Journal Majelis Paspama
Volume 2, Number 2, 2024 (No 138-144)
E.SSN 2987-1379 (Online)

Implementation of the Phase Coding Steganography Method for Embedding Secret Messages in Audio Media

Daniel S. Simbolon[1], Daniel Adrian Sirait[2], Stephen Gilbert R. Gulo[3]
Program Studi Teknik Informatika, Universitas Katolik Santo Thomas

Article Info
Corresponding Author:
Daniel S. Simbolon

ABSTRACT
The development of information technology has driven an increasing need for data security, particularly in the transmission of secret messages through digital media. One technique that can be used to maintain information confidentiality is steganography, which is the method of hiding messages within other media without causing noticeable changes. This study aims to implement the Phase Coding steganography method for embedding secret messages into digital audio media, so that the message is not easily detected by unauthorized parties. The Phase Coding method works by modifying the phase of the audio signal without significantly altering its amplitude, thereby maintaining audio quality and making it difficult to distinguish from the original audio by human hearing. In this study, the process includes preparing the audio file as a cover, converting the secret message into binary form, embedding the message using the Phase Coding technique, and extracting the hidden message. The implementation is carried out using a programming language to test the success of both embedding and retrieving the message. The results show that the Phase Coding method is capable of embedding secret messages into audio media with good performance without significantly degrading audio quality. The secret message can also be accurately extracted and recovered in its original form. Therefore, the Phase Coding steganography method can be considered an effective solution for securing information in audio-based media.

Keywords: Phase Coding Steganography, Secret Message Embedding, Audio Media

This is an open access article under the CC BY-NC license

INTRODUCTION

The rapid development of digital technology has brought significant impacts on the exchange and storage of information. Data in the form of text, images, audio, and video can now be easily transmitted through the internet. However, this convenience is also accompanied by increased information security risks, such as eavesdropping, data manipulation, and theft of confidential messages. Therefore, a technique is needed to maintain message confidentiality so that it cannot be easily accessed by unauthorized parties.

One approach that can be used to secure information is steganography. Unlike cryptography, which transforms messages into unreadable forms, steganography hides messages within a cover medium so that the existence of the message itself is not apparent. Audio media is one of the attractive choices for steganography because it has complex signal characteristics and a high tolerance for small modifications, allowing message embedding without significantly degrading audio quality.

The Phase Coding method is one of the audio steganography techniques that utilizes modifications in the phase of audio signals to embed secret messages. This method is chosen because phase changes are relatively difficult to detect by human hearing compared to amplitude changes. In this study, the Phase Coding method is implemented to embed secret messages into digital audio media, with the aim of testing embedding success, maintaining audio quality, and ensuring that the message can be accurately extracted.

LITERATURE REVIEW AND PROBLEM STATEMENT

Audio steganography has been widely studied as a method for hiding confidential information by exploiting the characteristics of sound signals. Several commonly used audio steganography methods include Least Significant Bit (LSB), Echo Hiding, and Phase Coding. The LSB method is relatively easy to implement but is vulnerable to attacks and signal modifications, while Echo Hiding utilizes the addition of echoes that are difficult to detect by human hearing. Meanwhile, the Phase Coding method works by modifying the phase of the audio signal and is known to have a high level of transparency because phase changes are difficult to distinguish by the human auditory system. Several studies have shown that Phase Coding can maintain good audio quality and offers better robustness compared to simpler audio steganography methods.

Although the Phase Coding method has advantages in maintaining audio quality and message confidentiality, its implementation still requires a solid understanding of digital signal processing and message embedding mechanisms. The problem addressed in this study is how to implement the Phase Coding steganography method on digital audio media to embed secret messages effectively, as well as how to evaluate the success rate of message extraction and the quality of the audio after the embedding process. Therefore, this research focuses on the design and implementation of the Phase Coding method and the evaluation of secret message embedding results in audio media.

METHOD

The research method used in this study is an experimental method, which involves designing, implementing, and testing an audio steganography application using the Phase Coding method. The system is developed as a Python-based desktop application with a graphical user interface to facilitate the processes of embedding and extracting secret messages. The media used in this study is digital audio in WAV format. The research stages consist of several interrelated steps, as follows.

Work Folder Creation

The initial stage involves creating a working folder used to store all supporting files in the research, including:

1. Audio steganography application source code,
2. Original WAV audio files,
3. Stego audio files (audio with embedded messages).

This working folder is created to simplify data management and maintain an organized research structure.

