Ju-ti : Jurnal Teknik Indonesia
ISSN : 2964-0490 (online)
Vol. 2, No. 01, 2023, pp. 13-17
https://jurnal.seaninstitute.or.id/index.php/juti

Discrete Wavelet Transform (DWT) Based Steganography Implementation

Gideon Adventus Simanungkalit[1], Daniel Syahputra Tarigan[2], Dinda Roulita Simangunsong[3]
Universitas Katolik Santo Thomas, Medan, Sumatera Utara

Article Info

Keywords:
Discrete Wavelet Transform,
Cryptography,
Encryption,
Description,
Data Security

ABSTRACT

Steganography is the art of hiding information in a medium in such a way that its presence is undetectable by a third party. One of the techniques used in image steganography is the Discrete Wavelet Transform (DWT), which allows the decomposition of an image into different frequency sub-bands, thus facilitating data embedding without sacrificing visual quality. This paper discusses the manual calculation of the application of DWT in image steganography, including the image decomposition steps, the process of message embedding in a particular sub-band, and image reconstruction using the inverse DWT. Experimental results show that this method is effective in hiding information while maintaining good image quality.

Corresponding Author:
Gideon Adventus Simanungkalit
Universitas Katolik Santo Thomas
gideonadventus93@gmail.com

1. INTRODUCTION

Steganography is a technique for hiding secret information in other media, such as images, audio, or video, so that the existence of the information cannot be detected by unauthorized parties.(Ari Anti et al., 2017). One of the methods used in steganography is the Discrete Wavelet Transform (DWT), which allows the transformation of signals or images from the spatial domain to the frequency domain.(Syahdilan & Prawira, 2024). By using DWT, the image can be decomposed into different frequency sub-bands, thus allowing the embedding of secret messages at certain wavelet coefficients without significantly affecting the visual quality of the image.

In recent years, research on the implementation of steganography using DWT has grown rapidly. Such as research examining the use of DWT techniques in the CIELab color space to improve the security and quality of the resulting stego-image. The results of the study showed that the resulting stego-image had fairly good imperceptibility, fidelity, and recovery.(Zakaria & Munir, nd).

In addition, other studies combine the DWT method with the Least Significant Bit (LSB) to insert secret messages into digital images. The DWT method is used for stego-cover transformation, while the LSB method is used for the message insertion process. The indicators of successful testing in this study are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), with the best MSE value of 7.03E-24 and PSNR of 298.2989 dB.

Previous studies have shown that data embedding in high frequency sub-bands such as LH, HL, and HH can produce stego-images that have good visual quality and are resistant to various attacks. For example,(Al-Hameed et al., 2023)proposed a DWT-based steganography technique to hide audio signals in images, which showed promising results in terms of imperceptibility and embedding capacity.

In addition, research conducted by(Ahmed, 2021)shows that the use of DWT in digital image steganography can increase resistance to JPEG compression attacks. This study proves that the use of high-frequency sub-bands allows for more stable data insertion without damaging the visual quality of the covered image.

Furthermore, research by(Nevriyanto et al., nd)explored the combination of DWT and Singular Value Decomposition (SVD) to improve the resilience against filtering and compression attacks. The results of this study show that the combination of these techniques can improve the embedding capacity while maintaining the visual quality of stego-images.

Although various steganography methods have been developed, there are still some challenges that need to be overcome. One of them is increasing the resilience of stego-images to steganalysis attacks, which is a technique used to detect the presence of hidden messages in digital media. In addition, maintaining the visual quality of stego-images so that significant differences are not detected by observers is also a major concern. Therefore, further research is needed to develop more secure and efficient steganography methods.

Based on the background, the purpose of this study is to implement and analyze the steganography method using Discrete Wavelet Transform (DWT) on digital images. This study will evaluate the performance of the proposed method in terms of imperceptibility, fidelity, and recovery of secret messages, and compare it with other steganography methods. It is expected that the results of this study can contribute to the development of safer and more efficient steganography techniques to protect confidential information in digital media.

2. RESEARCH METHODS

1. Wavelet Selection
   Using Haar wavelets for image decomposition.
2. Image Decomposition
   The 4x4 pixel grayscale image is converted into LL, LH, HL, and HH sub-bands.
3. Data Insertion
   Secret data is inserted in the HH sub-band.
4. Image Reconstruction
   Using inverse DWT to restore the image to its original form.
5. Message Extraction
   Perform DWT again to retrieve the inserted data.

