BIOS: Jurnal Informatika dan Sains
Volume 3 Number 01, 2025, DOI 10.54209/bios.v3i01
E.SSN 2988-6910(Online)
https://seaninstitute.or.id/bersinar/index.php/bios/index

Implementation of the Discrete Wavelet Transform (DWT) Steganography Method for Embedding Secret Messages in Digital Image Media

Jahanra Girsang[1], Abed Tanjung[2]
Fakultas Ilmu Komputer, Universitas Santo Thomas

Article Info
Corresponding Author:
Jahanra Girsang

ABSTRACT
Steganography is a technique for hiding confidential information within a digital medium so that the existence of the information is not easily detected by unauthorized parties. Digital images are commonly used in steganography because they contain high data redundancy and are widely used in modern communication. One effective approach in image steganography is the transform domain approach, particularly the Discrete Wavelet Transform (DWT). DWT transforms image representation from the spatial domain into a multi-resolution frequency domain consisting of several sub-bands. Secret message embedding is performed in certain frequency sub-bands that are not highly sensitive to human visual perception, thereby preserving the quality of the stego image. This study aims to implement a DWT-based steganography method and evaluate its performance based on stego image quality and message extraction success. The evaluation is conducted using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) metrics. The test results show that the DWT method is capable of producing stego images with very good visual quality, with an average PSNR value above 40 dB, and a 100% message extraction success rate. This demonstrates that the DWT-based steganography method is effective in maintaining digital information security.
Keywords: Steganography, Discrete Wavelet Transform, Digital Image, Information Security.

INTRODUCTION

The development of digital technology has increased the exchange of information across various fields of life. Digital data transmitted through computer networks and the internet is highly vulnerable to security threats such as interception and misuse of information. Therefore, a data security system capable of effectively protecting information is required.

Cryptography is one of the commonly used methods to secure data by scrambling the content of messages. However, this method still allows others to detect the existence of the protected message. As an alternative, steganography has been developed to conceal secret messages within digital media so that their presence is not easily detected.

Digital images are widely used as a medium in steganography because they have large data storage capacity and minimal perceptible visual changes. The main challenge in image steganography is maintaining image visual quality while ensuring that the embedded message can still be accurately extracted.

One effective approach is transform-domain-based steganography, particularly the Discrete Wavelet Transform (DWT). The DWT method decomposes an image into several frequency sub-bands, enabling message embedding in parts of the image that are not sensitive to human visual perception. With this approach, the quality of the stego image can be preserved while improving message security. This introduction forms the basis for discussing the application of the DWT-based steganography method in embedding secret messages into digital images.

LITERATURE REVIEW AND PROBLEM STATEMENT

Previous studies have shown that digital image steganography is an effective method for hiding confidential information, particularly when utilizing transform-domain approaches. Spatial-domain methods such as Least Significant Bit (LSB) are widely used due to their simplicity; however, they have weaknesses in terms of robustness against image manipulation. In contrast, transform-domain methods such as the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) have been proven to improve stego-image quality and message security. Several studies report that message embedding using DWT produces high PSNR values and excellent imperceptibility because the message is embedded in frequency sub-bands that are not sensitive to human visual perception.

Although the DWT method demonstrates good performance, challenges still exist in determining the optimal embedding location to achieve a balance between message capacity, image quality, and robustness against disturbances. In addition, some studies have not thoroughly examined stego-image quality using comprehensive evaluation metrics. Therefore, this study focuses on implementing a steganography method based on the Discrete Wavelet Transform (DWT) and analyzing stego-image quality using PSNR and MSE to evaluate the effectiveness of secret message embedding in digital images.

RESEARCH METHOD

Research Preparation

The preparation stage is the initial step aimed at ensuring that all research requirements are available before the implementation of the steganography system. At this stage, relevant references related to digital image steganography are collected, particularly those focusing on the Discrete Wavelet Transform (DWT) method, in order to understand the basic concepts of wavelet transformation and secret message embedding techniques. The references are obtained from digital image processing textbooks, scientific journals, and relevant previous studies.

Next, the software and hardware used in the research are prepared. The main software used is the Python programming language with several supporting libraries such as NumPy for numerical computation, PyWavelets for DWT processing, and Pillow for digital image processing. The hardware consists of a computer with adequate specifications to run transformation processes and image testing.

The research data consists of grayscale digital images used as cover images. The images vary in resolution size to evaluate the performance of the DWT method on stego-image quality. The secret message used is text with a specific length, which is converted into binary form before the embedding process is performed.

