International Journal of Safety and Security Engineering
Vol. 16, No. 5, May, 2026, pp. 1111-1119
Journal homepage: http://iieta.org/journals/ijsse

Enhanced Adaptive Discrete Wavelet Transform and Quantization Index Modulation Steganography Using Artificial Bee Colony

Muhammad Tahmidillah, Adifa Widyadhani Chanda Dlayla, Tohari Ahmad*

Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya 60111, Indonesia

Corresponding Author Email: tohari@its.ac.id

https://doi.org/10.18280/ijsse.160516

Received: 1 March 2026
Revised: 1 May 2026
Accepted: 25 May 2026
Available online: 31 May 2026

Keywords:
cybersecurity, data hiding, information security, steganography, network infrastructure

ABSTRACT

The rapid growth of the internet requires secure data transmission, making steganography essential for hiding information. The challenge in steganography is balancing the conflicting metrics of imperceptibility and robustness. This proposed method is an adaptive steganography method based on Discrete Wavelet Transform (DWT) and Quantization Index Modulation (QIM). Its main contribution is the application of the Artificial Bee Colony (ABC) algorithm to automatically optimize the QIM delta parameter, achieving an optimal trade-off. By embedding messages in the LH and HL sub-band coefficients, this method achieves superior visual quality with an average PSNR of 70 dB. Furthermore, its resistance to Gaussian noise attacks is significant, with a BER of 0.0078, which is much lower than that of the base line (0.1291). This result shows the proposed ABC-optimized approach is convenient in both visual quality and data reliability.

1. INTRODUCTION

The unprecedented expansion of internet connectivity has revolutionized global communications, enabling the seamless transmission of data across long distances [1]. However, this digital convenience comes at a high cost, as cybercriminals are increasingly able to misuse sensitive information on networks. To address these security challenges, two complementary approaches have been developed: cryptography [2] and steganography [3]. Recent developments have even encouraged the evolution towards public-key steganography that can be proven secure for identity verification mechanisms [4], while, on the other hand, the endless competition between data hiding and detection (steganalysis) is driving innovation in data security architecture [5]. While cryptography converts messages into unreadable ciphertext, steganography develops a more subtle approach by hiding the existence of the message or secret image. This technique involves invisibly embedding secret data into a harmless cover object, such as a digital image, to produce a stego-image that remains visually indistinguishable from the original.

The effectiveness of image steganography depends on achieving an optimal balance between three conflicting performance metrics. The first is imperceptibility: the stego-image must look exactly like the cover image so that the embedded data leaves no visible artifacts [6]. The second is capacity, which is the sensitive data that can be embedded without worsening security. Optimization methods such as Ant Colony Optimization (ACO) have been shown to significantly increase embedding capacity compared to older methods [7]. The last performance metric is robustness, which is the ability of the embedded data to withstand common manipulations and attacks, such as JPEG compression, on social media [8], while maintaining its extractability and integrity [5].

Steganography techniques are classified into spatial-domain and frequency-domain methodologies. The spatial domain approach, exemplified by the Least Significant Bit (LSB) process [9], offers simplicity and high embedding capacity but is vulnerable because it is susceptible to statistical analysis attacks and shows weak resistance to image processing operations. To overcome these limitations, frequency domain techniques have become increasingly popular due to their superior imperceptibility and enhanced robustness. These methods embed secret data into image transformation coefficients using mathematical transforms such as the Discrete Wavelet Transform (DWT) [10]. This DWT decomposes images into several frequency sub-bands, namely LL (approximation), LH (horizontal details), HL (vertical details), and HH (diagonal details), which offer a multi-resolution representation of image content. Research that embeds data into the middle-frequency sub-bands (LH and HL) achieves balanced evaluation metrics between imperceptibility and robustness because these sub-bands capture important edge information but are more difficult for the human eye to perceive as embedded compared to the low-frequency components [11, 12].

In the DWT domain, Quantization Index Modulation (QIM) stands out as a powerful embedding technique known for its exceptional robustness, especially when combined with a metaheuristic optimization approach [13]. However, QIM performance is highly dependent on a single parameter, namely the quantization step, denoted as delta (Δ). This parameter governs a fundamental trade-off: a smaller delta

value enhances imperceptibility but weakens robustness, while a larger value improves robustness at the expense of visual quality [14]. Recent studies also show that optimizing wavelet transformation coefficients, such as using Particle Swarm Optimization (PSO), is critical for preserving high image quality [15]. Consequently, manually selecting a fixed delta value is suboptimal because it fails to adapt to the coefficient characteristics of different cover images and payloads. Therefore, the main challenge is how to automatically determine the optimal delta value that maximizes imperceptibility and robustness for each combination of cover image and secret message.

This proposed method addresses these critical challenges by proposing an adaptive steganography framework that combines DWT and QIM with adaptive parameter optimization. The main contributions of this work are as follows:

(1) Multi-Objective Fitness Function: Design of a weighted fitness function that automatically evaluates imperceptibility and robustness, enabling intelligent trade-off optimization.
(2) Performance Improvement: The visual quality and capacity achieved in the research is better than existing methods.
(3) Adaptive embedding: Implementation of a dynamic approach in each image-message pair receives customized embedding parameters, rather than using static parameter selection.

This paper is organized into five main sections. Section I outlines the background and defines the core research problem. Section II reviews previous methods and current approaches to data hiding. Section III provides a detailed description of the proposed method. Section IV reports experimental findings and includes a comparative assessment with current techniques. Finally, Section V summarizes the study's contributions and suggests potential research for future experiments.

2. RELATED WORK

Prior work in image steganography can be broadly organized into three streams: spatial-domain methods, frequency-domain methods, and optimization-driven adaptive approaches. This review traces that trajectory and identifies the gap this paper addresses.

