Development Of Image Steganography Using LSB-DWT For Secure Communication System

S Rakshitha[1], Shwetha V S[2], Chitra D M[3], Srusti K N[4], Ravi J[5]
[1,2,3,4,5] *Department of Electronics and Communication Engineering, Global Academy of Technology, Bengaluru.*

***Abstract*—This work develops a hybrid image steganography technique specifically developed to enhance the security of communication by integrating Least Significant Bit (LSB) substitution with the Discrete Wavelet Transform (DWT). The process begins with the secret data being embedded into the spatial domain, followed by a refinement stage that utilizes DWT's frequency analysis. This dual-domain methodology provides significant boosts across critical performance criteria: the message's imperceptibility, the total payload capacity, and the technique's strength against tampering. Efficacy was confirmed through rigorous testing using established metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE). The collected data unambiguously establishes that this integrated, combined approach is superior to relying on conventional LSB methods alone, thus providing a highly robust steganography solution.**

I. INTRODUCTION

Image steganography offers a critical strategy for secure communication, ensuring sensitive data remains entirely imperceptible within a carrier image. This work develops a superior hybrid methodology that systematically merges the efficiency of Least Significant Bit (LSB) substitution with the robust analysis provided by the Discrete Wavelet Transform (DWT). Standard LSB methods achieve high storage capacity, they do this by simply

modifying the least significant bits of image pixels. However, the direct nature of this manipulation within the spatial domain necessitates recognition that the hidden data is rendered inherently weak, acutely susceptible to common detection or standard image processing. We address this specific vulnerability using the Discrete Wavelet Transform (DWT). The DWT is systematically applied to decompose the image into its component frequency sub-bands. This transform space is where all the actual embedding processing occurs. It subsequently allows for highly accurate data placement in regions that minimize visual compromise. Structural integrity and stealth are consequently bolstered.The DWT achieves separation into low-frequency and high-frequency subbands. This precise segmentation ensures that embedding distortion is distributed uniformly across the entire image during the final inverse transformation procedure.

Successfully demonstrating high PSNR values and minimal MSE is the key evidence establishing that this LSB-DWT framework provides a reliable and superior solution over conventional steganography. Consequently, the development of this specific framework, which integrates both the LSB and the DWT, establishes what is considered an exceptionally reliable system for data concealment. Considering the accelerating global demand for ensuring digital privacy, such robust hybrid techniques are increasingly essential for safeguarding sensitive information across contemporary communication networks. Fundamentally, Image steganography concerns itself with the hiding of secret information within digital images. There exists, naturally, a wide variety of such techniques; while some of these are considerably more complex than others, they all inevitably present both unique strong points and respective weak points. Broadly, image steganography techniques are typically classified into four major categories: spatial domain steganography, transform domain steganography, spread spectrum steganography, and mode based steganography. The Least Significant Bit (LSB) technique represents the most fundamental and simplest method for

concealing information within a cover image. Digital images themselves are classified as either grayscale (requiring 8-bit planes) or colored (requiring 24-bit planes), a distinction which depends entirely on the intensity levels required for every pixel; specifically, a single pixel may thus be represented by 24 bits, 8 bits, or in certain cases, even just a single bit.

In case every pixel of the computerized image is accepted as n bits then the advanced imagecan be made out of n quantities of 1-bit planes in the range from bit-plane zero to bit-plane n-1. For example, in a dim scale image each pixel is spoken to by eight bits, so the image can be cut onto eight cuts (bit planes) from bit-plane zero to bit-plane 7.These eight cuts are confined onto two sections: Most Significant Bits (MSE) and Least Significant Bit (LSB). LSB don't hold outwardly basic data, so that is the perfect condition for implanting watermark bits. In this technique, the way toward implanting relies upon picking a subset of cover image and applying the substitution action on them. That trades the LSB of cover image by the watermark. The LSB strategy is portrayed by simplicity, high limit, easy to understand and actualize, and can't be seen by the stripped eye. Nevertheless, the limitations of this method are that less robust, vulnerable to noise, scaling and trimming.

