



Implementation of SLT-DCT Steganography Method on Images to Improve the Quality of Steganography Images

Ramadani Ritonga^{1*}, Rika Rosnelly², Wanayumini³

¹Master of Computer Science, Faculty of Engineering and Computer Science, Universitas Potensi Utama, Medan. Indonesia

²Department of Computer Science, Faculty of Engineering and Computer Science, Universitas Potensi Utama, Medan. Indonesia

³Department of Informatic Engineering, Faculty of Engineering, Universitas Asahan, Kisaran. Indonesia

*Corresponding author: ritongaramadani8@gmail.com

Abstract - The study explores the implementation of a hybrid Slantlet Transform (SLT) and Discrete Cosine Transform (DCT) in the context of image steganography, focusing on enhancing the quality of stego images while maintaining a high level of imperceptibility. One of the main challenges in steganography is embedding secret messages into images without compromising their visual quality. In this research, the combination of SLT and DCT is applied to embed secret messages into cover images, with the hope that this method can preserve visual quality. The quality of the stego images is evaluated using two main metrics: Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE). PSNR is used as a measure to assess how well the steganographic image maintains high visual quality, while MSE serves to measure the difference between the original and stego images. Experimental results show that the hybrid SLT-DCT method significantly produces higher PSNR values compared to the individual implementation of SLT or DCT. This indicates that the combination of these two methods not only ensures better image quality but also enhances the security of the embedded message. Thus, this approach makes a significant contribution to the development of more efficient and effective steganography techniques, offering a solution that meets the need for high visualization while maintaining the integrity of the hidden data. The success of this method paves the way for further research in the field of steganography to explore other transformation combinations that can improve the results obtained.

Keywords: *Steganography; Image Processing; SLT; DCT; PSNR; MSE*

1. INTRODUCTION

In the era of digital communication advancement, securing sensitive information has become very important. Steganography, the art of hiding data in media files, has been widely adopted for secure communication [1], [2]. The main goal of steganography is to embed information in such a way that it is invisible to the human eye while ensuring that the embedded message can be retrieved accurately. Unlike cryptography, which protects data through encryption, steganography hides the existence of the message itself, making it difficult to detect [3], [4]. Various techniques have been used in digital steganography, including spatial domain methods and transform domain methods. Spatial domain techniques, such as the Least Significant Bit (LSB) method, embed data directly into pixel values but are more vulnerable to attacks and image modification [3]–[8]. Domain transformation techniques, such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Slantlet Transform (SLT), offer better robustness by embedding messages into frequency coefficients, making detection and deletion more difficult [9]–[11]. This study focuses on the implementation of a hybrid of SLT and DCT to optimize image steganography. SLT provides better localization and time decomposition capabilities compared to DWT, while DCT is widely used in image compression and steganography due to its high efficiency in maintaining image quality. By combining these two techniques, this study aims to improve the obscurity, robustness, and security of stego images. Previous research conducted by implementing Steganography using the SLT algorithm and image quality improvement using Huffman Coding on GreyScale Images revealed that the size of the Secret-Image affects the PSNR ratio obtained where the larger the secret image used, the smaller the PSNR ratio obtained. also conducted research by combining steganography techniques with its insertion model using the mathematical theory of the discrete cosine transform (DCT) combined with the mathematical theory of bilinear interpolation so that it can accommodate large messages, but the size of the resulting stego image is much larger than the cover image, and the resulting PSNR value is less than <30 db, the PSNR value drops below 30 db indicating a relatively low quality, where the distortion due to insertion is clearly visible.

The main challenge in image steganography lies in maintaining a high-quality stego image while ensuring that the inserted message remains undetected by potential observers. Traditional steganographic methods often grapple with issues such as image distortion, loss of essential details, and increased vulnerability to various types of attacks, which can compromise the integrity and confidentiality of the embedded information [12]–[14]. In light of these challenges, the proposed SLT-DCT method effectively harnesses the strengths of both Slantlet Transform (SLT) and Discrete Cosine Transform (DCT) to mitigate the drawbacks typically associated with conventional techniques. By combining these two transformations, the SLT-DCT method not only improves the imperceptibility of the hidden message but also enhances the robustness of the stego image against



