International Journal of Science and Informatics Technology (IJOSIT*)* ISSN: XXXX-XXXX
Vol 1, No 1, April 2026, pp. 14-20
https://www.ijosit.org/index.php/ijosit

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

Devi Sari Delima Tumanggor, Evaldo Manurung, Raymon Simamora
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

Abstract. The increasingly massive exchange of digital data in the information technology era increases the risk of information leaks and misuse, requiring security mechanisms that not only protect the content of messages but also conceal their existence. Steganography is one relevant solution because it can insert secret messages into digital media without arousing visual suspicion. This research aims to implement a Discrete Cosine Transform (DCT)-based steganography method for embedding and extracting secret messages in digital images using the Python programming language. The approach used includes level shifting, image transformation from the spatial domain to the frequency domain using DCT, message bit insertion into the middle frequency coefficients using the Least Significant Bit (LSB) technique, and the inverse DCT process to obtain the stego image and message extraction stage. The system is also equipped with a graphical user interface (GUI) to facilitate the encoding and decoding processes. Test results show that messages can be inserted and extracted back intact without causing significant visual changes to the stego image, thus maintaining image quality. These findings indicate that the DCT method has a high level of imperceptibility and is effective in enhancing the security of digital image-based information. Thus, the DCT-based steganography method can be a reliable alternative solution for security.

Keywords: Steganography, Discrete Cosine Transform, Image Security.

This is an open access article under theCC BY-NClicense

Corresponding Author:
Raymon Simamora
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

1. Introduction

The development of information and communication technology has driven massive growth in digital data exchange, whether in the form of text, images, audio, or video. This situation presents serious challenges in terms of information security, particularly with regard to confidentiality and the protection of sensitive data. In addition to cryptography, which focuses on securing the content of messages, steganography has developed as an alternative approach that conceals the very existence of messages within digital media. In the context of digital image processing, the use of frequency transformations such as Discrete Cosine Transform (DCT) is relevant because it can maintain visual quality while providing a space for data insertion that is relatively undetectable [1]. Therefore, the development of DCT-based steganography methods is important as part of a data security solution that is adaptive to developments in digital technology [2].

Although various steganography techniques have been developed, the main challenge still revolves around the balance between message insertion capacity, resistance to interference, and the visual quality of the inserted image [3]. Spatial domain-based approaches, such as Least Significant Bit (LSB) directly on pixels, tend to be easier to detect or vulnerable to image manipulation [3]. On the other hand, frequency domain-based methods offer better resistance, but their implementation is often not optimized in terms of selecting the appropriate embedding coefficients to maintain imperceptibility. This indicates a need to design and implement a DCT-based embedding scheme that can improve security without significantly compromising image quality [4].

This research aims to implement a Discrete Cosine Transform (DCT)-based steganography method in embedding secret messages in image media by utilizing bit embedding techniques in mid-frequency coefficients. The main scientific contribution lies in the design of an integrated system flow starting from frequency domain transformation, message embedding and extraction mechanisms, to the evaluation of the quality of the steganography image. Conceptually, the novelty of this research lies in the optimization of message embedding in the frequency domain using a combination of DCT and bit-level embedding techniques designed to improve imperceptibility while maintaining message integrity. This approach is expected to provide a more effective and applicable alternative in digital image-based information security.

2. Literature Review and Problem Statement

Various studies have examined the application of steganography in digital images, both in the spatial domain and the frequency domain. The Least Significant Bit (LSB) method in the spatial domain is known to be simple and has high insertion capacity, but it is relatively vulnerable to detection and image manipulation [3]. To improve robustness, a number of studies have developed frequency transformation-based approaches such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) . Shows that embedding in the frequency domain can improve robustness against compression and interference. Furthermore, DCT-based steganography techniques are widely applied to JPEG images by embedding messages in specific frequency coefficients to maintain visual quality [4]. Several studies have also combined DCT with LSB techniques to achieve a balance between imperceptibility and message capacity. However, these studies generally still face limitations in optimizing frequency coefficient selection, comprehensive quantitative evaluation of image quality, and integration of applicable and easy-to-use systems [5].