2.1 Spatial-domain steganography

Early steganography techniques primarily operated in the spatial domain, with LSB substitution being the most common approach due to its simplicity and high embedding capacity. However, traditional LSB methods are relatively vulnerable, including susceptibility to statistical attacks such as BER attacks and a lack of resistance to common image processing operations. To overcome these limitations, some research began incorporating optimization algorithms within the spatial-domain framework.

Metaheuristic algorithms have been shown to improve basic LSB techniques. For example, the Artificial Bee Colony (ABC) algorithm has been used to optimize block assignment for embedding, resulting in better security without shifting to the frequency domain [16]. The ACO-LSB method further applies adaptive exploration to select suitable pixels, improving embedding capacity by up to 30% [7]. In addition, ACO combined with a triangular chaotic map has been explored to enhance data randomness in image steganography [17]. Although the fundamental limitations of spatial-domain embedding remain unresolved, these studies demonstrate the potential of nature-inspired optimization algorithms in steganography.

2.2 Frequency-domain steganography

Research on the limitations of spatial-domain steganography has encouraged a shift toward frequency-domain approaches. Among these, the DWT is particularly advantageous because of its multi-resolution analysis capability and its compatibility with the characteristics of the human visual system. DWT optimized with the ABC algorithm has been applied to improve hiding capacity and visual quality, achieving an effective PSNR range [18]. This idea has also been extended through the use of the Lifting Wavelet Transform (LWT) and multi-objective ABC-optimized singular value decomposition (SVD) to develop a robust watermarking scheme [19]. In addition, DWT combined with Diamond Encoding has been used to embed secret data into wavelet coefficients, making the hidden information less vulnerable to compression and filtering attacks [20]. These studies indicate that frequency-domain embedding can better withstand common image manipulations that may destroy spatially embedded data.

Hybrid transform-based methods have also been proposed to strengthen steganographic security. A DWT-Discrete Cosine Transform (DCT) steganography method has been used to combine the advantages of both transformations by embedding encrypted data into selected sub-bands of the cover image [21]. This encrypt-then-embed model provides two layers of protection: cryptographic protection for the message content and steganographic protection for the embedding location. A similar hybrid approach integrates DWT, SVD-based image randomization, and threshold encryption, producing stego images with no visible difference from the original cover images [9]. In addition, time-based dynamic encryption has been incorporated into steganography to create a stronger dual-layer security mechanism [22]. Canonical Huffman Coding (CHC) has also been combined with DWT to improve embedding efficiency through simultaneous compression and transformation [23].

The integration of cryptographic techniques with steganographic embedding has emerged as a robust approach for protecting highly sensitive data. A variant of CDF-DWT combined with the ElGamal encryption algorithm has been developed for biomedical image steganography [24]. In this method, sensitive data are first encrypted and then embedded into wavelet coefficients. This pre-encryption step ensures that even if the steganographic layer is compromised, the extracted data remain cryptographically protected.

2.3 Optimization-driven and adaptive approaches

Recent developments in modern steganography have focused on the automatic optimization of embedding parameters, addressing the fundamental limitation that fixed parameters cannot adapt to varying image characteristics and security requirements. Learning Automata have been applied to optimize parameters for block-based QIM in the DWT domain [25]. This adaptive approach has also been extended

to the spatial-frequency hybrid domain, where Genetic Algorithms (GA) are used to determine the optimal change matrix for QIM [13]. In addition, recent survey research shows that deep learning-based methods are increasingly being used to automatically determine embedding costs, gradually replacing manually designed approaches [26]. These developments indicate that adaptive parameter selection can significantly improve the trade-off between imperceptibility and robustness.

PSO is another bio-inspired metaheuristic that has been successfully applied to steganographic parameter optimization. PSO has been used to determine optimal coefficients in the Dual-Tree Complex Wavelet Transform (DTCWT) domain for watermarking applications [15]. This approach reduces image distortion by identifying coefficients that can be modified without significantly degrading image quality. PSO is suitable for this optimization problem because it can efficiently search a large solution space while reducing the risk of being trapped in poor local solutions.

2.4 Research gaps

Despite recent research, several critical gaps remain in the current steganography literature. Table 1 summarizes the research gaps identified in previous studies. First, most existing methods use fixed or semi-adaptive embedding parameters that fail to exploit the unique characteristics of each image fully. Second, optimization approaches often focus on a single objective rather than optimizing both metrics simultaneously. Third, QIM-based methods, despite the theoretical advantages in robustness, have not been further explored in combination with advanced metaheuristic algorithms designed to address complex trade-off scenarios. This proposed method fills that gap by suggesting an adaptive steganography framework that uses ABC to improve the delta QIM parameter in the DWT domain. Unlike previous work, this method optimizes imperceptibility and robustness simultaneously by using a carefully designed multi-objective fitness function that achieves superior performance in both metrics.

Table 1. Comparison results from the proposed method

Method	Embedding Domain	Transform	Optimization Algorithm	Embedding Technique	Contribution
[7]	Spatial	-	Ant Colony Optimization (ACO)	LSB (4-bit) + Decoy bits + MD5 checksum integrity	ACO adaptively selects optimal pixels for 4-bit LSB embedding, augmented by a decoy-bit tampering detection mechanism and MD5 integrity verification.
[13]	Hybrid (Spatial + DCT)	DCT (8 × 8 blocks)	Genetic Algorithm (GA)	QIM on DCT	GA optimizes a per-block spatial change matrix that halves DCT computation in a hybrid domain, minimizing histogram distortion via NMSE with zero BER across all test cases.
[15]	Frequency (DTCWT)	DTCWT Level 4	Particle Swarm Optimization (PSO)	LSB on selected Low-Low sub-band	PSO selects optimal DTCWT Low-Low subband coefficients for LSB watermark embedding,
[16]	Spatial	-	Artificial Bee Colony (ABC)	LSB + Block Permutation	ABC algorithm optimizes the block assignment order for LSB-based secret image embedding, with block permutation serving as the security key.
[19]	Frequency (LWT)	LWT (3-level)	Multi Objective Artificial Bee Colony (MOABC)	SVD-based embedding on Low-High Subband	MOABC optimizes multiple scaling factors for SVD-based LWT watermarking, with chaotic logistic-map pre-encryption of the watermark to enhance security and robustness.
[20]	Frequency (DWT)	Haar DWT	-	Diamond encoding on 2 × 1	Diamond encoding on DWT coefficient pairs reduces embedding distortion compared to plain LSB, with random placement across Low-Low, High-Low, and Low-High sub-bands.
[25]	Frequency (DWT)	DWT (multi-level)	Learning Automata	Block QIM on DWT coefficients	Learning Automata distributes QIM distortion adaptively across DWT blocks sized by local edge density, requiring no side information at extraction.
Proposed Metod	Frequency (DWT)	Haar DWT Level 1 cH1 + cV1	ABC	Scalar QIM on top-N significant coefficients from concatenated cH1 + cV1 sub-bands	ABC directly optimizes the QIM delta parameter over concatenated cH1 + cV1 DWT sub-bands using a multi-objective fitness

