BIOS: Jurnal Informatika dan Sains
Volume 4 Number 01, 2026, DOI 10.54209/bios.v4i01
E.SSN 2988-6910(Online)
https://seaninstitute.or.id/bersinar/index.php/bios/index

Implementation of the Spread Spectrum Steganography Method for Embedding Secret Messages in Digital Image Media

Jonatan Carlos Rajagukguk[1], Yefta Roma Zebua[2], Wita Manik[3]
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas, Medan

Article Info
Corresponding Author:
Albert Julio Tampubolon

ABSTRACT
The development of information technology has increased the need for data security in the process of digital information exchange. In addition to cryptography, steganography has become an effective approach to maintaining data confidentiality by hiding messages within digital media without raising suspicion. One steganographic method with a high level of security is the Spread Spectrum method. This method works by spreading the message signal across a wide frequency spectrum so that it resembles noise and is difficult to detect. This study aims to examine and implement the Spread Spectrum steganography method in digital image media as a means of embedding secret messages. The method used includes the process of spreading the message using a pseudo-random code, embedding it into the image, and extracting the message on the receiver side. The results of the study indicate that the Spread Spectrum method is capable of hiding messages with a high level of imperceptibility and good robustness against disturbances. Therefore, this method is suitable for application in digital information security systems.
Keywords: Steganography, Spread Spectrum, Digital Image, Information Security

INTRODUCTION

The advancement of digital technology has had a significant impact on various aspects of life, particularly in the exchange of data and information. Information transmitted through computer networks and the internet is highly vulnerable to various security threats such as interception, manipulation, and data theft. This condition demands the existence of security mechanisms capable of protecting information from misuse by unauthorized parties. Therefore, information security has become a crucial aspect in modern communication systems.

So far, cryptography has been used to secure message content by transforming it into a form that cannot be read without a specific key. Although it is effective in protecting the content of messages, cryptography still has a weakness because the existence of encrypted messages can be detected and may raise suspicion. This can trigger attempts by other parties to break the encrypted message. As an additional solution, steganography has been developed to conceal the existence of the message itself by embedding it into digital media, making the message invisible and less likely to arouse suspicion.

One steganographic method that has high resistance to detection and interference is the Spread Spectrum method. This method adopts digital communication techniques by

spreading the message signal across a wide frequency spectrum, causing the hidden message to resemble natural noise in digital images. This uniform distribution of the message makes it difficult to detect or remove without knowledge of the spreading code. Therefore, research on the application of the Spread Spectrum method in digital image steganography is relevant and important as an effort to enhance digital information security. The objective of this study is to implement the Spread Spectrum steganography method to embed secret messages into digital image media effectively and securely.

LITERATURE REVIEW AND PROBLEM STATEMENT

Literature Review

Spread Spectrum is a communication technique originally developed for military purposes to enhance signal resistance against interference and eavesdropping. This technique works by spreading the information signal across a wide frequency spectrum, making it difficult to recognize and separate from noise. In the context of steganography, the Spread Spectrum method is used to distribute secret messages throughout the entire image with the help of pseudo-random codes, ensuring that the message is not concentrated in a specific area and is difficult to detect.

Several studies have shown that the Spread Spectrum method has advantages in terms of security and robustness compared to classical steganography methods such as Least Significant Bit (LSB). The LSB method is relatively easy to implement but is more vulnerable to image manipulation and statistical analysis. In contrast, Spread Spectrum provides better resistance to interference and detection attempts because the hidden message resembles natural noise within the image.

Digital images are chosen as the embedding medium due to their high data redundancy and widespread use in everyday data exchange, such as on social media and digital communication platforms. This redundancy allows secret messages to be embedded without causing significant visual changes. The combination of steganography and the Spread Spectrum method enhances message security while maintaining image quality, enabling secret messages to be hidden effectively without raising suspicion.

Problem Statement

Based on the literature review, the problems addressed in this study are:

1. How is the implementation process of the Spread Spectrum method in digital image steganography?
2. How effective is the Spread Spectrum method in hiding secret messages without degrading image quality?
3. What is the level of security of the Spread Spectrum method against detection and interference?

Characteristics of the Spread Spectrum Method in Steganography

The Spread Spectrum method has the main characteristic of distributing the message signal widely and uniformly across the media domain. This characteristic ensures that the hidden message is not localized in a specific area, making it difficult to detect through visual or statistical analysis. In steganography, this feature is highly advantageous because the hidden message resembles natural noise already present in digital images.