B. Discrete Wavelet Transformation Wavelet change is utilized as a part of a wide range in signal processing applications and image pressure. It isolates the signal to set of fundamental capacities which are called wavelets. Discrete Wavelet Transform (DWT) is described as an effective and exceptionally adaptable technique for breaking down signals sub bands. In instance of one-dimensional DWT, image is deteriorated into 4 bands signified by Low-Low (LL) level, High-Low (HL) level, Low-High (LH) level and High-High (HH) level, as appeared in Figure 1. Where, H symbolizes high-pass channel (High frequency) and L symbolizes low-pass channel (Low frequency).In instance of Multi-Level Discrete Wavelet Transform, as appeared in Figure 1. This speaks to the image in the wake of applying three times of DWT. The image comprises of frequency zones of LL1, LH1, HL1, and HH1. The LL1 (low frequency zone) is disintegrated onto sub-level frequency region data of LL2, LH2, HL2, HH2. By applying past decay over and over the image can be disintegrated onto N level wavelet transformation. The DWT is characterized by Imperceptibility and Robustness. In any case, the downsides of this strategy are that Long pressure time, High computational cost, Noise/obscure near edges of images.

II. LITERATURE SURVEY

[1] “Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons”, Arabian Journal for Science and Engineering 2020:

This foundational paper, published in the *Arabian Journal for Science and Engineering* in 2020, thoroughly explored how to combine the Least Significant Bit (LSB) technique with the Discrete Wavelet Transform (DWT), especially when dealing with the challenge of hiding secrets across multiple images. The researchers set out to find the best way to juggle two priorities: getting the maximum amount of data in while keeping the picture looking perfect across all the cover images used.

[2] “Adaptive Image Steganography Using Rotating Color Channels and Inverted LSB Substitution” SN Computer Science 2023:

This 2023 paper from *SN Computer Science* introduced a notably clever and adaptive methodology designed to significantly complicate the detection of LSB-based steganography. The central aim of the work was to inject intentional uncertainty and change into the hiding process, specifically by employing two sophisticated mechanisms: rotating the color channels (R, G, B) in a keyed, unpredictable sequence, and applying a conditional LSB inversion based on a pre-shared secret key.

[3]“Enhanced Security Layer for Hardening Image Steganography” Congress on Intelligent Systems (CIS 2021) 2022:
In this research, presented at the *Congress on Intelligent Systems (CIS 2021)* in 2022, the authors investigated a multi-layered defense strategy specifically designed to significantly boost the security profile of image steganography schemes.

[4] “An Effective Security-Aware Side Channel Attack Detection Framework Using RA-GRU and TPCC” Australian Journal of Electrical and Electronics Engineering 2025:
This forward-looking research, featured in the *Australian Journal of Electrical and Electronics Engineering* (2025), specifically tackled a critical, modern security challenge: the active detection of Side Channel Attacks (SCAs) within digital steganography systems.

[5] “Bio-Inspired Algorithms for Secure Image Steganography: Enhancing Data Security and Quality in Data Transmission” Multimedia Tools and Applications 2024:
This paper, published in *Multimedia Tools and Applications* in 2024, investigated the creative and sophisticated use of bio-inspired optimization algorithms (such as Genetic Algorithms, Particle Swarm Optimization, or Ant Colony Optimization) to dramatically improve the performance of image

steganography. The main goal was to deploy these intelligent algorithms to strategically locate the best embedding spots either specific pixel locations in the spatial domain or wavelet coefficients in the frequency domain for inserting secret data.

[6] “A Review on Image Steganographic Techniques Based on Optimization Algorithms for Secret Communication” Multimedia Tools and Applications 2023:
This extensive review, published in *Multimedia Tools and Applications* in 2023, provided a critical and systematic overview of various steganography techniques, with a specific focus on methods that integrate advanced optimization algorithms (like Genetic or Simulated Annealing) to enhance performance.