Based on a review of the literature, there is still a gap in the implementation of DCT-based steganography that is capable of simultaneously maintaining image visual quality, preserving message integrity, and providing an integrated system for the insertion and extraction processes. Previous studies have tended to focus on theoretical aspects or on improving only one performance parameter, such as capacity or robustness, without optimizing the overall balance. In addition, the selection of frequency coefficients for message insertion is often done without a systematic approach that considers optimal imperceptibility. Therefore, the research problem is formulated as follows: how to implement a Discrete Cosine Transform (DCT)-based steganography method with the appropriate insertion technique in the frequency domain so that messages can be inserted and extracted in their entirety without significantly reducing the visual quality of the image. This research aims to contribute through the design and implementation of an integrated DCT-based steganography system, with a focus on optimizing insertion in the mid-frequency coefficients to improve imperceptibility and information security effectiveness.

3. Material and Method

This section systematically describes the materials and methods used in the research, including the types of data used, supporting software, and the stages of the implementation procedure for the Discrete Cosine Transform (DCT)-based steganography method. The description is compiled to provide a clear picture of the research flow, starting from the image preparation process, transformation to the frequency domain, message insertion and extraction mechanisms, to system performance evaluation techniques. With this explanation, it is hoped that the research can be replicated and retested scientifically [4], [6].

3.1 Image Input

In this example, a grayscale image is used as the medium. Grayscale images have a single pixel intensity value ranging from 0 to 255, which facilitates the DCT calculation process. Example of image input [7]:

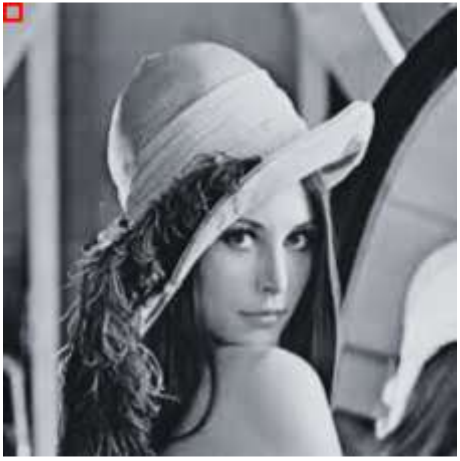


Figure 1. Image Input

From a 512×512 pixel grayscale image, an 8×8 pixel section of the image is selected. This 8×8 block is used because the standard DCT method works on 8×8 blocks. The pixel intensity values of the 8×8 block are arranged into a matrix as follows:

Table 1. 512×512 Pixel Image

120	122	125	130	135	138	140	142
118	120	123	128	133	136	138	140
115	118	120	125	130	132	135	138
112	115	118	122	128	130	132	135
110	112	115	118	122	125	128	130
108	110	112	115	118	120	122	125
105	108	110	112	115	118	120	122
102	105	108	110	112	115	118	120

Table 1 is an 8×8 block representation of a 512×512 pixel grayscale image, where each value indicates a gray intensity in the range of 0–255. The gradually increasing number pattern reflects the smooth brightness gradation in that part of the image. Blocks like this are commonly used in the Discrete Cosine Transform (DCT) process, because images are divided into 8×8 blocks before being transformed from the spatial domain to the frequency domain.

3.2 Level Shifting

Each pixel value is reduced by 128. The purpose of this step is to center the pixel values around zero using the formula

$$f'(x,y) = f(x,y) - 128$$

Table 2. Calculation results

-8	-6	-3	2	7	10	12	14
-10	-8	-5	0	5	8	10	12
-13	-10	-8	-3	2	4	7	10
-16	-13	-10	-6	0	2	4	7
-18	-16	-13	-10	-6	-3	0	2
-20	-18	-16	-13	-10	-8	-6	-3
-23	-20	-18	-16	-13	-10	-8	-6
-26	-23	-20	-18	-16	-13	-10	-8

Table 2 shows the results of the level shifting process on an 8×8 image block, which is done by reducing each pixel value by 128 (for example, 120 − 128 = −8). This process is performed before the Discrete Cosine Transform (DCT) so that the pixel value range, which was originally 0–255, shifts to −128 to 127, thereby centering the data around zero. This centering is important because DCT works more optimally when the input values have an average close to zero. Negative values in the table represent pixels that are darker than the median value (128), while positive values indicate pixels that are brighter than the median value.

