International Journal of Science and Informatics Technology (IJOSIT)
Vol 1, No 1, April 2026, pp. 21-29
https://www.ijosit.org/index.php/ijosit
ISSN: XXXX-XXXX

Implementation of the Discrete Fourier Transform (DFT) Steganography Method for Embedding Secret Messages in Image Media

Margan Rizkiano Ritonga, Maysya Faiftin Siringoringo, Cristina Situmorang
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

Abstract. Steganography is an information security technique that aims to hide secret messages within a storage medium so that their existence is not easily detected. Digital images are widely used as a medium for steganography because they have large storage capacity and good tolerance to pixel value changes. This study aims to implement and analyze a Discrete Fourier Transform (DFT)-based steganography method for embedding secret messages in digital images by utilizing the frequency domain. The methods used include transforming images from the spatial domain to the frequency domain using DFT, embedding secret messages in binary form in selected frequency coefficients, and performing inverse transformation using Inverse Discrete Fourier Transform (IDFT) to produce stego images. The extraction process is carried out by reading back the modified frequency coefficients. Evaluation is performed by comparing the visual quality of the original image and the stego image and testing the success of message extraction. Steganography is an information security technique. The results of the study show that the DFT-based steganography method is capable of producing stego images with visual quality that is very similar to the original image, making the secret message difficult to detect visually. However, there are still small differences in the message extraction results due to the rounding effect in the IDFT process. Overall, the DFT method is considered effective for hiding secret messages in digital images, but further development is needed to improve message extraction accuracy.
Keywords: Steganography, Discrete Fourier Transform, DFT, Information Security, Digital Images.

Corresponding Author:
Margan Rizkiano Ritonga
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

1. Introduction

The rapid development of digital technology has encouraged the increase of information exchange through various electronic media, such as text, digital images, audio, and video [1]. Digital information currently plays a very important role in various fields, including communication, education, business, and government. The ease of access and speed of data distribution through open networks, especially the internet, provide enormous benefits in supporting human activities. However, behind this convenience, there are various threats to information security, such as wiretapping, data theft, information manipulation, and data misuse by unauthorized parties. This situation makes information security one of the main issues in the development of modern information technology. Not only is protection of the message content needed, but also methods that can hide the existence of the message itself so as not to arouse suspicion during the transmission process. In the context of information security science, the need for hidden and adaptive security techniques is becoming increasingly urgent as digital analysis and attack capabilities develop [2].

One information security technique used to meet these needs is steganography, which is the technique of embedding secret messages into a cover medium so that the presence of the message cannot be detected by the naked eye. Digital images are often chosen as a medium for steganography because they have large storage capacity and good tolerance to small changes in pixel values. [3] In its application, digital image steganography can be performed in both the spatial domain and the transformation domain. The spatial domain method is relatively simple and easy to implement, but it has weaknesses in terms of resistance to image manipulation, such as compression, filtering, and reprocessing. In contrast, the transformation domain-based steganography method is considered superior because message insertion is performed on the frequency representation of the image, making it more resistant to various forms of manipulation. However, the transformation-based steganography approach still faces challenges, particularly in maintaining a balance between the visual quality of the stego image, message insertion capacity, and the accuracy of the message extraction process. This indicates a research gap related to optimizing the use of the frequency domain so that message insertion remains secure without significantly reducing system performance [4].

Based on these issues, this study aims to implement and analyze the Discrete Fourier Transform (DFT)-based steganography method in digital image media by utilizing the frequency domain as a medium for inserting secret messages. The DFT method is used to transform images from the spatial domain to the frequency domain, so that secret messages

ISSN: XXXX-XXXX

can be embedded in certain frequency coefficients that are less sensitive to visual changes [5]. The main scientific contribution of this research is the presentation of a systematic and easily replicable implementation of DFT-based steganography, accompanied by an evaluation of the visual quality of stego images and the success of the message extraction process. The novelty of this research lies in its implementative approach, which emphasizes the analysis of the influence of the transformation and inverse transformation (DFT–IDFT) processes on message extraction accuracy, thereby providing a clearer understanding of the potential and limitations of the DFT method in digital image steganography. Thus, this research is expected to serve as a reference for the development of frequency domain-based steganography methods in the future.

