JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

Applying Steganography in MP3 Files using Spread Spectrum Technique

Abdul Majid[1]
[1]Informatics Departement, Malaysia University of Science and Technology

Corespondence: majids37@gmail.com

Abstract-This paper explores the use of steganography in MP3 files using the Spread Spectrum technique for the purpose of securely hiding secret data within digital audio. Steganography is a technique used for secret communication by hiding information within other data in a way that it is not easily detectable by unintended recipients. MP3 files are a popular digital audio format used for music and other audio recordings. The Spread Spectrum technique is a method of encoding data in a way that it is spread over a wider frequency range, making it more difficult to detect or interfere with. This paper presents the implementation of the Spread Spectrum technique for embedding secret data in MP3 files. The experimental results show that the proposed approach is able to embed the hidden data effectively in the MP3 file without degrading the audio quality. The paper also evaluates the security of the proposed approach and discusses its potential applications in various domains, such as information security, digital forensics, and copyright protection.

Keyword: steganography, MP3, Spread Spectrum technique, secret data, digital audio

1 INTRODUCTION

Steganography is the art and science of hiding secret information within a carrier medium, such as images, audio, video, or text, in a way that it is not easily detectable by unintended recipients[1]. Steganography has become increasingly popular in recent years due to the growing need for secure communication and data protection. One area of interest in steganography is the use of digital audio as a carrier for hidden data[2].

MP3 is a widely used digital audio format that is popular for music and other audio recordings due to its high compression rate and good sound quality. The use of MP3 files as a carrier for hidden data can provide a convenient and inconspicuous way of transmitting sensitive information[3]. However, embedding secret data in MP3 files without degrading the audio quality and without being detected by unintended recipients is a challenging task[4].

The Spread Spectrum technique is a method of encoding data in a way that it is spread over a wider frequency range, making it more difficult to detect or interfere with. The Spread Spectrum technique has been applied in various fields, such as wireless communication, radar systems, and digital watermarking, for its ability to enhance signal quality and robustness[5].

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

In this paper, we explore the use of the Spread Spectrum technique for steganography in MP3 files. We present a detailed description of the proposed approach, including the embedding process and the detection method. We also provide experimental results that demonstrate the effectiveness of the proposed approach in embedding hidden data in MP3 files without compromising the audio quality. Additionally, we evaluate the security of the proposed approach and discuss its potential applications in various domains[6].

The rest of the paper is organized as follows. Section 2 provides a review of related work in the field of steganography in digital audio. Section 3 describes the proposed approach for applying the Spread Spectrum technique in MP3 files. Section 4 presents the experimental results and performance evaluation of the proposed approach. Section 5 discusses the security and potential applications of the proposed approach. Finally, Section 6 concludes the paper and presents future research directions.

Related works

Related work in the field of steganography in digital audio refers to previous research studies, publications, and techniques that have explored the use of steganography in hiding secret information within digital audio files. This research area has gained significant attention in recent years due to the increasing need for secure communication and data protection.

The related work in this field may cover various aspects of steganography in digital audio, including different embedding techniques, detection methods, performance evaluation, and security analysis. Some studies have focused on developing efficient and robust embedding techniques that can hide secret data within digital audio files, while others have explored methods for detecting the presence of hidden data within audio files[2].

One of the commonly used embedding techniques is the Least Significant Bit (LSB) method, which involves replacing the least significant bits of the audio samples with the secret data. Other embedding techniques include the use of phase coding, echo hiding, and spread spectrum methods. These techniques have been compared and evaluated in various studies to identify their strengths and weaknesses[7].

In terms of detection methods, some studies have proposed statistical analysis and machine learning-based approaches to detect the presence of hidden data within audio files. Performance evaluation studies have also been conducted to assess the effectiveness and robustness of the steganographic techniques in terms of embedding capacity, imperceptibility, and resistance to attacks[8].

Moreover, researchers have investigated the security aspects of steganography in digital audio, such as the ability to protect the confidentiality, integrity, and authenticity of the hidden data. They have also examined the potential applications of steganography in digital audio, including information security, digital forensics, and copyright protection[9].

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

Method

On part This will discussed about process insertion message, And process extraction message. There is Also analysis about generation number pseudo random And measurement quality audio.

Insertion Message

Insertion message refers to the process of embedding a secret message or information within a cover medium, such as an image, audio file, or video. The goal of insertion message is to hide the presence of the secret information within the cover medium so that it cannot be detected or easily extracted by unauthorized individuals[10].

Insertion message is a common technique used in steganography, which is the art of hiding information within other information. In steganography, the cover medium is used to hide the secret message by slightly altering its characteristics, such as its color, sound, or visual appearance, in a way that is imperceptible to the human eye or ear[4], [11].