In addition, the Spread Spectrum method is key-dependent, meaning that both the embedding and extraction processes rely heavily on the pseudo-random code used. Without the same key, the message cannot be correctly reconstructed. This provides an additional

layer of security compared to simple steganographic methods that do not use key-based spreading mechanisms.

In terms of robustness, Spread Spectrum is known for its strong resistance to minor disturbances such as noise addition or slight image manipulation. This is because the message is distributed across the entire image, so losing a small portion of the data does not immediately eliminate the entire hidden message.

RESEARCH METHODOLOGY

Spread Spectrum Method

The Spread Spectrum method works by distributing the message signal across a wide frequency spectrum using a pseudo-random code. In steganography, the secret message is first converted into a binary signal, then multiplied by a spreading code to produce a spread signal.

Research Procedure

The steps carried out in this study are as follows:

1. Preparing a digital image as the embedding medium
2. Converting the secret message into binary form
3. Generating a pseudo-random code as the spreading code
4. Performing the spreading process on the message
5. Embedding the spread signal into the image
6. Extracting and despreading to retrieve the original message
7. Stages of the Spread Spectrum Method

Conversion of Message into Binary Form

The secret message in text form is first converted into binary so it can be processed digitally. Each character is encoded using an 8-bit ASCII representation. This stage is important to ensure that the message can be evenly distributed within the image and is not easily detected.

Generation of Pseudo-Random Code

The pseudo-random code is used as a secret key in the Spread Spectrum method. It functions to distribute the message throughout the image so that it resembles noise.

Characteristics of the pseudo-random code:

a. Random in nature
b. Reproducible with the same seed
c. Difficult to predict without knowing the key

The security of the system heavily depends on the confidentiality of this code.

Message Spreading Process

The binary message is multiplied by the pseudo-random code to produce a spread signal. This process ensures that the message is not localized in a specific part of the image but distributed across the entire image. Advantages of this stage include:

a. The message is difficult to detect
b. More resistant to image manipulation
c. Resembles natural noise

Embedding into Digital Image

The spread signal is embedded into the pixel values of the digital image with low intensity so that it does not significantly affect visual quality. The embedding process is carefully performed to:

a. Avoid noticeable changes
b. Maintain image quality
c. Ensure the message can still be extracted

Extraction and Despreading Process

On the receiver side, extraction is performed using the same pseudo-random code. The hidden signal is extracted and then despread to recover the original binary message. If a different code is used, the message cannot be correctly reconstructed, thereby ensuring security.

Research Tools and Materials

Software

1. Python programming language
2. Digital image processing libraries
3. Windows operating system

Hardware

1. Laptop/PC
2. Storage media

Research Data

1. Digital images in JPG/PNG format
2. Secret messages in text form

Testing Parameters

The evaluation is conducted to assess the performance of the Spread Spectrum method based on the following parameters:

1. Imperceptibility
   Measures the visual difference between the original image and the stego image.
2. Extraction Accuracy
   Measures whether the message can be completely and correctly extracted.
3. Conceptual Security
   Evaluates the method's resistance to detection compared to the LSB method.

Explanation of Testing Parameters

Testing parameters are used to evaluate the performance of the developed steganographic system. The imperceptibility parameter is used to assess how noticeable the difference is between the original image and the stego image. The smaller the visible difference, the better the quality of the steganographic method applied.

Successful message extraction is the main indicator that the system is functioning properly. The extracted message must be identical to the original message without any loss or alteration. Meanwhile, the conceptual security parameter is used to evaluate the resistance of the Spread Spectrum method to detection and interference compared to simpler steganographic methods.

System Preparation

The steganographic system in this study is built using the Python programming language, supported by several digital image processing libraries. This programming language is chosen due to its extensive libraries and efficient support for image matrix processing. In the preparation stage, the digital image used as the embedding medium is ensured to be in good condition and suitable for computational processing. The image is tested beforehand to ensure there is no data corruption and that it has adequate visual quality.

After embedding the secret message using the Spread Spectrum method, the stego image is re-evaluated to observe any changes in visual quality. This evaluation aims to ensure that the embedding process does not produce significant visual differences between the original and the stego image, so that the presence of the hidden message is not easily detected by human observers. With this system preparation stage, it is expected that both the embedding and extraction processes can run optimally, resulting in a secure and reliable steganographic system.

RESULTS AND DISCUSSION

System Testing Results

System testing was conducted to evaluate the successful implementation of the Spread Spectrum Steganography method in embedding and extracting secret messages within digital audio media in WAV format. The system implementation was tested using a GUI-based application developed in Python (Tkinter).

