JPEG-Resistant DCT Steganography for Secure Communication

Israa Abdulkadhim Jabbar Al Ali[1], Zainab A. Abdulazeez[1,*], Rawaa.M.aljubouri[2]
[1]College of Education for Human Sciences, University of Kerbala, Karbala City, Iraq
[2]Presidency of University of Babylon, University of Babylon, Babylon, Iraq
Emails: israa.jabbar@uokerbala.edu.iq; zainab.abdulhameed@uokerbala.edu.iq; rawa.aljubouri18@uobabylon.edu.iq

Abstract

In this work, the researchers presented an ingenious new way to conceal secret messages within images, a practice called steganography. This technique embedded secret messages within images undetectably. To embed the secret data, it applies a mathematical trick called Discrete Cosine Transform (DCT) that is commonly used to compress image files to hide the secret data in areas of the image that are not too complex or too simple. The algorithm adaptively selected embedding locations based on image texture to the appearance of the image, choosing the most appropriate places to hide the secret and the picture to appear normal. This new method of hiding data is more magical and less detectable than older methods, which modify the smallest details of an image (so-called Least Significant Bit techniques). It examines the patterns of the image such as whether it is smooth or has many details and selects obscure, secure locations to conceal the message. They tried this with 1,000 images, and in each image, they embedded a small message (a paragraph of text). The pictures came out great afterwards with just minor adjustments that most people would not have noticed. 95% of the buried messages could be dragged out flawlessly even after the images had been reduced in size with the JPEG. An artificial intelligence-based high-tech detection tool only detected the hidden data half the time 52%, a significant improvement over the older techniques where it located 85 percent or 65% of the secrets.

Keywords: Steganography; Discrete Cosine Transform; Mid-Frequency Embedding; Texture-Adaptive Algorithm; JPEG Robustness; Steganalysis Resistance; Secure Communication

1. Introduction

In the digital era, securing confidential communication across network infrastructures was paramount. While cryptography encrypts messages, it does not conceal their existence, leaving them vulnerable to interception and cryptanalysis [1], [2]. Steganography addressed this by embedding secret data within innocuous digital media, rendered communication undetectable [3]. Nonetheless, the disadvantages of traditional steganographic schemes, e.g. LSB embedding, are quite severe: they are vulnerable to statistical detection, and are not robust to JPEG compression [4], [5]. Embedding in LSB also has the disadvantages of poor payload, possible degradation of image quality and transmission difficulties which were highlighted in a comparative studying of LSB embedding methods [6]. Such restrictions prevent their applicability in sensitive-security environments and more methods that are sophisticated are required.

Frequency-domain methods, particularly Discrete Cosine Transform (DCT)-based steganography, offer enhanced security by embedding data in frequency coefficients [7]. Prior DCT approaches, such as high-frequency [8] or low-frequency [9] embedding, compromise either robustness or imperceptibility due to compression artifacts or visual distortions. Recent machine learning-based steganography methods, leveraging CNNs or GANs [10], [11], dynamically select embedding locations but require extensive training data and computational resources, hindering real-time applications [12].

This study proposed a novel texture-adaptive mid-frequency DCT steganography method that overcame these limitations. The method employs a deterministic algorithm to select mid-frequency coefficients based on image

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

texture variance and energy distribution, ensuring high imperceptibility (PSNR: 38.12–41.75 dB, SSIM: 0.95–0.97) and steganalysis resistance (52% detection rate) without the computational overhead of machine learning [10]. Unlike static DCT methods [7], [8], the texture-adaptive approach optimizes embedding for each image, achieving 95% JPEG robustness (Table 3). This method outperforms LSB [3] and DWT-based techniques, offering a lightweight, interpretable solution for secure military, legal, and business communications [11].

1.1 Comparison of Related Works

The subsequent comparison contrasts the most important steganographic methods, LSB embedding, DWT-based steganography and several DCT-based schemes, with important measures: imperceptibility (PSNR and SSIM), resistance to JPEG compression (data recovery rate) and steganalysis (detection rate by contemporary tools). This comparison shows the drawbacks of current methods and forms a background to the suggested one.