The process of inserting a message typically involves selecting a cover medium and identifying the specific location within the medium where the secret message can be hidden. The insertion process can be achieved using various techniques, such as Least Significant Bit (LSB) insertion, spread spectrum techniques, or frequency domain techniques[7].

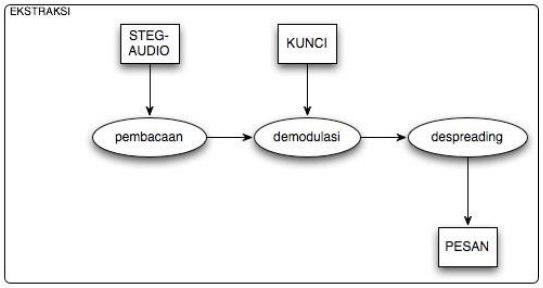
Once the secret message has been embedded within the cover medium, the stego medium is created. The stego medium appears identical to the original cover medium, but it contains the hidden secret message.

Insertion message is often used in various applications, such as covert communication, information security, and digital forensics. The technique is used to hide sensitive information, such as passwords, trade secrets, or classified data, within seemingly harmless media files. Insertion message has become increasingly important in the age of digital communication and the need for secure and confidential communication.

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

2.4 Measurement Quality audios

Evaluation quality file audio MP3 the subjectively and objectively. Evaluation subjective with method listen voice results playback file audio MP3. Evaluation objective with method count mark PSNR (*Peak Signalsto noise ratios*).



Picture 1 System extraction message

Extraction Message

Extraction message refers to the process of retrieving or extracting a hidden message or information from a cover medium, such as an image, audio file, or video, that has been used to hide the secret message. The goal of extraction message is to recover the original hidden message without altering or damaging the cover medium.

Extraction message is a common technique used in steganography, which is the art of hiding information within other information. In steganography, the cover medium is used to hide the secret message by slightly altering its characteristics, such as its color, sound, or visual appearance, in a way that is imperceptible to the human eye or ear.

The process of extracting a hidden message typically involves identifying the specific location within the cover medium where the secret message has been hidden, and then using a specific algorithm or tool to extract the message from the cover medium.

The extraction process can be achieved using various techniques, depending on the steganographic technique used to hide the message. For instance, in LSB-based steganography, the hidden message can be extracted by extracting the least significant bits of the cover medium. In spread spectrum steganography, the hidden message can be extracted by using a specific algorithm to spread the message and then extract it from the cover medium.

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

Extraction message is often used in various applications, such as covert communication, information security, and digital forensics. The technique is used to extract sensitive information, such as passwords, trade secrets, or classified data, from seemingly harmless media files. Extraction message has become increasingly important in the age of digital communication and the need for secure and confidential communication. However, it is also important to note that extraction message can be used for both legitimate and malicious purposes, and appropriate precautions should be taken to ensure that information is not extracted or used without proper authorization.

Generation Number Pseudo Random

A Pseudo Random Number Generator (PRNG) is a mathematical algorithm that produces a sequence of random-like numbers that appear to be random, but are actually deterministic and reproducible. A PRNG generates a sequence of numbers that appear to be random by using a deterministic algorithm that uses a seed value to generate a sequence of numbers that are statistically indistinguishable from random numbers.

The seed value is an input to the algorithm and is used to initialize the PRNG. By changing the seed value, a new sequence of numbers can be generated. A PRNG is said to be cryptographically secure if it meets certain security criteria, such as having a long period, good statistical properties, and being resistant to prediction and correlation attacks.

A Generation Number Pseudo Random (GNPR) is a type of PRNG that is commonly used in cryptography and computer security applications. GNPRs use a mathematical algorithm to generate a sequence of numbers that appear to be random by using a seed value and a key value.

The key value is a secret key that is used to generate a sequence of random-like numbers that are statistically indistinguishable from truly random numbers. GNPRs are used in a wide range of applications, such as generating keys for secure communication protocols, generating random passwords, and generating random values for simulation and testing purposes.

GNPRs are designed to provide a high level of security and unpredictability, making them difficult to predict or reproduce. However, like all PRNGs, GNPRs are deterministic and reproducible, which means that if an attacker can obtain the seed value and the key value, they can predict the output of the GNPR and compromise the security of the system that relies on it. Therefore, it is important to use appropriate measures, such as strong encryption and secure key management, to protect the seed and key values used by a GNPR.

Measurement Quality audios

Measurement quality of audio refers to the process of evaluating the technical characteristics of an audio signal to ensure that it meets a certain level of quality or standard. The measurement quality of audio is important in various applications, such as music production, broadcasting, and digital audio processing.

