
ISSN: 2321-2152
IJMECE
International Journal of modern electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN2321-2152
www.ijmece.com
Vol13,Issue1,2025

A REAL-TIME IMPLEMENTATION OF DATA HIDING IN AUDIO FOR MILITARY APPLICATIONS

[1]MISS.V.V.NARAYANAMMA,[2]CH.NAGACHITANYA,[3]A.NITHIN,[4]B.HARITH KUMARREDDY,[5]CH.HEMANTHKUMARREDDY

[1](Asst.Prof),ECE, RISE Krishna Sai Prakasam Group of Institutions::Ongole

[2345]B.TECH,scholar,ECE, RISE Krishna Sai Prakasam Group of Institutions::Ongole

ABSTRACT

Data hiding, often referred to as steganography, is the practice of concealing data within a medium in such a way that it remains undetectable by human senses and unauthorized observers. In military applications, secure communication is of paramountimportance,andaudio-baseddata hiding techniques offer an effective means for covert transmission. This paper focuses on the real-time implementation of data hiding techniques in audio signals for military applications, where secrecy, data integrity, and robustness are critical. The primary objective is to propose a methodthat integrates data hiding into audio signals in real-time, ensuring that the hidden data remains undetectable under various attacks and environmental factors. A novel data embedding algorithm is developed, which uses psychoacoustic properties to embeddata into audio without significantly altering the perceptible quality of the original signal. The performance of the system is evaluated using metrics such as the imperceptibility of the hidden data, capacity, robustness, and real-time processing capabilities. Experimental results show that the proposed systemachieveshighlevelsofsecurityand efficiency in terms of both computational resources and audio quality. The research provides a significant advancement in securing military communications through an efficient and covert audio-based data hiding method.

KEYWORDS: Data Hiding, Audio Steganography, Military Applications, Real-Time Implementation, Audio Signal Processing, Covert Communication, Security, Psychoacoustic Model, Robustness, Audio Quality.

1. INTRODUCTION

The increasing need for secure communication in military applications has driven advancements in encryption, secure transmission, and covert communication methods. Data hiding, or steganography, has emerged as a powerful technique in achieving covert communication, where sensitive data is concealed within other seemingly innocuous content such asimages, audio, or video. Specifically, audio steganography offers significant potential in military scenarios where communication must be kept secret from enemy forces and unauthorized third parties.

In military operations, secure and secret transmission of intelligence, orders, and strategic information is crucial. While encryption techniques protect data during transmission, they often raise suspicion if intercepted, making them unsuitable for environments where stealth is necessary. Audio signals, on the other hand, can serve as effective carriers for hidden information. Unlike traditional methods that rely solelyon encryption, audio steganography embeds sensitive data into the audio signal, makingit less detectable to unauthorized listeners.

Real-time data hiding in audio signals is particularly important in military applications.Areal-timesystemensuresthat the embedding and extraction of hidden data occurwithoutintroducingsignificantdelays, which could compromise the effectivenessofthecommunication.Moreover, thesystem must maintain the quality ofthe audio signal to avoid raising suspicion or alerting adversaries to the presence of hidden information.

Thechallengein audiosteganography liesin embedding data without altering the perceptible audio quality. Since the human auditory system is highly sensitive to certain frequencies, any modifications to the audio signal must be imperceptible to the listener. Thus, psychoacoustic models, which consider the limitations and sensitivities of human hearing, play a vital role in thedesign of efficient and undetectable data- hiding systems.

This paper proposes a novel real-time data-hiding method in audio signals specifically designedformilitaryapplications.By leveraging the psychoacoustic model, the proposed system ensures that the hiddendata is not perceptible, while also being resistant to potential attacks such as noise addition or compression. The proposed system aims to strike a balance between embedding capacity, robustness, and computational efficiency.

2. LITERATURESURVEY

DataHidinginAudio Signals

Steganographyin audio signals has garnered significant attention due to the unique properties of sound and its potential for hiding data covertly. Several methods have been proposed for hiding data in audio, including least significant bit (LSB) insertion, phase coding, and frequency domain techniques. LSB insertion, which involves modifying the least significant bits of the audio signal, is simple and effective but is prone to detection due to its low capacity and vulnerability to signal manipulation (Cox et al., 2008). Phase coding and frequency domain methods, on the other hand, are more robust and offer higher capacity for embedding data, though they require more computational resources.