Note: Discrete Cosine Transform (DCT); Dual-Tree Complex Wavelet Transform (DTCWT); Discrete Wavelet Transform (DWT) and Quantization Index Modulation (QIM); Lifting Wavelet Transform (LWT); Quantization Index Modulation (QIM); singular value decomposition (SVD); Normalized Mean Squared Error (NMSE); Bit Error Rate (BER)

3. PROPOSED METHOD

This study introduces a steganography method that combines DWT with the ABC algorithm to optimize the Delta parameter in the QIM embedding process. Firstly, experiments used 512 × 512 grayscale images from SIPI dataset [27], followed by another dataset for validation. This section provides a detailed explanation of the proposed method, divided into two main parts, namely the embedding process and the extraction process.

3.1 Embedding process

This section explains the complete proposed embedding workflow used in the proposed method shown in Figure 1. The process begins by loading the cover image and the secret message that has been converted into a binary bit stream. If the image is still in RGB format, it is converted to grayscale to simplify signal processing. Next, a level 1 DWT transformation is performed on the grayscale image. This

transformation breaks the image into different frequencies using low-pass and high-pass filters, which produce the LL, LH, HL, and HH sub-bands. The focus of this algorithm is on the HL (horizontal) and LH (vertical) detail coefficients, which are combined to form the embedding area. The selection of this area is crucial because it guarantees imperceptibility. Once the area is ready, the ABC algorithm begins by randomly initializing the solution population. In this step, the solution is the value of (Δ (Delta)), which is the quantization step parameter that determines how strongly the data is embedded. The algorithm generates several (N_E) initial solutions randomly within a specified range ($\Delta_{min} - \Delta_{max}$) using Eq. (1).

$$\Delta_i \sim U(\Delta_{min}, \Delta_{max}) \text{ for } i = 1, \dots, N_E \quad (1)$$

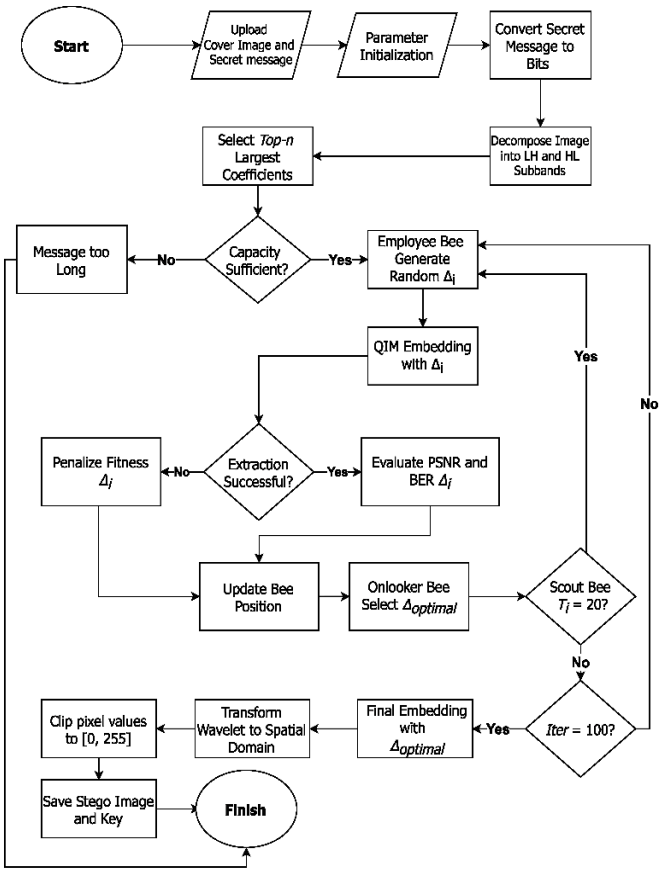


Figure 1. Embedding process workflow

After a set of random (Δ) values is generated, each value must be tested for quality. This test is performed by embedding a message into a temporary image using the (Δ_i) value, with the aim of seeing how well the image's visual quality and data robustness are balanced. Therefore, the next step is to calculate the fitness value (f_i) for each (Δ_i). This evaluation function serves as the primary benchmark for determining whether a (Δ) solution is worth keeping or should be discarded using Eq. (2).

$$f_i = f_{eval}(\Delta_i) \quad (2)$$

In group-based optimization algorithms such as ABC, it is essential to detect if a solution has stagnated (not improved after several attempts). To facilitate this mechanism, a trial counter array named (T_i) is created. In the initial stage, since no improvement or neighbor search process has been performed, all values in this array are set to 0 for each solution (i) using Eq. (3). Later, this value increases each time the solution fails to improve until the limit is reached, at which point the scout bees reset the value to 0 again.

