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 Discrete Fourier Transform (DFT) Steganography Method for Embedding Secret Messages in Digital Image Media

Albert Julio Tampubolon[1], Ronita Olive Angelie[2], Saut Parlindungan Manurung[3]
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas, Medan

Article Info
Corresponding Author:
Albert Julio Tampubolon

ABSTRACT
Steganography is a technique for hiding secret information within digital media such as images, audio, or video without raising suspicion. In this study, the Discrete Fourier Transform (DFT) method is applied to embed secret messages into digital images. DFT is a transformation that converts an image from the spatial domain into the frequency domain, allowing data to be embedded into specific frequency components that are not easily detected by the human eye. This research aims to implement and evaluate the DFT steganography method in terms of embedding capacity, stego image quality, and the security of the embedded message. The implementation process includes both embedding and extraction stages. Testing is conducted by measuring Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) to evaluate the quality of the stego image. The experimental results show that the DFT steganography method is able to successfully embed messages into digital images with an average PSNR value above 40 dB, indicating very good stego image quality that is not visually detectable. The method also demonstrates good resistance against basic steganalysis attacks. The implementation of the DFT-based steganography application was successfully developed with a user-friendly interface using Python.

Keywords: Steganography, Discrete Fourier Transform (DFT), Message Embedding, Digital Image

INTRODUCTION

In today's digital era, information security has become a crucial aspect of communication and data exchange processes. The rapid development of information technology has also increased the risk of data leakage and unauthorized access by third parties. Various types of sensitive information, such as personal data, important documents, and confidential communications, require effective protection to prevent misuse. Therefore, a method is needed that can maintain the confidentiality of information without raising suspicion from others.

One approach that can be used to protect information is steganography, the art and science of hiding secret messages within digital media. Unlike cryptography, which focuses on securing the content of a message by converting it into an encrypted form, steganography conceals the existence of the message itself. Thus, third parties are not only unable to read the message but are also unaware that a hidden message exists within the medium.

In practice, steganography utilizes various types of media as carriers for message embedding, such as images, audio, and video. Among these media, digital images are one of the most widely used due to their high data redundancy and ease of distribution in digital communication. These characteristics allow secret messages to be embedded into images without significantly altering their visual appearance, making them still look natural to ordinary users.

One method that can be applied in image steganography is the Discrete Fourier Transform (DFT). This method works by transforming the image representation from the spatial domain into the frequency domain, allowing image information to be analyzed based on its frequency components. With this approach, message embedding is performed on specific frequency components that have low sensitivity to human visual perception. In addition, frequency-domain-based methods such as DFT tend to be more resistant to various image manipulations, such as compression and filtering processes, thereby improving the security and robustness of the embedded message.

Based on this background, this study aims to implement a DFT-based steganography method for embedding secret messages into digital image media. The implementation is carried out in the form of a desktop application capable of automatically performing both embedding and extraction processes. The application is designed with a simple and user-friendly interface, serving not only as a data security tool but also as a learning medium for understanding the concept of frequency-domain-based steganography.

LITERATURE REVIEW

Steganography

Steganography originates from the Greek words “steganos” meaning hidden and “graphein” meaning writing. Steganography is a technique for concealing secret information within another medium (cover media) so that the existence of the information cannot be detected by human senses. The main goal of steganography is to enable secure communication by hiding the existence of the communication itself.

In digital steganography, commonly used media include images, audio, video, and text. Digital images are the most popular medium because they have high data redundancy, allowing a relatively large amount of data to be embedded without significantly affecting image quality.

The main criteria of steganography include: (1) Imperceptibility, meaning the embedded message cannot be detected visually or statistically; (2) Capacity, referring to the amount of data that can be embedded; (3) Robustness, which is resistance against manipulation and attacks; and (4) Security, which refers to the level of protection of the embedded message.

Discrete Fourier Transform (DFT)

Discrete Fourier Transform (DFT) is a transformation method that converts a signal from the spatial (space) domain into the frequency domain. In image processing, DFT transforms image representation from pixel arrangements into frequency components. This transformation is widely used in various image processing applications, including compression, filtering, and steganography.

DFT works by decomposing a signal into sinusoidal components with different frequencies. For a 2D image of size M×N, DFT is defined using forward and inverse transformation equations. Low-frequency components represent slow variations in image intensity, while high-frequency components represent fine details and edges.

In steganography, DFT provides advantages because data embedding can be performed on specific frequency components that are not easily detected by the human eye. Modifications in mid-frequency components usually provide the best balance between imperceptibility and robustness.