3.3 Calculating the DCT Transformation

The resulting level shifting matrix is then calculated using the 2-dimensional DCT formula [8]:

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f'(x,y)\ \cos\left(\frac{(2x+1)u\pi}{16}\right)\cos\left(\frac{(2y+1)v\pi}{16}\right)$$

This process converts data from pixel values into frequency coefficients. The result is a DCT coefficient matrix.

Table 3. DCT transformation calculation results

-415	-22	-15	-6	3	2	1	0
-18	-14	-9	4	3	1	0	0
-12	-8	6	3	-2	1	0	0

-6	-3	4	2	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Tabel 3 tersebut merupakan hasil transformasi DCT pada blok citra 8×8. Nilai F(0,0) = −415 adalah koefisien DC yang merepresentasikan rata-rata intensitas blok dan biasanya bernilai paling besar. Koefisien lainnya disebut AC yang menggambarkan variasi frekuensi, dari frekuensi rendah (kiri atas) hingga frekuensi tinggi (kanan bawah). Bagian frekuensi menengah di tengah matriks umumnya digunakan untuk penyisipan pesan karena mampu menjaga kualitas visual citra sekaligus mempertahankan ketahanan pesan.

3.4 Frequency Division and Message Insertion Process

Message insertion is performed on the DCT coefficients of the middle frequencies, not directly on the image pixels, by selecting specific positions in the matrix such as DCT(2,2) = 6, DCT(2,3) = 3, and DCT(3,2) = −2 because these areas are able to maintain visual quality and are relatively stable against compression [9]. The embedding process is performed using the Least Significant Bit (LSB) method on the selected coefficients. For example, if the embedded message is 1 bit (m = 1) and the coefficient is 6 (binary 110), then the LSB is already 1, so no change is needed. However, if the message bit is 0, the coefficient can be changed to 4 (binary 100) so that the last bit matches the message to be embedded [10].

3.5 Inverse DCT

After insertion is complete, Inverse DCT is performed to return the frequency coefficients to pixel values [11].

$$f'(x,y) = \frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7} C(u)C(v)F(u,v)\cos\left(\frac{(2x+1)u\pi}{16}\right)\cos\left(\frac{(2y+1)v\pi}{16}\right)$$

Table 4 . Inverse DCT Calculation

-8	-6	-3	2	7	10	12	14
-10	-8	-5	0	5	8	10	12
-13	-10	-8	-3	2	4	7	10
-16	-13	-10	-6x	0	2	4	7
-18	-16	-13	-10	-6	-3	0	2
-20	-18	-16	-13	-10	-8	-6	-3
-23	-20	-18	-16	-13	-10	-8	-6
-26	-23	-20	-18	-16	-13	-10	-8

Table 4 shows the 8×8 image block after the inverse DCT process and return to the spatial domain, where one value has been modified (marked −6x) as a result of message bit insertion in the previous stage. This change is very small and insignificant to the overall pattern of values, so that visually the difference in the image is almost undetectable. This shows that insertion at medium frequencies is able to maintain image imperceptibility.

3.6 Reverse Level Shifting

The IDCT result values are then added back with 128: $f(x,y) = f'(x,y) + 128$
If there are values outside the range of 0–255, then the values are rounded or truncated [12].