Data Preparation

At the data preparation stage, the user selects a digital audio medium through the “Upload WAV Audio” feature available in the application interface. The WAV format is chosen because it is lossless, allowing phase modifications to be performed without significantly

degrading audio quality. In addition, the audio is converted into mono form to simplify signal analysis using FFT.

Message Embedding Process (Embedding)

After the audio media is successfully uploaded, the user inputs a secret message in text form through the application. The system then processes the message by converting it into binary representation. Next, the system applies the Phase Coding method by transforming the audio signal from the time domain into the frequency domain using the Fast Fourier Transform (FFT).

In the frequency domain, the system modifies the phase of the audio signal at certain frequency components according to the binary values of the secret message, without changing the magnitude of the signal. After the embedding process is completed, the signal is transformed back into the time domain using the Inverse FFT (IFFT) and saved as a stego audio file.

Message Extraction Process (Extraction)

At the extraction stage, the system reads the stego audio file and applies FFT again to analyze the phase of the audio signal. The secret message bits are extracted based on the phase values that were modified during the embedding process. The extracted binary data is then converted back into text form and displayed in the “Hidden Message” section of the application.

The test results show that the secret message can be successfully extracted and matches the original message without any changes. This proves that the implemented Phase Coding method has a high level of accuracy and is able to maintain audio quality transparency, making it effective for securing information in digital audio media.

RESULTS AND DISCUSSION

Based on the implementation results, the Phase Coding steganography method was successfully applied to digital audio media in WAV format by utilizing the Fast Fourier Transform (FFT). The developed system, in the form of a Python-based desktop application, is capable of performing both embedding and extraction of secret messages automatically through a graphical user interface.

During the embedding stage, the secret message entered by the user is first converted into binary code. The binary message is then embedded into the audio signal by modifying the phase of selected frequency components in the frequency domain obtained from the FFT transformation. This process is carried out without altering the magnitude of the audio signal, so the resulting changes do not significantly affect audio quality. The test results show that the produced stego audio sounds almost identical to the original audio, making the presence of the hidden message difficult to detect by the Human Auditory System.

In the extraction stage, the application re-analyzes the phase of the stego audio signal to retrieve the embedded message bits. The extraction process continues until the system detects an end-of-message marker, after which the retrieved bits are converted back into text form. Based on the test results, the extracted secret message was successfully recovered in full and matched the original message without any alteration.

These results indicate that the Phase Coding method has a high level of extraction accuracy and is able to maintain good stego-audio quality. In addition, the implementation in a desktop application simplifies the steganography process for users without requiring direct

interaction with the program code. Therefore, the Phase Coding method can be considered effective for hiding confidential information in digital audio media.

