Login : Jurnal Teknologi Komputer
ISSN : 2302-9692 (print) | 2723-8695 (online)
Vol. 18, No. 02, 2024, pp. 102-106
LOGIN http://login.seaninstitute.org/index.php/Login

The Implememtation Of Hiding Information By Using Discrete Wavelet Transform (DWT)

Devi Silvia Simbolon[1], Kevin Enrique Keliat[2], Kristian Sigalingging[3], Vicky Nainggolan[4], Rifelson Sipayung[5]
Fakultas Ilmu Komputer Universitas Katolik Santo Thomas, Jl. Setia Budi No. 479F, Tanjung Sari, Kec. Medan Selayang, Kota Medan, Sumatra Utara 20135 , Indonesia

Article Info

Keywords:

Steganography, Discrete Wavelet Transform, Signal Processing, Data Hiding, Digital Security.

ABSTRACT

Steganography using Discrete Wavelet Transform (DWT) is a technique for embedding information into an image without significantly altering its visual quality. This study aims to analyze the effectiveness of DWT in securing hidden messages within digital images. DWT decomposes image signals into approximation and detail coefficients, allowing data embedding in the high-frequency components while preserving the most essential image features. The research methodology involves converting secret messages into numerical form, applying DWT to the image, embedding data into the detail coefficients, and reconstructing the image using inverse DWT. The results show that this approach enables secure and imperceptible data hiding while maintaining image quality. Additionally, DWT provides advantages in signal analysis, data compression, and noise resistance, making it a robust technique for steganography. The study concludes that DWT is an effective method for secure data embedding with minimal distortion, offering potential applications in digital watermarking and confidential communication.

Corresponding Author:

Devi Silvia Simbolon
Fakultas Ilmu Komputer Universitas Katolik Santo Thomas, Jl. Setia Budi No. 479F, Tanjung Sari, Kec. Medan Selayang, Kota Medan, Sumatra Utara 20135 , Indonesia
E-mail: devisilvia03@gmail.com

1. INTRODUCTION

The rapid advancement of digital communication has led to an increasing demand for data security and confidentiality. The rise of cyber threats and unauthorized access has made information protection a critical concern. One of the methods used to ensure secure data transmission is steganography, a technique that conceals information within digital media, such as images, audio, or video, in a way that remains imperceptible to the human eye (Johnson & Jajodia, 1998).

Among various steganographic techniques, Discrete Wavelet Transform (DWT) has gained significant attention due to its ability to hide information efficiently while maintaining image quality (Kaur & Kaur, 2014) . DWT enables the decomposition of an image into different frequency components, allowing data embedding in high-frequency coefficients while preserving the most significant features of the image. Previous studies have demonstrated that DWT-based steganography offers better imperceptibility and robustness compared to spatial domain techniques, such as Least Significant Bit (LSB) substitution (Zhang et al., 2016).

The effectiveness of DWT in steganography depends on its ability to balance imperceptibility, security, and embedding capacity. Several researchers have proposed improvements to DWT-based steganographic methods to enhance data-hiding performance (Singh & Singh, 2020). However, further analysis is required to evaluate its potential in real-world applications.

This research aims to analyze the effectiveness of Discrete Wavelet Transform (DWT) in secure data embedding within digital images while maintaining image quality. The findings of this study are expected to contribute to the development of more secure and efficient steganographic techniques for digital communication and cybersecurity applications.

2. METHODS

Research Approach

This study applies the Discrete Wavelet Transform (DWT) method for steganography by embedding secret messages into an image while maintaining visual quality. The process involves several steps: data preparation, wavelet decomposition, data embedding, and inverse transformation for reconstruction.

