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 Cosine Transform (DCT) Steganography Method for Embedding Secret Messages in Image Media

Amsal Tampubolon[1], Michael Ginting[2], Eunike Charina I. Tarigan[3]
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas, Medan

Article Info
Corresponding Author:
Amsal Tampubolon

ABSTRACT
Steganography is a technique for hiding secret information within a cover medium so that the existence of the message is not easily detected. One of the steganography methods widely used in image media is the Discrete Cosine Transform (DCT), which works by transforming an image into the frequency domain before message embedding is performed. This study aims to implement a DCT-based steganography method for embedding secret messages into image media and to analyze the quality of the resulting stego images. The embedding process is carried out by modifying DCT coefficients in certain image blocks so that the resulting changes are not visually noticeable. The experimental results show that the DCT method is able to embed secret messages into images with a low level of distortion while maintaining visual quality. Thus, the DCT steganography method is proven to be effective as one of the image-based information security techniques.

Keywords: Steganography, Discrete Cosine Transform (DCT), Message Embedding, Digital Image, Information Security.

INTRODUCTION

In the current digital era, data security is very important to protect information from unauthorized access [1]. Steganography originates from the Greek language, meaning “hidden writing” [2]. The basic concept of digital steganography consists of three main elements, namely the cover object as the carrier medium, the message as the secret information, and the stego key as the secret key [2]. Steganography is a method of transmitting secret information through public communication channels without raising suspicion, so that third parties are unaware of the existence of hidden messages [3].

A steganographic method can be considered good if it meets several criteria, namely the embedded message is not detectable (imperceptibility), the cover medium after embedding remains nearly identical to the original (fidelity), the secret message can withstand various processing or modifications applied to the cover medium (robustness), and the embedded information can be properly extracted (recovery) [4]. The advantage of steganography compared to cryptography is its ability to conceal secret messages without arousing suspicion from adversaries [5]. Steganography provides various digital media as carriers for message embedding, such as images (JPEG, bitmap, GIF), audio (WAV, VOC, MP3), as well as other media such as text files, HTML, PDF, and so on [6].

DCT (Discrete Cosine Transform) is one of the effective steganography techniques because it produces compressed representations, which do not raise suspicion about the

existence of secret data. In addition, DCT is more resistant to manipulation of the stego object compared to other steganography methods such as LSB, which has limited embedding capacity and is sensitive to filtering processes [7]. DCT is a lossy compression scheme that works by transforming NxN blocks from the spatial domain into the DCT domain [8]. The system implementation is carried out by encoding messages using image steganography, where the encrypted message is hidden within a color image (RGB) in the Discrete Cosine Transform domain using a Spread Spectrum embedding technique [9]. Data embedding using DCT has the advantage that information can be inserted into less significant coefficient bits [10].

LITERATURE REVIEW

Image steganography is an information security technique that hides secret messages within digital media so that their existence is difficult to detect by unauthorized parties. This method is divided into spatial domain and transform domain approaches. In the transform domain, such as the Discrete Cosine Transform (DCT), an image is converted from the spatial domain into the frequency domain so that data can be embedded into coefficients that are less sensitive to human visual perception [11]. In addition, the development of machine learning and reinforcement learning integration has begun to be utilized to improve the performance of DCT-based steganography. One recent approach is the use of deep reinforcement learning for adaptive DCT block selection, allowing a better balance between image quality and embedding security, and demonstrating the current research direction in this field [12].

As an example, a study conducted by Sujarwo (2025) proved that the application of DCT can produce high PSNR values and low MSE values. This condition indicates that the visual differences after the embedding process are very minimal, making it difficult to detect by human visual observation. These findings indicate that this method has a higher level of effectiveness compared to spatial-domain-based steganography techniques when evaluated through simple visual analysis [13].

RESEARCH METHOD

This study employs an experimental method by designing, implementing, and testing an image steganography application based on the Discrete Cosine Transform (DCT) combined with the Least Significant Bit (LSB) technique. This approach aims to achieve a balance between image quality (imperceptibility), message extraction success (recovery), and embedding robustness.