distortions and manipulations. This innovative approach aims to provide a more secure and high-quality steganography solution, ensuring that the visual characteristics of the original image are preserved while maintaining the secrecy of the embedded information. Furthermore, the integration of these transformations opens up avenues for greater capacity in message embedding without compromising image quality, making it an optimal choice for applications that require both security and fidelity in data transmission. Overall, the SLT-DCT method represents a significant advancement in the field of steganography, positioning itself as a reliable technique for safeguarding sensitive information in digital imagery[15]–[17]. Furthermore, the implementation of the SLT-DCT method demonstrates a systematic approach to addressing the prevalent issues found in traditional steganography. By leveraging the spatial and frequency domain strengths, this hybrid technique significantly reduces the likelihood of detection while simultaneously enhancing the visual integrity of the stego image. In addition, the SLT component offers improved localization and better handling of image features, further safeguarding against attacks that may exploit underlying image structures. The DCT element contributes by preserving important frequency information, ensuring that the embedding process does not disrupt the overall quality. Experimental results indicate that the SLT-DCT method yields higher PSNR values and lower MSE compared to conventional approaches, reinforcing its effectiveness. As a result, this method not only fulfills crucial requirements for steganographic applications—such as imperceptibility and robustness—but also sets a new standard for future research and development in the field, paving the way for even more advanced techniques that can effectively protect digital communications in an increasingly interconnected world.

2. METHODS

This study uses a hybrid SLT-DCT approach to embed and extract hidden messages in images. The methodology consists of the following steps. The steganography method begins with a Cover Image, which is a cover image used to hide the secret message. This image is designed to look normal to observers, so that the presence of the message is not detected. Furthermore, in the Secret Message stage, the message to be hidden can be text, numbers, or other data that needs to be secured from unauthorized parties. This process is then continued with Encoding Processing, where steganography techniques are applied through two methods: Steganography SLT (Singular Value Decomposition), which inserts a message by changing the singular value of the image, and Steganography DCT (Discrete Cosine Transform), which involves changing the frequency coefficient of the image. The result of this process is a Stego Image, which is an image that looks similar to the cover image, but now contains the secret message in it. The last stage is Testing, which aims to ensure that the secret message has been successfully inserted and can be extracted again without damaging the quality of the stego image. By following this process, sensitive information can be hidden within the image effectively. The General System Design is shown in Figure 1.

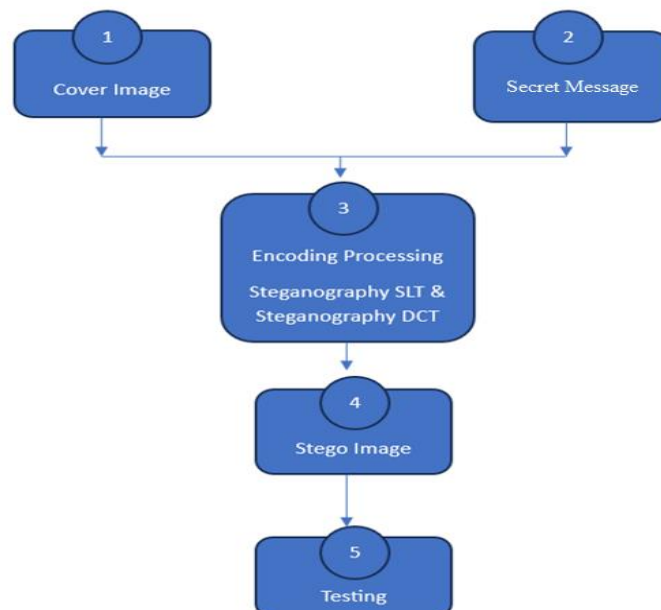


Figure 1. General System Design




a. Cover Image Selection

Citra yang digunakan dalam penelitian ini adalah citra digital dalam format JPEG, yang memiliki resolusi 256x256, 512x512, dan 1024x1024 piksel. Resolusi yang bervariasi ini menyediakan spektrum yang luas untuk menguji efektivitas teknik steganografi. Citra sampul berfungsi sebagai media utama untuk menyembunyikan pesan rahasia, yang memainkan peran



penting dalam memastikan bahwa data yang disematkan tetap tidak dapat dibedakan dari citra asli. Dengan memilih resolusi yang berbeda, penelitian ini bertujuan untuk mengevaluasi bagaimana ukuran dan kualitas citra memengaruhi proses steganografi. Citra dengan resolusi yang lebih tinggi biasanya menawarkan lebih banyak piksel, yang berpotensi memungkinkan kapasitas data yang lebih besar tanpa penurunan kualitas visual yang nyata. Sebaliknya, citra dengan resolusi yang lebih rendah dapat menantang metode tersebut dengan membatasi ruang yang tersedia untuk penyisipan pesan. Oleh karena itu, menganalisis kinerja metode hibrida SLT-DCT di seluruh resolusi ini tidak hanya menilai efektivitasnya tetapi juga fleksibilitasnya dalam menangani berbagai kualitas citra. Pendekatan komprehensif ini penting untuk memahami aplikasi praktis steganografi dalam skenario dunia nyata, di mana format dan ukuran citra yang berbeda umumnya ditemukan. Dengan menggunakan berbagai resolusi, penelitian ini berupaya memberikan wawasan lebih mendalam tentang bagaimana faktor-faktor ini memengaruhi keamanan pesan tersembunyi dan integritas keseluruhan gambar sampul.