$$T_i = 0, for\ i = 1, \dots, N_E \quad (3)$$

Next, to determine the quality of a solution (Δ), the first parameter measured is imperceptibility, or how invisible the embedded message. This parameter is calculated using PSNR. The higher PSNR more similar the stego image is to the original image. However, for this PSNR value to be combined with other metrics in the objective function, it needs to be normalized using Eq. (4) to normalize the PSNR value (f_{psnr}) that the visual quality target is in the range of 30 dB (poor) to 70 dB (good). If the PSNR is above 70, the value is considered maximum (0), and division by 40 is used to scale the value into the range of 0 to 1.

$$f_{psnr}(\Delta) = \max\left(0, \frac{70 - PSNR}{40}\right) \quad (4)$$

The second important parameter is robustness. A successful steganography system must be able to preserve the secret message even if the image is attacked (such as with noise or compression). This robustness is measured using BER, which is the ratio of bit errors that occur when the message is extracted. A series of experiments was conducted by varying the weights assigned to PSNR and BER across different configurations, and it was observed that unbalanced weighting consistently led to an imbalance increasing the PSNR weight caused the optimizer to sacrifice robustness, resulting in a low BER score, while increasing the BER weight reduced the inaudibility level below the threshold. The selected weights (0.7 for PSNR and 0.3 for BER) represent the configuration that yields the most balanced result between imperceptibility and robustness, which is consistent with the inherent characteristics of the DWT domain where frequency-domain modifications have a relatively stronger perceptual impact than bit-level errors. This BER test is conducted to obtain an accurate evaluation, with the attack simulation being performed repeatedly (N_{trials}). The following uses Eq. (5) to calculate the average BER (f_{ber}) of the original bitstream compared to the bitstream extracted from the attacked stego image.

$$f_{ber}(\Delta) = \frac{1}{N_{trials}} \sum_{t=1}^{N_{trials}} \text{BER}_{trial}(t) \quad (5)$$

After obtaining the normalized values for visual quality (f_{psnr}) and robustness (f_{ber}), the next step is to combine them into a single total fitness value (f_{eval}) using Eq. (6). This combination uses a weighted sum method, where (W_{psnr}) is the weight for PSNR (0.3) and (W_{ber}) is the weight for BER (0.7). This weighting indicates that in this scenario, data resilience (BER) is considered more important than visual quality.

$$f_{eval}(\Delta) = \left(W_{psnr} \cdot f_{psnr}(\Delta)\right) + \left(W_{ber} \cdot f_{ber}(\Delta)\right) \quad (6)$$

In the core iteration of the ABC algorithm, the first phase is called Employed Bee. In this phase, each worker bee attempts to improve the current solution by searching for new food

sources in its vicinity (searching for new deltas from surrounding deltas (Δ_i) using Eq. (7)). This procedure is done by modifying the current value of (Δ_i) using information from the random neighbor solution (Δ_k). The variable (ϕ) is a random number between -1 and 1, which indicates the direction and length of the search step. If this new candidate solution (v_i) has a better fitness value ($f_{eval}(\Delta_i) > f_{eval}(v_i)$), then the old solution is replaced by ($v_i \rightarrow \Delta_i$), and if not, the old solution ($f_{eval}(\Delta_i) < f_{eval}(v_i)$) is kept ($\Delta_i$) (greedy selection).

$$v_i = \Delta_i + \phi(\Delta_i - \Delta_k) \tag{7}$$

After the worker bee phase is complete, information about food source quality is shared with the onlooker bee. Before the observer bee chooses which solution to explore further, the previously calculated fitness value (f_i) must be converted into a non-negative fitness score (S_i) using Eq. (8). This equation ensures that the smaller the error, the greater the fitness score. This is necessary because the probability selection process requires increasingly larger positive values for increasingly better solutions.

$$S_i = \frac{1}{1 + f_i}, \text{where } f_i \geq 0 \tag{8}$$

Based on the calculated fitness score (S_i), the ABC algorithm then determines the probability (P_i) for each solution. This probability establishes the likelihood of the observer bee choosing a solution for further enhancement through roulette wheel selection using Eq. (9). Solutions with higher fitness exhibit a greater probability of being selected. This algorithm imitates the natural behavior of bees, which tend to swarm around food sources that are richer in nectar.

$$P_i = \frac{S_i}{\sum_{j=1}^{N_E} S_j} \tag{9}$$

During the search process, solutions sometimes become stuck in local optima and progress further. Scout bees play a crucial role in this situation, if a solution (Δ_i) does not improve within a specific limit, marked by the counter value (T_i) reaching 20 iterations, then that solution is considered stuck. The scout bee then discards that solution and randomly generates an entirely new solution within the delta range using Eq. (10). This random value generation refreshes the population and maintains solution variety.

$$\Delta_i = \text{random}(\Delta_{min}, \Delta_{max}) \tag{10}$$

Once the maximum number of iterations (100) is reached and all phases (Employed, Onlooker, and Scout) are completed, the algorithm produces a final population of solutions. The process terminates by selecting the best (Δ) value from the global population using Eq. (11). The best value is defined as the value that produces the minimum objective function (f_i) because (f_i) is the fitness that combines BER and PSNR. This value is called ($\Delta_{optimal}$) and is utilized for the final embedding process.

$$\Delta_{optimal} = \arg\min_{\Delta_i}(f_i) \tag{11}$$

After ($\Delta_{optimal}$) is found, this value is used to embed all message bits into the original coefficients (c_i) using the QIM method, resulting in modified coefficients (c_i'). The last step is to restore the image so it can be seen. The modified frequency coefficients are reinserted into the DWT structure, then an Inverse Discrete Wavelet Transform (IDWT) is performed. This inverse process converts the data from the frequency domain back to the spatial domain, generating the final stego image.

3.2 Extraction process

This section describes the complete extraction workflow used in the proposed method shown in Figure 2. The extraction process begins by loading two main components, namely the stego image (an image that has been embedded with a message) and the secret key. At this stage, the stego image appears visually identical to the original image but contains hidden data in its frequency domain. The key plays a crucial role because it includes all the optimal parameters generated by ABC during the embedding process, including information about the DWT decomposition level used, the exact coordinate position of the coefficients, and the specific HL and LH sub-band areas where the data is hidden. Without this key, the receiver cannot find the valid data extraction location.