2. Literature Review and Problem Statement

Previous studies have shown that steganography is an effective information security technique for hiding secret messages in digital media, especially digital images. The steganography approach to digital images is generally divided into spatial domain and transformation domain methods [6]. Spatial domain methods, such as modifying bits in pixel values, are relatively simple and have a large insertion capacity, but tend to be less resistant to image manipulation and are easily detected through statistical analysis. As an alternative, transformation domain methods utilize the frequency representation of images so that messages are inserted into specific transformation coefficients that are not too sensitive to visual changes. One widely used transformation method is the Discrete Fourier Transform (DFT), which converts images from the spatial domain to the frequency domain by separating image information into amplitude and phase components. In its implementation, the secret message is first converted into binary form so that it can be structurally inserted into the selected frequency coefficients [7]. This process is then completed with a reverse transformation using Inverse Discrete Fourier Transform (IDFT) to produce the stego image. The results of various studies show that DFT-based steganography is capable of producing stego images with visual quality that is very similar to the original image, thereby maintaining the level of imperceptibility [8]. Image quality evaluations generally show low distortion values and a fairly high message extraction success rate. However, these studies also reveal several limitations, such as increased computational complexity, dependence on the selection of appropriate frequency coefficients, and the potential for message extraction errors due to rounding effects in the inverse transformation process. In addition, some studies still focus on quantitative results without providing an in-depth analysis of the relationship between the frequency transformation process, image visual quality, and the reliability of the extracted message [9].

Based on a review of previous studies, it can be identified that there are research gaps that are still open for further study. Although DFT-based steganography methods have been proven to improve the security and visual quality of stego images, the implementation and comprehensive analysis of the effect of message insertion in the frequency domain have not been fully discussed comprehensively. The main issue that arises is how to ensure that the message insertion process not only produces high-quality stego images, but also guarantees the accuracy and consistency of message extraction. In addition, the selection of frequency coefficients for the insertion process is still often done statically and has not been systematically analyzed for various image characteristics and message lengths, thus potentially affecting the stability of the hidden message. Therefore, this research problem is formulated as how to implement a Discrete Fourier Transform-based steganography method in a structured manner on digital images and analyze the effect of the insertion process in the frequency domain on the visual quality of the image and the success of message extraction. This research aims to contribute scientifically through an implementative and analytical approach that emphasizes the relationship between frequency transformation, imperceptibility of stego images, and the reliability of hidden data. Thus, this research is expected to enrich the study of digital image steganography and serve as a basis for the development of more accurate, secure, and efficient message hiding methods.

3. Material and Method

This section describes the materials and methods used in the research in a systematic and structured manner. The description includes the type of data or research material, supporting software, and the stages of the method applied in the process of inserting and extracting secret messages. The methods used are organized logically so that they can be replicated by other researchers. The explanation in this chapter focuses on how the research was conducted, starting from data preparation, image transformation, message insertion, to the evaluation stage of the Discrete Fourier Transform (DFT)-based steganography system performance [6].

 ISSN: XXXX-XXXX

3.1 Overview of Methods and Image Representation

This study implements steganography techniques in the frequency domain using Discrete Fourier Transform (DFT). The main principle of this method is to hide secret messages by modifying the frequency coefficients of digital images, so that the changes made do not cause significant visual differences, but the secret messages can still be extracted properly. The frequency domain approach was chosen because it is more resistant to visual interference and image manipulation than methods that work directly in the spatial domain [10].

In general, the steganography process in this study consists of two main stages, namely the message embedding process and the message extraction process. In the embedding stage, the secret message is embedded into the digital image by modifying the coefficients resulting from the DFT transformation. Next, in the extracting stage, the stego image is reanalyzed to obtain the secret message that was previously embedded by reading the changes in the frequency coefficients at the same location [5].