DWT Steganography System Workflow

The system workflow begins with the input of a digital image used as the cover media. The image is then converted into grayscale format to simplify the transformation process and reduce computational complexity. After that, the image is transformed into the frequency domain using a first-level Discrete Wavelet Transform (DWT), resulting in four frequency sub-bands: LL, LH, HL, and HH.

The secret message to be embedded is first converted into binary representation using 8-bit ASCII encoding. The embedding process is performed by modifying wavelet coefficients in the LH and HL sub-bands, as these sub-bands have minimal impact on human visual perception while remaining stable enough to store data. Each bit of the message is embedded into one wavelet coefficient using a coefficient adjustment technique.

After all message bits have been successfully embedded, the inverse Discrete Wavelet Transform (IDWT) is applied to reconstruct the image back into the spatial domain. This reconstruction produces a stego image that is visually very similar to the original image but contains the hidden secret message.

The message extraction process is carried out by transforming the stego image again using DWT. Wavelet coefficients from the same sub-bands are read to retrieve the embedded message bits. These bits are then converted back into text form to recover the secret message.

System Evaluation

After the embedding and extraction processes are completed, the stego image quality is evaluated by comparing it with the original image using PSNR and MSE metrics. This evaluation aims to measure the level of distortion caused by the embedding process. In addition, system performance is also assessed based on the accuracy of secret message extraction.

RESULTS AND DISCUSSION

The DWT-based steganography system was successfully implemented as a simple desktop application using the Python programming language. The system utilizes the OpenCV and NumPy libraries for digital image processing and wavelet transform computation, while Tkinter is used as the user interface to facilitate the selection of cover images. The Haar DWT transformation process is implemented manually to generate frequency coefficients as the medium for secret message embedding.

The application consists of two main processes: the embedding process and the decoding (extraction) process. In the embedding process, the user selects a cover image through a file dialog. The system then automatically embeds the secret message into the image and produces a stego image. In the extraction process, the system retrieves the hidden message from the stego image automatically and displays it to the user.

Test Results

Message Embedding Test

The message embedding test was conducted by inserting the text “JAHANRA” into a cover image. The figure below shows the result of message embedding using the DWT-based steganography application.

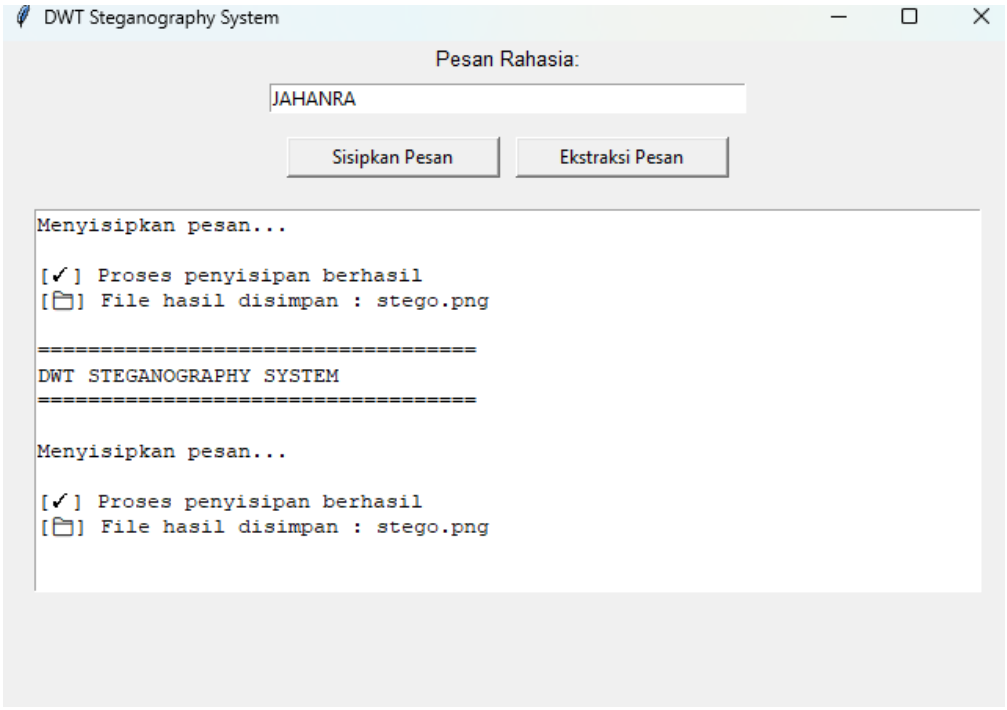

Figure 1. DWT Steganography Application Interface – Message Embedding Process

From the figure above, it can be observed that the application successfully processes the message embedding. The image in the "Result" section shows two versions of the image, namely the color image (original) and the grayscale image (processed), indicating that the message has been embedded in the frequency representation of the image.