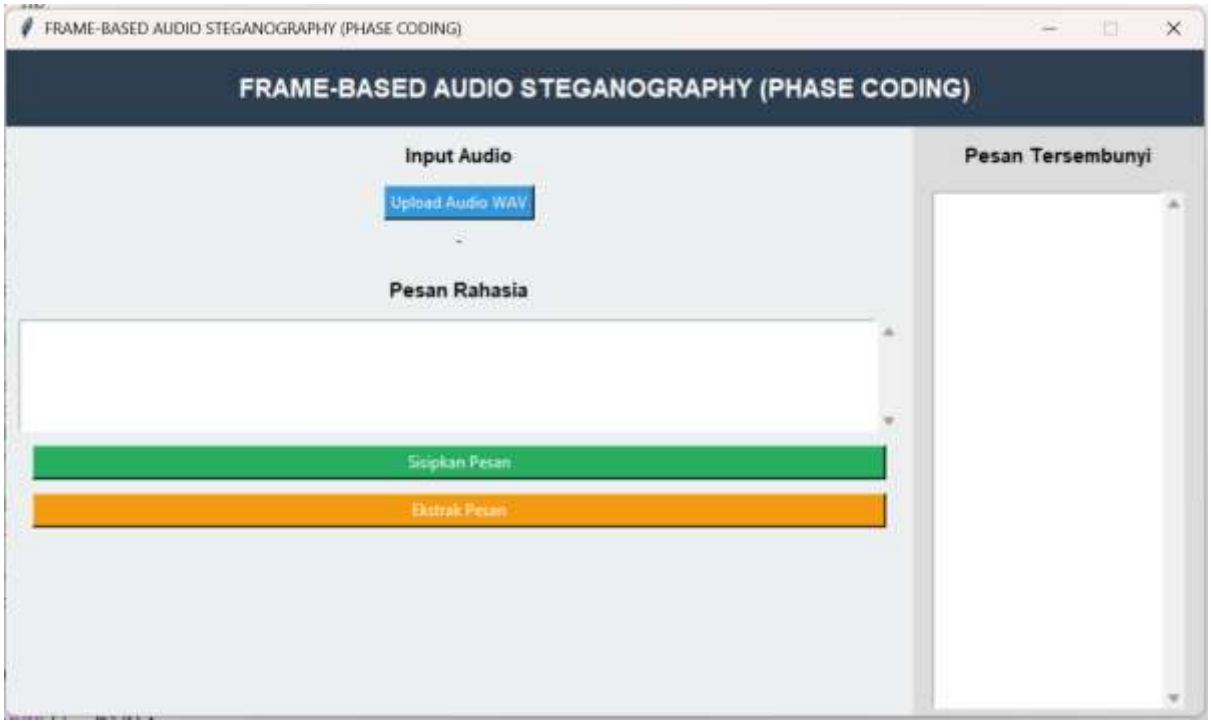

Figure 1. Initial Interface of the Phase Coding Audio Steganography Application

The initial interface of the Frame-Based Audio Steganography (Phase Coding) application. In this interface, the user can select an audio file in WAV format and prepare a secret message that will be embedded into the audio.

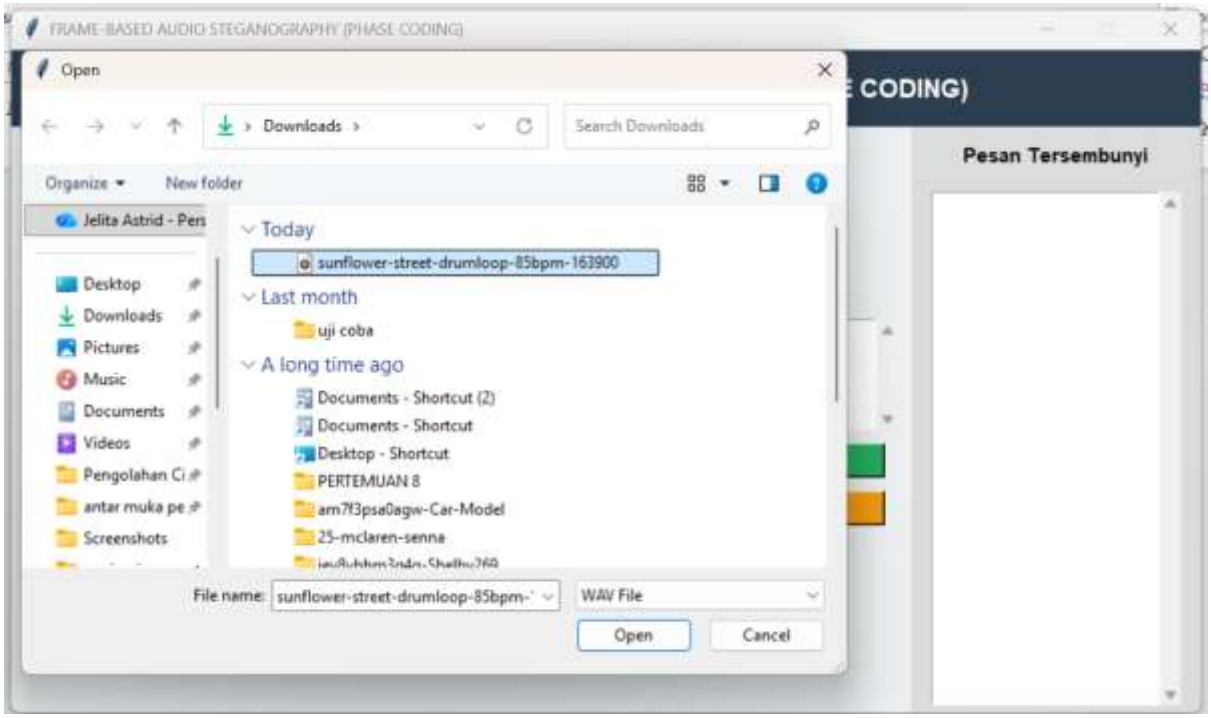

Figure 2. WAV Audio File Selection Process as Cover Media

The process of selecting a WAV audio file through the “Upload WAV Audio” feature. The selected audio file is used as the medium for embedding a secret message using the Phase Coding method.