The digital images used in this study are mathematically represented as a two-dimensional matrix containing pixel intensity values. For grayscale images, each matrix element represents the gray level at a specific position with an image size of M\times N. Meanwhile, for color images, the image is represented in three color channels, namely red, green, and blue [8]. Each color channel is treated as a separate grayscale image and processed independently. The DFT transformation, message insertion, and image reconstruction processes are performed on each color channel so that the color characteristics of the original image are preserved.

A grayscale digital image is represented as a two-dimensional matrix:

$$f(x,y), \quad 0 \le x < M,\ 0 \le y < N$$

For RGB color images, the transformation is performed on each color channel (R, G, B).

3.2 Two-Dimensional Fourier Transform

1. Discrete Fourier Transform (DFT)
   DFT is used to transform images from the spatial domain to the frequency domain [11]:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\ e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

   Dimana:
   $F(u,v)$ = complex frequency coefficient
   u, v = frequency index
   $j = \sqrt{-1}$

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\ e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

   Magnitude and phase:

$$|F(u,v)| = \sqrt{R^2 + I^2}, \qquad \theta(u,v) = \tan^{-1}\left(\frac{I}{R}\right)$$

2. Inverse Discrete Fourier Transform (IDFT)

$$f(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)\, e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

3.3 Message Embedding Process

1. Message Conversion
   Text message → ASCII → binary:

$$m = \{b_1, b_2, b_3, \dots, b_k\}, \quad b_i \in \{0,1\}$$

2. Frequency Location Selection
   Medium frequency coordinates (uk, vk) are selected to maintain visual quality.
3. Magnitude Insertion Model

$$|F'(u_k, v_k)| = |F(u_k, v_k)| + \alpha \cdot b_i$$

   So that the new coefficient:

$$F'(u_k, v_k) = |F'(u_k, v_k)|\, e^{\,j\theta(u_k, v_k)}$$

4. To maintain the Fourier symmetry of the real image:

$$F'(M - u_k,\, N - v_k) = F^*(u_k,\, v_k)$$

5. Stego Image Reconstruction

$$f'(x, y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F'(u, v)\; e^{\,j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)}$$

6. Message Extraction Process
   a. Perform DFT on the stego image → $F'(u, v)$
   b. Take the magnitude at the same coordinates
   c. Bit extraction:

$$\hat{b}_i = \begin{cases} 1, & |F'(u_k, v_k)| - |F(u_k, v_k)| \geq \frac{\alpha}{2} \\ 0, & \text{lainnya} \end{cases}$$

   d. Bit → ASCII → text

7. Steganography Performance Evaluation
   a. Mean Squared Error (MSE)

$$\text{MSE} = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \big(f(x, y) - f'(x, y)\big)^2$$

   b. Peak Signal-to-Noise Ratio (PSNR)

$$\text{PSNR} = 10 \log_{10} ! \left(\frac{255^2}{\text{MSE}}\right)$$

   c. Structural Similarity Index (SSIM)

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

 ISSN: XXXX-XXXX

8. System Flowchart

Embedding Flowchart The flowchart shown illustrates the workflow of a Discrete Fourier Transform (DFT)-based steganography system consisting of two main processes, namely message embedding and message extraction. This diagram helps clarify the structured stages of the system from input to output [12].

a. Embedding Process Flowchart

The embedding process begins with the original image (cover image) that will be used as a medium for storing secret messages. This image is then processed using DFT transformation to convert the image from the spatial domain to the frequency domain. It is in this frequency domain that the message information will be embedded. Next, the secret message is converted into binary form so that it can be inserted into the numerical frequency coefficient data. The message bits are then embedded into specific DFT coefficients, usually at medium frequencies, so that the changes are not visually noticeable but remain stable. After all the message bits have been embedded, the system performs an Inverse DFT (IDFT) to return the image to the spatial domain. The end result of this process is a stego image, which is an image that contains a secret message without any noticeable visual differences from the original image.

b. Extraction Process Flowchart

The extraction process begins with the input of a stego image, which is an image suspected of containing a hidden message. This image is transformed back into the frequency domain using DFT. Once in the frequency domain, the system will take the frequency coefficients at the same position as the location where the message was inserted. From these coefficients, the system extracts the message bits by reading the changes in value that occurred as a result of the embedding process. The bits obtained are then converted back into text form, so that the original secret message can be read again. If the process runs correctly, the extracted message will be the same as the message that was embedded previously.