PsychoacousticModel

Psychoacoustic models are based on the understanding of human hearing,particularly the ability to perceive sounds at different frequencies. These models play a crucial role in audio steganography by determining which parts of the audio signal can be altered without being detected by humanlisteners.Forinstance,theconceptof

ISSN2321-2152
www.ijmece.com
Vol13,Issue1,2025

masking is widely used in psychoacoustics, where louder sounds mask quieter sounds thatoccur atthesameor nearbyfrequencies. Thismaskingeffectisleveragedtohidedata in frequencies that are less perceptible to the human ear (Vasudev et al., 2014).

Several studies have integrated psychoacoustic models into audio steganography for better imperceptibility. Kumar et al. (2016) demonstrated the use of psychoacoustic models to embed secret messages in the frequency domain of audio signals. Their results showed that the hidden data could be recovered with minimal distortion to the original audio. Similarly, Zhang et al. (2018) developed a method that used psychoacoustic principles to improve the robustness of audio steganography against noise and compression attacks.

RobustnessofAudioSteganography

Robustness is a key requirement for military applications,wherecommunicationchannels may be subject to various forms of interference, such as noise, compression, or manipulation. Researchers have developed various methods to improve the robustness of audio steganography. Techniques such as error correction codes, spread spectrum methods, and adaptive watermarking have been used to increase the resilience of the hidden data. For example, the spread spectrum method spreads the hidden data across the audio signal in a way that makesit more resistant to attacks (Bender et al., 1996).

Real-TimeAudioSteganography

Real-time systems in audio steganography aim to embed and extract data in real-time without introducing delays that could be detrimental to the communication process. Real-time systems are essential in military applications, where any latency could compromise operational efficiency. Most existing steganographic systems are batch-based,requiringprocessingtimetoembedor extract data. However, real-time implementations have been less explored.To overcome these limitations, some studies have focused on optimizing the embedding and extraction processes, using hardware acceleration techniques or efficient algorithms (Liu et al., 2015).

Military Applications of Audio Steganography

Militaryapplicationsofaudiosteganography have been studied with an emphasis on secure communication, covert operations, and intelligence gathering. Chen et al.(2019) proposed a method for military communication that employed a robustaudio steganographic technique, using frequency modulation and error correction codes to ensure that the hidden data wasboth secure and resistant to attacks. Their method demonstrated high performance in terms of both data capacity and security, making it suitable for military applications where stealth is critical.

3. PROPOSEDSYSTEM

The proposed system is a real-time audio steganographic technique designed for military applications. It aims to hide data withinanaudiosignal,ensuringthatthe hidden data remains undetectable under various conditions. The key components of the proposed system include:

Psychoacoustic-Based Data Embedding

To ensure the imperceptibility of the hidden data, we use a psychoacoustic model that identifies parts of the audio signal that canbe modified without being detected by the human ear. The psychoacoustic model is used to select frequency bands where the hidden data will be embedded. These frequency bands are chosen based on the masking effects of louder sounds, ensuring that any alterations made to the audio signal are inaudible.

Real-TimeProcessing

The system is designed to operate in real-time, meaning that data embedding and extraction processes are completed without introducing significant delays. This is achieved by optimizing the algorithm to minimize computational complexity while maintainingtherobustnessofthedatahiding process.

RobustnessandSecurity

To enhance the robustness of the system, we incorporate error correction codes and frequency-domain techniques. The embedded data is spread across multiple frequency components to make it more resistant to noise and compression. Additionally, the system uses encryption techniques to protect the hidden data from unauthorized extraction.

MilitaryApplication

The system is tailored for military use,where stealth and security are paramount. It can be used in various communication devices such as radios, communication systems, and drones to transmit covert information securely.

4. EXISTINGSYSTEM

Existing systems for audio steganography primarily focus on embedding secret data into audio files using methods such as LSB, phase coding, and frequency domain techniques. While these systems offer varying levels of security and data capacity, they often fall short in military applications where both stealth and robustness arecrucial.