Results of Message Embedding Execution

At this stage, the user selects a WAV audio file as the cover medium and inputs a text message as the secret message. The system then performs the embedding process using the Spread Spectrum method with a predefined secret key.

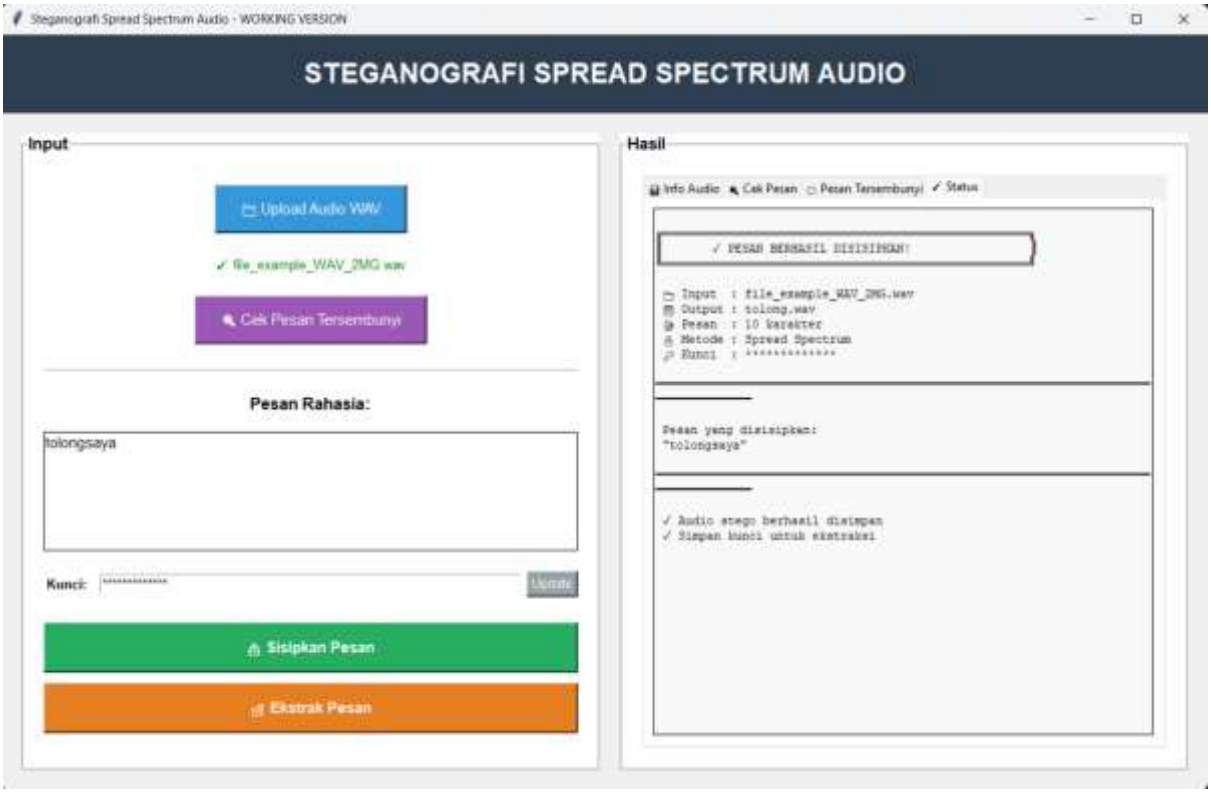


Figure 1. Spread Spectrum Steganography Application

Execution Results

The execution results show that:

1. The WAV audio file was successfully loaded, and its information was displayed, including the number of channels, sample rate, number of frames, audio duration, and estimated message capacity.
2. The secret message was successfully converted into binary data and embedded into the audio signal.