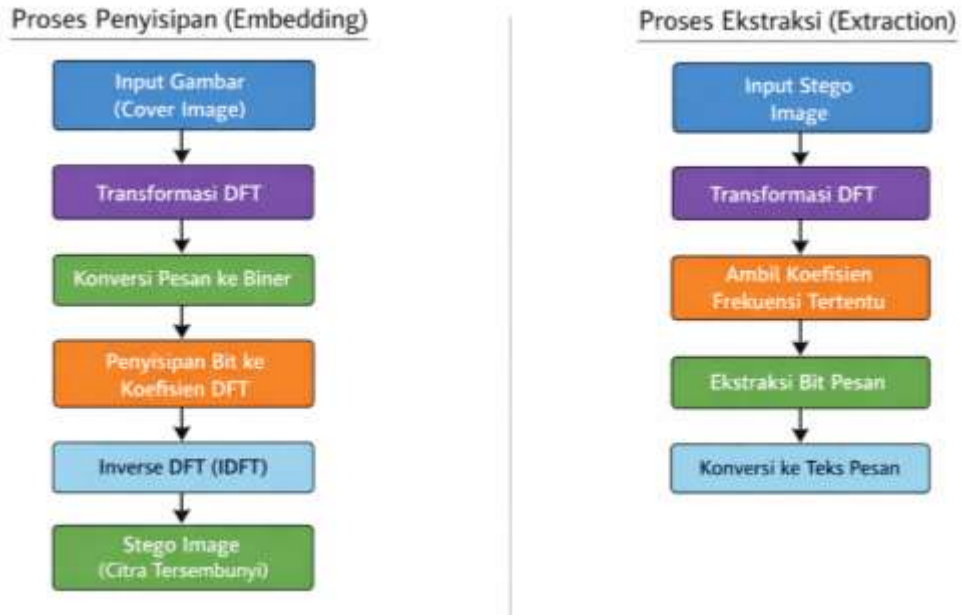

Figure 1. DFT Embedding and Extraction Flowchart

This figure shows the workflow of a Discrete Fourier Transform (DFT)-based steganography system, which consists of two main processes: message embedding and message extraction. In the embedding process, the host image is transformed into the frequency domain using DFT, then the secret message is converted into binary form and embedded into selected frequency coefficients before inverse DFT is performed to produce the stego image. Meanwhile, in the extraction process, the stego image is transformed back into the frequency domain to retrieve the modified coefficients, extract the message bits, and convert them back into text form.

ISSN: XXXX-XXXX

4 Research And Discussion

This section discusses the research results obtained from the application of the Discrete Fourier Transform (DFT)-based steganography method to digital images. The results presented include the process of message insertion and extraction as well as the evaluation of stego image quality. The discussion focuses on interpreting the research results to assess the effectiveness of the method in maintaining the visual quality of images and the success of message concealment.

4.1 Results I: Message Insertion and Extraction in Medium-Sized Images

Based on the results of testing the Discrete Fourier Transform (DFT)-based steganography program, a digital image measuring 640 × 594 pixels was used as the medium for storing secret messages. The image has a large number of pixels, allowing the message to be inserted without causing significant visual changes. In the DFT method, the message is not inserted directly into the pixel values, but rather into the frequency coefficients resulting from the transformation of the image into the frequency domain.

The secret message inserted during the insertion process is the text “suka”. The message is converted into binary form based on ASCII representation and a message end marker is added as a delimiter. The converted binary data is then inserted into a number of selected DFT frequency coefficients, with the aim of maintaining the quality of the inserted image so that it resembles the original image.