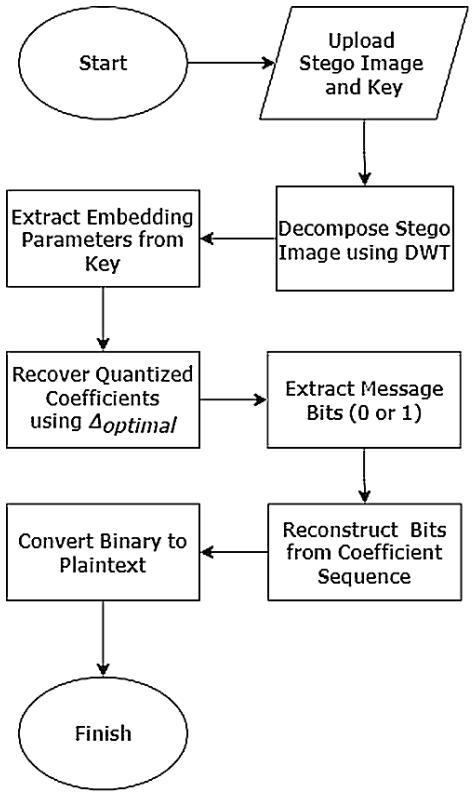


Figure 2. Extraction process workflow

Like the embedding process, the next step is to convert the stego image from the spatial domain back to the frequency domain. The image is changed using the DWT based on the level set in the key. After the transformation is complete, the system uses the index information from the key to map and retrace the embedding area in the one-dimensional array of the HL and LH subbands. The algorithm then isolates specific coefficients in the selected subband that contain message bits, separating the data signal from other coefficients that do not contain secret messages.

After the coefficient location is found, the system reads the

index list (I) from the secret key to process each modified coefficient (c_i'). At this step, extraction is performed using the inverse of QIM. The distance of each coefficient value is analyzed relative to the 0-bit quantization point ($\Delta_{\text{optimal}} \times n$, where $n \in \{0,2,4,6,\ldots\}$) and bit 1 ($\Delta_{\text{optimal}} \times n$, where $n \in \{1,3,5,7,\ldots\}$). The message bits (0 or 1) are determined based on the proximity of the coefficient value to the nearest quantization point. This process ensures that even if there is a bit of distortion in the image, the most possible bit value can still be recovered.

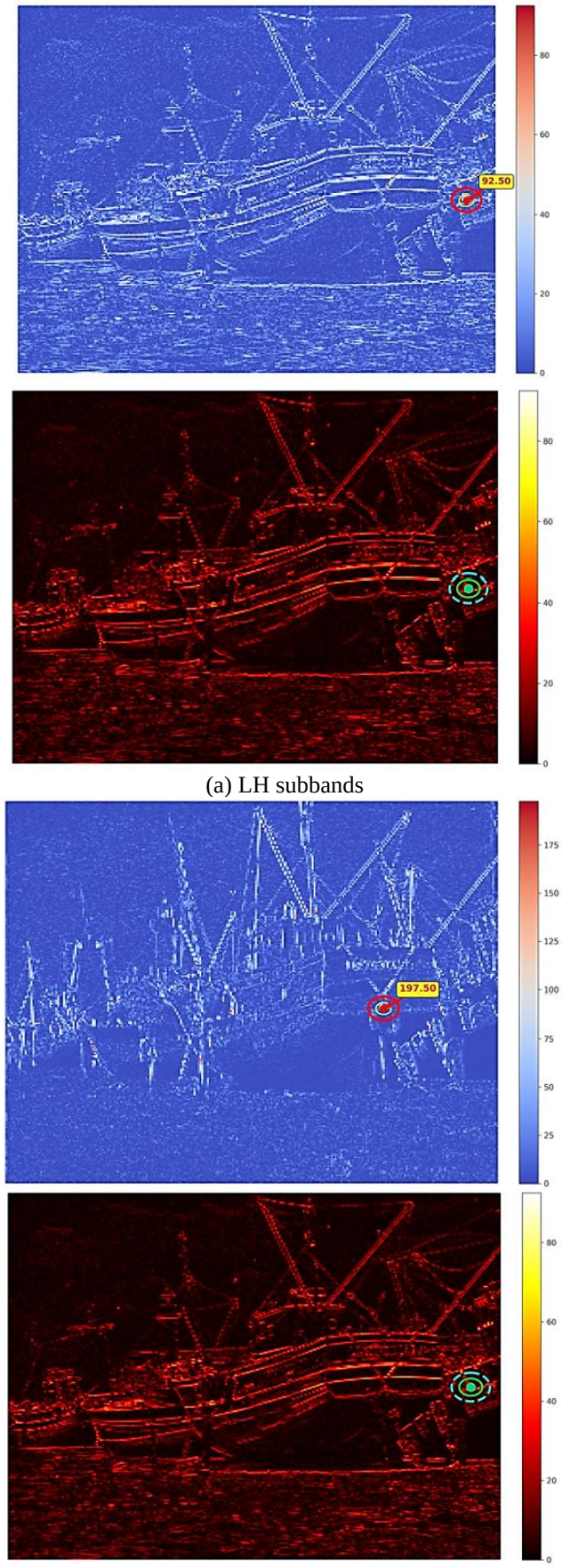
The binary bits successfully extracted from each coefficient are then collected and combined in sequence. This process puts the message's original data structure back together. Each bit taken from the nearest point will then be arranged in length until it reaches the total length of the specified message, forming a complete single-bit stream and restoring the structure of the secret message. The final step is to convert the bitstream to represent the secret message, using the reconstructed bitstream into byte units (8 bits). This collection of bytes is then converted or translated back into plain text format. The result is a secret message that can be read and understood by the receiver.