3. RESULTS AND DISCUSSION

Manual Calculation Implementation

1. Key Formation

At this stage, the key formation process is carried out based on the wavelet transform of the original data:

1. Wavelet Selection
   Certain wavelets, for example Haar or Daubechies, are used for signal decomposition.
2. Coefficient Extraction
   The original image or signal is decomposed into LL (low-low), LH (low-high), HL (high-low), and HH (high-high) sub-bands.
3. Key Making
   The key is formed from the characteristics of the selected sub-band coefficients and is used for the encryption process.

Manual Computation Implementation: Suppose we want to encrypt the message "HELLO" using DWT with Haar wavelets on a 4x4 pixel grayscale image:

a. Step 1: Convert Message to ASCII
   H = 72 (01001000), E = 69 (01000101), L = 76 (01001100), L = 76 (01001100), O = 79 (01001111)
   Binary representation of message: 01001000 01000101 01001100 01001100 01001111
b. Step 2: Image Representation in Matrix
   Initial grayscale image:

   [52 55 61 66]
   [70 61 68 73]
   [90 85 80 75]

[60 65 70 75]

c. Step 3: Wavelet Transform (DWT)
The image is decomposed into LL, LH, HL, and HH sub-bands.
HH Sub-band:
[2 -3 1 -2]
[-4 3 -2 1]
[5 -2 4 -3]
[-1 2 -3 1]

2. Encryption To encrypt data using DWT, the following steps are performed:
   1. DWT Transformation
      Transform an image or signal using DWT.
   2. Secret Data Insertion
      Secret information is inserted in the HH sub-band by changing the values based on the message bits. Insertion example:
      [2 -3 0 -2] → 01001000 (H)
      [-4 2 -2 1] → 01000101 (E)
      [5 -2 4 -2] → 01001100 (L)
      [-1 2 -3 0] → 01001111 (O)
   3. Data Reconstruction (IDWT)
      After the data is embedded, the signal or image is restored to its original form through inverse DWT (IDWT). The final image remains similar with slight changes in pixel intensity values.
3. Manual Calculation Implementation
   Message extraction Perform DWT again on the steganography image. Take the value of the modified HH sub-band. Convert back to binary and then to ASCII characters: 01001000 01000101 01001100 01001100 01001111

Results Analysis

The changes only occur in the HH sub-band, so the image quality is maintained without losing significant information.(Gao & Zeng, 2019).

Processing Results Table

Step	Description	Results
Message Conversion	Converting characters to binary representation	01001000 01000101 01001100 01001100 01001111
Image Representation	4x4 grayscale image matrix	[52 55 61 66] [70 61 68 73] [90 85 80 75] [60 65 70 75]
DWT Decomposition	Generate HH sub-band	[2 -3 1 -2] [-4 3 -2 1] [5

The implementation of steganography using Discrete Wavelet Transform (DWT) has been proven to provide advantages in maintaining the visual quality of images, increasing data security, and ensuring the accuracy of data extraction. This study focuses on data embedding in the HH sub-band that represents high image details, which has proven to be effective in hiding information without sacrificing visual quality.(Yulion et al., 2024).

In this study, the visual quality of the image is maintained because the changes made only occur in the HH sub-band. This sub-band contains high-frequency information that is not very sensitive to human visual perception, so the modifications made to insert secret data do not cause significant visible distortion. This is in line with research(Gupta & Dhanda, nd) which shows that the use of DWT for audio steganography produces stego-images with good visual quality and are difficult to detect.

Data security is also increased by using DWT compared to the Least Significant Bit (LSB) method. In the LSB method, data is embedded in the least significant bits in the image pixels, which is vulnerable to steganalysis attacks. However, in DWT, data is embedded in the frequency domain, which makes it more difficult to detect because changes occur in the wavelet coefficients that are not

directly visible. Research conducted by(Ruswiansari & Novianti, nd) also proved that the combination of DWT with Singular Value Decomposition (SVD) can increase resistance to steganalysis attacks.

In addition, the accuracy of data extraction in this method is also very high. The extraction process is carried out by performing a wavelet transform back (Inverse DWT) to retrieve the data inserted in the HH sub-band. The experimental results show that the inserted message can be extracted accurately without losing information. This finding is consistent with research conducted by(Meidyrosha et al., nd), which shows that DWT is able to maintain the integrity of the embedded data even when subjected to image compression or manipulation. Thus, the implementation of DWT-based steganography is not only effective in hiding information, but also provides better protection against detection attacks and ensures high data accuracy.

