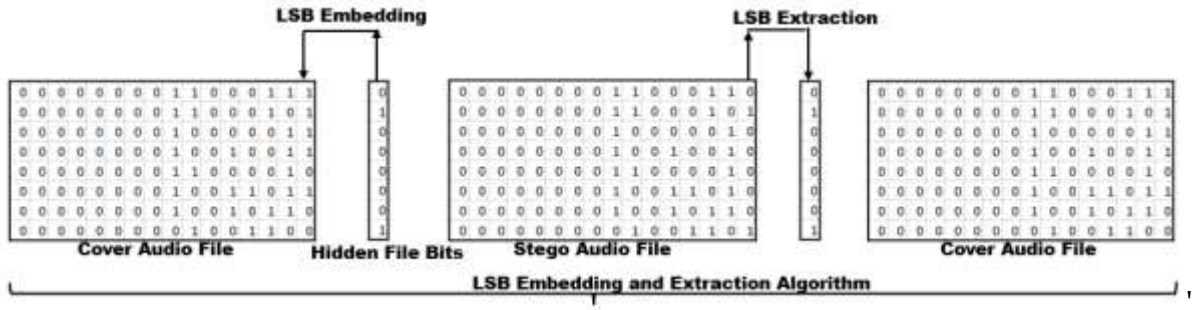


Figure 6: LSB algorithm in cover audio files

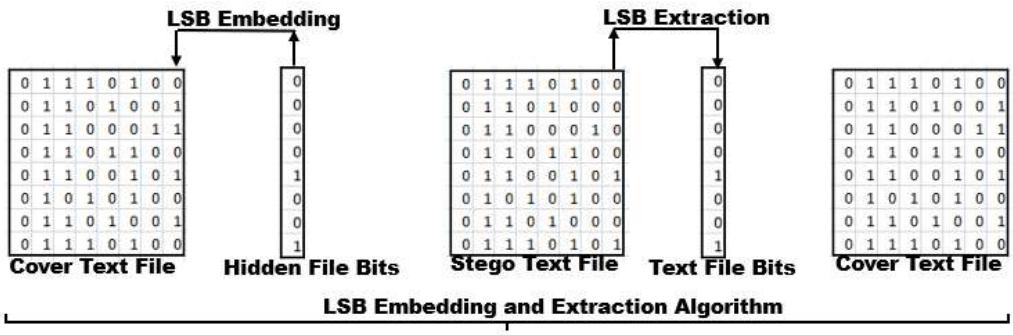


Figure 7: LSB algorithm in cover text files

IV. RESULTS AND DISCUSSION

The least significant bit (LSB) algorithm was tested in MATLAB using audio and text files to evaluate its performance. The audio files used in this study are from the Free Spoken Digit Dataset (FSDD) [16], consisting of recordings of spoken digits in WAV files sampled at 8 kHz. The text files (.txt) are from a Question-Answer Dataset containing question-answer pairs generated from 690,000 words of cleaned Wikipedia text. This dataset includes three files (S08, S09, and S10) categorized by student year. Each entry contains the article title, question, answer, difficulty ratings from the questioner and answerer, and the article file name [17]. Table 1 lists the specifications of the cover text and audio files (WAV). Mean Squared Error (MSE) and Bit Error Rate (BER) were used to evaluate the LSB algorithm. These metrics determine the more effective steganography method for cybersecured communication.

Table 1: Specification of Cover Audio and Text Files

Audio Files	
Bits per sample	16
Number of Samples	3370-5083
Sample Rate	8000Hz
Channel	1
Audio Type	Music
Duration in Seconds	0.4-0.6
Text Files	
Bits per byte	8
Length (Bytes)	3415-5512

Equation (1) [18] quantifies distortion as the average squared difference between the cover and stego files.

BER, as defined in Equation (2) [18], represents the ratio of incorrect bits after embedding to the total number of embedded bits. Lower MSE and BER values result in higher fidelity with minimal distortion in stego files, ensuring the reliability of the steganographic process.

$$\mathrm{MSE} = \frac{1}{\mathrm{P}}\sum_{\mathrm{k}=1}^{\mathrm{P}}(\mathrm{Q_k} - \mathrm{R_k})^2 \quad (1)$$

Q_k and R_k are the cover and stego files for the k^{th}samples or characters, and P is the total number of samples or characters.

