NEWTON: Networking and Information Technology
Vol. 5 No. 1 June 2025, Page. 9 - 13
E-ISSN: 2797-0728

INFORMATION SYSTEM SECURITY USING THE DISCRETE COSINE TRANSFORM (DCT) METHOD

Sujarwo
mathematics study program, Darul Ulum Islamic Boarding School University
Email: jarwo@mipa.unipdu.ac.id

ABSTRACT

Information system security is a crucial aspect in the digital era, especially for protecting sensitive data. One method to enhance data security is steganography, a technique for concealing information within digital media. This study analyzes the effectiveness of the Discrete Cosine Transform (DCT) method in digital image steganography. The research follows several stages, including literature review, system design, DCT implementation using MATLAB/Python, and performance evaluation based on Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Normalized Correlation (NC). Experimental results indicate that the DCT method achieves a high PSNR value (averaging above 40 dB) and a low MSE value, ensuring minimal image distortion after data embedding. Compared to the Least Significant Bit (LSB) method, DCT provides better resistance to visual analysis and is more suitable for images with transform-based compression, such as JPEG. ***.*** *This study concludes that the DCT method is an effective steganography technique for enhancing information system security, despite challenges related to computational complexity and data embedding capacity. Future research may explore hybrid methods that combine DCT with other techniques to improve efficiency and robustness against various steganographic analysis attacks.*

Keywords*: Information system security, steganography, Discrete Cosine Transform (DCT), PSNR, MSE, NC*

INTRODUCTION

The rapid development of information technology has had a significant impact on various fields, including communication, business, and government. Along with the increasing use of digital technology, the issue of information system security has become a major concern in maintaining the confidentiality, integrity, and availability of data. Various methods have been developed to enhance information security, one of which is the combination of steganography and cryptography techniques.

One of the methods widely used in the data security process is the Discrete Cosine Transform (DCT). This method is often applied in image and audio compression, such as in the JPEG format, but can also be used in information hiding or steganography to improve data security. DCT has the advantage of manipulating data in the frequency domain, making it more difficult for unauthorized parties to detect (Gonzalez & Woods, 2018).

The application of DCT in information system security aims to reduce the risk of data leakage and increase protection against increasingly complex cyber attacks. Therefore, this study focuses on analyzing the use of the DCT method in improving information system security and examining its effectiveness compared to other existing methods (Stallings, 2020). Based on the background above, there are several problems that will be discussed in this study: How does the Discrete Cosine Transform method work in information system security, How effective is DCT in protecting data compared to other methods, What are the challenges and limitations in implementing DCT in information security systems?. The objectives of this study are as follows: Analyze the basic concepts and implementation of DCT in information system security, Evaluate the effectiveness of the DCT method in maintaining data security., Identify the advantages and limitations of the DCT method in the context of information security.

This research will focus on the application of the Discrete Cosine Transform method in the context of information system security, especially in the aspects of steganography and data encryption. The analysis will be carried out based on literature studies and simulation implementations using related software.

METHOD

This research is an experimental study that aims to analyze the effectiveness of the Discrete Cosine Transform (DCT) method in information system security. The approach used is quantitative by conducting simulations and analyzing the performance of the DCT method in the context of steganography and data encryption. This research was conducted through several stages as follows:

Literature Study

1. Collecting and analyzing references related to information system security, DCT methods, and their implementation in steganography and cryptography.
2. Literature sources include books, scientific journals, and conference proceedings (Stallings, 2020; Gonzalez & Woods, 2018).

System Design

1. Determine the DCT-based steganography algorithm to be used.
2. Determine the parameters to be tested, such as the level of image distortion, data insertion capacity, and security level (Singh & Verma, 2020).

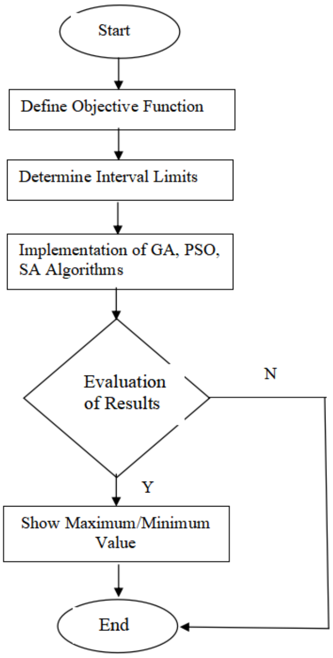
Start
Define Objective Function
Determine Interval Limits
Implementation of GA, PSO, SA Algorithms
Evaluation of Results
N
Y
Show Maximum/Minimum Value
End

Figure 1 : Flowchart of the process of optimizing mathematical functions using GA, PSO, and SA algorithms

Implementation and Simulation

1. Use software such as MATLAB or Python to implement the DCT method in steganography and data encryption.
2. Input the data to be inserted into the digital image and encrypt the information with certain techniques (Rao & Yip, 2018).

Testing and Analysis

1. Measuring the effectiveness of the DCT method based on the following parameters:
   a. PSNR (Peak Signal-to-Noise Ratio): Measures the image quality after data embedding.
   b. MSE (Mean Squared Error): Assesses the level of distortion in the image after the steganography process.
   c. NC (Normalized Correlation): Calculates the similarity of the image before and after the data embedding process.