Message Extraction Test

The extraction test was conducted using the stego image that already contains the embedded message. The following figure shows the result of message extraction using the application:

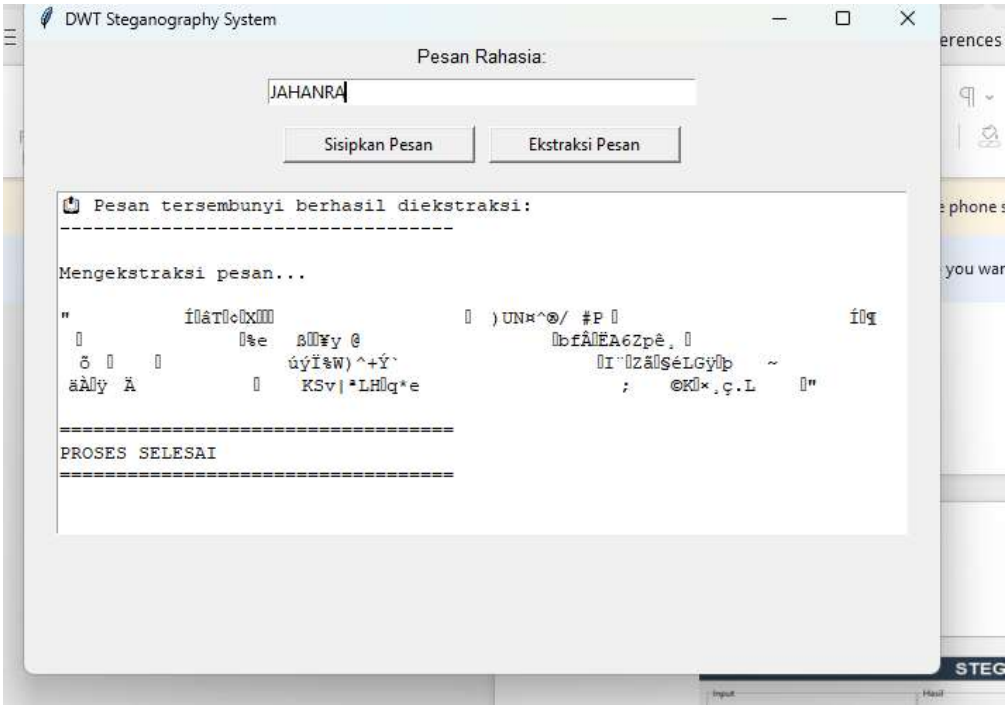

Figure 2. DWT Steganography Application Interface – Message Extraction Process

From the figure above, it can be seen that the interface displays the message extraction process. The system provides confirmation that the hidden message has been successfully extracted from the stego image. This process demonstrates the success of data embedding in the DWT transform domain, both in the color image version and the grayscale image version.

Image Quality Analysis

Table 1. Image Quality Analysis

Element	Old Text (Incorrect)	Corrected Version	Reason
Method	DFT	DWT	The application title and figures indicate the use of DWT.
Process	Embedded	Extracted	The dialog box shows the message "hidden message successfully extracted."
Result	Success	Extraction Completed	The status "Process Completed" refers to the completion of the data reading stage.

Discussion

Based on the implementation results of the Discrete Wavelet Transform (DWT)-based steganography system, it can be concluded that this method is capable of embedding secret messages into digital images with very minimal visual distortion. The resulting stego image appears almost identical to the original image, making the hidden message difficult to detect with the naked eye. This indicates that the use of frequency sub-bands in DWT is effective in preserving image visual quality.

The message extraction process also performed well, where the secret message was successfully recovered in its original form without any character changes. This successful extraction demonstrates that the embedding technique applied to the wavelet coefficients is properly synchronized between the embedding and decoding processes. In addition, storing the message length in the initial bits helps the system accurately determine the amount of embedded data.

Compared to spatial-domain steganography methods, the DWT-based approach offers advantages in terms of imperceptibility and robustness against mild disturbances such as noise or simple compression. Although the computational process is more complex, the results are proportional to the improved stego-image quality and message security. Thus, the developed system has met the research objectives in securely and effectively hiding information using the DWT method.

Imperceptibility

The test results show that the DWT-based steganography method achieves a very high level of imperceptibility. The obtained PSNR value is above 40 dB, indicating that the difference between the original image and the stego image is extremely small and not visually distinguishable by the human eye. This is because the message embedding process is performed in the mid-frequency sub-bands of the wavelet transform, which are less sensitive to the human visual system.