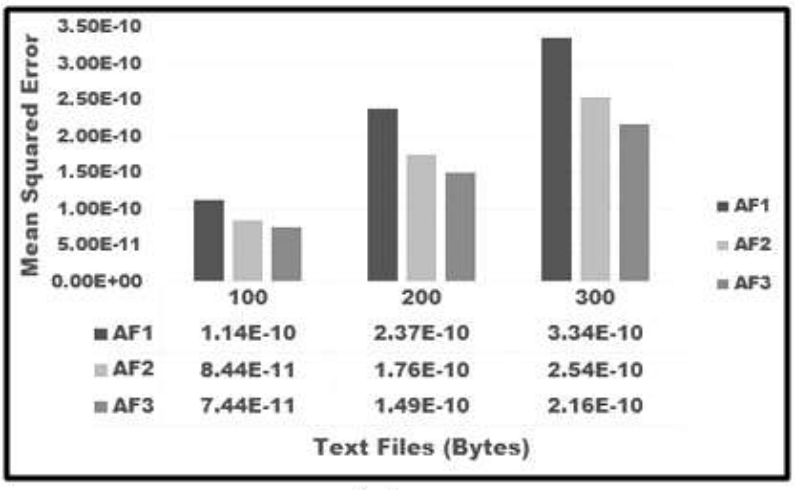
$$\mathrm{BER} = \frac{\mathrm{S_{error}}}{\mathrm{S_{bits}}} \quad (2)$$

S_{error} is the number of incorrect bits, and S_{bits} is the total number of bits embedded in the cover file.

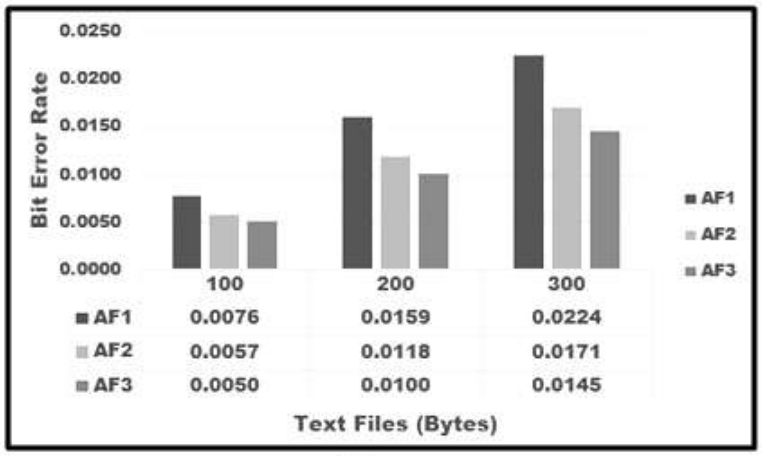
1. Audio Steganographic Communication for Cybersecurity

The objective is to select the most suitable steganography method for communicating hidden messages in cybersecurity. Eighteen simulations embedded hidden messages in audio and text files. The average MSE for audio and text steganography is 1.82E-10 and 0.022806, respectively. Similarly, the BER for audio and text steganography is 1.22E-02 and 0.022806. Figures 8a, 8b, 9a, and 9b illustrate the MSE and BER for the audio and text steganography. The x-axis in Figures 8a and 8b represents the size of text files (in bytes) hidden within cover audio files (AF1, AF2, and AF3). Similarly, the x-axis in Figures 9a and 9b represents the size of text files (in bytes) hidden within cover text files (TF1, TF2, and TF3). The y-axis in Figures 8a and 9a represents the mean squared error. In Figures 8b and 9b, the y-axis represents the bit error rate. Based on these metrics, it is concluded that audio steganography provides a more secure means of transmitting hidden messages. Cover audio files have sufficient redundancy to support higher embedding capacity, while controlled variability in stego audio files using the LSB algorithm enhances the security of embedded data against detection and modification. Cybersecurity applies to various fields, such as the smart grid, vehicular communication, smart city, and smart eHealth system [1]. Using audio files as cover media enhances cybersecurity compared to embedding in text files.