4. CONCLUSION

Advantages of DWT-Based Steganography in Detection Steganography using Discrete Wavelet Transform (DWT) is more difficult to detect than the Least Significant Bit (LSB) method because the hidden message insertion process is carried out in the frequency domain, not directly in the spatial domain. This causes the resulting changes to be more hidden and not easily recognized by visual analysis techniques or statistical-based steganalysis attacks. Security of Insertion in the HH Sub-band In the DWT transform, the image is divided into four sub-bands: LL (Low-Low), LH (Low-High), HL (High-Low), and HH (High-High). Insertion of secret messages in the HH sub-band is safer because this component represents high detail or image texture that is usually not easily visible to the human eye. Thus, modifications to this sub-band will not significantly interfere with the visual quality of the image, making insertion more difficult to detect without in-depth analysis. Application of DWT in Digital Security and Watermarking DWT method is often used in various digital security applications, such as steganography and watermarking, because of its ability to hide information while maintaining good visual image quality. In digital watermarking, DWT allows the embedding of watermarks that are resistant to various forms of manipulation, such as compression, rotation, and filtering. The nature of DWT which can separate low and high frequency information makes it ideal for securing digital content, such as images, videos, and electronic documents.

REFERENCES

Ahmed, B. T. (2021). A systematic overview of secure image steganography. *International Journal of Advances in Applied Sciences*, *10*(2), 178–187. https://doi.org/10.11591/ijaas.v10.i2.pp178-187

Al-Hameed, S. A. A., Abdullah, H. N., Khalf, N. H., & Alghazo, J. M. (2023). An Enhanced Steganography Approach for Concealing Audio in Images Using Double Density-Dual Tree Wavelet Transform. *Revue d'Intelligence Artificielle*, *37*(5), 1237–1244. https://doi.org/10.18280/ria.370516

Ari Anti, U., Harsa Kridalaksana, A., & Marisa Khairina, D. (2017). *STEGANOGRAFI PADA VIDEO MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN END OF FILE (EOF)*. *12*(2).

Gao, H., & Zeng, W. (2019). Image compression and encryption based on wavelet transform and chaos. *Computer Optics*, *43*(2), 258–263. https://doi.org/10.18287/2412-6179-2019-43-2-258-263

Gupta, S., & Dhanda, N. (n.d.). *Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT)*. *17*(2), 32–44. https://doi.org/10.9790/0661-17253244

Meidyrosha, M. N., Wahidah, I. H., & Saidah, S. (n.d.). *Perancangan Integrasi Watermarking Pada Kompresi Video H.265 Dengan Metode Discrete Wavelet Transform Dan Spektral Tersebar Design Of Watermarking Integration On Video H.265 Compression With Discrete Wavelet Transform And Spread Spectrum Methods*.

Nevriyanto, A., Erwin, E., Sutarno, S., & Siswanti, D. (n.d.). *Image Steganography Using Combine of Discrete Wavelet Transform and Singular Value Decomposition for More Robustness and Higher Peak Signal Noise Ratio*.

Ruswiansari, M., & Novianti, A. (n.d.). *IMPLEMENTASI DISCRETE WAVELET TRANSFORM (DWT) DAN SINGULAR VALUE DECOMPOSITION (SVD) PADA IMAGE WATERMARKING IMPLEMENTATION DISCRETE WAVELET TRANSFORM (DWT) AND SINGULAR VALUE DECOMPOSITION (SVD) ON IMAGE WATERMARKING*.

Syahdilan, A., & Prawira, M. A. (2024). IMPLEMENTASI ALGORITMA DISCRETE WAVELET TRANSFORM UNTUK MENAMBAHKAN INVISIBLE WATERMARKING PADA CITRA DIGITAL. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Issue 6).

Yulion, K., Prakoso, S., Chrisnanto, Y. H., Kasyidi, F., Yani, A., Terusan, J., Sudirman, J., Cimahi, K., & Barat, J. (2024). STEGANOGRAFI METODE INVERTED LSB MENGGUNAKAN POLA ADAPTIF DAN DCT. In *Jurnal Informatika & Rekayasa Elektronika)* (Vol. 7, Issue 2). http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

Zakaria, A., & Munir, R. (n.d.). *STEGANOGRAFI CITRA DIGITAL MENGGUNAKAN TEKNIK DISCRETE WAVELET TRANSFORM PADA RUANG WARNA CIELab*.