Table 1. Cover Image

No	Image Name	Size	Size (Bytes)	Image
1	Loudspeaker	256 x 256 piksel	78,725 bytes	
2	Infocus	512 x 512 piksel	187,672 bytes	
3	Laptop	1024 x 1024 piksel	767,799 bytes	

b. Secret Message Preparation

The secret message is a text file (*.txt) that is first converted into a binary stream before embedding.

c. SLT Transformation

The cover image undergoes Slantlet Transform (SLT) decomposition, dividing the image into four sub-bands: LL (Low-Low), LH (Low-High), HL (High-Low), and HH (High-High). SLT enhances time localization and improves robustness.

d. DCT Transformation on HH Sub-band

The HH sub-band obtained from the SLT transformation is further processed using Discrete Cosine Transform (DCT). DCT converts spatial domain data into frequency components, making it suitable for embedding data securely.

e. Message Embedding

The binary stream of the secret message is embedded into selected frequency coefficients of the DCT-transformed HH sub-band, ensuring minimal distortion and high imperceptibility.

f. Inverse Transformation

After embedding the message into the cover image, inverse transformations, specifically inverse DCT and inverse SLT, are applied sequentially to reconstruct the stego image. The inverse DCT restores the original frequency components, while the inverse SLT aligns the spatial data modified during embedding. This meticulous process ensures that the stego image retains its visual integrity and effectively conceals the hidden message.



g. Stego Image Evaluation

The quality of the stego image is assessed using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) to ensure high imperceptibility and minimal distortion.

h. Message Extraction

To retrieve the secret message, the stego image undergoes SLT and DCT decompositions, allowing extraction of the embedded data from the frequency coefficients. The experimental evaluation involves comparing the performance of SLT-DCT with traditional steganographic methods to assess improvements in image quality and robustness.







3. RESULTS AND DISCUSSION

The evaluation of the proposed SLT-DCT method is carried out by testing various image sizes, ranging from small to large resolutions, to understand the extent to which this method can work effectively in the context of steganography. In this process, the results of this hybrid technique are compared with existing conventional steganography techniques, such as the LSB (Least Significant Bit) method and single DCT. This comparison aims to assess the superiority of the SLT-DCT method in terms of stego image quality, message storage capacity, and resistance to analysis or detection. The experimental results are presented in detail, which include metric values such as Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE), which provide deep insights into the effectiveness and efficiency of the proposed technique. By presenting comprehensive data and in-depth analysis, this study aims to make a significant contribution to the development of more secure and state-of-the-art steganography. The experimental results are presented as follows

1. Image Quality Testing

The quality of images after testing was done by comparing PSNR (Peak Predictive Signal Recurrence Ratio), (Mean Square Error) of image hiding information before and after the results mean. Test on a variety of different image sizes: including yaitu 256x256, 512x512, and 1024x1024 pixels.

Table 2. Results of Analysis of the Quality of Original Images and Stego Images

No	Image Name	Size	Original Image	Stego Image
1	Loudspeaker	256 x 256 piksel		
2	Infocus	512 x 512 piksel		
3	Laptop	1024 x 1024 piksel		

Some test images used in this study are the original image (cover image) and the result of message insertion (stego image). By visually observing the two types of images, there is no difference between the original image and the stego image, which shows that steganography with the SLT-DCT algorithm is able to maintain the visual quality of the intended image well.