In contrast, text steganography is less effective due to the lack of redundancy in text files. The average MSE and BER values of 0.022806 indicate higher distortion and error rates, facilitating the detection of hidden messages during communication. The MSE for audio steganography is calculated using continuous sample values, as audio signals are inherently continuous. Small changes in these sample values are usually imperceptible to the human ear. In contrast, text steganography uses binary values, where even a minor change can noticeably alter the text. This makes comparing MSE between audio and text challenging, as audio is continuous, and text is discrete. While calculating MSE based on binary values may offer consistency across data types, it does not accurately reflect perceptual changes in audio, which are better captured by differences in sample values. Even a slight modification in the stego text file, such as a single-bit change, can disrupt the text flow by altering the corresponding character. This disruption makes the stego text more susceptible to steganalysis attacks, reducing its robustness. Encrypting hidden messages before embedding them in text files enhances the security of text steganography.

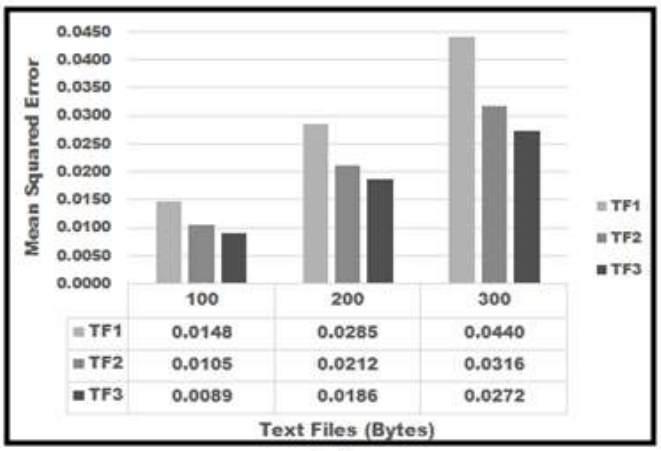


(a)

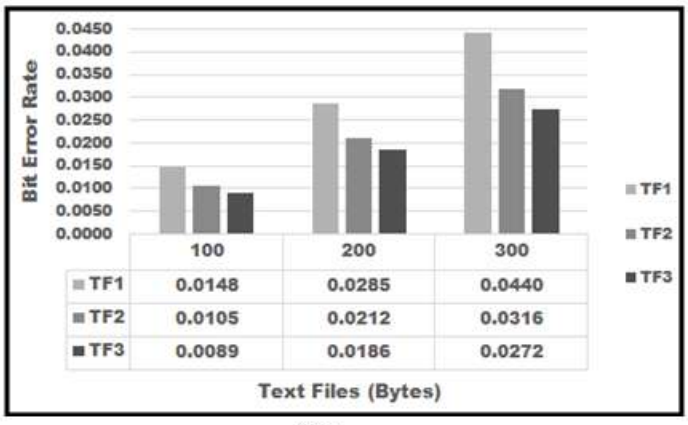


(b)

Figure 8: Results of (a) MSE and (b) BER for 300 bytes of hidden messages embedded in audio files



(a)



(b)

Figure 9: Results of (a) MSE and (b) BER for 300 bytes of hidden messages embedded in text files

V. CONCLUSION

This chapter compared text and audio steganography for cyber-secure communication. Text messages were embedded in cover audio and text files using the LSB algorithm. The average MSE of 1.82E-10 measured the distortion level in audio steganography, while the average BER of 1.22E-02 determined the number of incorrect bits in the stego audio files. These results indicate reduced distortion and reliable transmission of hidden messages, enhancing cybersecurity. In comparison, text steganography, with an average MSE and BER of 0.022806, was less effective in resisting steganalysis. In the future, the traditional LSB approach can be modified by embedding hidden messages in more significant bits to increase the payload capacity while maintaining security.

REFERENCES

[1] Wasyihun Sema Admass,Yirga Yayeh Munaye, and Abebe Abeshu Diro , "Cyber security: State of the art, challenges and future directions", Cyber Security and Applications,2(2024),100031, https://doi.org/10.1016/j.csa.2023.100031.