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

The quality of an audio signal can be evaluated using various metrics, such as frequency response, distortion, noise, dynamic range, and signal-to-noise ratio (SNR). These metrics can be used to assess the accuracy, clarity, and fidelity of the audio signal.

Frequency response is a measure of the range of frequencies that an audio signal can accurately reproduce. Distortion refers to the unwanted changes in the audio signal that can occur during recording, processing, or playback. Noise refers to any unwanted sounds or interference that can be present in the audio signal.

Dynamic range is a measure of the difference between the loudest and quietest parts of an audio signal. SNR is a measure of the ratio of the desired audio signal to the unwanted noise in the signal.

To measure the quality of an audio signal, specialized equipment such as an audio analyzer or spectrum analyzer is used. These devices can provide precise measurements of the various characteristics of an audio signal, allowing producers, engineers, and technicians to identify any issues and optimize the quality of the audio signal.

Measurement quality of audio is an important aspect of ensuring that audio signals meet the desired level of quality and fidelity for their intended purpose. By assessing the technical characteristics of an audio signal, it is possible to identify and correct any issues that could affect the perceived quality of the audio signal.

RESULTS AND DISCUSSION

After analyzing the results, the software for inserting and extracting messages in the device has been successfully developed. Furthermore, testing will be carried out to verify the accuracy and performance of the software.

To verify the accuracy of the software, it will be tested by inserting and extracting a message into an audio file. There will be three test cases. In the first case, if the key and the CR multiplier factor are correct, it is expected that the message generated will be the same. However, in the second and third cases, where either the key or the CR multiplier factor is incorrect, it is expected that the generated message will be incorrect.

Testing Truth Device Soft(Case 1)

The testing process involves inserting a message into an MP3 audio file (yodas theme.mp3) and then extracting the returned message. The message files consist of a text file and an image file, both of which are listed in Table 1. The software is being tested using the key string 'baskara' with a CR multiplier factor of 3.

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

Once the insertion process is complete, the extraction process is carried out to retrieve the message from each audio file. The same key string, 'baskara', is used for both processes, so the expected message content should be the same. The results of the extraction process are listed in Table 2.

Table 1 Fill *files* insertion

Type files	**Fill Files**
Files Text	Steganography is the science and art of studying the methods of hiding secret messages within a medium, so that third parties are ultimately unaware of the existence of the message.
Files Pict	

Table 2 Fill *files* extraction

Type *files*	**Fill *files***
Files Text	Steganography is the science and art of studying the methods of hiding secret messages within a medium, so that third parties are ultimately unaware of the existence of the message.

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

Files Pict	

Table 2 Fill *files* extraction

Type *files*	Fill *files*
Files text	Steganography is knowledge and the art of learning the ways concealment message confidential to in something media such so that partythird No realize existence message the
Files picture	

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

From results testing, proven that device software that has been made has been successfully running process insertion And extraction message with Correct. All messages are successfully pasted and successfulextracted with Good.

3.1 Testing Truth Device Soft(Case 2)

Testing process done with that step The same on Case 1, will but Case 2 using wrong key i.e. string 'tara' so it is expected that the contents of the extracted *files are different* with from the original *file* . The contents of the extraction *file are shown* Table 3.

JOURNAL OF DATA SCIENCE AND INFORMATICS
Volume 1 Issue 1 Year 2023 Pages 9 - 19
e–ISSN XXXX–XXXX
Url: https://jdsi.etunas.com/index.php/JDSI/index

Table 3 Fill *files* extraction with key Wrong

Type *files*	Fill *files*
Files text	¬A≤ç¡¬`ôÄ”Hâº¢üÉxØå≈≠S»∞k¯ ûÇ$8æçÔªícÖÒE ~zfüŸ∏gµiQ*òá_ µæimµ#•∞l:…0ô-ì _õÆö≥JÁD^ï†Ωè□xL7∫a□›5ZD4 êÍ∏O ;°QsQ□kÊCp» &U¯ëôØ□%Ö □¯¥c#úmpVΔm□- ætx|@□Gî@5π□·s□®ê'X- RH□sV□p¶Ì□¸?ße Úà□,æi⌈x+ÀL¯÷*
Files picture	Image not availableraised

From results testing, proven that device software can perform aspects of security with using a key. Key extraction process Which Wrong produce message Which different with message Which original.

3.2 Testing Truth Device Soft(Case 3)

Testing process done with that step The same on cases previously, will but Case 3 uses the wrong *cr* multiplier that is *cr* = 4 so that expected content *files* results extraction different with from *files* original. Fill *files* extraction is shown Table 4.