Scope and Method Approach

The steganography method applied is a DCT-based LSB hybrid approach, where DCT transformation is used as the basis for image analysis, while the message embedding process is performed by modifying the least significant bit (LSB) of image pixel values. This approach is chosen because it is relatively simple to implement while still providing better resistance compared to the pure LSB method.

Research Tools and Materials

The tools and materials used in this study are as follows:

Software

1. Python programming language
2. Tkinter library as a graphical user interface (GUI)

3. OpenCV for digital image processing
4. NumPy for numerical computation
5. SciPy for DCT and inverse DCT transformations

Hardware: Laptop or computer with Windows operating system.

Test Data

1. Digital images in PNG, JPG, and JPEG formats
2. Secret messages in text form

Research Stages

The research stages are carried out as follows:

a. Literature study on image steganography and DCT methods
b. Algorithm design for embedding and extraction processes
c. Implementation of the algorithm using Python programming language
d. Development of a user interface using Tkinter
e. System testing and result analysis

Message Embedding Process (Embedding)

Based on the developed program code, the embedding process is carried out through the following steps:

a. The user selects a cover image through the application interface
b. The secret message is appended with a delimiter to mark the message boundary
c. The message is converted into binary form using 8-bit ASCII representation
d. The system reads the digital image and extracts the blue channel, which is relatively more stable to visual changes
e. The message bits are embedded into the least significant bit (LSB) of the blue channel pixel values sequentially
f. The resulting stego image is saved in PNG format without compression to maintain data integrity

Message Extraction Process (Extraction)

The extraction process is carried out through the following steps:

a. The user selects the stego image through the application
b. The system reads the blue channel of the stego image
c. The message bits are extracted from the LSB of each pixel
d. The extracted bits are converted back into text form
e. The extraction process stops when the message delimiter is detected

User Interface Design

The user interface is designed using the Tkinter library and consists of three main tabs: Hide Message, Extract Message, and Information. This interface allows users to interact with the system intuitively without requiring technical understanding of steganographic algorithms.

RESULTS AND DISCUSSION

System Implementation Results

The interface consists of an image selection menu, secret message input, embedding process button, and message extraction feature. The result of this research is an image steganography application based on a DCT-based LSB hybrid approach that is capable of embedding and extracting secret messages in digital images. The application runs properly in a desktop environment, and all main features function according to the design.

During the message embedding process, the system successfully stored the secret message within the image without causing significant visual changes. This indicates that the implemented algorithm is able to maintain the quality of the stego image. The following are the stages of message embedding using DCT-based steganography:

a. The user runs the application by executing the Python program file. After the application is launched, the main steganography application window will appear.
b. Message Embedding Process (Embedding)

The steps of message embedding are as follows:

1. The user opens the Hide Message tab

Figure 1. Hide Message

2. The user selects a cover image by clicking the Select Image button.

Figure 2. Select Image

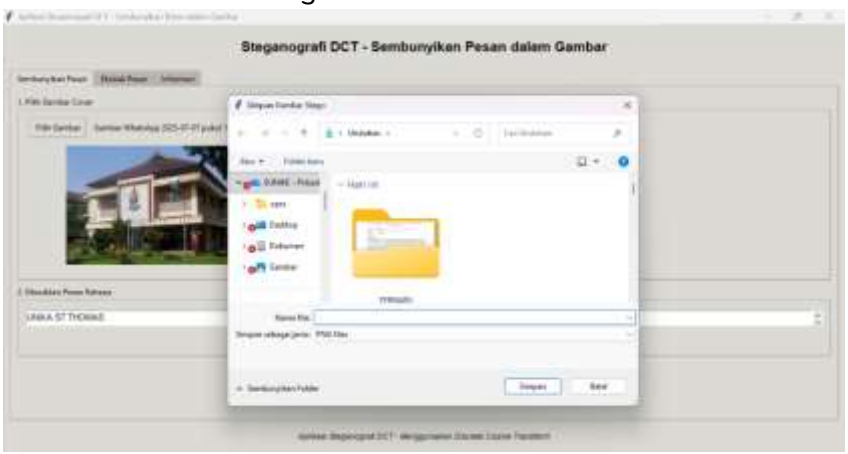
3. The system displays an image preview and embedding capacity information.