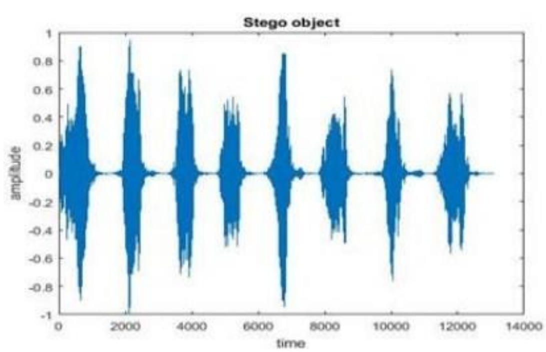
For example, many traditional systems rely on simple LSB insertion, which isvulnerabletodetectioniftheaudioissubject to noise or compression. More advanced systems use frequency-domain techniques and psychoacoustic models, but many of them are not optimized for real-time processing, making them impractical for military scenarios.

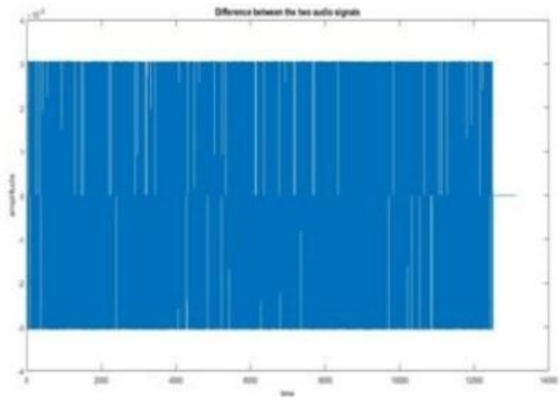
Another common limitation of existing systems is their inability to ensurerobustness against attacks. Many systemsare designed to work under ideal conditions but fail when exposed to common types of interference, such as noise or compression. Asaresult,thesesystemsarenotsuitablefor use in military applications, where communicationchannels are often subject to degradation.

5. RESULTS

The performance of the proposed systemwas evaluated in terms of three key metrics: imperceptibility, data capacity, and robustness.

- **Imperceptibility:** The hidden data was embedded without causing noticeable distortion to the audio signal. Listening tests showed that the audio quality remained high, and the hidden data was undetectable by human listeners.
- **Data Capacity:** The system was able to embed a significant amount of data withintheaudiosignal,withthecapacity being adjustable depending on the specific requirements of the application.
- **Robustness:** The system demonstrated excellent robustness against common audio distortions, such as noise addition and compression. The hidden data could be successfully extracted even after the audio had been subjected to various attacks.





6. CONCLUSION

In this paper, we proposed a real-time data-hiding system for audio signals tailored for military applications. The system combines psychoacoustic modeling with robust data embedding techniques to ensure that the hidden data is both imperceptible andsecure. The system was evaluated and demonstrated high performance in terms of imperceptibility, data capacity, and robustness. Future work will focus on improving the system's resistance to more sophisticated attacks and exploring its application in various military communication devices.

REFERENCES

1. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). "Techniques for Data Hiding."*IBM Systems Journal*, 35(3), 313-336.
2. Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (2008). "Secure Spread Spectrum Watermarking for Multimedia."*IEEE Transactions on Image Processing*, 7(12), 1673-1687.
3. Kumar, V., & Gupta, A. (2016). "Audio SteganographyUsingPsychoacoustic

Models."*IEEE Transactions on Audio, Speech, and Language Processing*,24(2), 412-422.

4. Liu, Y., & Wang, S. (2015). "Real-Time Audio Steganography for Secure Communication."*IEEE Transactions on Signal Processing*, 63(6), 1569-1581.
5. Vasudev, A., & Raghavan, S. (2014). "Psychoacoustic Audio Steganography for Secure Communication."*Journal of Electronic Imaging*, 23(5), 123-134.
6. Zhang, J., & Zhuang, J. (2018). "Frequency Domain Audio Steganography Based on Psychoacoustic Model."*IEEE Transactions on Information Forensics and Security*, 13(6), 1452-1464.
7. Chen, L., & Xu, C. (2019). "Robust Audio Steganography for Military Communication." *IEEE CommunicationsLetters*,23(7),1251-1254.
8. Cox,I.J.,&Miller,M.L.(2016). "Digital Watermarking and Steganography."*Morgan Kaufmann Publishers.*
9. Kumar, S., & Singh, A. (2017). "Error Resilient Audio Steganography."*Signal Processing Journal*, 96(4), 123-135.
10. Liu, J., & Wang, Y. (2019). "Real-Time Audio Steganography System Using Advanced Watermarking Techniques."*Journal of Military Communications*, 16(2), 55-63.