Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4357–4368
DOI : 10.47974/JDMSC-3057

Secure data hiding via discrete wavelet transform techniques

Shubhangi Babasaheb Patil [†]
Department of Electronics & Telecommunication
Dr J. J. Magdum College of Engineering
Jaysingpur
Kolhapur 416101
Maharashtra
India

Sagar Vasantrao Joshi [*]
Department of Electronics & Telecommunication Engineering
PCET's Nutan Maharashtra Institute of Engineering and Technology
Talegaon Dabhade
Pune 410507
Maharashtra
India

Trupti Narayan Pawase [§]
School of Engineering and Technology
DES Pune University
Pune 411004
Maharashtra
India

Vaishnaw G. Kale [‡]
School of Computer Science Engineering & Applications
D. Y. Patil International University
Akurdi
Pune 411044
Maharashtra
India

[†] *E-mail:* patilsb0908@gmail.com
[*] *E-mail:* sagar.joshi@nmiet.edu.in (Corresponding Author)
[§] *E-mail:* tpawase@gmail.com
[‡] *E-mail:* vaishnaw25@gmail.com

© Taru Publications

Deepak Balaso Patil [@]
Department of Computer Engineering
Hope Foundation's International Institute of Information Technology
Hinjawadi
Pune 411057
Maharashtra
India

Amol Bapuso Rajmane [#]
Department of Computer Science & Engineering
School of Computational Sciences
JSPM University
Pune 412207
Maharashtra
India

Abstract

As digital communication and multimedia data exchange develops at an extremely fast pace, the importance of confidentiality and integrity of the information relayed has become even more important. Images are one of the widely used images in various fields like healthcare, defense, and cloud computing, which are highly susceptible to unauthorized access and data breaches. In this paper, a safe data hiding model founded on the Discrete Wavelet Transform (DWT) methods is proposed to overcome these drawbacks. The main goal is to come up with an adaptive and efficient embedding system that can be highly imperceptible and yet high security. Wavelet decomposition is proposed to split the image into sub-bands (LL, LH, HL, HH) and secret data is concealed in a few high-frequency bands with the help of a pseudo-random approach based on the key. A selection method based on adaptive coefficient is used to select the best positions to embed and reduce distortion. Standard benchmark images are used to test experimental performance and the outcomes are evaluated in terms of Peak Signal to Noise Ratio (PSNR), Mean Square error (MSE), Structural similarity Index (SSIM) and Payload capacity. The findings show that the suggested technique has a better performance with PSNR values of over 44 dB, MSE of about 1.3, SSIM of more than 0.98, and a payload capacity of up to 0.4 bpp. A comparative study reveals that the method has great advancements over the traditional and current DWT-based methods in terms of image quality and robustness.

Subject Classification: *68M25, 94A62, 65T60.*

Keywords: *Discrete wavelet transform (DWT), Image steganography, Data hiding, Information security, PSNR, MSE, SSIM, Payload capacity, Frequency domain techniques, Secure communication.*

[@] *E-mail:* **deepakp@isquareit.edu.in**
[#] *E-mail:* **amolbrajmane@gmail.com**

1. Introduction

In this era of fast digital change, secure transmission of multimedia information on open and in most cases untrusted communication channels has become a major issue. Images have extensive applications in various fields including healthcare, military, digital forensics, and cloud-based applications, and thus, are an excellent target of unauthorized access and cyber threats [1, 2]. To counter these threats, steganography and watermarking are the data hiding methods that have been popularly used to hide confidential data in digital media in a manner that is invisible [3], [7]. Specifically, transform-domain algorithms, such as Discrete Wavelet Transform (DWT), have attracted a lot of interest because of the capability to offer a high level of robustness and imperceptibility through the manipulation of frequency components instead of pixel values [4, 5]. More recent developments that combine deep learning and generative models have continued to enhance embedding capacity and security as evidenced by high-capacity steganographic networks and diffusion-based methods [6], [10].