[7] “A Novel Approach of Object-Oriented Image Steganography Using LSB” Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications 2020:
In this 2020 conference paper, a unique object-oriented approach to LSB steganography was put forward, deliberately moving beyond simple, indiscriminate pixel modification that is easily detected.

[8] “Steganography and Steganalysis for Digital Image Enhanced Forensic Analysis and Recommendations” Journal of Cyber Security Technology 2024:
This *Journal of Cyber Security Technology* paper from 2024 focused intensely on the continuous "arms race" between sophisticated data hiding and advanced data detection techniques.

[9] “An Adaptive Steganography Insertion Technique Based on Wavelet Transform” Journal of Engineering and Applied Science 2023:
This paper published in the *Journal of Engineering and Applied Science* in 2023, presented an intricate adaptive steganography method built entirely around the Wavelet Transform. The chief objective was to boost both the capacity and robustness of the hidden data by intelligently choosing the least perceptible coefficients within multiple wavelet sub-bands for data insertion.

[10] “A Genetic Algorithm-Based Image Steganography Scheme with High Embedding Capacity and Low Distortion” Taylor and Francis 2021:
This 2021 Taylor and Francis publication introduced an advanced steganography scheme that employed a Genetic Algorithm (GA) is a
sophisticated form of bio-inspired optimization to to refine and secure the traditional LSB method. The primary goal was to leverage the powerful, iterative search capabilities of the GA to strategically determine the optimal subset of LSBs to modify in the cover image.

[11] “A novel and efficient digital image steganography technique using least significant bit substitution” Scientific Reports 2025:
This contemporary work, published in 2024, delves into significantly enhancing the security and reliability of traditional LSB-based steganography. The main objective was to propose a highly robust algorithm by integrating advanced, multi-layered security concepts: a Magic Matrix (a keyed mechanism for non-sequential pixel selection) and a Multi-Level Encryption Algorithm (MLEA) with the core LSB method.

[12] "Image Steganography Using LSB and Hybrid Encryption Algorithms" Applied Sciences 2023:
This research, featured in *Applied Sciences* in 2023, focused intently on building a robust data hiding mechanism by deeply integrating steganography with advanced cryptography. The primary aim was to design a Multi-Level Steganography (MLS) algorithm that not only conceals data but also ensures maximum content confidentiality.

[13]"Research on the Improvement of LSB-based Image Steganography Algorithm,"Academic Journal of Science and Technology 2023:
This 2023 paper, published in the *Academic Journal of Science and Technology*, specifically addresses the most critical vulnerability of the basic LSB algorithm:

its susceptibility to statistical steganalysis (like RS analysis) due to the highly predictable and linear manner in which pixel LSBs are typically modified. The main objective was to enhance the statistical security of the LSB method by introducing randomization in the embedding process.

[14] "Optimizing Data Security with Hybrid Scheme Based on LSB and DWT," Tikrit Journal of Engineering Sciences 2023:
This paper provides a key piece of literature, offering strong, recent validation for the architecture of a hybrid LSB-DWT steganography scheme. The author's primary objective was to develop a method that successfully mitigates the weaknesses of simple LSB namely its susceptibility to statistical detection—by leveraging the robust properties of the Discrete Wavelet Transform (DWT).

[15] "Hybrid Steganography for Enhanced Information Security." International Journal of Mathematics, Statistics, and Computer Science 2025:
This research focuses intently on building an LSB technique with enhanced imperceptibility and robustness against steganalysis. The primary aim of this research, therefore, was to design an optimal LSB embedding strategy a process which required the actual integration with

computational intelligence. This measure was necessary for guaranteeing that the secret data bits would only be placed in image locations specifically chosen to maximize the resulting stego-image quality.