The resulting stego images show that visually there are no noticeable differences between the images before and after message insertion. This is because the data insertion is performed in the frequency domain with relatively small changes in value, making it difficult to detect by human visual observation. Thus, the DFT method is able to maintain the visual quality of the image even after a secret message has been inserted.

During the extraction stage, the stego image is reprocessed using DFT transformation to read the modified frequency coefficients. These coefficient values are converted back into binary data, then translated into text form. However, the extracted message in this test did not match the original message and produced characters that were not read correctly. This indicates that there are still inconsistencies in the decoding process. The inconsistency in the extraction results may be caused by differences in the selection or order of frequency coefficients between the insertion and extraction processes, the effect of rounding values in the inverse DFT process, or small disturbances in the frequency values that cause changes in the message bits. Nevertheless, these results still show that the DFT-based steganography method is capable of hiding secret messages well without significantly reducing the visual quality of the image, but it still needs improvement so that the message extraction process can produce messages that are the same as the inserted messages.

Figure 2. Message Insertion and Extraction Process on a 640 × 594 Pixel Image

The message insertion and extraction process on a medium-sized image is shown in Figure 2. The figure shows the interface of the DFT-based steganography system at the encode and decode stages.

 ISSN: XXXX-XXXX

4.2 Test Results II: Analysis of Bit Insertion on the Number of Frequency Coefficients

Based on the results of testing the Discrete Fourier Transform (DFT)-based steganography program, a 160 × 160 pixel digital image was used as the medium for storing secret messages. The image has a total of 25,600 pixels, but not all pixels are modified in the insertion process. The insertion is performed in the frequency domain by utilizing the coefficients resulting from the DFT transformation of the image [8].

The secret message entered is the text "gasuka," which is then converted into binary form using 8-bit ASCII representation. After adding the end-of-message marker, the length of the binary data becomes 64 bits. This binary data is then inserted into 64 DFT frequency coefficients, so that each bit of the message is represented by one frequency coefficient. The coefficients used are selected so that changes in frequency values do not cause significant visual differences in the inserted image.

Visually, the stego image does not show any noticeable differences compared to the original image. This is because the message is inserted into the frequency domain with very small changes in value, making it difficult to detect by human visual observation. The number of message bits and the number of frequencies used are displayed in the program as indicators that the insertion process has been carried out in accordance with the length of the message entered.

The resulting stego image does not visually show any significant differences compared to the original image. This is due to the message insertion being performed in the frequency domain with very small value changes, making it difficult for human visual observation to detect. Information on the number of message bits and the number of frequencies used is displayed in the program as an indicator that the insertion process has been carried out according to the length of the input message.

During the extraction stage, the stego image is reprocessed using DFT transformation to read the modified frequency coefficient values. The extraction process produces binary data which is then converted back into text. However, the resulting text does not match the original message and displays unreadable characters. This indicates an inconsistency in the decoding process, which may be caused by differences in the order of the frequency coefficients read, rounding errors in the frequency values, or failure to detect the end-of-message marker. Overall, the test results show that the DFT-based steganography method is capable of hiding secret messages well without significantly altering the visual quality of the image. However, the success of message extraction still needs improvement so that the embedded messages can be accurately reconstructed.