Figure 3. Image Preview and Embedding Capacity Information

4. The user enters the secret message into the provided text box.

Figure 4. Entering the Secret Message into the Text Box

5. The user clicks the Hide Message button.



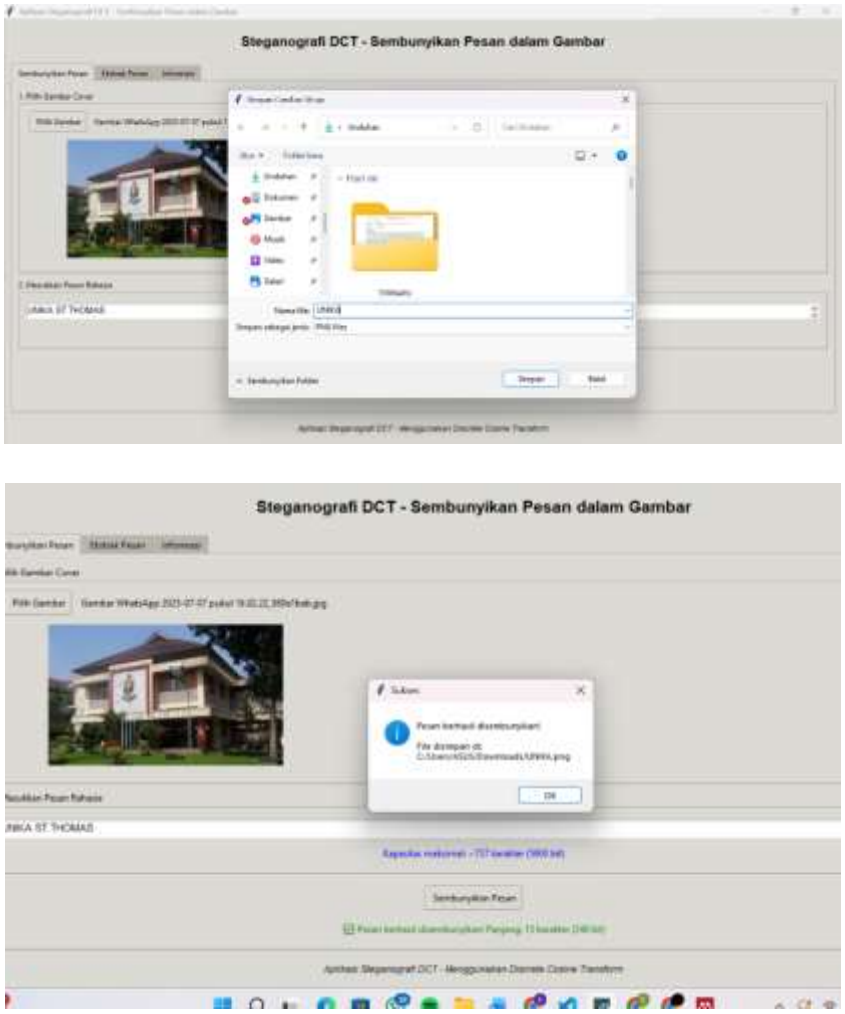


Figure 5. Hide Message

6. The system processes the message embedding and saves the stego image in PNG format.

Message Extraction Process (Extraction)

Steps for message extraction:

1. The user runs the application.

Figure 6. Running the Application

2. The user selects the stego image through the application.

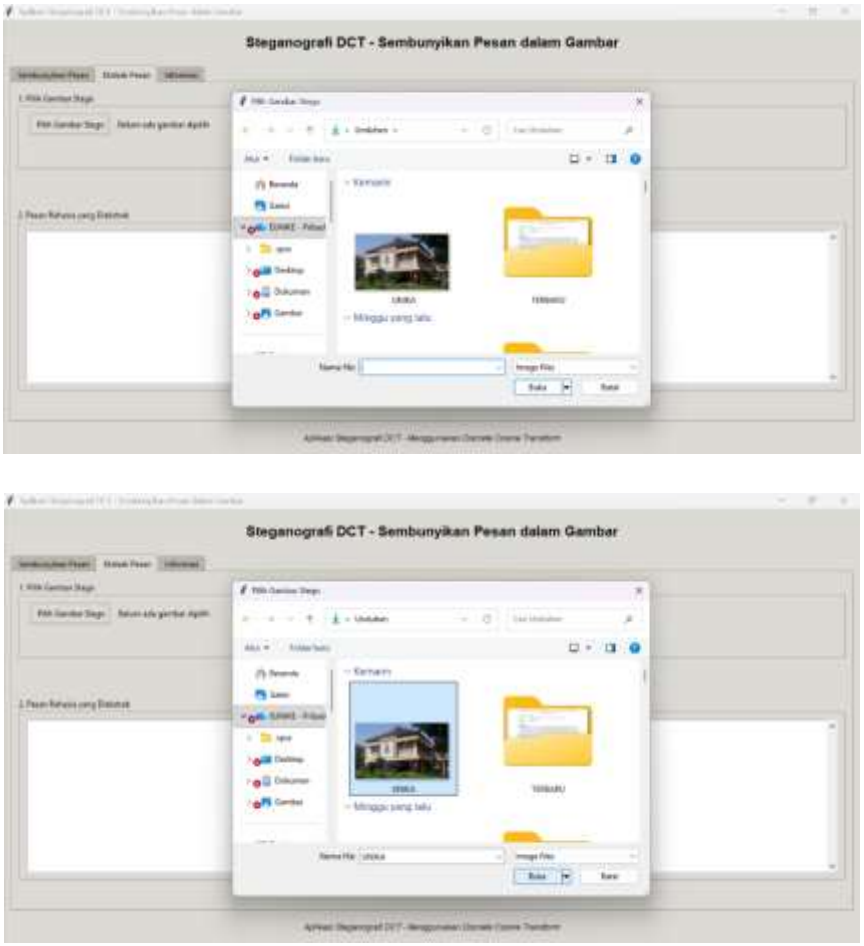


Figure 7. Selecting the Image

3. The selected image is displayed.

Figure 8. Displaying the Image

4. The user clicks the Extract Message button. If the process is successful, a pop-up information message appears stating “Message successfully extracted”.