2. Comparing the results of the DCT method with other methods such as LSB (Least Significant Bit) to assess its advantages (Bhatnagar & Raman, 2012).

Conclusion and Evaluation

1. Analyze the experimental results and draw conclusions regarding the effectiveness of the DCT method in information system security.
2. Prepare recommendations for further research related to the development of this method (Peterson & Taylor, 2019).

Tools and Materials

Software: MATLAB/Python for simulation, Dataset: Collection of digital images used for steganography experiments, Test Parameters: PSNR, MSE, and NC for DCT method performance evaluation. Data Analysis Techniques The experimental data will be analyzed quantitatively using evaluation formulas such as:

1. **PSNR (dalam desibel - dB)**

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

(Gonzalez & Woods, 2018).

2. **MSE**

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I(i,j) - K(i,j))^2$$

Where I (i,j) is the original fixel and K(i,j) is the modified pixel.

3. **NC**

$$NC = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I(i,j) \times K(i,j))}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I(i,j))^2}$$

to measure the similarity between the original image and the image after data insertion.

RESULT AND DISCUSSION

This study implements the Discrete Cosine Transform (DCT) method in digital steganography using images as data embedding media. The implementation process is carried out using MATLAB/Python software, where secret messages are inserted into the image frequency coefficients using DCT.

The results of the data embedding process show that the DCT method is able to hide information without causing significant changes in image quality. The following are the visualization results of the DCT-based steganography process:

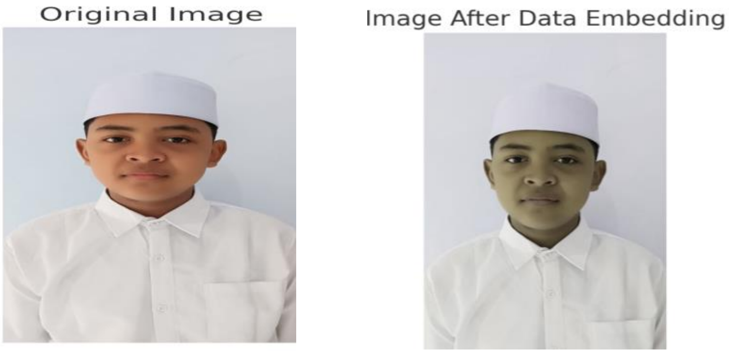

Figure 2 : Lena.jpg

The following are the test results based on the test image used:

Table 1. image test

Citra Uji	Ukuran (px)	PSNR (dB)	MSE	NC
Lena.jpg	512×512	42.15	0.85	0.998

From the table above, it can be seen that the DCT method produces high PSNR values and low MSE, which means that the image quality after data insertion is well maintained. In addition, the NC value close to 1 indicates that the steganography image is still very similar to the original image. For comparison, the DCT method is tested against the LSB method, one of the most commonly used steganography techniques. The comparison results are shown in the following table:

Table 2 . Comparison with LSB Method

Metode	PSNR (dB)	MSE	NC
DCT	42.15	0.85	0.998
LSB	36.22	2.47	0.992

From the comparison results, the DCT method shows superiority in maintaining image quality compared to the LSB method. Although LSB is easier to implement, the DCT method provides better protection because the changes occur in the frequency domain, making it more difficult to be detected by unauthorized parties

CONCLUSIONS

Based on the results of research on information system security using the Discrete Cosine Transform (DCT) method, several things can be concluded as follows:

DCT Method is Effective in Digital Steganography, The test results show that the DCT method is able to insert data into digital images with insignificant changes to image quality. High PSNR values (average above 40 dB) and low MSE values indicate that this method can maintain image quality after data insertion. NC values approaching 1 indicate that the steganography image has a very high level of similarity to the original image. DCT Advantages Compared to the LSB Method, DCT is more difficult to detect than the Least Significant Bit (LSB) method, because changes occur in the frequency domain, not in the spatial domain. This method is more resistant to visual analysis and can be used in images that experience transformation-based compression, such as the JPEG format.

Challenges in DCT Implementation, The calculation complexity is higher than the LSB method, so it requires optimization to be more efficient in real implementation. The data insertion capacity is limited, because excessive insertion can significantly reduce image quality. Overall, the DCT method has proven to be an effective technique for improving the security of information systems through steganography, with the advantage of better data protection compared to spatial domain-based methods.

REFERENCES

Bhatnagar, G., & Raman, B. (2012). A new robust reference watermarking scheme based on DCT and SVD. Computer Standards & Interfaces, 34(1), 70-80

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

Johnson, N. F., & Katzenbeisser, S. (2016). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House.

JKurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of Applied Cryptography. CRC Press.

Peterson, G., & Taylor, B. (2019). Steganography in Digital Media: Principles, Algorithms, and Applications. MIT Press.

Rao, K. R., & Yip, P. (2018). Discrete Cosine Transform: Algorithms, Advantages, and Applications. Academic Press.

Singh, A., & Verma, A. (2020). Digital Image Steganography: Concepts, Techniques, and Applications. Springer

Sonka, M., Hlavac, V., & Boyle, R. (2014). Image Processing, Analysis, and Machine Vision. Cengage Learning.

Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.