4. RESULT AND DISCUSSION

This section presents the results of experiments evaluating the performance of the proposed DWT with QIM optimized by ABC using PSNR and BER from various attacks. Figure 3 illustrates the application of DWT using Haar wavelets on a boat cover image, showing the highest coefficient magnitudes in the LH subband (92.50) and HL subband (197.50). These magnitudes represent edges and textures that the QIM embedding method modifies based on an optimized quantizer to determine bit embedding.

The experimental results using SIPI dataset are shown in Tables 2–4, comparing the proposed method with the studies [25, 28, 29, 30], while those of the study [31] are provided in Figure 4. To analyze further, the study [32] is also taken for Table 3. Figure 4 shows the PSNR distribution across 100 test images from the Universal Image Embedding dataset at a 256-bit payload, ranging from approximately 51 dB to over 61 dB with an average of 56.60 dB, confirming that embedding modifications remain imperceptible to the human eye. Table 2 presents PSNR results across different cover images and payload sizes. PSNR decreases as payload increases, consistent with the imperceptibility-capacity trade-off. The Airplane image achieves the highest PSNR (77.80 dB at 64 bits and 74.33 dB at 256 bits), while the Boat image records the lowest among small-payload images (65.00 dB at 64 bits and 61.89 dB at 256 bits). The House and Butterfly images, tested at a fixed 12,288-bit payload, yield PSNR values of 52.78 dB and 56.91 dB respectively, both remaining above the accepted imperceptibility threshold in the steganography literature.

Table 3 compares imperceptibility against Evsutin and Kultaev [25] and Lyu et al. [32]. The proposed method achieves PSNR values of 63.17-69.28 dB for payloads of 64-256 bits, outperforming Evsutin and Kultaev [25] by over 15 dB across the same range. At a 12,288-bit payload, the proposed method still maintains 56.19 dB, exceeding the best result of both comparison methods, confirming the efficiency of ABC-based delta optimization in minimizing embedding distortion.



(a) LH subbands

(b) HL subbands

Figure 3. Magnitude Discrete Wavelet Transform (DWT)

Table 4 presents the robustness in terms of BER against four methods [25, 28, 29, 30]. The proposed method works well under additive noise, with BER of 0.0078 under Gaussian

noise and 0.0156 under Salt and Pepper noise, outperforming all comparison methods except [29] on Gaussian noise. Both the proposed method and [25] achieve a perfect BER of 0 under high quality JPEG compression, indicating that QIM itself is robust to mild lossy compression. However, the proposed method has higher BER in aggressive compression (0.4179), resizing (0.4218), median filtering (0.4257) and average filtering (0.5234).

Table 2. Comparison results from SIPI dataset image

Image	Payload (bits)	PSNR (dB)
Baboon	64	71.03
	128	70.67
	196	70.35
	256	70.09
	12.288	54.27
Pepper	64	69.54
	128	69.19
	196	69.10
	256	68.60
	12.288	54.48
Airplane	64	77.80
	128	76.27
	196	75.17
	256	74.33
	12.288	54.35
Boat	64	69.28
	128	68.32
	196	65.58
	256	63.17
	12.288	54.15
Tank	64	70.00
	128	69.15
	196	68.91
	256	68.07
	12.288	54.26
Moon	64	70.50
	128	70.08
	196	69.63
	256	68.59
	12.288	51.05
House	64	65.00
	128	64.86
	196	64.57
	256	61.89
	12.288	52.78
Butterfly	64	65.46
	128	64.54
	196	62.67
	256	62.00
	12.288	56.19

Table 3. Comparison of imperceptibility results between the proposed and the previous methods

Method	Payload (bits)	PSNR (dB)
Proposed Method	64	69.28
	128	68.32
	196	65.58
	256	63.17
	12.288	56.19
[25]	64	51.10
	128	50.20
	196	49.30
	256	47.70
[32]	1288	51.10

Table 4. Comparison of robustness results from the proposed method and the previous method

BER Attack	Proposed Method	[25]	[28]	[29]	[30]
Gaussian noise (0.005)	0.0078	0.1291	0.0265	0.0035	0.0255
Resizing (0.8)	0.4218	0.1962	0.0733	0.0011	0.2072
Median Filtering (3 × 3)	0.4257	0.1954	0.0866	0.0539	0.1039
Average Filtering (3 × 3)	0.5234	0.2637	0.1071	0.0622	0.1485
JPEG compression (Quality Level = 90-100%)	0	0	-	-	-
JPEG compression (Quality Level = 70%)	0.4179	0.0213	0.1062	0.1294	0.0155
Salt and Pepper (0.01)	0.0156	0.0689	0.0808	0.0711	0.0971

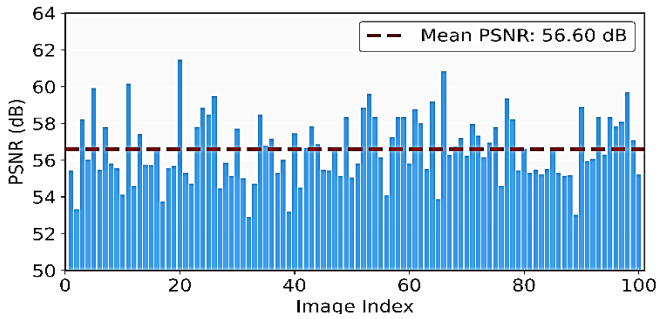


Figure 4. Mean of the PSNR values obtained from 100 of the universal image

To further evaluate the security of the proposed method against modern steganalysis detectors, the stego images were tested with two deep learning-based steganalysis networks, namely SiaStegNet [33] and ZhuNet [34]. SiaStegNet achieved a detection accuracy of 45.02% while ZhuNet achieved 42.64%, which is close to the theoretical baseline of 50% for random guessing. The results show that the proposed method produces stego images that are statistically indistinguishable from clean cover images even under learning-based steganalysis, confirming that the ABC-optimized QIM embedding does not introduce detectable statistical anomalies that modern detectors can exploit.