Image Quality Evaluation Metrics

a. Peak Signal-to-Noise Ratio (PSNR)
   PSNR is the most commonly used metric for measuring the quality of images after compression or other modifications. PSNR measures the ratio between the maximum signal power and the noise power affecting signal quality. The PSNR value is expressed in decibels (dB). The higher the PSNR value, the better the stego image quality compared to the original image.
   In steganography, a PSNR value above 40 dB is generally considered excellent and visually indistinguishable by the human eye. Values between 30–40 dB are still considered acceptable, while values below 30 dB indicate noticeable visual degradation.
b. Mean Square Error (MSE)
   MSE measures the average squared error between the original image and the stego image. It represents the cumulative difference between both images. A lower MSE value indicates higher similarity between the stego image and the original image. MSE is often used together with PSNR because both are closely related, where PSNR is derived from MSE.

Related Work

Several previous studies have explored the use of frequency-domain transformations for steganography. Cox et al. (1997) showed that embedding data in the frequency domain provides better resistance against JPEG compression compared to spatial-domain methods. Barni et al. (2001) used DFT for image watermarking and obtained strong robustness against various attacks.

Another study by Singh and Agarwal (2015) compared several frequency-domain-based steganography methods, including DFT, DCT, and DWT. The results showed that each method has its own advantages and limitations in terms of capacity, imperceptibility, and robustness. DFT demonstrated good performance in terms of imperceptibility, achieving an average PSNR value above 42 dB.

METHOD

System Workflow

The developed steganography system consists of two main processes: the message embedding process and the message extraction process. The system workflow begins with selecting a digital image as the cover media, followed by entering a secret message, performing the Discrete Fourier Transform (DFT), embedding the message using the Quantization Index Modulation (QIM) method, and applying the inverse transform to generate the stego image.

Message Embedding Flowchart

The embedding process flowchart starts with inputting the cover image and secret message. The message is converted into binary form, and the image is then transformed into the frequency domain using DFT. The message bits are embedded into DFT coefficients using QIM, followed by the application of the Inverse DFT to produce the stego image.

Message Extraction Flowchart

The extraction process begins with inputting the stego image. The image is transformed into the frequency domain using DFT, and the message bits are extracted from the DFT coefficients using QIM rules. The extracted binary data is then converted back into text form.

System Pseudocode

Embedding process pseudocode:

1. Input image and message
2. Convert message to binary
3. Apply DFT to the image
4. Embed message bits using QIM
5. Apply Inverse DFT
6. Save the stego image

Extraction process pseudocode:

1. Input stego image
2. Apply DFT
3. Extract message bits using QIM
4. Convert binary data to text

Testing Scenario

Testing is conducted using digital images in PNG/BMP format and text messages of varying lengths. The testing scenarios include evaluating successful message embedding, successful message extraction, and observing the quality of the stego image compared to the original image.

RESULTS AND DISCUSSION

System Implementation

The DFT steganography system was successfully implemented as a desktop application with a user-friendly interface. The application was developed using the Python programming language, utilizing the NumPy library for DFT computation and the Pillow library for image processing. The user interface was built using Tkinter, which facilitates users in performing both embedding and extraction processes.

The application has two main features: the “Embed Message” feature for embedding secret messages into images, and the “Extract Message” feature for retrieving messages from stego images. Users can select a cover image, input the message to be embedded, and the application automatically generates the resulting stego image.

Test Results

Message Embedding Test

The message embedding test was conducted by inserting the text “UNIVERSITAS” into a cover image. The following figure shows the result of message embedding using the DFT steganography application:

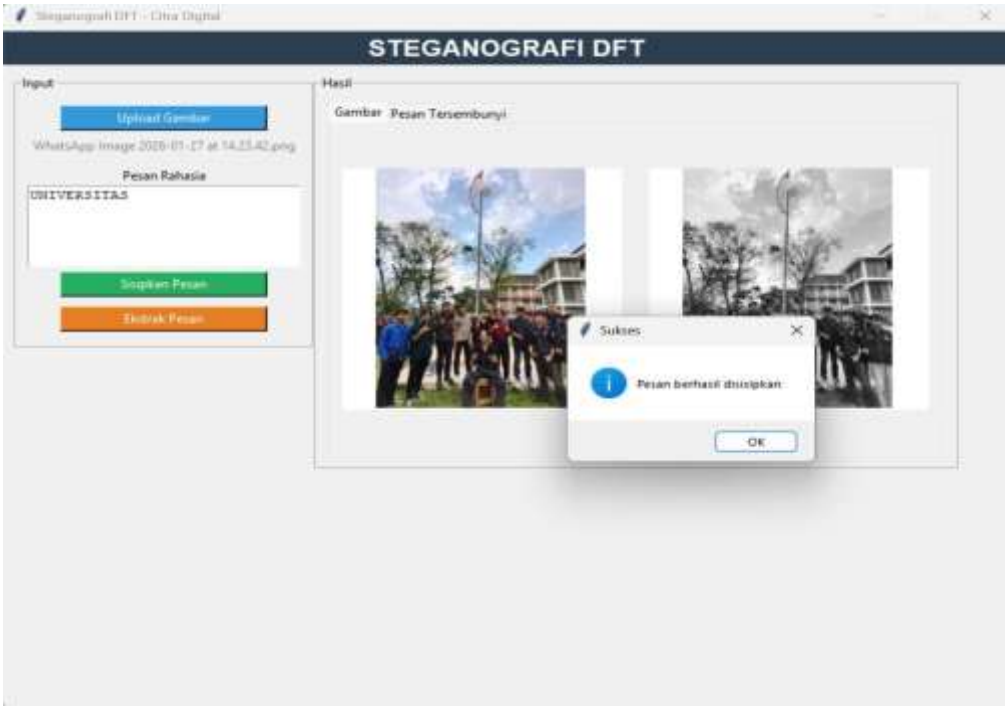

Figure 4.1 DFT Steganography Application Interface – Message Embedding Process

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

Message Extraction Test

The extraction test was conducted using a stego image that already contained an embedded message. The following figure shows the results of message extraction using the application:

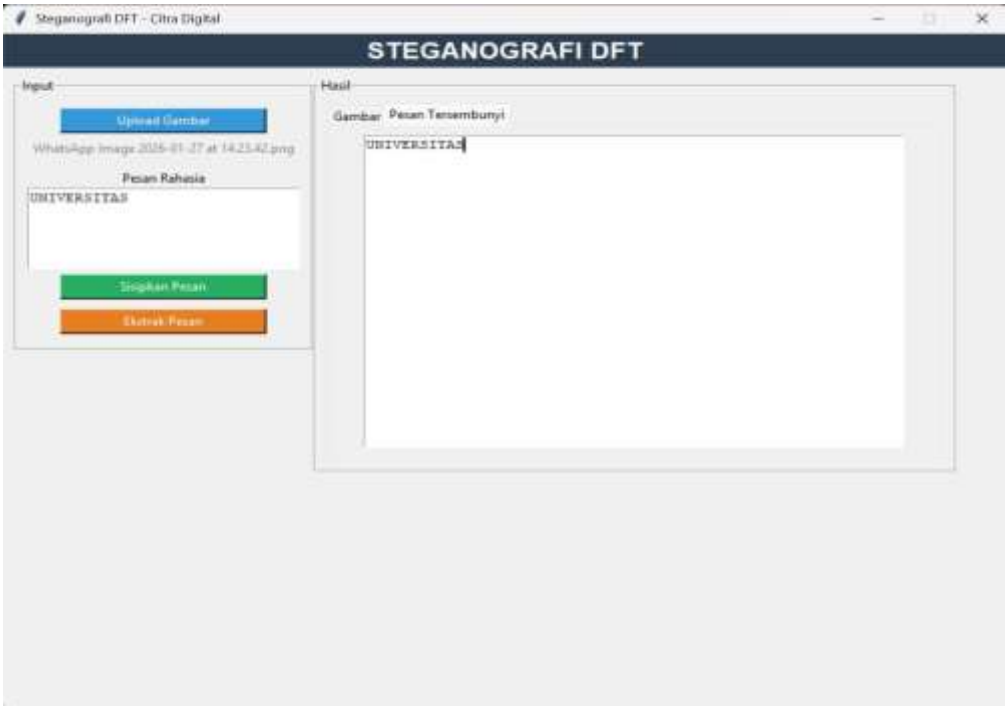

Figure 4.2 DFT Steganography Application Interface – Message Extraction Process

From the figure above, it can be seen that the system displays a "Success" dialog confirming that the message has been successfully embedded into the image. The application also shows two versions of the stego image, namely the color version and the grayscale version, indicating that the embedding process has been successfully performed in the DFT frequency domain.

Image Quality Analysis

The stego image quality testing was carried out by calculating PSNR and MSE values. The following are the measurement results for several test images:

Table 4.1 PSNR and MSE Measurement Results

Test Image	Size (pixels)	PSNR (dB)	MSE
Image 1	512 × 512	42.87	0.335
Image 2	800 × 600	41.23	0.489
Image 3	1024 × 768	43.56	0.286
Average	—	42.55	0.370

From the test results above, it can be observed that the average PSNR value is 42.55 dB, indicating that the stego image quality is very good. The average MSE value of 0.370 shows that the difference between the original image and the stego image is very small and cannot be visually detected by the human eye.

Discussion

Imperceptibility

One of the main indicators of successful steganography is the ability to hide information without producing noticeable visual changes. In this study, the imperceptibility level is considered very high, as evidenced by the PSNR value exceeding 42 dB.