1.1.1 Least Significant Bit (LSB) Embedding

- Description: LSB embedding altered the least significant bits of pixel values to conceal data, and was valued because of its simplicity and minimal computing expense.
- Shortcomings:
- imperceptibility: Obtains low PSNR (25.5028.30 dB) and SSIM (0.850.89), which causes visible distortions [3].
- Robustness: JPEG compression removes 10% of data because it is a spatial-domain e [13].
- Security: It is highly susceptible, and CNN-based steganalysis detects it with 85 percent accuracy [4].
- Limitation: LSB trades its simplicity with lack of security and lack of robustness and cannot be used in secure and modern applications.

1.1.2 DWT-Based Steganography

- Description: Discrete Wavelet Transform (DWT): A DWT approach incurs the data into the wavelet coefficients, making use of localization in frequency domain, resulting in a better performance compared to spatial approaches.
- Shortcomings:
- Imperceptibility: medium PSNR (32.15 35.60 dB) and SSIM (0.88 0.91) [14].
- Robustness: Only 60 percent data can be recovered after JPEG compression because the high-frequency sub-bands are dropped [15].
- Security: 70 percent detection accuracy with powerful steganalysis and therefore moderate security [15].
- Limitation Although superior to LSB, the greater computing complexity and poor robustness limit the practicality of DWT.

1.1.3 High-frequency DCT Embedding (Emmanuel)

- Description: In this scheme data is incorporated in high frequency DCT coefficients to maintain the quality of visual image.
- Shortcomings:
- Undetectability: A decent setting of PSNR (34.5037.80 dB) and SSIM (0.890.92) [8].
- Robustness: Poor JPEG robustness (30% recovery); high-frequency coefficients are not kept during compression, as they do not change much with image quality (high frequencies perceptually known as noise).
- Security: Medium defense (65 percent strength) to steganalysis.
- Weakness: It is susceptible to compression which limits its applicability in real life condition.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

1.1.4 DCT Embedding low-Frequency (El Rahman)

- Description: The method addresses the low-frequency DCT coefficients in order to ensure robustness.
- Shortcomings:
- Imperceptibility: PSNR(28.90- 31.20 dB), SSIM (0.85- 0.88) low and made visible artifacts [9].
- Robustness: improved JPEG robustness (70 percent recovery) with a trade off to image quality.
- Security: A close detection rate of steganalysis (65%) as compared to high-frequency detection.
- Limitation: The performance parameter is so strongly inclined on the side of robustness versus imperceptibility, that it becomes not very useful.

1.1.5 Steganography that implements Machine Learning (Bohra & Soni, 2024; Sanjalawe et al., 2022)

- Description: These techniques use CNNs or GANs to choose embedding locations in an adaptive way and hope to perform best.
- Shortcomings:
- Imperceptibility: Not measurable because PSNR and SSIM are high and variable [10], [11].
- Robustness: Non-uniform JPEG robustness according to model design.
- Security: Better immunity against steganalysis, need of large computational resources.

Disadvantage: These methods are computationally expensive and require vast amount of data, thus are not suitable lightweight applications..

2. Problem Definition and Related Works

2.1 Problem Definition

Steganography hid data in digital media, enabled covert communication. The encryption techniques protect message contents while leaving the detection of communication possible thanks to the detectable encryption presence. Basic implementation makes the Least Significant Bit (LSB) embedding method the main traditional tool in stenographic approaches. Standard steganographic methods experience two major shortcomings due to weak compression resistance and the capability of statistical evaluation and visual indications for hidden data detection. To take a specific example, LSB techniques reach PSNR = 51 dB and SSIM = 0.99, but are time-consuming (22-71 s), are not at all resistant to domain-other than spatial compression and are still, at that, easily detectable by a steganalysis software [6].
The proposed research implemented a steganographic technique using DCT which operated in the frequency domain rather than modifying pixel values. During embedding operations secret data goes into mid-frequency DCT coefficients to create a scheme which improves security together with visual quality and resistance to attacks [2].

2.2 Drawbacks of Conventional Steganographic Techniques

2.2.1 Least Significant Bit (LSB) Embedding

Secret data embedment using LSB-based approaches alters specific bits from least significant pixel values. The technique proves valid since it requires low processing power and supports big data insertion capacity [3].