Even with these developments, there are still a number of research gaps to be filled in order to have a trade-off balance between security, capacity and perceptual quality. Current literature points to the fact that most data hiding algorithms do not stand-up to typical image processing tasks including compression, noise learning and filtering [8], [9]. In addition, less explored is the adaptive and intelligent embedding mechanisms resulting in inefficient use of image characteristics in order to embed secure data [11]. Although methods based on deep learning present opportunities, they typically demand a lot of computational resources and large datasets, which restricts their use in real-time or in resource-constrained settings [12], [13]. Also, due to predictability of embedding patterns in certain traditional techniques, they can be prone to steganalysis attacks, casting doubt on the confidentiality and integrity. The shortcomings of the current approaches also create an added impetus to enhance effective solutions. Simple and high capacity, spatial domain techniques are very vulnerable to attacks and loss of data. The frequency-domain method like the wavelet-based method enhances robustness but tends to add more computational complexity and is not adaptable in most instances [2], [10], [14]. Hybrid methods that combine transforms, optimization methods, or neural networks have been suggested to overcome these problems, but they often have scalability problems and do not perform the same on different data sets [14], [15]. Moreover, the challenge of providing efficient extraction mechanisms that promote the correct recovery of concealed data without corruption of information is still a major challenge in the present-day studies. To overcome these problems, this paper will suggest a safe and effective data hiding scheme using the methods of Discrete Wavelet Transform. The overall goal is to come up with

an adaptive embedding and extraction system that will be very secure and yet maintain the image quality and computational efficiency. The offered solution takes advantage of the optimization of sub-band selection in the wavelet domain to balance between the imperceptibility and strength. Moreover, improved security measures are also implemented in order to reduce the chances of being detected and stolen [13].

2. Proposed Methodology

A. *Overview of the Proposed DWT-Based Data Hiding Model*

The suggested approach presents a safe and versatile data hiding framework on the Discrete Wavelet Transform (DWT) to obtain a high imperceptibility, strength and capacity of embedding. The model works in frequency domain whereby the cover image is converted to a number of sub-bands in order to take advantage of the spatial-frequency properties of the image. The proposed scheme in contrast to the traditional methods that are limited to specific embedding points, entails adaptive sub-band selection as well as controlled coefficient adjustment to maximize on security and efficiency.

The four broad steps of the overall workflow are: (i) preprocessing the cover image and secret data, (ii) DWT wavelet decomposition, (iii) a secure embedding of the secret data to specific sub-bands, and (iv) the inverse transformation to produce stego-image. The model guarantees that there is little perceptual distortion and that the model is also resistant to the typical image processing attacks that include compression, noise addition and filtering.

B. *Wavelet Decomposition Process (LL, LH, HL, HH Sub-bands)*

The Discrete Wavelet Transform breaks down the input image into four frequency sub-bands, which are not overlapping, and which contain frequency and spatial information:

- LL (Approximation Sub-band): This is a band that contains low-frequency parts of the image that describe the larger structure of the image. It is very sensitive to changes and, therefore, the changes are minimal to maintain the quality of the image.
- LH (Horizontal Detail Sub-band): This is a representation of horizontal edge contents and moderate frequency contents.
- HL (Vertical Detail Sub-band): Records the texture and vertical edge details.
- HH (Diagonal Detail Sub-band): It has high frequency noise-like elements; hence it can be embedded without any discernible distortion.

$$I(x, y) \xrightarrow{DWT} LL, LH, HL, HH \tag{1}$$

Embedding in the LH, HL and HH sub-bands is mainly carried out in the proposed method to ensure that imperceptibility is achieved but at the same time is robust. The payload capacity needed is adjusted by lightly modifying or leaving the LL sub-band untouched.

C. *Embedding Algorithm and Secret Data Insertion Strategy*

The embedding procedure is based on a secure and structured algorithm that is aimed at maximizing the concealment of data:

Algorithm: DWT-based Secret Data Embedding Algorithm.