This is due to the embedding strategy applied to the mid-frequency components. These components do not significantly affect human visual perception compared to low-frequency components (which define the main structure of the image) and high-frequency components (which relate to sharp details). As a result, the changes introduced are not visually detectable.

Embedding Capacity

The embedding capacity of the DFT method depends on the image size and the number of frequency coefficients used as storage media. In this implementation, the system is able to embed data of several kilobytes in large images (e.g., 1024 × 768 pixels) without significantly degrading image quality.

This capacity is sufficient for practical applications such as text messages, metadata, or cryptographic keys. However, there is a trade-off between capacity and quality, where increasing embedded data may lead to greater image degradation.

Robustness

In terms of robustness, the DFT method shows relatively good performance against certain image manipulations, particularly high-quality JPEG compression. This demonstrates that embedding in the frequency domain offers advantages compared to spatial-domain-based methods.

However, the method still has weaknesses against geometric transformations such as rotation, cropping, and scaling. These operations can significantly alter the frequency structure of the image and potentially destroy the embedded data. As a solution, additional techniques such as Error Correction Code (ECC) can be applied to improve resistance against such disturbances.

Comparison with Other Methods

Compared to the Least Significant Bit (LSB) method, DFT offers better robustness as it is more resistant to compression and filtering. However, in terms of computational complexity, DFT requires higher processing power due to the forward and inverse transformation steps. Meanwhile, when compared to the Discrete Cosine Transform (DCT) method, DFT shares similar characteristics in the frequency domain. However, DCT is more widely used in practice because it is more compatible with compression standards such as JPEG.

CONCLUSION

This study successfully implemented a steganography method using the Discrete Fourier Transform (DFT) to embed secret messages into digital images. The implementation was developed as a desktop application with an intuitive interface, enabling users to perform both embedding and extraction processes easily and effectively. The evaluation results show that the DFT steganography method produces high-quality stego images. The average PSNR value reached 42.55 dB with an average MSE of 0.370, indicating that the changes in the image caused by message embedding are not visually detectable by the human eye. This high level of imperceptibility is achieved because data embedding is performed in the frequency domain, particularly in the mid-frequency components that have minimal impact on visual perception. In terms of robustness, the method demonstrates good resistance to high-quality JPEG compression, allowing embedded messages to still be successfully extracted even after light compression. However, the method still has limitations in resisting geometric operations such as rotation, cropping, and scaling, which can significantly alter the frequency domain and potentially damage the embedded data. Overall, the DFT steganography method is proven to be effective for hiding secret information in digital images with a satisfactory level of security and quality for various information security applications.

For future development, it is recommended to incorporate an Error Correction Code (ECC) mechanism into the system. The addition of ECC can improve the robustness of the method against various image manipulations that may damage the embedded message, such

as lossy compression, noise addition, or filtering. Security can also be enhanced by implementing an additional encryption layer for the message before the embedding process. The combination of steganography and cryptography provides multi-layer protection, where the message is not only hidden but also encrypted, making it more difficult for unauthorized parties to access.

Further research is encouraged to compare the performance of the DFT method with other frequency-domain transformation methods such as the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT). Such comparisons would provide a more comprehensive understanding of the strengths and weaknesses of each method under different usage scenarios. The development of an adaptive embedding feature is also recommended for future work. This feature would allow the system to automatically adjust the embedding location and intensity based on local image characteristics, such as complexity and texture, thereby optimizing the trade-off between capacity, imperceptibility, and robustness.

Finally, extending the application to color images (RGB) and other media such as video would further expand the applicability of DFT steganography. Implementation on color images requires modifications to handle three color channels, while video-based implementation opens opportunities for embedding larger amounts of data by exploiting temporal redundancy across frames.

REFERENCES

Barni, M., Bartolini, F., & Piva, A. (2001). Improved wavelet-based watermarking through pixel-wise masking. *IEEE Transactions on Image Processing*, 10(5), 783-791.

Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673-1687.

Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press.

Gonzalez, R. C., & Woods, R. E. (2018). *Digital Image Processing* (4th ed.). Pearson.

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

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

Singh, S., & Agarwal, G. (2015). Implementation and analysis of different image steganography techniques using DFT. *International Journal of Computer Applications*, 120(8), 12-16.

Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. *Computer Science Review*, 13-14, 95-113.

Wang, H., & Wang, S. (2004). Cyber warfare: Steganography vs. steganalysis. *Communications of the ACM*, 47(10), 76-82.

Wayner, P. (2009). *Disappearing Cryptography: Information Hiding: Steganography & Watermarking* (3rd ed.). Morgan Kaufmann.