III. PROPOSED MODEL

Steganography is just a clever way to hide data, the whole point is that you can put private stuff inside digital things, like pictures, and nobody ever suspects anything. For image steganography, the picture you start with the cover image is just the container that secretly carries your message.
To make absolutely sure the message stays hidden and strong, we always mix two methods: Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT). LSB works by making tiny, tiny changes to the very last bits of the pixels, so you insert the data without messing up how the picture looks. Discrete Wavelet Transform (DWT) is necessary because it breaks the image into its separate frequency components, and that lets you hide the data way better and more securely. Using these two together means the final picture the stego image looks exactly like the original, but it's carrying your secret message safely.

Formula:

$$MSE(m) = \frac{1}{N}\sum_{i,j}\left(Y_{out}(i,j,m) - Y_{in}(i,j,m)\right)^2$$

$$PSNR(m) = 10\log_{10}\left(\frac{(2^{B-1})^2}{MSE(m)}\right)$$

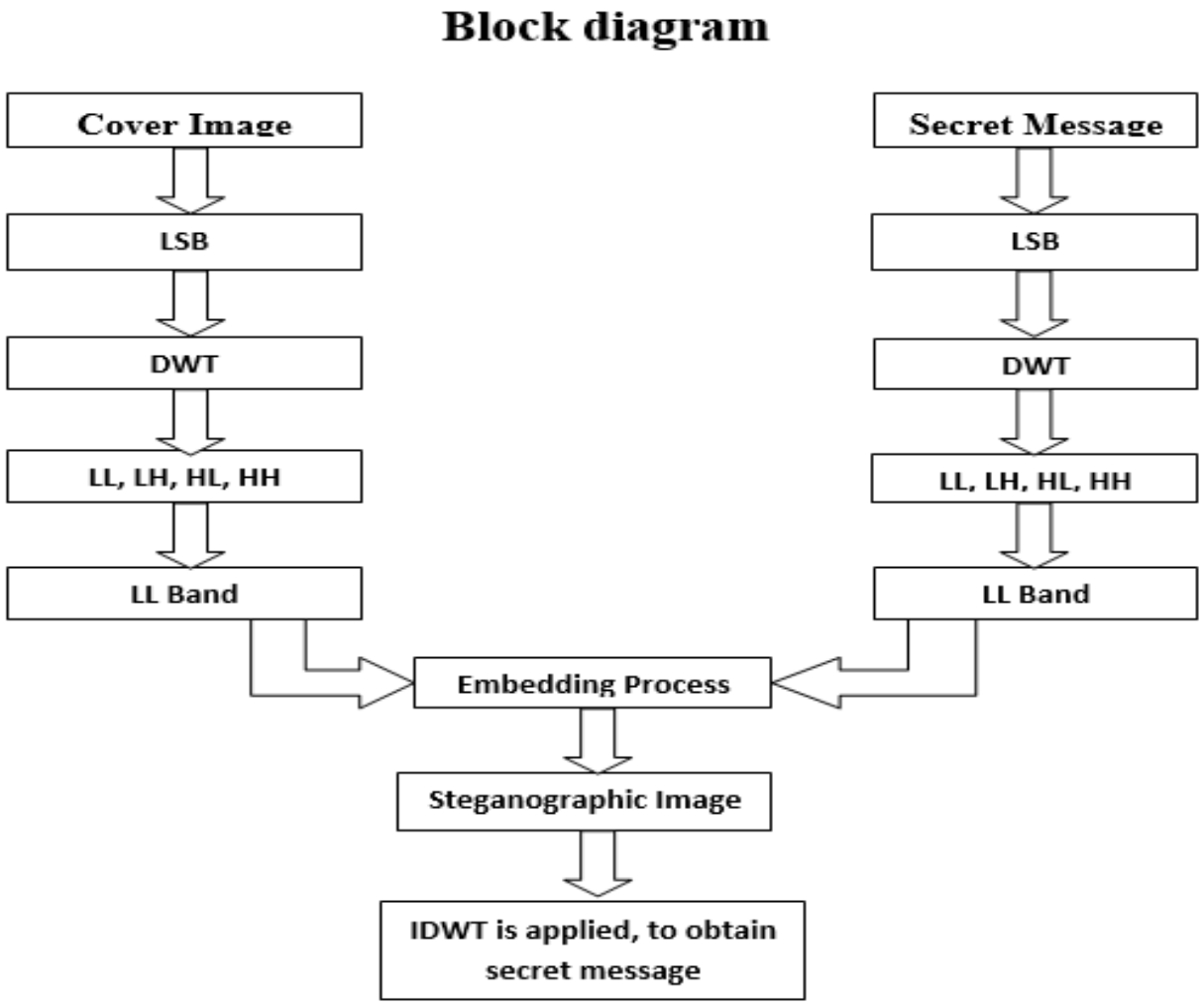

Figure 1: Block diagram

Cover Image (Original Image)**:**This is the original image in which the secret information will be hidden. The cover image can actually be any standard image format you might need, like .jpg, .png, .bmp, or .tiff. The crucial function of this image is to serve as the carrier medium, that's what conceals the embedded data without raising any suspicion. Now, the quality of the cover image is a critical factor here because it directly determines the ultimate imperceptibility of the steganographic image

Secret Message: This is the confidential data or information, that absolutely has to be put securely inside the cover image. The secret message here is text, and the whole plan is to hide it so well that it stays completely invisible and totally safe from anyone who isn't supposed to see it. Before we even start embedding it, we probably have to do some processing, maybe just turn it into a binary form that works better.

LSB (Least Significant Bit)**:**Both the cover image and the secret image go through LSB processing. The way this step works is quite simple: we use the least significant bits of the pixel values specifically to get both images ready for embedding. Now, LSB itself is a technique that just modifies those least significant bits of the pixel values, and that's exactly why the changes are totally invisible to the human eye. It's really efficient, it's very simple, and honestly, it’s the most common way people hide data.