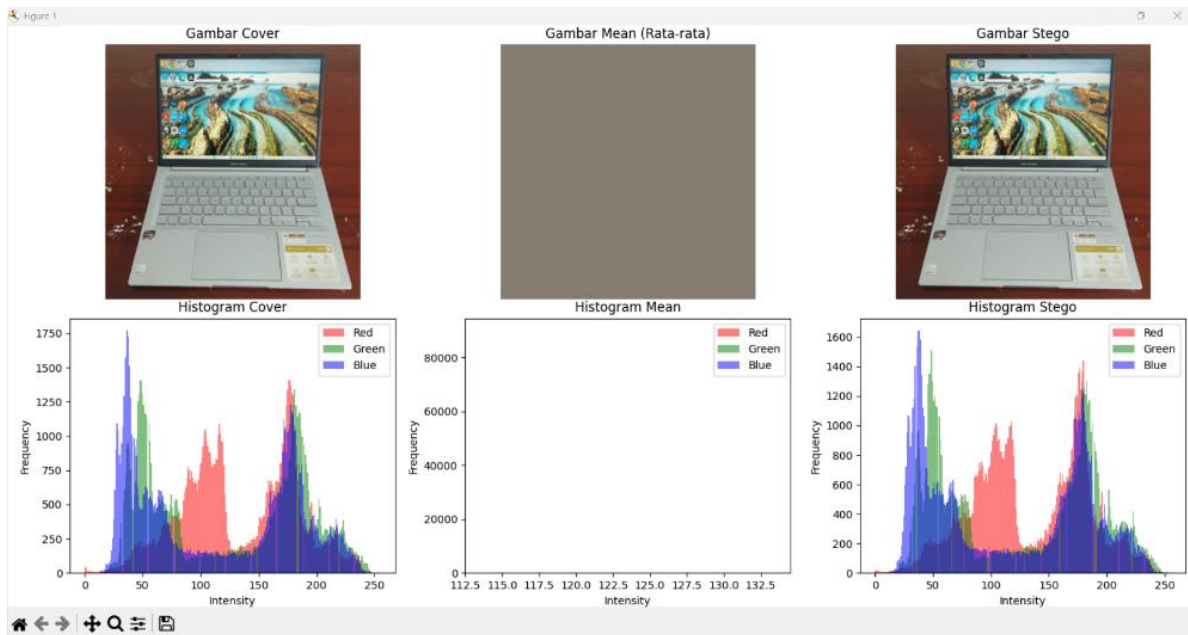


Figure 2. Histogram Comparison of Results in SLT-DCT Algorithm

In this Laptop image which shows a comparison of the histogram results of the original image and the SLT-DCT steganography image tested with a size of 1024 x 1024 pixels with a message capacity of 1,200 characters, the difference in the histogram between the original image and the steganography image can be seen, with the naked eye the difference between the original image and the steganography image is not clearly visible, but in the histogram there is a difference between the histogram of the original image and the histogram of the steganography image.

2. Message Capacity

Message capacity testing aims to determine the maximum amount of data that can be inserted into a digital image without causing significant visual quality degradation. The main parameters used to evaluate are the number of successfully inserted characters and the PSNR (Peak Signal-to-Noise Ratio) value after insertion.

Table 3. Message Capacity Test Results on the SLT-DCT Algorithm

No	Image Name	Size	Message Capacity (Characters)	PSNR (db)	MSE
1	Loudspeaker	256 x 256 piksel	50	Before : 27.68 After : 34.31	Before : 111.02554 After : 24.11830
2	Infocus	512 x 512 piksel	250	Before : 27.86 After : 37.48	Before : 106.53212 After : 11.61312
3	Laptop	1024 x 1024 piksel	600	Before : 27.53 After : 35.94	Before : 114.73656 After : 16.54878

After testing the message capacity on the SLT method, the DCT results are still not good, especially if the message capacity is high then the PSNR value decreases. In this test with the combined SLT-DCT method, the PSNR and MSE results get good results even though the message capacity is large. Testing the Message capacity in steganography can be determined by several methods, one of the most widely used methods is by measuring the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) values. The quality of the steganography image is said to be good if the PSNR value is 40 dB or more. The next test result is a comparison of the PSNR value on the cover image inserted with the message on the SLT, DCT and SLT-DCT algorithms, the inserted cover image has a size of 256x256, 512x512 and 1024x1024 with the number of characters inserted is 10,000 characters.