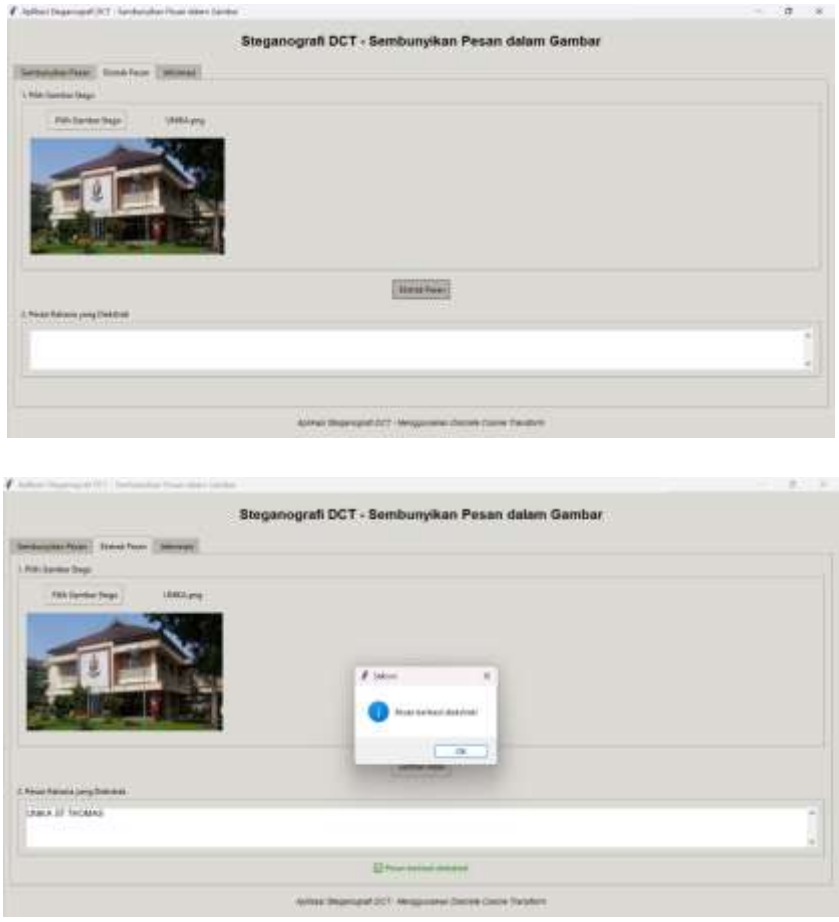


Figure 9. Extract Message

1. Imperceptibility and Fidelity Analysis
   The imperceptibility analysis was conducted by visually comparing the cover image and the stego image. Based on the observations, no noticeable differences were found between the two images. The embedding of the message into the LSB of the blue channel causes very minor pixel value changes that are not detectable by the human eye. In addition, the visual structure of the image remains well preserved, indicating that the method satisfies the fidelity aspect. This shows that using the blue channel as the embedding medium is an appropriate choice for maintaining image quality.
2. Message Extraction Success (Recovery) Analysis
   The extraction testing shows that the secret message can be fully and accurately retrieved as originally embedded. The use of a delimiter as an end-of-message marker helps the system accurately determine message boundaries, thereby improving the reliability of the extraction process. The success of this recovery process indicates that the implemented method has a good level of data consistency.
3. Robustness Analysis
   Although the embedding process is carried out using the LSB technique, the use of the lossless PNG storage format improves the resistance of the embedded data against information loss. In addition, the use of DCT concepts as the basis for image analysis provides potential for further development to enhance robustness against image manipulation such as compression and filtering. Compared to the pure LSB method, this hybrid approach produces more stable results in both message storage and extraction processes.

Discussion

The results of this study indicate that the implementation of the DCT-based LSB hybrid steganography method is capable of operating optimally in both the embedding and extraction of secret messages in digital images. The developed system not only successfully performs its main functions but also demonstrates good performance in terms of image quality and data reliability.

From the perspective of image quality (imperceptibility and fidelity), the test results show that the generated stego images have a very high level of similarity to the original images. This is due to the embedding technique applied to the least significant bit (LSB) of the blue channel, which is physiologically less sensitive to human visual perception. As a result, the changes in pixel values are insignificant and do not produce visible distortion. This finding reinforces the theory that the selection of specific color channels can influence the quality of steganographic results.

In addition, the combination with the Discrete Cosine Transform (DCT) provides an important contribution to maintaining image structural stability. The transformation into the frequency domain allows the identification of image components that are less sensitive to modification, thereby making data embedding more secure. This is consistent with previous studies stating that transform-domain-based methods have advantages over pure spatial-domain approaches in preserving visual quality.

In terms of extraction success (recovery), the system demonstrates a high level of accuracy. All embedded messages can be fully extracted without any information loss. The use of a delimiter as an end-of-message marker has proven effective in preventing data reading errors. This indicates that the system maintains strong data consistency during both the embedding and extraction processes.

Furthermore, regarding robustness, the method shows fairly good performance, particularly due to the use of the lossless PNG format. This prevents embedded data from being damaged by compression processes. However, when compared to full transform-domain steganography methods, this hybrid approach still has limitations in handling image manipulations such as JPEG compression, cropping, or intensive filtering. Therefore, although it performs better than pure LSB methods, its robustness can still be improved in future research.