Table 5. Reverse Level Shifting calculation results

120	122	125	130	135	138	140	142
118	120	123	128	133	136	138	140
115	118	120	125	130	132	135	138
112	115	118	122	128	130	132	135

110	112	115	118	122	125	128	130
108	110	112	115	118	120	122	125
105	108	110	112	115	118	120	122
102	105	108	110	112	115	118	120

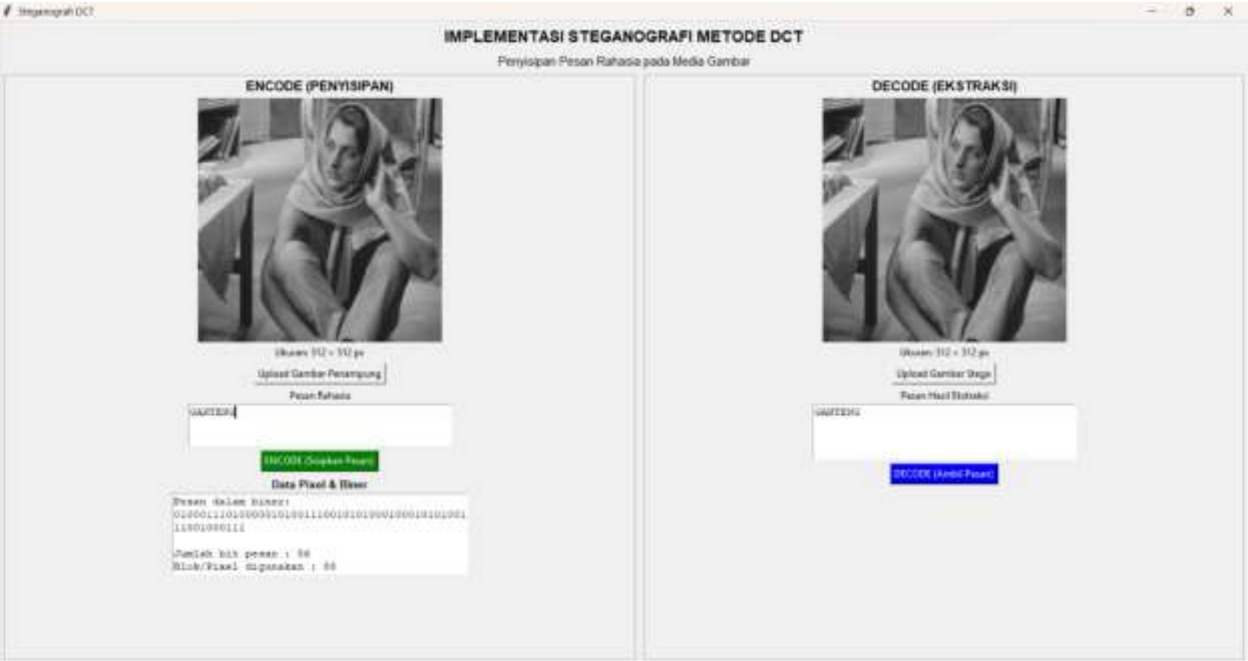
The final image is called a stego-image. Visually, the stego-image does not differ significantly from the original image, but it contains a secret message.

4. Result And Discussion

This section presents the results of the implementation of the method and an analysis of the performance of the DCT-based steganography system that has been developed.

4.1 Encoding and Decoding Results

The results of testing the process of embedding (encoding) and extracting (decoding) messages in digital images. The evaluation focused on the success of returning the message in its entirety and the visual quality of the stego image produced with variations in Figure 1.