Table 4. The results of the comparison of image quality with 10,000 character messages inserted






No	Image Name	Size	Algoritma	PSNR (db)	MSE
1	Loudspeaker	256 x 256 piksel	SLT	34.27	24.11476
			DCT	34.30	24.13578
			SLT-DCT	40.28	24.24576
3	Infocus	512 x 512 piksel	SLT	37.47	11.64502
			DCT	37.48	11.61158
			SLT-DCT	41.47	11.64822
5	Laptop	1024 x 1024 piksel	SLT	35.94	16.55398
			DCT	35.94	16.54851
			SLT-DCT	42.94	16.55541

Table 4 shows the results of image quality comparison by inserting a message of 10,000 characters using various steganography algorithms: SLT, DCT, and SLT-DCT, on three images with different sizes. For the Loudspeaker image (256 x 256 pixels), SLT produces a PSNR of 34.27 dB and an MSE of 24.11476, while DCT shows a slightly higher PSNR of 34.30 dB, but with a small difference in MSE (24.13578). On the other hand, SLT-DCT gives better results with a PSNR of 40.28 dB and an MSE of 24.24576, indicating that this hybrid algorithm significantly improves the quality of the stego image. For Infocus images (512 x 512 pixels), the PSNR for SLT and DCT are relatively close to each other, namely 37.47 dB and 37.48 dB, with MSE of 11.64502 and 11.61158, indicating balanced performance. SLT-DCT again shows superiority with PSNR of 41.47 dB, although its MSE is slightly higher (11.64822) compared to DCT and SLT. Meanwhile, for Laptop images (1024 x 1024 pixels), SLT and DCT have lower PSNR values of 35.94 dB with higher MSE (16.54851 and 16.55398). However, SLT-DCT achieves PSNR of 42.94 dB and MSE of 16.55541, indicating its success in maintaining the stego image quality despite the larger image size. Overall, the experiments show that the SLT-DCT algorithm consistently produces better stego image quality than SLT or DCT individually, indicating the effectiveness of this method in embedding messages without compromising the visual quality of the image and increasing the security level of the hidden message. This method provides a solid foundation for further development in steganography techniques, with the results showing great potential for real-world applications in the field of data security.



3. Stego Image Resilience

Stego image resilience testing is done by manipulating data on the image, such as cropping, which removes some image data, Rotation, which rotates the direction of the image, Resize, which changes the image size, convert, which changes the image format, CS, which performs contrast stretching. The following will explain the results of the SLT-DCT steganography image resilience analysis with example data, namely Loudspeaker with an original image size of 78,725 bytes, with a size of 256 x 256 pixels, with a file format of jpg.

Table 5. Resilience of SLT-DCT Steganography Images on Loudspeakers

Process Test	Image	Size (bytes)	Extraction Process	Information
Cropping		48,644 bytes	Fail	Remove other parts of the image
Rotate		52,122 bytes	Fail	Rotate the image 180 degrees
Resize		28,914 bytes	Fail	Resize 256x256 pixels to 128x128 pixels



Convert		96,570 bytes	Succeed	Change format from jpg to PNG
CS		65,471 bytes	Succeed	Adding contrast stretching to an image

From the table above, it can be seen that from the five manipulation experiments carried out, only 2 experiments did not damage the message, namely changing the format to PNG and adding Contrast stretching.

Table 6. Comparison of Steganography Image Resilience of SLT, DCT, and SLT-DCT on Laptops

Process Test	Extraction Process SLT	Extraction Process DCT	Extraction Process SLT-DCT	Information
Cropping	Fail	Fail	Fail	Remove other parts of the image
Rotate	Fail	Fail	Fail	Rotate the image 180 degrees
Resize	Fail	Fail	Fail	Resize 256x256 pixels to 128x128 pixels
Convert	Fail	Succeed	Succeed	Change format from jpg to PNG
CS	Fail	Succeed	Succeed	Adding contrast stretching to an image

From the table above, it can be seen from the five manipulation experiments carried out, in the SLT steganography image all attacks or image data manipulations carried out can damage the message in the steganography image so that the message in the image cannot be returned to its original form, while the process test on the DCT steganography image, from 5 process tests there are 2 successful process tests or steganography images are resistant to 2 attacks including the Convert process and the addition of Contrast Stretching. While the process test on the SLT-DCT steganography image is the same as DCT steganography, it is able to withstand 2 attacks, namely Convert and Contrast Stretching.

4. CONCLUSION

This study presents a hybrid SLT-DCT approach for image steganography that significantly enhances imperceptibility and robustness in the embedding process. By effectively utilizing the strengths of both Slantlet Transform (SLT) and Discrete Cosine Transform (DCT), this method successfully achieves higher Peak Signal-to-Noise Ratio (PSNR) and lower Mean Square Error (MSE) compared to conventional steganographic techniques. The experimental results validate the effectiveness of this combined approach, demonstrating its ability to conceal messages within images with minimal visual distortion. Furthermore, the findings suggest that the hybrid method not only preserves the quality of the cover image but also ensures the security of the hidden data. Future research could delve into additional optimizations, such as exploring different encoding techniques and image formats, as well as integrating encryption methods to bolster security further. By enhancing these aspects, the potential for this hybrid approach could be expanded, making it a more robust solution for secure communication in various applications. Overall, the study reinforces the promise of the SLT-DCT technique as a significant advancement in the field of image steganography.