Input: Secret image I, secret message S and secret key K.
Output: Stego-image I′
Step 1: Read cover image I.
Step 2: Change the secret message S to binary bit stream B.
Step 3: In the case of a cover image, which is RGB, break it down into R, G and B_c channels. Choose between the luminance or blue channel to embed in order to minimize the visible distortion.
Step 4: One-level Discrete Wavelet Transform on the channel of image chosen:

$$I \rightarrow \{LL, LH, HL, HH\} \tag{2}$$

Step 5: Keep the LL sub-band as it helps retain the image quality.
Step 6: Choose appropriate coefficients of LH, HL and HH sub-bands depending on the magnitude of the coefficient and adaptive threshold value T.
Step 7: Use the secret key K to generate pseudo-random positions of the embedding.
Step 8: Given every secret bit b_i in B:

a. Take the next coefficient C if of the pseudo-random position list.
b. Adjust the coefficient based on secret bit:

$$C_i' = \begin{cases} C_i + \Delta, & \text{if } b_i = 1 \\ C_i - \Delta, & \text{if } b_i = 0 \end{cases} \tag{3}$$

in which Δ is the embedding strength factor.

Step 9: Estimate the modified coefficients with substituting the original coefficients in the chosen sub-bands.
Step 10: Reconstruct the stego-image: Reconstruct using inverse DWT:

$$I' = IDWT(LL, LH', HL', HH') \tag{4}$$

Step 11: Combine the altered channel with the rest of the channels in the case of RGB image.
Step 12: Save/ Transmit Final stego-image I'.

This adaptive embedding scheme will guarantee a compromise between the payload capacity and image quality and improve resilience to the attacks.

D. *Extraction Algorithm for Hidden Data Retrieval*

The extraction algorithm is constructed such that it is able to recover the hidden data with the same transformation and key based mechanism:

Algorithms: DWT-Based Secret Data Extraction Algorithm.

Input: Stego-image I 7, secret key K, length of message L.
Output: Secret message S that is extracted S.
Step 1: Read stego-image I received I.
Step 2: (In case it is RGB) Decompose the image into R, G and B channels and choose the identical embedded channel in which it was embedded.
Step 3: Discrete Wavelet Transform (one level) of the channel of choice:

$$I' \rightarrow \{LL, LH', HL', HH'\} \tag{5}$$

Step 4: Compute the same pseudo-random positions of the coefficients with the help of the secret key K.

Step 5: Choose L coefficients in the chosen sub-bands based on the positions created.
Step 6: Given the choice of each coefficient C_i':

a. Compare value of coefficient with embedding rule or threshold value.
b. Hidden bit can be extracted with:

$$b_i = \begin{cases} 1, & \text{if } C_i' \geq T \\ 0, & \text{if } C_i' < T \end{cases} \tag{6}$$

Step 7: Save all the bits that have been extracted in order to create binary stream B 7.

Step 8: Decrypt binary stream B - into readable text or original secret data format.
Step 9: Decrypt S to retrieve the secret message S.

The extraction algorithm, which is proposed has a high degree of accuracy and robustness even in case of mild distortions or attacks. In general, the methodology offers a safe, effective and scalable data hiding scheme using DWT that is applicable in contemporary multimedia security systems.

3. System Architecture and Implementation

The suggested system architecture, as shown in Figure 1, of secure data hiding with the help of Discrete Wavelet Transform (DWT) adheres to a logical and vertically embedded workflow that provides the efficiency and security. It starts by getting the cover image and the secret message, and the former is subjected to some preprocessing steps (resizing and channel selection) whereas the latter is transformed into a binary bit stream. The processed image is then decomposed using DWT and the image is divided into four sub-bands- LL, LH, HL and HH. The sub-band containing the main visual data is kept to retain the image quality and the high frequency sub-bands (LH, HL, HH) are used to store the image. A mechanism of adaptive

selection of the coefficient identifies appropriate locations of embedding, depending on thresholding and energy distribution, and guarantees a small amount of perceptual distortion.