From the implementation perspective, the use of a Tkinter-based interface provides ease of use for users in operating the application. This is an added value, as the system not only focuses on technical aspects but also considers usability. With an intuitive GUI, even non-technical users can easily utilize the application.

Compared to previous studies, the results of this research are consistent with findings that combining spatial-domain and transform-domain methods can improve steganographic performance. The added value of this study lies in its simple yet effective implementation, making it a practical solution for image-based information security.

Overall, this study shows that the DCT-based LSB hybrid method is a balanced approach in terms of image quality, embedding capacity, and implementation simplicity. However, to achieve higher security, further development is needed, such as integration with cryptographic algorithms or the application of artificial intelligence techniques to improve system adaptability against various types of attacks.

CONCLUSION

Based on the results of this study, it can be concluded that the Discrete Cosine Transform (DCT) method is effective for embedding secret messages in digital image media. The developed application is able to embed and extract messages properly without significantly degrading the visual quality of the image. The use of a Tkinter-based graphical user interface also simplifies system operation for users. Future research may further enhance this method by incorporating cryptographic techniques or machine learning approaches to improve system security.

REFERENSI

[1] D. H. Zulfikar, "Data Hiding menggunakan Play Fair Kriptografi dan Steganografi pada Domain DCT dengan Operasi Logika XOR," *J. Softw. Eng. Comput. Intell.*, vol. 3, no. 01, pp. 18–28, 2025, doi: 10.36982/jseci.v3i01.5410.

[2] R. Fahmi, B. Rizky, M. Z. Mubaraq, R. Sahara, and I. S. Panjaitan, "Evaluasi Teknik Steganografi dan Efektivitasnya dalam Perlindungan Informasi," vol. 2, no. 1, pp. 19–21, 2026.

[3] D. Zulfikar and H. Hermanto, "Hamming Code in JPEG Image Steganography within the Discrete Cosine Transform Domain," *J. Appl. Informatics Comput.*, vol. 9, no. 3, pp. 868–875, 2025, doi: 10.30871/jaic.v9i3.9387.

[4] D. H. Zulfikar, "Quality Factor terhadap Kapasitas Pesan Rahasia pada Steganografi Citra JPEG dan Kualitas Citra Stego," vol. 6, no. 2, 2020.

[5] R. K. Dewi and R. Munir, "PERBANDINGAN BERBAGAI METODE STEGANOGRAFI PADA CITRA DIGITAL," pp. 289–300.

[6] H. Barasa, "Penyembunyian Pesan Teks Tersandi dengan Algoritma Massey Omura Pada Gambar Berdasarkan Metode Stegano F5," vol. 1, no. 1, pp. 13–22, 2021.

[7] A. Halim *et al.*, "TEKNIK STEGANOGRAFI DISCRETE COSINE TRANSFORM DAN ALGORITMA RSA UNTUK MENYISIPKAN PESAN PADA AUDIO," vol. 8, no. 1, pp. 1–9, 2024.

[8] M. M. Dct-dwt, A. S. Pratama, and I. M. Suartana, "Analisis Kualitas Stego Video dalam Penyisipan Data," vol. 05, pp. 13–18, 2021.

[9] A. R. Mido *et al.*, "Perancangan Aplikasi Steganografi Menggunakan Metode Discrete Cosine Transformation berbasis Android," pp. 25–36.

[10] R. Fahmi, N. Imanudin, I. Kustiawan, and S. Elvyanti, "Steganografi Citra Digital Menggunakan Pendekatan Least Significant Bit dan Discrete Cosine Transform," no. 207.

[11] K. R. Malik *et al.*, "OPEN A hybrid steganography framework using DCT and GAN for secure data communication in the big data era," pp. 1–23, 2025.

[12] R. Yang, L. Liu, B. Han, and F. Hu, "Deep Reinforcement Learning-Based DCT Image Steganography," pp. 1–19, 2025.

[13] V. N. June, "INFORMATION SYSTEM SECURITY USING THE DISCRETE COSINE TRANSFORM (DCT) METHOD," vol. 5, no. 1, 2025.