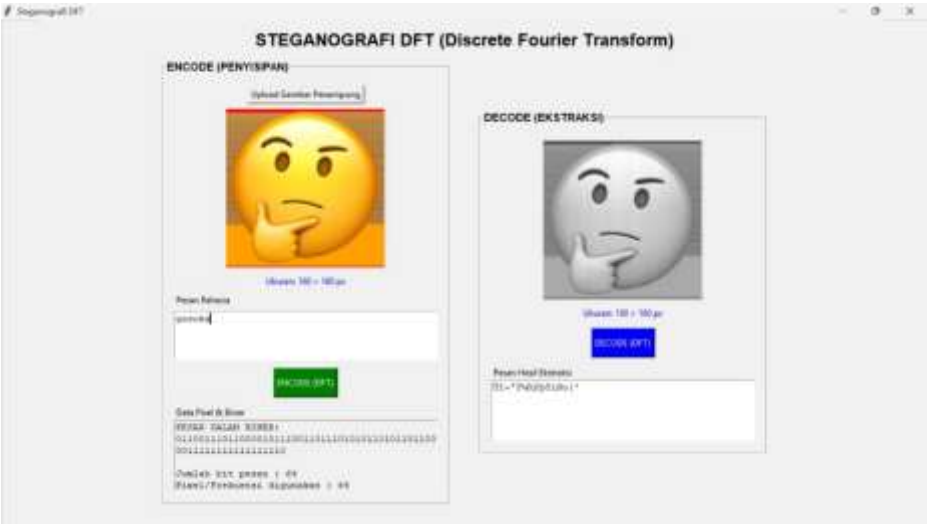

Figure 3. Bit Insertion and Extraction Process in a 160 × 160 Pixel Image

Figure 3 shows the relationship between the number of message bits inserted and the number of frequency coefficients used in the DFT-based steganography process.

4.3 Test Results III: Detailed Simulation of the Encoding and Decoding Process

Based on the results of the Discrete Fourier Transform (DFT)-based steganography simulation, a digital image measuring 820 × 826 pixels was used as the medium for storing the secret message. An image of this size provides a large number of pixels, allowing for a more detailed transformation to the frequency domain. In this method, the message is not inserted directly into the image pixel values, but rather into the frequency coefficients resulting from the DFT transformation.

The secret message inserted during the insertion stage is the text “lazy.” The message is converted into binary form based on ASCII representation and a message end marker is added as a delimiter. The binary representation of the message is displayed directly in the insertion simulation section, allowing users to see the binary data that will be inserted into the image frequency coefficients.

During the encoding simulation process, the system displays in detail each step of inserting message bits into specific frequency coefficients. The information displayed includes the frequency position used, the real value of the DFT coefficient before or after modification, and the inserted message bits. Insertion is carried out gradually at several predetermined frequency positions, so that the data change process can be observed transparently.

The image results after the insertion process retain a visual appearance similar to the original image. This shows that the changes in frequency coefficient values made during the insertion process do not have a significant visual impact, making the secret message difficult to detect visually. During the decode simulation stage, the stego image is reprocessed using DFT transformation to extract the embedded message. The extraction process is also displayed in stages, where the system shows the frequency position read, the real value of the frequency coefficient, and the bits successfully extracted from each position. The extracted bit data is then reassembled into a binary sequence and converted into text form.

Based on the extraction simulation results shown, the message obtained does not fully match the original message inserted and produces unreadable characters. This indicates that there are still discrepancies in the extraction process, which may be caused by differences in coefficient values due to the inverse DFT process, rounding of numerical values, or inaccuracies in the selection and reading of frequency positions.

Overall, this DFT steganography simulation provides a clear picture of the message insertion and extraction mechanisms in the frequency domain. The step-by-step simulation displayed helps in understanding how each message bit is mapped to the frequency coefficients of the image. Although the visual quality of the image is maintained, the message extraction results show that this method still needs improvement so that secret messages can be accurately reconstructed.