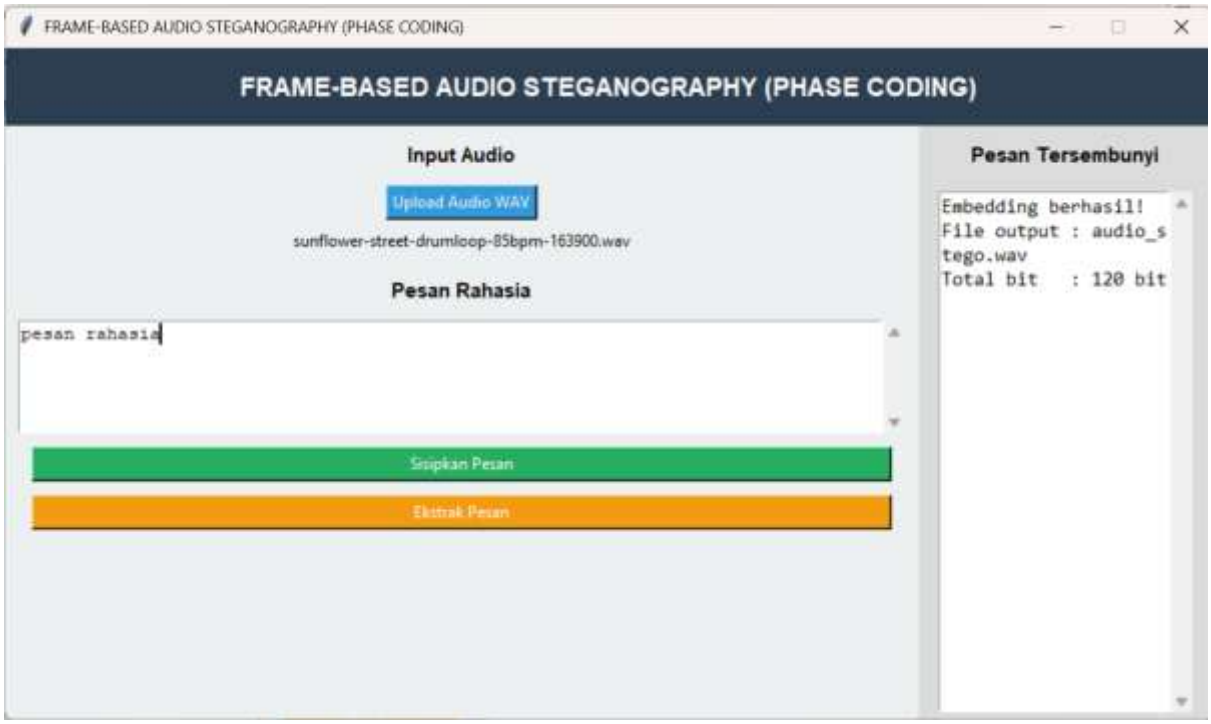

Figure 3. Result of Secret Message Embedding into Audio (Stego Audio)

The result of the secret message embedding process into the audio. The system displays information indicating that the embedding process was successful, including the generated stego audio filename and the number of message bits successfully embedded.