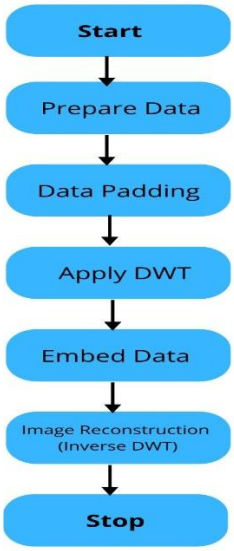

Figure 1. Flowchart

Data Preparation

The secret message is first converted into numerical format using ASCII encoding. The cover image is selected and preprocessed to ensure compatibility with DWT transformation. If necessary, padding is applied to adjust the image size to the power of two, ensuring optimal wavelet decomposition.

Discrete Wavelet Transform (DWT) Application

DWT is applied to the cover image, breaking it down into approximation (low-frequency) and detail (high-frequency) coefficients. Data is embedded into the high-frequency coefficients to minimize perceptible distortions. This study uses Haar wavelet filters for transformation due to their simplicity and efficiency.

Data Embedding Process

The numerical representation of the secret message is embedded into the high-frequency coefficients of the image. The embedding process modifies the wavelet coefficients in a way that maintains the integrity of the cover image while allowing for secure data hiding.

Image Reconstruction using Inverse DWT

After data embedding, inverse DWT is applied to reconstruct the image with the embedded message. This process ensures that the modified image retains its original appearance while securely storing hidden information.

3. RESULTS AND DISCUSSION

Implementation of Discrete Wavelet Transform (DWT) in Steganography

The implementation of Discrete Wavelet Transform (DWT) in steganography is carried out by dividing the image into frequency components and embedding secret data into the high-frequency

coefficients. DWT decomposes the signal into two parts: Detail Coefficients (high-frequency) and Approximation Coefficients (low-frequency) using the formula.

1. Approximation Coefficients (low-frequency (g)) :
   $g = \frac{1}{\sqrt{2}}$ [1,1] ➡ g = [0.7071, 0.7071]
2. Detail Coefficients (high-frequency (h)):
   $h = \frac{1}{\sqrt{2}}$ [1, −1] ➡ h = [0.7071, −0.7071]

Data Embedding Process and Image Reconstruction

The secret message, which has been converted into numerical form, is embedded into the high-frequency components of the transformed image. After embedding, the inverse DWT is applied to reconstruct the image while preserving its original visual quality. The following is a manual calculation example of the Discrete Wavelet Transform using the Haar filter with a simple signal. Suppose we want to embed the message "A" into a signal. We will convert the text into numerical format and apply DWT.

Step 1: Prepare Data

Embedded message**: "HA"** ⟹H = 72 (ASCII)
A = 65 (ASCII)

Numerical data: data_numerik = [72,65]

Original signal: audio_data = [100, 150, 200, 250]

Step 2: Data Padding

For DWT, the data length must be a power of two. We add zero padding to ensure the correct length:

data_numerik = [72, 65, 0, 0] (padded with zeros)

audio_data = [100, 150, 200, 250] (remains the same)

Step 3: Apply DWT

We compute the DWT using the Haar filter for four elements as follows:

Approximation Coefficients (Low-Pass Filter):

A[0] = (100 + 150) / √2 = 176.78

A[1] = (200 + 250) / √2 = 318.20

Detail Coefficients (High-Pass Filter):

D[0] = (100 - 150) / √2 = -35.36

D[1] = (200 - 250) / √2 = -35.36

Resulting Coefficients:

Approximation Coefficients (A): [176.78, 318.20]

Detail Coefficients (D): [-35.36, -35.36]

Step 4: Embed Data

We insert the numerical data [72, 65] into the detail coefficients:

Before embedding: D = [-35.36, -35.36]

D[0] = -35.36 + 72 = 36.64

D[1] = -35.36 + 65 = 29.64

After embedding: D = [36.64, 29.64]

Step 5: Image Reconstruction (Inverse DWT)

After embedding, we apply inverse DWT to retrieve the modified data:

A = [176.78, 318.20] (remains unchanged)

D = [36.64, 29.64]

Reconstructed Values:

Reconstruction[0] = A[0] / √2 + D[0] / √2 = 150.9

Reconstruction[1] = A[0] / √2 - D[0] / √2 = 99.08

Reconstruction[2] = A[1] / √2 + D[1] / √2 = 245.96

Reconstruction[3] = A[1] / √2 - D[1] / √2 = 204.03

Final Reconstructed Signal: [150.9, 99.08, 245.96, 204.03]

This demonstrates that the embedding process modifies the signal while preserving its structure, ensuring that the secret message remains hidden.