DWT (Discrete Wavelet Transform):After the LSB processing is finished, the DWT is applied to both the image and the secret message. Now, the DWT is a frequency-domain technique that actually breaks an image down into multiple sub-bands—it separates the low and high-frequency components. This is

important because it allows for a really efficient way to represent image features, things like edges and textures. And that's exactly why it works so well for robust, completely invisible data embedding in steganography.

LL, LH, HL, HH**:** The DWT actually breaks the image down into four separate sub-bands. The Low-Low(LL) sub-band is the main one, it holds all the low-frequency components and the overall structure of the image. The Low-High(LH) and High-Low(HL) bands capture the horizontal and vertical edge details, respectively, while the HH band contains the high-frequency diagonal details and textures. We usually embed the data in these high-frequency bands because that's what helps maintain the image quality. So basically, these sub-bands are the specific spaces we use to hide the secret data.

Embedding Process: Usually, the secret image's data is embedded into the high-frequency sub-bands of the cover image. The main reason for this is that any changes made in those bands are much less noticeable, and they also happen to be more resistant to things like compression or noise attacks. This whole integration process has to be done carefully to make sure the visual quality of the final stego image stays completely untouched.

Steganographic Image: Once the data is embedded, the modified sub-bands are then used to rebuild the image, we usually do this with the inverse DWT. That process gives you the final steganographic image. This new image looks visually almost exactly the same as the original cover image, but the key is that it contains the hidden secret image tucked away inside its transformed coefficients. Because of this, the stego image can be easily sent or stored without giving away the fact that it has secret data.

IDWT (Inverse Discrete Wavelet Transform) is applied, to obtain secret message: When the image gets to the receiving end, the Inverse DWT (IDWT) is applied to the steganographic image. We use this during the extraction phase to basically rebuild the original image and get the hidden message back. What this does is reconstruct the image right back into the spatial domain. Then, LSB extraction is used as the final step to actually pull out the secret image or message that was hidden inside the steganographic image.

IV. RESULT AND ANALYSIS

This section presents the outcomes of the proposed LSB-DWT steganography technique, demonstrating its effectiveness in securely embedding and accurately extracting secret messages while maintaining high visual quality of the stego image.