Results of this study have direct implications on real world security systems. The high PSNR values imply that the proposed method can be used in the systems based on visual inspection without detection. The good BER performance in additive noise confirms that hidden payloads can survive transmission over noisy channels, which is vital in military or government communications. However, the lower robustness to geometric and filtering attacks implies that the technique is better suited for a controlled transmission environment where the image is unlikely to be manipulated in an aggressive way, e.g. in a hospital network or in encrypted cloud storage. The weaknesses indicate that the ABC optimization can adjust the

quantization step to resist noise, but it does not consider the spatial desynchronization caused by geometric transformations and the smoothing effect caused by filtering operations. In addition, the proposed method demonstrated compression resistance using the JPEG standard at two quality levels, exceptionally high quality (90–100%), where both the proposed and baseline methods achieved perfect results (0). However, the proposed method suffers in robustness under resizing, averaging filtering, and median filtering attacks. The irregular performance can be explained by the nature of the QIM mechanism and the DWT embedding domain. Averaging and median filters are low-pass filters that smooth local variations within an image, heavily suppressing or destroying the embedded signals. Moreover, geometric attacks like resizing cause severe desynchronization, as the QIM extraction process must be precisely aligned spatially and in frequency to properly assign the coefficients to the corresponding quantization bins. The pixel interpolation in resizing an image changes the original DWT coefficient values irreversibly, forcing them out of their optimal quantization ranges, resulting in a high BER. On the other hand, the method is robust to additive noise (Gaussian and Salt & Pepper) because the ABC algorithm can optimize the QIM quantization step size, thus providing a sufficient tolerance margin that absorbs the random amplitude variations, as long as the spatial structure of the image is perfectly aligned.

5. CONCLUSION

The proposed method proposes a steganography method based on DWT with QIM whose delta parameter is optimized by ABC algorithm. The method achieves higher PSNR values and robustness against additive noise attacks, maintaining low BER under Gaussian noise in several cover images. The proposed approach results in the stego image with better visual quality and less distortion as compared with existing methods. Additionally, the steganalysis evaluation with SiaStegNet and ZhuNet attained the detection accuracy of 45.02% and 42.64% respectively, which is close to the random guessing baseline, confirming the resistance of the method to modern learning-based steganalysis.

However, the method is sensitive to geometric and structural attacks with BER values higher than 0.42 for the resizing, median filtering and average filtering conditions, which indicates that spatial transformations and frequency-smoothing operations are still a challenge for the current QIM-ABC scheme. Future work should address these limitations by exploring geometric correction mechanisms, expanding the embedding to the LL and HH subbands, and exploring different delta parameters for each bit to further improve the imperceptibility-robustness trade-off.

ACKNOWLEDGMENT

This research is funded by Institut Teknologi Sepuluh Nopember (ITS) and managed under the Beasiswa Unggulan (BU) Scheme, (Contract No. 486/PKS/ITS/2026).

The authors express their sincere gratitude to all members of the Cyber Security Research Group, Net-Centric Computing (NCC) Laboratory, Department of Informatics, ITS, for their continuous support and insightful discussions.

REFERENCES

[1] Quach, S., Thaichon, P., Martin, K.D., Weaven, S., Palmatier, R.W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50: 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

[2] Windarta, S., Suryadi, S., Ramli, K., Pranggono, B., Gunawan, T.S. (2022). Lightweight cryptographic hash functions: Design trends, comparative Study, and future directions. IEEE Access, 10: 82272–82294. https://doi.org/10.1109/ACCESS.2022.3195572

[3] Azam, M.H.N., Ridzuan, F., Sayuti, M.N.S.M., Azni, A.H., Zakaria, N.H., Potdar, V. (2025). A systematic review on cover selection methods for steganography: Trend analysis, novel classification and analysis of the elements. Computer Science Review, 56: 100726. https://doi.org/10.1016/j.cosrev.2025.100726

[4] Zhang, X., Chen, K.J., Zhao, N., Zhang, W.M., Yu, N. (2025). Provably secure public-key steganography based on admissible encoding. IEEE Transactions on Information Forensics and Security, 20: 3161–3175. https://doi.org/10.1109/TIFS.2025.3550076

[5] Muralidharan, T., Cohen, A., Cohen, A., Nissim, N. (2022). The infinite race between steganography and steganalysis in images. Signal Processing, 201: 108711. https://doi.org/10.1016/j.sigpro.2022.108711

[6] Albkosh, F.M.A., Mohamed, A.S.S., Albakoush, A.A., Albkush, A.A. (2024). An enhanced method to secure the high embedding capacity steganography based on LSB indicator. In 2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Tripoli, Libya, pp. 494–499. https://doi.org/10.1109/MI-STA61267.2024.10599765

[7] Jasim, Z.K.J., Kurnaz, S. (2024). An improved image steganography security and capacity using ant colony algorithm optimization. Computers, Materials & Continua, 80(3): 4643-4662. https://doi.org/10.32604/cmc.2024.055195

[8] Duan, D.L., Shen, S.Y., Yu, S.S., Yuan, Y.B., Zhou, Q.D. (2024). Robust image steganography model based on discrete-dual-tree complex wavelet transform and invertible neural network. In 2024 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, pp. 272–279. https://doi.org/10.1109/IPEC61310.2024.00054

[9] Khandelwal, J., Sharma, V.K., Singh, D., Zaguia, A. (2022). DWT-SVD based image steganography using threshold value encryption method. Computers, Materials & Continua, 72(2): 3299–3312. https://doi.org/10.32604/cmc.2022.023116

[10] Gurumurthy, S.B., Danti, A. (2022). Image steganography using discrete wavelet transform and convolutional neural network. In 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, pp. 862–868. https://doi.org/10.1109/IIHC55949.2022.10060110

[11] Makansi, O., Çiçek, Ö., Marrakchi, Y., Brox, T. (2021). On exposing the challenging long tail in future prediction of traffic actors. In 2021 IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, QC, Canada, pp. 13147–13157. https://doi.org/10.1109/ICCV48922.2021.01290