Implementation with Code Program

To ensure that the implementation of DWT in the code program aligns with the theory, a manual calculation of the wavelet transform on the digital image was performed. This calculation includes the decomposition of the image into approximation and detail coefficients, as well as the embedding of the secret message into the high-frequency coefficients.

```
Masukkan pesan yang akan disisipkan (misal: HA): HA
Sinyal Input: [100 150 200 250]
Pesan yang akan disisipkan: HA

=== Proses Discrete Wavelet Transform (DWT) ===
Sinyal asli: [100 150 200 250]
Koefisien Approximation sebelum penyisipan: [np.float64(176.77669529663686), np.float64(318.19805153394634)]
Koefisien Detail sebelum penyisipan: [np.float64(-35.35533905932737), np.float64(-35.35533905932737)]
Perhitungan Approximation[0]: ( 100 + 150 ) / sqrt(2) = 176.77669529663686
Perhitungan Detail[0]: ( 100 - 150 ) / sqrt(2) = -35.35533905932737
Perhitungan Approximation[1]: ( 200 + 250 ) / sqrt(2) = 318.19805153394634
Perhitungan Detail[1]: ( 200 - 250 ) / sqrt(2) = -35.35533905932737

=== Proses Penyisipan Pesan ===
Pesan dalam bentuk ASCII: [72, 65]
Pesan setelah padding: [72 65]
Koefisien Detail setelah penyisipan: [36.64466094 29.64466094]
Perhitungan setelah penyisipan: Koefisien Detail awal + Pesan ASCII

=== Proses Rekonstruksi Sinyal ===
Sinyal setelah rekonstruksi: [150.91168825  99.08831175 245.96194078 204.03805922]
Perhitungan Rekonstruksi:
Sinyal[0] = ( 176.77669529663686 + 36.64466094067263 ) / sqrt(2) = 150.9116882454314
Sinyal[1] = ( 176.77669529663686 - 36.64466094067263 ) / sqrt(2) = 99.08831175456855
Sinyal[2] = ( 318.19805153394634 + 29.64466094067263 ) / sqrt(2) = 245.96194077712553
Sinyal[3] = ( 318.19805153394634 - 29.64466094067263 ) / sqrt(2) = 204.03805922287435
```

Figure 2. Result of Testing with Python

The test results of the Python code show that the manual calculation of the Discrete Wavelet Transform (DWT) matches the implementation in Python. From the image, it is evident that the approximation and detail coefficient values obtained from the manual calculation are consistent with the DWT transformation results generated by the code. This proves that the DWT algorithm has been correctly implemented, allowing data embedding in high-frequency coefficients without altering the main structure of the image.

GUI-Based Testing

To facilitate users in implementing steganography based on Discrete Wavelet Transform (DWT), a graphical user interface (GUI) has been developed that allows users to:

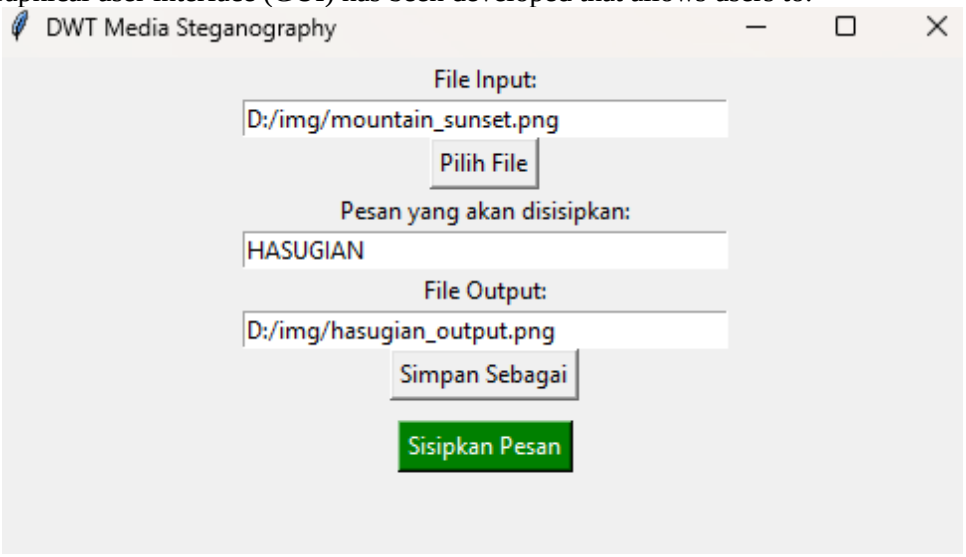

Figure 3. GUI-Based Testing

This GUI is an interface for DWT Media Steganography, allowing users to embed messages into images using Discrete Wavelet Transform (DWT).

1. File Input: Selects the image to be used.
2. Message: Users enter the secret text to be embedded.

3. File Output: Specifies the storage location for the steganography result.
4. "Embed Message" Button: Starts the process of embedding the message into the image.

This application makes it easy for users to hide secret messages without manually writing code.

Figure 4. Image Input

Figure 5. Image Output

The steganography process using Discrete Wavelet Transform (DWT) successfully embeds a message without altering the visual quality of the image. The stego image remains similar to the original image, demonstrating that the DWT method is effective without significant distortion. The embedded message can be extracted with high accuracy, ensuring the success of the algorithm.

4. CONCLUSION

This study demonstrates that the use of Discrete Wavelet Transform (DWT) in steganography enables secure and undetectable information hiding within digital images. By utilizing high-frequency coefficients, this method can embed messages without significantly altering the visual quality of the image. Both manual testing and Python code implementation confirm that DWT preserves the main structure of the image while ensuring the successful extraction of hidden messages. Additionally, the development of a GUI interface makes it easier for users to apply this technique without requiring manual programming. Thus, DWT is proven to be an effective method for steganography, with potential applications in data security and confidential communication.

REFERENCE

Al-Haj, A. (2007). Combined DWT-DCT digital image watermarking. Journal of computer science, 3(9), 740-746.

Al-Haj, A., Mohammad, A. A., & Bata, L. (2011). DWT-based audio watermarking. Int. Arab J. Inf. Technol., 8(3), 326-333.

Kaur, H., & Kaur, J. (2014). Image Steganography Using Discrete Wavelet Transform and Fuzzy-BP Network. International Journal of Computer Applications, 92(9), 1–5.

Po-Yueh, P. Y., & Lin, H. J. (2006). A DWT based approach for image steganography. International Journal of Applied Science and Engineering, 4(3), 275-290.

Singh, R., & Singh, J. (2020). A comparative analysis of spatial and transform domain steganography techniques. Multimedia Tools and Applications, 79, 14461–14493.

Zhang, T., Wang, D., & Liu, Y. (2016). An Improved DWT-Based Image Steganography Method. Multimedia Systems and Signal Processing, 53(4), 341–356.

Shaik, A., & Thanikaiselvan, V. (2021). Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification. Journal of King Saud University-Computer and Information Sciences, 33(7), 878-889.

Veselska, O., Lavrynenko, O., Odarchenko, R., Zaliskyi, M., Bakhtiiarov, D., Karpinski, M., & Rajba, S. (2022). A wavelet-based steganographic method for text hiding in an audio signal. Sensors, 22(15), 5832.