[2] Farhan Ullah, Hamad Naeem, Sohail Jabbar, Shehzad Khalid, Muhammad Ahsan Latif, Fadi Al-Turjman, and Leonardo Mostarda, "Cyber Security Threats detection in Internet of Things using Deep Learning approach", IEEE Access, https://doi.10.1109/ACCESS.2019.2937347.

[3] Jagpreet Kaur, and K .R. Ramkumar, "The recent trends in cyber security: A review", Journal of King Saud University –Computer and Information Sciences, 34 (2022) 5766–5781, https://doi.org/10.1016/j.jksuci.2021.01.018

[4] Regner Sabillon, Jeimy Cano, Victor Cavaller, and Jordi Serra, "Cybercrime and Cybercriminals: A Comprehensive Study", International Journal of Computer Networks and Communications Security, 4(6), 2016, pp.165–176

[5] A. Rasmi, and M. Mohanapriya, "An Extensive Survey of Data Hiding Techniques", Indian Journal of Science and Technology, 9(28),2016,https://doi.org/10.17485/ijst/2016/v9i28/90457

[6] Mohammed Abdul Majeed, Rossilawati Sulaiman, Zarina Shukur and Mohammad Kamrul Hasan, "A Review on Text Steganography Techniques", Mathematics, 2021, 9, 2829,https://doi.org/10.3390/math9212829

[7] Stefan Katzenbeisser and Fabien A.P. Petitolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House computing library, 2000.

[8] Danish Shehzad and Tamer Dag, "A Novel Image Steganography Technique based on Similarity of Bits Pairs",2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC 2017), 2017.

[9] Sushma Bahuguna and Sandeep Jain, "A Review of LSB-Based Audio Steganography Techniques", International Journal of Computer Engineering and Technology (IJCET) 12(3), 2021, pp. 1-7, https://doi.org/10.34218/IJCET.12.3.2021.001.

[10] IfraBilal, Mahendra Singh Roj,Rajiv Kumar and P K Mishra, "Recent Advancement in Audio Steganography",2014 International Conference on Parallel, Distributed and Grid Computing,IEEE,pp 402-405.

[11] Dingwei Tan, Yuliang Lu, Xuehu Yan, and Xiaoping Wang, "A Simple Review of Audio Steganography",2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2019),IEEE,pp.1409-1413

[12] Thi-Kien Dao and Trong-The Nguyen, "Recent Information Hiding Techniques in Digital Systems: A Review", Journal of Information Hiding and Multimedia Signal Processing, (15),1, 2024 pp.10-20.

[13] Mohd Hilal Muhammad, Hanizan Shaker Hussain, Roshidi Din, Hafiza Samad, and Sunariya Utama, " Review on feature-based method performance in text steganography",Bulletin of Electrical Engineering and Informatics,10(1),2021, pp. 427-433, https://doi.10.11591/eei.v10i1.2508.

[14] Milad Taleby Ahvanooey, Qianmu Li, Jun Hou, Ahmed Raza Rajput and Yini Chen, "Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis", Entropy, 2019, 21, 355, https://doi:10.3390/e21040355.

[15] May Alanzy, Razan Alomrani, Bashayer Alqarni, and Saad Almutairi, ”Image Steganography Using LSB and Hybrid Encryption Algorithms”, Applied Sciences. 2023, 13, 11771. https://doi.org/10.3390/app132111771.

[16] Zohar Jackson, César Souza, Jason Flaks, Yuxin Pan, Hereman Nicolas, & Adhish Thite. (2018, August 9).Jakobovski/free-spoken-digit-dataset: v1.0.8 (Version v1.0.8).Zenodo. http://doi.org/10.5281/zenodo.1342401

[17] Smith, N. A., Heilman, M., & Hwa, R. (2008, September). Question generation as a competitive undergraduate course project. In Proceedings of the NSF Workshop on the Question Generation Shared Task and Evaluation Challenge.

[18] M. M. Mahmoud and H. T. Elshoush, “Enhancing LSB Using Binary Message Size Encoding for high capacity, Transparent and Secure Audio Steganography-An Innovative Approach,” IEEE Access, 10, pp. 29954–29971, 2022, doi: 10.1109/ACCESS.2022.3155146.