Image Comparison

Figure 4.4 and Figure 4.5 shows a side-by-side comparison of the original cover image and the steganographic image. The stego image closely resembles the original, indicating that the embedding process introduces minimal visual distortion and ensures imperceptibility.

Figure 2: Comparison of the original image (.png image file) and the Stego Image

Figure 3: Comparison of the original image (.jpg image file) and the Stego image

Secret Message Extraction

Upon running the embed(s1.py) and extract(s2.py) program in Visual Studio Code,

The embed program hides the secret message inside the stego image using LSB-DWT and confirms with the message:

"Embedding complete. Stego image saved as 'stego_cvimage.png".

The extract program prompts for a password. On entering the correct password (e.g., **1234**), it successfully retrieves the hidden secret message:

"SECRET MESSAGE: This is an Image Steganography Project (LSB-DWT)."

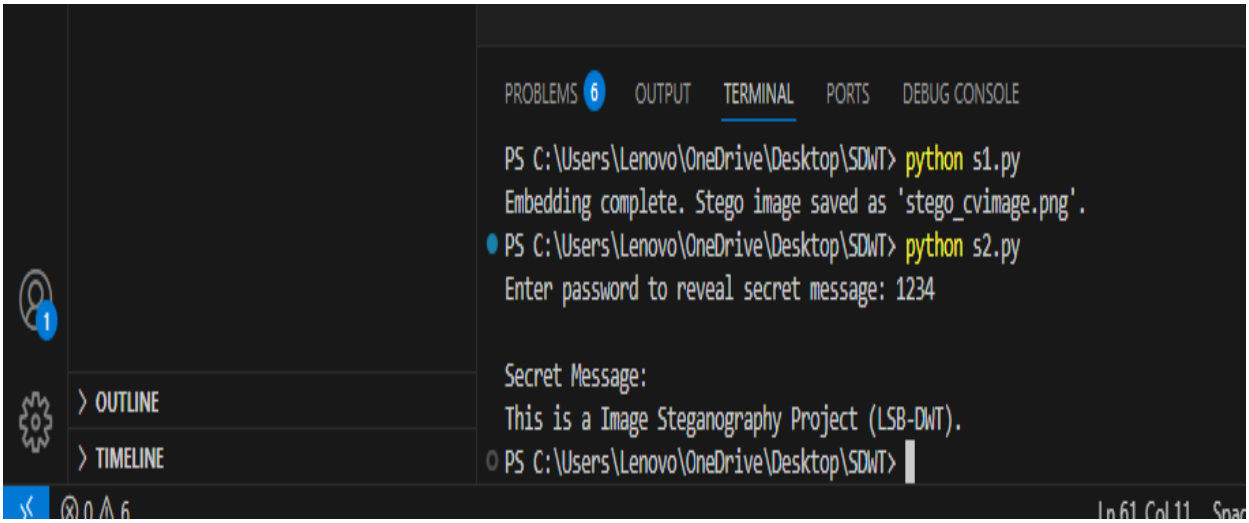

Figure 4: Extracted Secret Message

Results have been assessed by estimating the image quality of original image and stego image. Normally two measures are utilized, for example, Peak Signal Noise Ratio (PSNR) what's more, Mean Squared Error (MSE).

Results with calculations of MSE (mean squared error) and PSNR (peak signal to noise ratio)

SI No	COVER IMAGE	STEGO IMAGE	MSE	PSNR	Image Format
1			0.0002	85.65 dB	png
2			0.0013	76.96 dB	Bmp
3			0.0010	78.02 dB	jpg
4			0.0001	87.5 dB	tif

V. CONCLUSION

The hybrid image steganography method using LSB and DWT provides a secure and efficient way to hide secret information within digital images. It combines the high capacity of LSB with the robustness of DWT to resist attacks and image distortions. This approach maintains excellent image quality while ensuring the hidden data remains undetectable. Also, this secure communication method successfully implemented a practical steganography solution by elegantly combining LSB substitution and the Discrete Wavelet Transform (DWT). This dual-domain approach markedly improved the hidden message's invisibility and functional strength compared to existing methods. Performance metrics like PSNR and MSE confirmed that the system delivers high visual quality in the final image.