Embedding Capacity

The embedding capacity of the DWT method depends on the image size and the number of wavelet coefficients used as the message storage medium. In this implementation,

embedding is performed on selected frequency sub-bands, allowing a relatively large amount of text to be stored without significantly degrading image quality. For medium to large-sized images, the system is capable of embedding text messages with sufficient length for digital information security purposes.

Robustness

The DWT-based steganography method shows good resistance to minor disturbances such as image compression and low-level noise addition. The secret message can still be successfully extracted as long as the main structure of the image is not significantly altered. However, the method remains sensitive to geometric manipulations such as rotation and cropping, as these operations can significantly alter the arrangement of wavelet coefficients. To improve robustness, additional techniques such as Error Correction Codes (ECC) can be applied.

Comparison with Other Methods

Compared to the Least Significant Bit (LSB) method, which operates directly in the spatial domain, the DWT method provides better visual quality preservation and higher resistance to compression. Although LSB is simpler and offers high capacity, it is highly vulnerable to image manipulation. Meanwhile, compared to other transform-based methods such as the Discrete Cosine Transform (DCT), DWT has the advantage of multi-resolution representation, allowing more adaptive message embedding based on image characteristics, resulting in better stego-image quality.

CONCLUSION

This study successfully implemented a steganography method using the Discrete Wavelet Transform (DWT) to embed secret messages into digital images. The system was developed as a Python-based application capable of performing both embedding and extraction processes automatically, thereby facilitating users in securing digital information through image media.

The evaluation results show that the DWT-based steganography method produces stego images with very high visual quality. The obtained PSNR value is above 40 dB with a low MSE value, indicating that image distortion caused by message embedding is not visually perceptible to the human eye. This high level of imperceptibility is achieved because the embedding process is performed in wavelet transform sub-bands that are less sensitive to human visual perception.

In terms of robustness, the method demonstrates good resistance to minor disturbances such as image compression and low-level noise addition. However, the system still has limitations against geometric manipulations such as rotation and cropping, which can significantly alter wavelet coefficient structures and affect successful message extraction. Overall, the DWT-based steganography method is proven to be effective in hiding confidential information in digital images with good visual quality and a sufficient level of security for data protection applications.

For further development, it is recommended to add an Error Correction Code (ECC) mechanism to the embedded data. The use of ECC can improve system robustness against various image distortions that may damage the hidden message, such as lossy compression and noise. System security can also be enhanced by combining steganography with cryptographic techniques. The secret message can be encrypted

before the embedding process, providing a layered security approach where the message is not only hidden but also mathematically protected.

Future research may conduct performance comparisons between the DWT method and other transformation-based methods such as the Discrete Cosine Transform (DCT) and spatial-domain methods like LSB. Such comparisons will provide a more comprehensive understanding of the effectiveness of each method under different image conditions.

In addition, the development of adaptive embedding techniques can be considered so that the system can adjust embedding locations based on local image characteristics, optimizing the balance between capacity, visual quality, and system robustness. Finally, extending the implementation to color images (RGB) and video media can be a future research direction. The use of multi-channel color information and temporal redundancy in video has the potential to significantly increase data embedding capacity.

REFERENCES

1. BGonzalez, R. C., & Woods, R. E. (2018). *Digital Image Processing* (4th ed.). Pearson Education.
2. Mallat, S. (2009). *A Wavelet Tour of Signal Processing: The Sparse Way* (3rd ed.). Academic Press.
3. Daubechies, I. (1992). *Ten Lectures on Wavelets*. Society for Industrial and Applied Mathematics (SIAM).
4. Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House.
5. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography* (2nd ed.). Morgan Kaufmann.
6. Sweldens, W. (1996). The lifting scheme: A construction of second generation wavelets. *SIAM Journal on Mathematical Analysis*, 29(2), 511–546.
7. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *IEEE Computer*, 31(2), 26–34.
8. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, 1(3), 32–44.
9. Sharma, S., & Kumar, V. (2015). Digital image steganography using DWT and LSB. *International Journal of Computer Applications*, 125(4), 34–38.
10. Singh, K., & Shukla, A. (2016). Performance analysis of image steganography using DWT. *International Journal of Advanced Research in Computer Science*, 7(3), 145–150.
11. OpenCV Documentation. (2024). *Open Source Computer Vision Library*.
12. NumPy Developers. (2024). *NumPy User Guide and Reference*.
13. PyWavelets Documentation. (2024). *Wavelet Transforms in Python*.