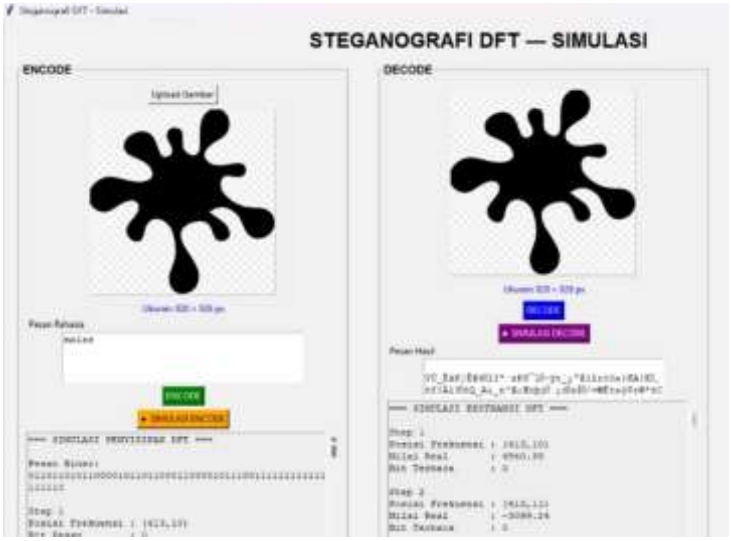

Figure 4. Simulation of DFT-Based Message Encoding and Decoding Processes

Simulation display of the message insertion and extraction process showing message bits, frequency coefficient positions, and extracted message results.

5 Conclusion

This study shows that Discrete Fourier Transform (DFT)-based steganography is capable of hiding secret messages in digital images with a good level of imperceptibility, so that the visual quality of the stego image remains similar to the original image. The implementation results prove that insertion in the frequency domain is effective in minimizing visual distortion and addresses the main problem related to the need for steganography methods that are difficult to detect with the naked eye. However, the test results also reveal limitations in the extraction stage, where the message obtained is not completely

identical to the original message. This confirms the existence of a research gap in the aspect of decoding reliability, as formulated in the problem statement. Thus, this study contributes to proving the effectiveness of DFT as a method of embedding messages in digital images while opening up opportunities for further development to improve message extraction accuracy.

6 References

[1] A. H. Hasugian, I. Rusydi, and P. Apriani, "TEKNIK STEGANOGRAFI DISCRETE COSINE TRANSFORM DAN ALGORITMA RSA UNTUK MENYISIPKAN PESAN PADA AUDIO," 2024. [Online]. Available: http://ojsamik.amikmitragama.ac.id

[2] K. Dharma Kusumah, J. Pragantha, and N. Jaya Perdana, "STEGANOGRAPHY IMPLEMENTATION OF INSERTION OF CONFIDENTIAL DATA ON DIGITAL IMAGE MEDIA," International Journal of Application on Sciences, Technology and Engineering, vol. 1, no. 2, pp. 695–702, May 2023, doi: 10.24912/ijaste.v1.i2.695-702.

[3] D. Sebagai et al., "STEGANOGRAFI GAMBAR MENGGUNAKAN METODE LEAST SIGNIFICANT BIT PADA CITRA DENGAN OPERASI XOR TUGAS AKHIR."

[4] A. Tauhid, M. Tasnim, S. A. Noor, N. Faruqui, and M. A. Yousuf, "A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform," Journal of Information Security, vol. 10, no. 03, pp. 117–129, 2019, doi: 10.4236/jis.2019.103007.

[5] B. Yafis and H. Rijal, "Analisa Respon Frekuensi Citra Digital Menggunakan Metode Transformasi Fourier Diskrit," 2023.

[6] P. R and I. R.J, "An Overview of Digital Image Steganography," International Journal of Computer Science & Engineering Survey, vol. 4, no. 1, pp. 23–31, Feb. 2013, doi: 10.5121/ijcses.2013.4102.

[7] Y. Ariyanto et al., "STEGANOGRAFI MENGGUNAKAN METODE DISCRETE FOURIER TRANSFORM (DFT)."

[8] A. Soni, J. Jain, and R. Roshan, Image Steganography using Discrete Fractional Fourier Transform.

[9] B. Cornelius, "Makalah IF4020 Kriptografi-Teknik Informatika ITB-Semester I Tahun," 2025.

[10] L. Vinitha Sree, "Steganography Using Dft Based Texture Synthesis," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 9, p. 2, 2020, [Online]. Available: www.ijstr.org

[11] M. Solikhin, Y. Pratama, P. Pasaribu, J. Rumahorbo, and B. Simanullang, "Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT)," 2022.