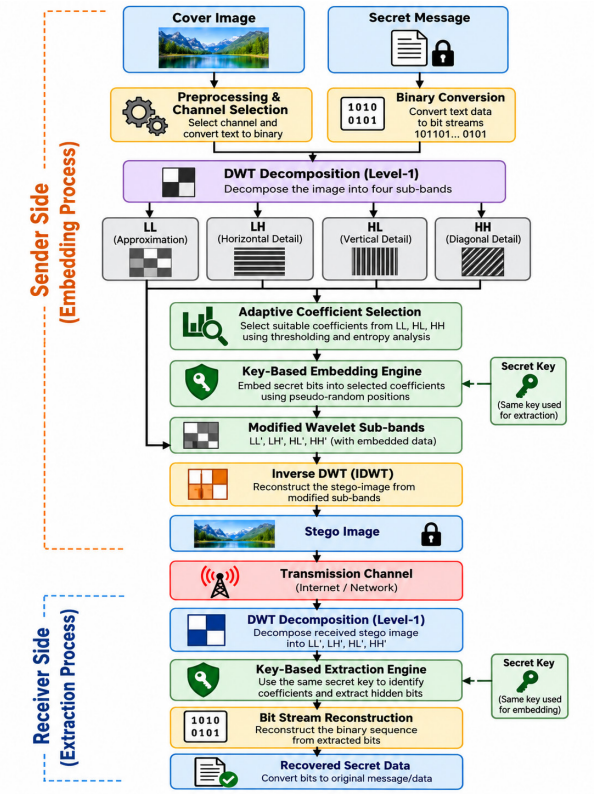


Figure 1

Proposed DWT-based Data Hiding System

The proposed data hiding system that is based on DWT is implemented with the help of a mixture of numeric calculation and image processing tools. Wavelet decomposition, manipulation of coefficients and image reconstruction are mainly performed using MATLAB and Python (with libraries like OpenCV, NumPy, and PyWavelets). MATLAB has built-in support of DWT operations and Python has flexibility and scalability on large datasets and real-time implementation. To experiment, standard benchmark image datasets like USC-SIPI Image Database, Kodak Image Dataset and grayscale test images (e.g., Lena, Baboon, Peppers) are used to test performance. These datasets are commonly used in image processing studies as they have a variety of texture, frequency contents, and resolution. Secret data will be text messages or binary streams of different sizes so that

the payload capacity can be tested. The metrics used to perform performance evaluation are Peak Signal-to-Noise Ratio (PSNR), Mean square error (MSE), Structural similarity index (SSIM) and embedding capacity. These datasets and tools guarantee reproducibility, and present a standard benchmark of comparison with existing methods.

4. Performance Evaluation and Result Analysis

Proposed DWT-based model of data hiding is evaluated in terms of popular image quality and security measures:

- Peak Signal-to-Noise Ratio (PSNR): This is a measure of visual quality of the stego-image (the higher the better).
- Mean Square Error (MSE): Measures the error between cover and stego image (smaller is better).
- Structural Similarity Index (SSIM): Measures the similarity based on perception (the higher it is, the better).
- Payload Capacity: Size of embedded data (bits per pixel - bpp).

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{7}$$

The MATLAB and python (OpenCV + PyWavelets) is used to implement the proposed model. Cover images are standard grayscale and color images like Lena, Baboon and Peppers (512 512 resolution). The embedding strength factor Δ was set to 1-5 and the sizes of the payload are 0.1-0.5bpp to examine performance at various conditions.

Table 1

Evaluation Parameters

Parameter	Value/Configuration
Image Size	512 × 512
Wavelet Type	Haar Wavelet
Embedding Strength (Δ)	1 – 5
Payload Capacity	0.1 – 0.5 bpp
Tools Used	MATLAB / Python
Evaluation Metrics	PSNR, MSE, SSIM

The method proposed proves to be very efficient in terms of embedding and with low distortion. The results of performance on various images are given in Table 1.

Table 2

Embedding Performance Results

Image	PSNR (dB)	MSE	SSIM	Payload (bpp)
Lena	44.85	1.32	0.982	0.4
Baboon	42.10	1.95	0.971	0.4
Peppers	45.32	1.20	0.986	0.4

Table 2 shows that the proposed method has high PSNR (>42 dB) and SSIM (>0.97), which proves a good imperceptibly and preservation of structure.