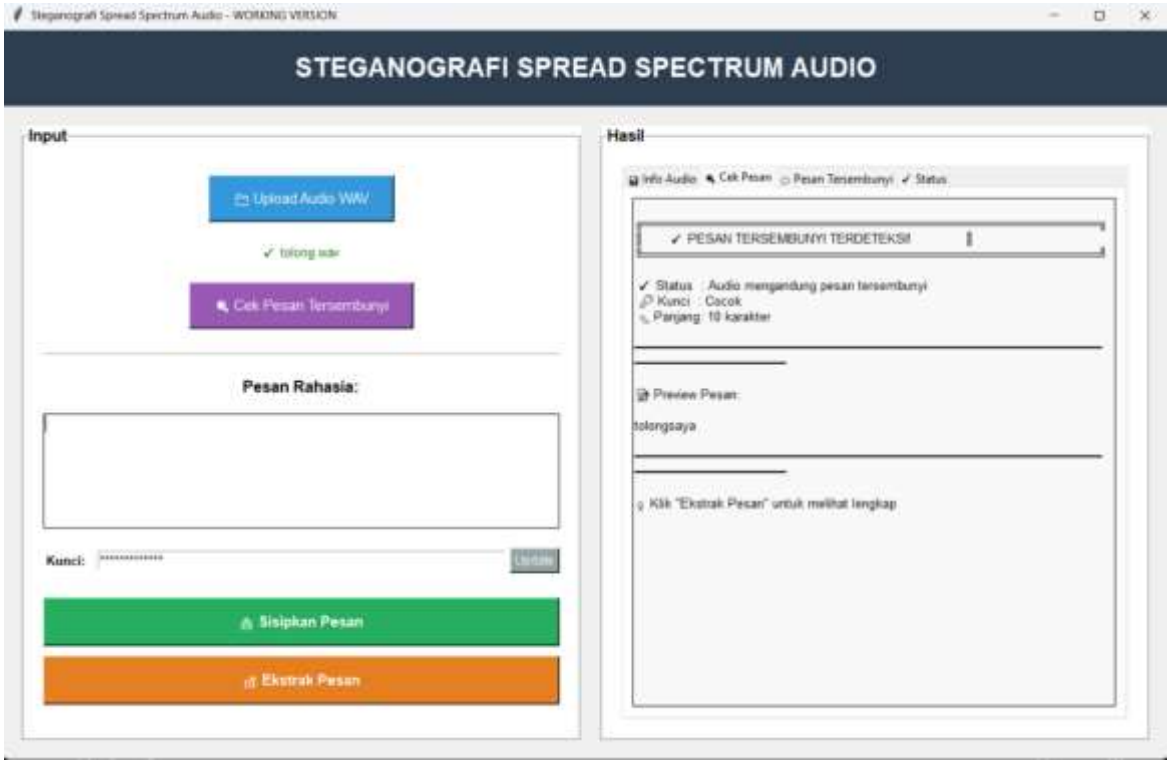
3. The system generated a new audio file (stego audio) without significant changes in audio quality perceptible to human hearing.
4. The embedding process ran without errors as long as the message length did not exceed the audio capacity.

Visually, the application displays the status *"Message Successfully Embedded"*, along with information on message length, the method used, and the name of the steganography output file.

Results of Message Extraction Execution

The extraction stage is carried out by reloading the stego audio file that contains the hidden message. The extraction process uses the same secret key as the embedding process.

Figure 2. Extraction Process



Extraction Testing Results

The extraction testing results show that:

1. The system is able to read the audio signal and regenerate an identical pseudo-noise sequence.
2. The message length information is successfully detected through the message header embedded at the beginning of the audio data.
3. The secret message can be fully extracted and is identical to the original message.
4. No character loss or decoding errors occur as long as the audio file has not been manipulated.

Discussion

Analysis of the Effectiveness of the Spread Spectrum Method

The Spread Spectrum method works by distributing the message signal across the entire audio signal domain using a pseudo-noise sequence. Based on the test results, this method has proven to be effective due to the following factors:

a. Imperceptibility (Invisibility)

The changes in the audio signal caused by message embedding are very minimal due to the use of a low strength parameter. This results in the difference between the original audio and the stego audio being nearly undetectable by human hearing. In other words, the audio quality remains preserved even after the message has been embedded.

b. Security
The security of the system heavily depends on the secret key used to generate the pseudo-noise sequence. Without the correct key, an external party cannot reconstruct the signal spreading pattern, making the message impossible to extract. This provides a significant additional layer of security compared to simpler steganography methods.

c. Robustness (Resistance)
Since the message is spread across the entire audio signal, the method demonstrates good resistance to minor disturbances such as noise addition or small signal modifications. Unlike the LSB method, which stores data at specific positions, Spread Spectrum can still preserve information even if part of the data is damaged.

In addition, this method shows fairly strong robustness against minor interference. Because the message is distributed throughout the audio signal, damage to a small portion of the data does not immediately eliminate the entire information. This is different from methods such as LSB, which store data at specific positions and are therefore more vulnerable to changes. Thus, Spread Spectrum is more resistant to noise or small manipulations that commonly occur during digital data transmission.