2.2.1.1 Drawbacks of LSB embedding:

- The statistical deviations created by LSB modification allow detection systems to perform histogram analysis and RS steganalysis combined with chi-square tests.
- LSB methods operate in spatial image domains thus making them vulnerable to compression since JPEG processing removes high-frequency data containing hidden information [13].
- The combination of image resizing operations with basic rotations along with the addition of noise makes hidden data highly susceptible to degradation.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

- LSB-based steganography keeps insufficient security levels because detection tools recognize this method thus making it ineffective for protected information requirements [4].

2.2.1.2 How the Proposed Method Solves These Issues:

- DCT embedding operates through changes to frequency coefficients in order to produce undetectable statistical modifications.
- JPEG compression along with cropping and resizing operations did not compromise the security of information concealed utilizing the new method.

2.2.2 Steganography Depends on Discrete Wavelet Transform (DWT)

DWT-based methods divide images into two areas that include low-frequency and high-frequency sub-band components before they embed secret data within the high-frequency components [14].

2.2.2.1 Drawbacks of DWT steganography:

- The process of implementing DWT requires more computational resources than both LSB and DCT [15].
- The compression approach for high-frequency sub-bands contributes to data loss through Lossy Embedding during the process.

2.2.2.2 How the Proposed Method Solves These Issues:

- Information stored through the DCT system remains less detectable because it is placed in medium-frequency image sections yet remains invulnerable to detected breaches [16].
- Because of its high computational power and JPEG integration DCT emerges superior to DWT as an image compression method.

2.2.3 Spatial Domain vs. Frequency Domain Steganography

Routine methods operate in the spatial domain through direct modifications of pixel values whereas DCT and frequency domain approaches modify transformed frequency coefficients of images [7].

Table 1: Performance Across Different Texture Levels

Texture Level	**Number of Images**	**Avg. PSNR (dB)**	**Avg. SSIM**
Low Texture	320	40.8	0.965
Medium Texture	420	40.2	0.962
High Texture	260	39.6	0.958

The proposed technique delivers superior performance because it integrates DCT analysis with mid-frequency embedding methods, which provide excellent security and undetectable quality.

- By uniting DCT with mid-frequency embedding users, gain both high resistances to attacks and excellent distortion independence.
- DCT-based embedding acts as a successful steganography method because statistical steganalysis cannot identify its presence.
- The proposed method operates as a JPEG-friendly system compatible for practical usage.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

2.3 Contributions of This Work

The study introduces an upgraded DCT-based steganographic system which produces the following outcome:

- Higher imperceptibility (PSNR: 30.41 dB – 33.25 dB, SSIM: 0.92 – 0.94)
- Improved security against steganalysis
- Compression resistance (JPEG, resizing, cropping)
- The proposed method maintains a satisfactory relationship between system reliability and data

2.3.1 Limitations of Prior DCT-Based Methods

DCT-based steganography embeds data in frequency coefficients, offering advantages over spatial-domain methods like LSB [3], [4], [17]. However, prior DCT approaches often underperform due to static coefficient selection. Emmanuel [8] embed data in high-frequency coefficients, achieving reasonable imperceptibility (PSNR: 34.50–37.80 dB, SSIM: 0.89–0.92) but poor robustness against JPEG compression (30% recovery, Table 3). High-frequency coefficients are prone to loss during compression, as JPEG quantization discards these components, leading to data degradation. Conversely, El Rahman [9] targets low-frequency coefficients, improving JPEG robustness (70%) but compromising visual quality (PSNR: 28.90–31.20 dB, SSIM: 0.85–0.88) due to noticeable distortions in perceptually significant image regions. Both methods lack adaptability, selecting coefficients without considering image content, resulting in suboptimal trade-offs between imperceptibility, robustness, and security (65% detection rate, Table 3). The proposed texture-adaptive method overcomes these limitations by dynamically selecting mid-frequency coefficients based on texture variance and energy distribution (Section 15), achieving superior metrics (PSNR: 38.12–41.75 dB, SSIM: 0.95–0.97, 95% JPEG robustness, 52% detection rate).