ACKNOWLEDGMENT

The authors would like to thank the Master of Computer Science Program for its support and sponsorship. And we also thank the research collaboration of Universitas Potensi Utama and Universitas Asahan for supporting this research.



REFERENCES

- [1] Z. Wang, M. Zhou, B. Liu, and T. Li, "Deep Image Steganography Using Transformer and Recursive Permutation," *Entropy*, vol. 24, no. 7, 2022, doi: 10.3390/e24070878.
- [2] Rahul and Jyoti, "Image Steganography: A Review," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 12, 2023, doi: 10.22214/ijraset.2023.57655.
- [3] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 2, 2022, doi: 10.1109/TDSC.2020.3004708.
- [4] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2971528.
- [5] T. Indriyani, S. Nurmuslimah, A. Taufiqurrahman, R. K. Hapsari, C. N. Prabiantissa, and A. Rachmad, "Steganography on Color Images Using Least Significant Bit (LSB) Method," 2023. doi: 10.2991/978-94-6463-174-6_5.
- [6] H. W. Tseng and H. S. Leng, "A reversible modified least significant bit (LSB) matching revisited method," *Signal Process. Image Commun.*, vol. 101, 2022, doi: 10.1016/j.image.2021.116556.
- [7] W. F. Al Maki, I. B. Muktyas, S. Arifin, Suwarno, and M. K. B. M. Aziz, "Implementation of a Logistic Map to Calculate the Bits Required for Digital Image Steganography Using the Least Significant Bit (LSB) Method," *J. Comput. Sci.*, vol. 19, no. 6, 2023, doi: 10.3844/jcssp.2023.686.693.
- [8] G. Miftakhul Fahmi, K. N. Isnaini, and D. Suhartono, "IMPLEMENTATION OF STEGANOGRAPHY ON DIGITAL IMAGE WITH MODIFIED VIGENERE CIPHER ALGORITHM AND LEAST SIGNIFICANT BIT (LSB) METHOD," *J. Tek. Inform.*, vol. 4, no. 2, 2023, doi: 10.52436/1.jutif.2023.4.2.340.
- [9] E. H. Rachmawanto, C. A. Sari, Y. P. Astuti, and L. Umaroh, "A robust image watermarking using hybrid DCT and SLT," in *Proceedings - 2016 International Seminar on Application of Technology for Information and Communication, ISEMANTIC 2016*, 2017. doi: 10.1109/ISEMANTIC.2016.7873857.
- [10] D. Sinaga, E. H. Rachmawanto, C. A. Sari, D. R. I. M. Setiadi, and N. A. Setiyanto, "An Enhancement of Data Hiding Imperceptibility using Slantlet Transform (SLT)," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, 2018, doi: 10.22219/kinetik.v4i1.702.
- [11] G. Panda, P. K. Dash, A. K. Pradhan, and S. K. Meher, "Data compression of power quality events using the slantlet transform," *IEEE Trans. Power Deliv.*, vol. 17, no. 2, 2002, doi: 10.1109/61.997957.
- [12] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimed. Tools Appl.*, vol. 80, no. 6, 2021, doi: 10.1007/s11042-020-10035-z.
- [13] P. D. Shah and R. S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Eng. Sci. Technol. an Int. J.*, vol. 24, no. 3, 2021, doi: 10.1016/j.jestch.2020.11.008.
- [14] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Process. Image Commun.*, vol. 65, 2018, doi: 10.1016/j.image.2018.03.012.
- [15] X. Xiang and B. Shi, "Evolving generation and fast algorithms of slantlet transform and slantlet-Walsh transform," *Appl. Math. Comput.*, vol. 269, 2015, doi: 10.1016/j.amc.2015.07.094.
- [16] A. Jabbar, A. Hashim, and Q. Al-Doori, "Secured Medical Image Hashing Based on Frequency Domain with Chaotic Map," *Eng. Technol. J.*, vol. 39, no. 5A, 2021, doi: 10.30684/etj.v39i5a.1786.
- [17] L. Widyawati, I. Riadi, and Y. Prayudi, "Comparative Analysis of Image Steganography using SLT, DCT and SLT-DCT Algorithm," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 1, 2020, doi: 10.30812/matrik.v20i1.701.