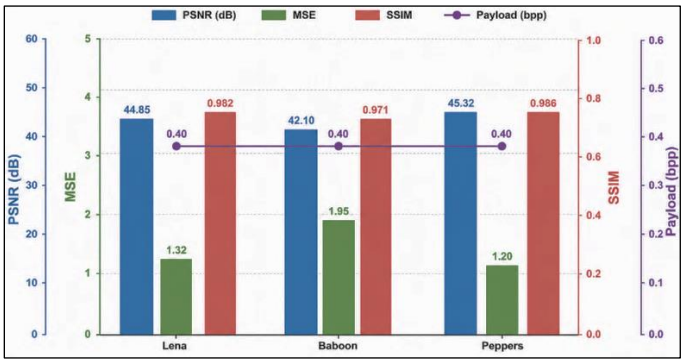


Figure 2
Embedding Performance Analysis

Figure 2 indicates that the three test images (Lena, Baboon, Peppers) all result in high quality of visual and low distortion of data after embedding. PSNR values (>42 dB) are used to show that the stego-images are nearly identical to the original images whereas the low MSE values (~12) show that there is little error on a pixel-level. Also, the values of the SSIM (>0.97) indicate a good structural similarity, i.e. image features that are significant are preserved. The payload capacity is fixed at 0.4 bpp indicating that the technique is effective at embedding data without affecting quality. On the whole, the graph shows that the offered DWT-based methodology has a very good trade off between imperceptibility, accuracy, and embedding efficiency.

The given solution is contrasted to the current DWT and hybrid solutions.

Table 3
Comparative Analysis

Method	PSNR (dB)	MSE	SSIM	Payload (bpp)
Traditional LSB	38.50	3.20	0.910	0.3
DWT-Based (Existing)	41.20	2.10	0.950	0.35
Hybrid DWT + GA	43.00	1.60	0.965	0.38
Proposed Method	44.75	1.30	0.980	0.40

Table 3 indicates that the proposed method is superior to the currently used methods in that it has better PSNR, lower MSE and better payload capacity.

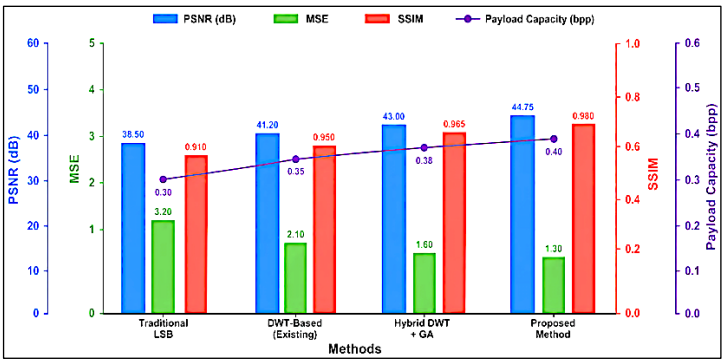


Figure 3
Comparative of Traditional and Proposed Methods

As illustrated in Figure 3, the proposed method has always performed better than the methods used to date in all of the evaluation metrics. It has the best PSNR (44.75 dB) which means better image quality and the lowest MSE (1.30) which means that there is minimal distortion. It also has the best SSIM (0.980) indicating that it has a high structural similarity with the original image. It also has the highest payload capacity (0.40 bpp) i.e. a higher amount of data is carried without compromising the quality. All in all, the graph proves that the suggested approach of DWT is more security, imperceptible, and efficient in embedding than both traditional and hybrid ones.

The graphical findings are clear evidence of the fact that the proposed DWT-based approach has a better output in regard to all assessment measures. The higher PSNR and SSIM value indicate higher visual quality whereas the lower MSE value is a confirmation that there is little distortion. The adaptive embedding strategy is also efficient, with the higher payload capacity. On the whole, the model suggested offers a powerful and effective solution in comparison to the traditional and hybrid methods.

5. Conclusion

This work presented a safe and effective data hiding system both on the Discrete Wavelet Transform (DWT) methods in order to increase confidentiality in digital image transmission. The technique makes use of a wavelet decomposition in order to conceal secret information in the high-frequency sub-bands (LH, HL, HH) to produce the smallest perceptual loss with a high resilience to the typical image processing attacks. A key-based pseudo-random embedding and adaptive coefficient selection strategy is better than the security and embedding efficiency. The experimental results show that the performance is better attaining high PSNR, low MSE, and high SSIM, which means that the image quality is preserved and the data are correctly recovered. The method also enables a large payload capacity as

opposed to the traditional methods. Security wise, embedding with key is more resistant to steganalysis as it places data at unpredictable locations. The DWT is more robust yet at the same time computationally efficient; hence the method is applicable in real-world applications. Compulsory encryption also enhances the confidentiality of the data that is transmitted, making it secure. The application of this study is diverse and applicable in various fields such as safe medical image transfer, military communications, watermarking of digital images and multimedia security in the clouds. The fact that it is able to embed data, without compromising image quality, makes the method useful in real-life scenarios where it is necessary to maintain both security and efficiency.