GANTENG

```
Pesan dalam biner:
010001110100000101001110010101000100010101001
11001000111

Jumlah bit pesan : 56
Blok/Pixel digunakan : 56
```

GANTENG

Figure 2. Display of decode and encode results

Figure 2 shows the results of the encoding process, in which the system not only inserts the secret message but also displays technical information in the form of a binary representation of the message and the use of pixel blocks. After the user enters the message and presses the ENCODE button, the text is automatically converted to ASCII-based binary form (each character is 8 bits), so that the length of the message determines the number of bits that must be inserted. The system then calculates the capacity of the 512×512 pixel image, which has been divided into 8×8 blocks, to ensure that the number of bits does not exceed the capacity, and the insertion is done gradually in several DCT blocks to maintain visual quality. Although what is displayed is pixel and binary data, the insertion process actually occurs on the mid-frequency DCT coefficients, not directly on the pixels, so that the changes are spread out smoothly and are difficult to detect. This information also serves as a reference during the decoding process, where the stego image is again divided into 8×8 blocks, transformed with DCT, bits on selected coefficients are read and rearranged, then converted into text; the success of extraction corresponding to the original message demonstrates the consistency and reliability of the method.

4.2 Simulation of Secret Message Insertion

This subsection presents a simulation of the process of inserting secret messages into images using the DCT method to describe the embedding mechanism systematically.

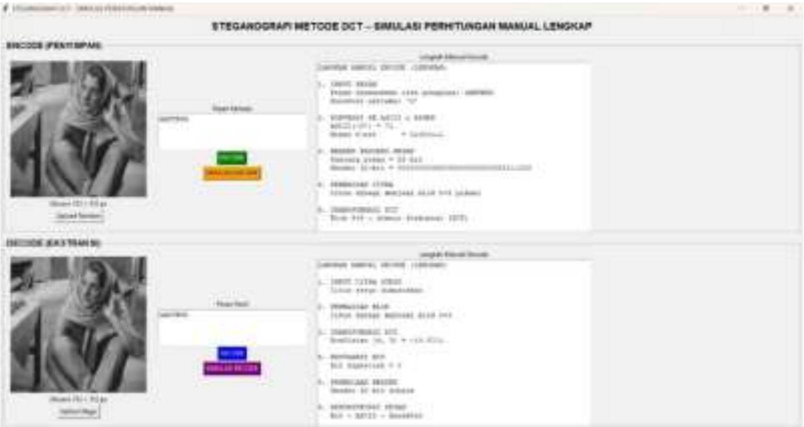

STEGANOGRAFI METODE DCT – SIMULASI PERHITUNGAN MANUAL LENGKAP
ENCODE (PENYISIPAN)
DECODE (EKSTRAKSI)

Figure 3. Simulation of Decoding and Encoding Secret Messages

In the Encode (Insertion) section, the user enters a secret message, then the system displays manual steps that include: reading a 512×512 pixel image, dividing the image into 8×8 blocks, and converting the message to ASCII code and binary form (each character is 8 bits). After that, a DCT transformation is performed on one of the image blocks to move the data from the spatial domain to the frequency domain. Next, one bit of the message is inserted into the mid-frequency DCT coefficient using the LSB method. This process explicitly shows the coefficients before and after modification, so you can see how small changes are made without significantly affecting visual quality. After insertion is complete, inverse DCT (IDCT) is performed to return the block to the spatial domain and generate the stego image. In the Decode (Extraction) section, the simulation shows the reverse process of the encode stage. The stego image is read back, divided into 8×8 blocks, and then transformed using DCT. The coefficients previously used for insertion are identified, and the bits in the LSB position are extracted. The obtained bits are then arranged according to the message length, converted back from binary to ASCII, and reconstructed into the original text.

4.3 Discussion

The implementation results show that the developed DCT-based steganography method is capable of consistently embedding and extracting messages without causing significant visual changes to the image. During the encoding and decoding stages (Figure 1), the message was successfully restored in its entirety according to the original message, confirming that the mechanism for selecting intermediate frequency coefficients and the LSB technique worked stably. The technical information shown in Figure 2 shows that the system not only performs insertion, but also calculates the image capacity based on 8×8 block division and ensures that the number of message bits matches the capacity. This shows that the system controls the balance between insertion capacity and visual quality, thereby minimizing image distortion.