[12] Durafe, A., Patidar, V. (2022). Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover. Journal of King Saud University-Computer and Information Sciences, 34(7): 4483–4498. https://doi.org/10.1016/j.jksuci.2020.10.008

[13] Melman, A., Evsutin, O. (2025). Hybrid domain based data embedding using quantization index modulation and metaheuristic optimization. Knowledge-Based Systems, 329: 114429. https://doi.org/10.1016/j.knosys.2025.114429

[14] Liu, J., Song, X.F., Li, G.P., Han, K. (2023). Robust JPEG image steganography using wavelet domain SVD and adaptive QIM. In 2023 8th International Conference on Signal and Image Processing (ICSIP), Wuxi, China, pp. 434–438. https://doi.org/10.1109/ICSIP57908.2023.10270839

[15] Bsoul, A.A.R., Ismail, A.B. (2025). Optimizing image watermarking with dual-tree complex wavelet transform and particle swarm intelligence for secure and high-quality protection. Applied Sciences, 15(3): 1315. https://doi.org/10.3390/app15031315

[16] Banharnsakun, A. (2018). Artificial bee colony approach for enhancing LSB based image steganography. Multimedia Tools and Applications, 77: 27491–27504. https://doi.org/10.1007/s11042-018-5933-5

[17] Bhandari, M., Panday, S., Bhatta, C.P., Panday, S.P. (2022). Image steganography approach based ant colony optimization with triangular chaotic map. In 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India, pp. 429–434. https://doi.org/10.1109/ICIPTM54933.2022.9753917

[18] Kaur, A., Kaur, R., Kumar, N. (2015). Image steganography using discrete wavelet transformation and artificial bee colony optimization. In 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, pp. 990–994. https://doi.org/10.1109/NGCT.2015.7375269

[19] Abdulazeez, A.M., Hajy, D.M., Zeebaree, D.Q., Zebari, D.A. (2021). Robust watermarking scheme based LWT and SVD using artificial bee colony optimization. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 21(2): 1218–1229. https://doi.org/10.11591/ijeecs.v21.i2.pp1218-1229

[20] Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., Gupta, B. (2017). Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimedia Tools and Applications, 76: 18451–18472. https://doi.org/10.1007/s11042-016-3930-0

[21] Vyas, A.O., Dudul, S.V. (2019). Hybrid DWT-DCT image steganography for encrypted secret image. In 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), Nagercoil, India, pp. 1–7. https://doi.org/10.1109/ICRAECC43874.2019.8995111

[22] Navyamol, K.T., Jose, R.T. (2025). Enhancing DeepFace algorithm performance for emotion detection: An adaptive vision preprocessing approach using FER-2013 dataset. Signal, Image Video Process, 19: 11020. https://doi.org/10.1007/s11760-025-04676-6

[23] Babu, A.R., Al-Fatlawy, R.R., Veeranjaneyulu, K., G, D., Kumar, K.S. (2024). Canonical Huffman Coding (CHC)-Discrete Wavelet Transform (DWT) method for image steganography. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, pp. 1–4. https://doi.org/10.1109/ICICACS60521.2024.10498392

[24] Rekha, K.S., Joe, M., Swathy, M., Raghini, M., Darshini, B.P. (2023). A steganography embedding method based on CDF-DWT technique for data hiding application using Elgamal algorithm. Biomedical Signal Processing and Control, 80(1): 104212. https://doi.org/10.1016/j.bspc.2022.104212

[25] Evsutin, O., Kultaev, P. (2021). An algorithm for embedding information in digital images based on discrete wavelet transform and learning automata. Multimedia Tools and Applications, 80(7): 11217–11238. https://doi.org/10.1007/s11042-020-10316-7

[26] Luo, W.Q., Wei, K.K., Li, Q.S., Ye, M.X., Tan, S.Q., Tang, W.X., Huang, J.W. (2024). A comprehensive survey of digital image steganography and steganalysis. APSIPA Transactions on Signal and Information Processing, 13(1): 1–67. https://doi.org/10.1561/116.20240038

[27] The USC-SIPI image database. (2025) Signal and Image Processing Institute. http://sipi.usc.edu/database/.

[28] Priyanka, Maheshkar, S. (2017). Region-based hybrid medical image watermarking for secure telemedicine applications. Multimedia Tools and Applications, 76: 3617–3647. https://doi.org/10.1007/s11042-016-3913-1

[29] Thabit, R., Khoo, B.E. (2017). Medical image authentication using SLT and IWT schemes. Multimedia Tools and Applications, 76: 309–332. https://doi.org/10.1007/s11042-015-3055-x

[30] Lei, B.Y., Tan, E. L., Chen, S.P., Ni, D., Wang, T.F., Lei, H.J. (2014). Reversible watermarking scheme for medical image based on differential evolution. Expert Systems with Applications, 41(7): 3178–3188. https://doi.org/10.1016/j.eswa.2013.11.019

[31] Singh, R. (2022). 130k images (512x512)-Universal image embeddings. Kaggle. https://www.kaggle.com/datasets/rhtsingh/130k-images-512x512-universal-image-embeddings.

[32] Lyu, S., Xu, X.Q., Liu, L., Por, L.Y. (2025). Secure steganography based on chaos-aided quantization index modulation. In Proceedings of the 20th ACM Asia Conference on Computer and Communications Security (ASIA CCS '25). Association for Computing Machinery, New York, NY, USA, pp. 727–738. https://doi.org/10.1145/3708821.3736215

[33] You, W.K., Zhang, H., Zhao, X.F. (2021). A siamese CNN for image steganalysis. IEEE Transactions on Information Forensics and Security, 16: 291–306. https://doi.org/10.1109/TIFS.2020.3013204

[34] Zhang, R., Zhu, F., Liu, J.Y., Liu, G.S. (2020). Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis. IEEE Transactions on Information Forensics and Security, 15: 1138–1150. https://doi.org/10.1109/TIFS.2019.2936913