However, this method still has several limitations. One of the main challenges is its sensitivity to large-scale signal manipulations, such as lossy compression or audio format conversion. These processes can significantly alter the signal structure, thereby disrupting the message extraction process. In addition, the selection of parameters such as the strength value must be done carefully, because if it is too high it may degrade audio quality, while if it is too low it may reduce extraction success.

Overall, this discussion shows that the Spread Spectrum method is able to provide a balance between media quality, message security, and resistance to interference. These advantages make it a promising approach in the development of steganography systems, especially for digital audio media. With further development, this method can be optimized for various conditions and more complex information security requirements.

System Performance Analysis

Based on the conducted experiments:

1. The system is able to dynamically adjust the message length according to the audio media capacity.
2. The execution time is relatively efficient because the computation process is carried out using an optimized numerical library (NumPy).
3. The GUI-based interface provides ease of use, even for non-technical users.

However, the system has several limitations:

1. The system only supports the WAV audio format, making it less flexible for other formats such as MP3 or AAC.
2. The method is quite sensitive to heavy signal manipulation, especially lossy compression, which can damage the signal structure and remove hidden information.

3. The strength parameter must be carefully adjusted, as excessively high values may significantly degrade audio quality.

CONCLUSION

Based on the results of the research and discussion on the implementation of the Spread Spectrum steganography method for embedding secret messages in digital audio media, the following conclusions can be drawn: The Spread Spectrum method has been proven effective in hiding secret messages within WAV audio media with a high level of imperceptibility. The difference between the original audio and the stego audio is almost indistinguishable by human hearing. The system implementation using Python with the NumPy and Wave libraries was successfully carried out. The system is able to perform both embedding and extraction processes accurately using a pseudo-random sequence generated from a secret key. Message security is ensured through the use of a secret key, which is converted into a seed for generating the pseudo-noise sequence. Without the correct key, the message cannot be properly extracted. The Spread Spectrum method demonstrates good robustness against minor disturbances. The distribution of the message across the entire audio signal domain makes this method more resistant compared to simpler methods such as Least Significant Bit (LSB). The GUI interface developed using Tkinter makes it easier for users to perform audio uploading, message embedding, and message extraction without requiring deep technical knowledge. Message embedding capacity depends on the length of the audio and the parameters used. The longer the audio duration, the greater the message capacity that can be embedded. The system has limitations in terms of supported audio format (only WAV) and sensitivity to heavy audio manipulation such as lossy compression. Based on the results of the study and discussion, several suggestions can be considered for future research development. This study still has room for improvement in terms of method, media, and system evaluation. Future research is recommended to extend the Spread Spectrum method to other digital media such as color images, videos, or audio in various formats, to evaluate its performance across different media types. In addition, testing under various manipulation conditions such as compression, noise addition, or resizing should be conducted to measure the robustness of the method more comprehensively. From the implementation perspective, the steganography system can be enhanced by adding quantitative evaluation parameters such as Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) to provide a more objective analysis of the stego media quality. The use of additional security techniques, such as a combination of steganography and cryptography, is also recommended to improve message security. Furthermore, the development of a more interactive system interface and support for multiple platforms is expected to improve usability. With these improvements, the Spread Spectrum method is expected to be more widely applicable in future digital information security systems.

REFERENCES

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons.Cox et al. (2007) - Digital Watermarking

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. Boca Raton: CRC Press.Gopalan (2003) - Audio steganography

Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Boston: Artech House.Katzenbeisser & Petitcolas (2000) - Information hiding

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography*. Burlington: Morgan Kaufmann.Marvel et al. (1999) - Spread spectrum steganography

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Boston: Pearson Education.Petitcolas et al. (1999) - Information hiding survey

Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. *IEEE Journal on Selected Areas in Communications*, 16(4), 474–481.Schneier (1996) - Applied cryptography

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *IEEE Computer*, 31(2), 26–34.Stallings (2017) - Network security

Marvel, L. M., Boncelet, C. G., & Retter, C. T. (1999). Spread spectrum image steganography. *IEEE Transactions on Image Processing*, 8(8), 1075–1083.

Gopalan, K. (2003). Audio steganography using bit modification. *IEEE International Conference on Acoustics, Speech, and Signal Processing*.

Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color and gray-scale images. *IEEE Multimedia*, 8(4), 22–28.

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, 1(3), 32–44.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding – A survey. *Proceedings of the IEEE*, 87(7), 1062–1078.

Simmons, G. J. (1984). The prisoners' problem and the subliminal channel. *Advances in Cryptology (CRYPTO '83)*, 51–67.