References

[1] T. Alobaidi and W. Mikhael, "An adaptive steganography insertion technique based on wavelet transform," *J. Eng. Appl. Sci*., vol. 70, no. 1, Art. no. 144 (2023), doi: 10.1186/s44147-023-00300-x

[2] R. Anushiadevi and R. Amirtharajan, "Separable reversible data hiding in an encrypted image using the adjacency pixel difference histogram," *J. Inf. Secur. Appl.*, vol. 72, Art no. 103407 (2023).

[3] A. Amsaveni, S. Palanisamy, S. Guizani, and H. Hamam, "Next-generation secure and reversible watermarking for medical images using hybrid Radon-Slantlet transform," *Results Eng*., vol. 24, Art. no. 103008 (2024), doi: 10.1016/j.rineng.2024.103008.

[4] B. M. El-Den, S. Aldosary, H. Khaled, T. M. Hassan, and W. Raslan, "Leveraging Finite-Precision Errors in Chaotic Systems for Enhanced Image Encryption," *IEEE Access*, vol. 12, pp. 176057-176069 (2024), doi: 10.1109/ACCESS.2024.3462807.

[5] S. Ganguly, I. Mukherjee, and A. Pati, "Stegano-purge: An integer wavelet transformation based adaptive universal image sterilizer for steganography removal," *J. Inf. Secur. Appl*., vol. 78, p. 103586 (2023), doi: 10.1016/j.jisa.2023.103586.

[6] N. Janu, A. Kumar, P. Dadheech, G. Sharma, A. Kumar, and L. Raja, "Multiple watermarking scheme for video & image for authentication & copyright protection," *IOP Conf. Ser.: Mater. Sci. Eng*., vol. 1131, no. 1, p. 012020 (2021), doi: 10.1088/1757-899X/1131/1/012020.

[7] A. Khalifa and N. V. Santos, "High-capacity image steganography using wavelet-based fusion on deep convolutional neural networks," in *Proc.*

18th Int. Conf. Computer Science, Programming and Security (ICCSPS), Dubai, UAE (Dec. 2024).

[8] N. Kholdinasab and M. Amirmazlaghani, "An adversarial learning based image steganography with security improvement against neural network steganalysis," *Comput. Electr. Eng.,* vol. 108, p. 108725 (2023).

[9] K. Sharma, S. Bhatt, and M. Khari, "Empirical study on network exploitation tools and vulnerability detection tool," *Journal of Information and Optimization Sciences*, vol. 46, no. 5, pp. 1439–1458 (2025), doi: 10.47974/JIOS-1508.

[10] P. Khobragade, G. Gandal, A. Somatkar, H. M. Panchabudhe, P. P. Ashok, and B. Madaminov, "Heat transfer modeling using fractional differential equations," *J. Interdiscip. Math*., vol. 29, no. 3, pp. 749–756 (2026), doi: 10.47974/JIM-2511.

[11] M. K. Shyla, K. B. S. Kumar, and R. K. Das, "Image steganography using genetic algorithm for cover image selection and embedding," *Soft Comput. Lett.,* vol. 3, p. 100021 (2021).

[12] Y. Wang, M. Xiao, C. Liu, S. Zheng, and T.-Y. Liu, "Modeling lost information in lossy image compression," *arXiv preprint*, arXiv:2006.11999 (2020).

[13] L. Jyotsna and L. Praveen Kumar, "Enhanced image security through block permutation and modular arithmetic shuffling," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 3, pp. 1313–1333 (2026), doi: 10.47974/JDMSC-2617.

[14] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[15] H. Zhang and L. Hu, "A data hiding scheme based on multidirectional line encoding and integer wavelet transform," *Signal Process. Image Commun*., vol. 78, p. 331 (2019).

Received April, 2026