The manual simulation in Figure X further clarifies the internal mechanism of the algorithm, starting from message conversion to binary, DCT transformation, modification of mid-frequency coefficients, to the inverse DCT process and message re-extraction. The changes that occur in the coefficients are small and distributed, so they do not have a significant impact on the visual structure of the image. These results directly answer the research question that has been formulated, namely how to implement a DCT method that is able to maintain image imperceptibility while preserving message integrity. Unlike spatial domain approaches that are more easily detected, this method shows that insertion in the mid-frequency domain provides a better balance between security, capacity, and visual quality. Thus, this research fills the previous gap by presenting an integrated, process-transparent implementation that has been proven effective through consistent encode-decode testing.

5. Conclusion

This study successfully implemented a Discrete Cosine Transform (DCT)-based steganography method for embedding secret messages in digital images by utilizing mid-frequency coefficients and the Least Significant Bit (LSB) technique. The test results showed that the encoding and decoding processes were consistent, where messages could be extracted back in their entirety without causing significant visual changes to the stego image. The transformation process to the frequency domain, the selection of 8×8 blocks, and the level shifting and inverse DCT mechanisms proved to be able to maintain a balance between insertion capacity and image visual quality. Thus, this method is effective in improving information security because the insertion is done in the frequency domain, which is more difficult to detect than the spatial domain. For further research, it is recommended to conduct quantitative testing using evaluation parameters such as PSNR, MSE, and SSIM to measure image quality objectively, as well as to test the method's resistance to compression, cropping, and noise. In addition, the development of adaptive schemes in selecting DCT coefficients or integration with encryption techniques prior to the embedding process could be the direction of further research to improve the security and robustness of the system more comprehensively.

6. References

[1] M. E. Danlami, L. L. Raymond, and T. Solomon, “Hybridization of Cryptography and Steganography to Achieve Secret Communication,” International Journal of Advances in Engineering and Management (IJAEM), vol. 5, p. 428, 2023, doi: 10.35629/5252-0508428437.

[2] R. Apau, M. Asante, F. Twum, J. Ben Hayfron-Acquah, and K. O. Peasah, “Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review,” PLoS One, vol. 19, no. 9 September, Sep. 2024, doi: 10.1371/journal.pone.0308807.

[3] K. R. Malik et al., “A hybrid steganography framework using DCT and GAN for secure data communication in the big data era,” Sci. Rep., vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-01054-7.

[4] “INFORMATION SYSTEM SECURITY USING THE DISCRETE COSINE TRANSFORM (DCT) METHOD”.

[5] T. Babu, R. R. Nair, M. T. Rajesh, and S. Kishore, “Secure Data Embedding in Digital Images: Enhancing Covert Communication with LSB-Based Techniques,” in Procedia Computer Science, Elsevier B.V., 2025, pp. 2091–2100. doi: 10.1016/j.procs.2025.04.459.

[6] M. Abd Al-Hassan Hussein and A. S. Mahdi Ass Ali Hassan Khidhir, “Video Data Steganography Based on Discrete Cosine Transform Method Supervised by,” 2010.

[7] 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.

[8] A. Shajin Nargunam, “STEGANOGRAPHY ALGORITHM BASED ON DISCRETE COSINE TRANSFORM FOR DATA EMBEDDING INTO RAW VIDEO STREAMS.”

[9] E. Walia and P. Jain, “An Analysis of LSB & DCT based Steganography,” 2010.

[10] S. M. A. Al-Momen and L. E. George, “Image Hiding Using Magnitude Modulation on the DCT Coefficients,” 2010.

[11] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, “Hiding data in images using steganography techniques with compression algorithms,” Telkomnika (Telecommunication Computing Electronics and Control), vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[12] S. Napitupulu, R. Revaldo Siagian, R. Simanullang, K. Daniel Manalu, and C. Fao Silalahi, “Implementation of DCT Based Steganography Algorithm to Hide Infor-mation in Images-Septrian Napitupulu et.al Implementation of DCT Based Steganography Algorithm to Hide Information in Images,” Indonesia Article Info ABSTRACT Corresponding Author, vol. 1, 2013.