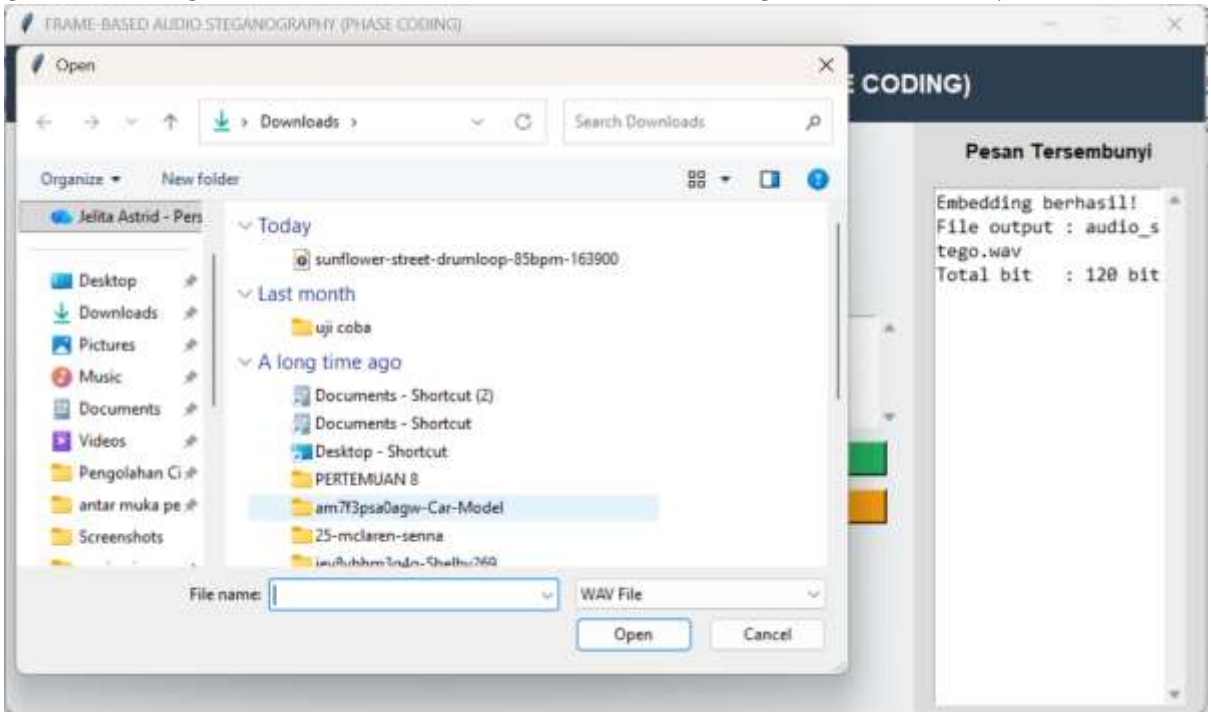

Figure 4. Selection Process of Stego Audio for Secret Message Extraction

The process of selecting the stego audio file used for secret message extraction. The stego audio file is selected through an Open File dialog and then analyzed by the system to retrieve the hidden message.

This research shows that the Phase Coding method has a major advantage in maintaining audio quality after the embedding process. This is because the modifications occur only in the phase of the signal, not in the amplitude, so it does not produce audible distortion for humans. Therefore, this method is highly suitable for audio steganography applications that require a high level of transparency.

In addition, the perfect accuracy achieved in message extraction demonstrates that the method has good reliability in maintaining data integrity. The fact that the extracted message remains unchanged proves that the system is able to preserve information completeness even after undergoing transformations between the time domain and frequency domain.

From a security perspective, the Phase Coding method is superior to simpler methods such as Least Significant Bit (LSB), because phase modifications are more difficult to detect both visually through signal analysis and auditorily. This makes the method more resistant to detection attempts and basic attacks aimed at revealing hidden messages.

However, this study still has limitations, particularly in terms of relatively low message embedding capacity compared to other methods. In addition, this research has not yet tested the robustness of the method against various attacks such as audio compression (e.g., MP3), noise addition, or other signal manipulations. Therefore, future research is recommended to evaluate the robustness of the Phase Coding method under these conditions and to develop hybrid techniques to improve both capacity and security of message embedding.

CONCLUSION

Based on the design, implementation, and testing conducted in this study, it can be concluded that the Phase Coding steganography method was successfully applied to embed secret messages into digital audio media. The embedding process is performed by modifying the phase of the audio signal without significantly altering its amplitude, so that the resulting audio quality remains natural and does not produce noticeable differences to listeners. The test results show that secret messages can be embedded and extracted correctly in accordance with the original message. This demonstrates that the Phase Coding method has a good level of reliability in maintaining message integrity and is able to preserve audio quality after the embedding process. In addition, the phase modifications used in this method are relatively difficult to detect by the human auditory system, making the presence of hidden messages not easily identified by unauthorized parties. Therefore, the Phase Coding method can be considered an effective alternative for securing information in audio-based media. This study also shows that audio steganography has great potential for further development, particularly in improving embedding capacity, enhancing robustness against disturbances, and implementing it in more complex information security systems.

REFERENCES

1. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal, 35*(3–4), 313–336.
2. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital watermarking and steganography* (2nd ed.). Morgan Kaufmann.

3. Djebbar, F., & Ayad, B. (2014). Audio steganography by phase modification. Dalam *Proceedings of SECURWARE 2014*. Lisbon, Portugal.
4. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information hiding: Steganography and watermarking – Attacks and countermeasures*. Kluwer Academic Publishers.
5. Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*. Artech House.
6. Kaur, A., & Singh, K. (2016). A review on audio steganography techniques. *International Journal of Computer Applications, 150*(1), 15–19.
7. Saragih, R. A. (2006). Metode parity coding versus metode spread spectrum pada audio steganography. Dalam *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.
8. Sayed, M. H., & Wahbi, T. M. (2024). Information security for audio steganography using a phase coding method. *European Journal of Theoretical and Applied Sciences, 2*(1).
9. Sembiring, Z. (2017). Perbandingan metode low bit coding dengan phase coding pada digital audio watermarking. *Journal of Informatics and Telecommunication Engineering*.
10. Yang, G. (2025). An improved phase coding audio steganography algorithm. *Journal of The Colloquium for Information Systems Security Education, 12*(1). https://doi.org/10.53735/cisse.v12i1.195