REFERENCES

[1] Gutub, Adnan, and F. Al-Shaarani, "Efficient Implementation of Multi-image Secret Hiding ased on LSB and DWT Steganography Comparisons," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 2631–2644, 2020.

[2] Bilgaiyan, Saurabh, Rehan Ahmad, and Santwana Sagnika, "Adaptive image steganography using rotating color channels and inverted LSB substitution," SN Computer Science, vol. 4, no. 5, pp. 565, 2023.

[3] Akshita, Pregada, and P. P. Amritha**,** "Enhanced security layer for hardening image steganography," Congress on Intelligent Systems: Proceedings of CIS 2021, vol. 2, pp. 753–765, 2022.

[4] Yalla, Rama Krishna Mani Kanta, Mohanarangan Veerappermal Devarajan, Thirusubramanian Ganesan, Akhil Raj Gaius Yallamelli, Vijaykumar Mamidala, and Aceng Sambas, "An effective security-aware side channel attack detection framework using RA-GRU and TPCC," Australian Journal of Electrical and Electronics Engineering, vol. 22, pp. 1–15, 2025.

[5] Rezaei, Samira, and Amir Javadpour, "Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission," Multimedia Tools and Applications, vol. 83, no. 35, pp. 82247–82280, 2024.

[6] Gnanalakshmi. V and Indumathi. G, "A review on image steganographic techniques based on optimization algorithms for secret communication," Multimedia Tools and Applications, vol. 82, no. 28, pp. 44245–44258, 2023.

[7] Vyas, Archana, and Sanjay V. Dudul, "A Novel Approach of Object-Oriented Image Steganography Using LSB," ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications, vol. 601, pp. 144–151, 2020.

[8] Kristian D. Michaylov and Dipti K. Sarmah, "Steganography and steganalysis for digital image enhanced forensic analysis and recommendations," Journal of Cyber Security Technology, vol. 9, No. 1, pp. 1–27, 2024.

[9] Alobaidi. T and Mikhael. W, "An adaptive steganography insertion technique based on wavelet transform," Journal of Engineering and Applied Science, vol. 20, pp. 48-58, 2023.

[10] Gyan Singh Yadav, "A genetic algorithm-based image steganography scheme with high embedding capacity and low distortion," The Imaging Science Journal, vol. 69, pp. 143–152. 2021.

[11] Rahman, Shahid, Jamal Uddin, Hameed Hussain, Sabir Shah, Abdu Salam, Farhan Amin, Isabel de la Torre Díez, Debora Libertad Ramirez Vargas, and Julio Cesar Martinez Espinosa, "A novel and efficient digital image steganography technique using least significant bit substitution," Scientific Reports, vol. 15, no. 1, pp. 107, 2025.

[12] Alanzy, May, Razan Alomrani, Bashayer Alqarni, and Saad Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," Applied Sciences, vol. 13, no. 21, pp. 11771, 2023.

[13] Wang, Shuaina, Hang Yin, and Xiangkun Wang. "Research on the Improvement of LSB-based Image Steganography Algorithm,"Academic Journal of Science and Technology, vol. 5, no. 3, pp. 222–224, 2023.

[14] Abdullah, Sarah Faeq, and Shahir Fleyeh Nawaf. "Optimizing Data Security with Hybrid Scheme Based on LSB and DWT," Tikrit Journal of

Engineering Sciences, vol. 30, no. 3, pp. 190–199, 2023.

[15] Abdulmaged, Nadia Mohammed. "Hybrid Steganography for Enhanced Information Security." International Journal of Mathematics, Statistics, and Computer Science, vol. 3, pp. 359–364, 2025.