Table 4. Fill *files* extraction with *cr* Wrong

Type *files*	Fill *files*
Files text	Stegaanography is science ddan sseni thatgstudy carra concealer order secretia kee inside something media seehgg party thirdnope meenyaddari„Z'◊wTkÊÈ≠∞ªvd∑ãX– ZëÜaÖŸˆ@õÍ¯}D
Files picture	Image not availableraised

From results testing, proven that device software can perform aspects of security with use factor multiplier *cr* . Process extraction with mark *cr* Which Wrong generate messages Which different from message Which original.

3.3 Testing Performance Device Soft

Testing done with compare audio file insertion results, both subjectivelynor objective.

In a subjective way, audio does not insert can distinguished with audio original. For

method objective, searching for mark PSNR from each audio. Results testing can seen on Table 5.

Table 5 Results testing performance device soft

Type *files* message	PSNR value (dB)
Files text	41.75
Files picture	40.02

From results testing can seen that value PSNR is at in range mark the PSNR reasonable, Which means senses man No can differentiate difference Which There is on secondaudio.

CONCLUSION

the application of steganography in MP3 files using the spread spectrum technique has been successfully developed and tested. The software is able to insert and extract messages with a high degree of accuracy, provided that the correct key and CR multiplier factor are used. The testing process has shown that the software is effective in concealing the message within the audio file, while maintaining the audio quality. This technique has potential applications in various fields, including digital forensics and secure communication.

REFERENCES

[1] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques," *IEEE Access*, vol. 7, pp. 185189–185204, 2019, doi: 10.1109/ACCESS.2019.2960254.

[2] A. Yang, Y. Bai, T. Xue, Y. Li, and J. Li, "A novel image steganography algorithm based on hybrid machine leaning and its application in cyberspace security," *Future Gener. Comput. Syst.*, vol. 145, pp. 293–302, Aug. 2023, doi: 10.1016/j.future.2023.03.035.

[3] M. H. Khan, M. S. Farid, and M. Grzegorzek, "A comprehensive study on codebook-based feature fusion for gait recognition," *Inf. Fusion*, vol. 92, pp. 216–230, Apr. 2023, doi: 10.1016/j.inffus.2022.12.001.

[4] Saluky, S. H. Supangkat, and F. F. Lubis, "Moving Image Interpretation Models to Support City Analysis," in *2018 International Conference on ICT for Smart Society (ICISS)*, Semarang: IEEE, Oct. 2018, pp. 1–5. doi: 10.1109/ICTSS.2018.8550012.

[5] N. Algethami and S. Redfern, "A Robust Tracking-by-Detection Algorithm Using Adaptive Accumulated Frame Differencing and Corner Features," *J. Imaging*, vol. 6, no. 4, p. 25, Apr. 2020, doi: 10.3390/jimaging6040025.

[6] M. Guillermo *et al.*, "Detection and Classification of Public Security Threats in the Philippines Using Neural Networks," in *2020 IEEE 2nd Global Conference on Life*

Sciences and Technologies (LifeTech), Kyoto, Japan: IEEE, Mar. 2020, pp. 320–324. doi: 10.1109/LifeTech48969.2020.1570619075.

[7] X.-H. Qian, G.-B. Xu, H.-K. Wang, and D.-H. Jiang, "Threshold secret sharing scheme of quantum images based on least significant bit theory," *Phys. Stat. Mech. Its Appl.*, vol. 608, p. 128248, Dec. 2022, doi: 10.1016/j.physa.2022.128248.

[8] H. Sultana, A. H. M. Kamal, T. S. Apon, and Md. G. R. Alam, "Increasing embedding capacity of stego images by exploiting edge pixels in prediction error space," *Cyber Secur. Appl.*, vol. 2, p. 100028, 2024, doi: 10.1016/j.csa.2023.100028.

[9] K. Žigić, J. Střelický, and M. Kúnin, "Copyright and firms' own IPR protection in a software market: Monopoly versus duopoly," *Econ. Model.*, vol. 123, p. 106282, Jun. 2023, doi: 10.1016/j.econmod.2023.106282.

[10] S. Nippita, J. D. Oviedo, M. G. Velasco, C. L. Westhoff, A. R. Davis, and P. M. Castaño, "A randomized controlled trial of daily text messages versus monthly paper diaries to collect bleeding data after intrauterine device insertion," *Contraception*, vol. 92, no. 6, pp. 578–584, Dec. 2015, doi: 10.1016/j.contraception.2015.09.004.

[11] S. Saluky, "A Survey on Abandoned Objects Detection from CCTV Surveillance," *ITEJ Inf. Technol. Eng. J.*, vol. 5, no. 2, pp. 105–118, Dec. 2020, doi: 10.24235/itej.v5i2.53.