2.3.2 Machine Learning Trends in Steganography

Recent steganography research increasingly leverages machine learning to enhance embedding strategies. In Abdulazeez et al. classical supervised classifiers, such as Random Forest and SVM, have also been found to be exceptionally efficient in deriving high-resolution texture information out of images (up to and including plant disease classification assignments) [18]. Bohra [10] integrate DCT with CNNs to predict optimal embedding locations, improving security against steganalysis but requiring extensive training data (e.g., BOSSBase 1.01) and computational resources. Sanjalawe [11] propose a two-layer encoding scheme using neural networks to maximize data capacity, achieving high imperceptibility but at the cost of complex model training and potential overfitting to specific image types. Generative Adversarial Networks (GANs) have also gained traction, generating stego images that mimic cover image statistics [10], yet they demand significant computational power and may produce unpredictable artifacts, limiting real-time applicability [19]. These methods excel in adaptability but lack the interpretability and efficiency of rule-based approaches. The proposed method, by contrast, uses a deterministic texture-adaptive algorithm (Section 15), requiring no training data and offering computational efficiency (7.8–58.2 seconds, Table 2) and generalizability across diverse images (USC-SIPI dataset). While machine learning methods may outperform in specific scenarios with large datasets, their complexity hinders deployment in resource-constrained environments like military or e-governance systems (Section 10).

2.3.3 Broader Steganography Context

Other notable works include Hamidi et al. [20], who evaluated data hiding for tamper-proofing and copyright protection, and Kombrink [21], who use wavelet decomposition for statistical embedding. Moreover, the Random Forest and SVM supervised learning approaches had been used on similar images-analysis tasks such as disease recognition in crop photographs Abdulazeez et al. [18], indicating the overall feasibility of these cultures in identifying minor patterns. Bernard [22] focus on detecting LSB embedding, while Westfeld [23] analyzed steganalysis attacks. These studies highlight the evolving landscape of steganography, where the proposed method's balance of simplicity, robustness, and security positions it as a practical alternative to both traditional and machine learning-based approaches.

3. Practical Applications of DCT

A new DCT steganography system maintains strong imperfection levels (PSNR: 38.12–41.75 dB, SSIM: 0.95–0.97) at the same time as it provides resistance to detection (52% detection rate) to enable secure data encryption in multiple domains. Image data from drones receives tactical information like coordinates through this method to maintain covert communications despite JPEG file damage at 95% capacity. The system protects e-governance voting security through voter ID integration within JPEG image logos which enables free election results monitoring while remaining undetectable at low levels. The process of digital watermarking integrates copyright metadata into media images which maintains quality and protects copyright metadata against scaling operations

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

thus safeguarding intellectual property. Corporate letterheads containing sensitive data such as contracts permit confidential exchange between businesses while meeting privacy requirements. Military operations along with governmental functions and media organizations and corporate entities utilize the method because it provides data protection which remains invisible

4. DCT (Discrete Cosine Transform)

The Discrete Cosine Transform (DCT) converted time-domain signals into frequency components for audio and visual data processing. The signaling process becomes possible after using this transformation method [24].

The DCT technique finds applications in the technical realm to minimize JPEG and MPEG files while dividing visual content into individual sections for separate processing. Through this approach the tone components of each block are presented. Low high-frequency tones with fast speed patterns contribute minimal value to the complete visual representation [25].

The DCT number values get modified during JPEG space-saving operations to reduce their bit length requirements. Cutting the file size through compression tends to reveal defects that will be noticeable in the final version. The reduction of image defects is achievable through chroma subsampling which lowers color detail and entropy coding which uses short codes for frequent color values [26].

DCT provides exceptional performance when compressing image data while keeping maintenance of visual quality. Sometimes the strengths of DCT compression get overshadowed by defects which appear as block shapes or visual distortions during intensive compression leading viewers to doubt the quality of the image [27].

4.1 Comparison of DCT with Other Methods

The dataset carries out Discrete Cosine Transform (DCT) steganography analysis and tests against conventional steganographic techniques. While most of the studies in the dataset focus on DCT's individual application, a few studies hint at the comparative advantages of DCT over alternative steganographic techniques, particularly in terms of compression efficiency and robustness against attacks [28].

The frequency domain processing of DCT through coefficient modification protects embedded data so effectively that it withstands image manipulations like cropping and resizing better than spatial LSB techniques fulfil. DCT demonstrates natural robustness properties that make it suitable for multimedia application use [29].

The research by A. A. Attaby indicated Digital Covariance Transform delivers exceptional image quality before inserting substantial data content. Visual fidelity remains stable at considerable data embedding rates which the authors recognize as its most important advantage [30].

The foundation of DCT in JPEG compression provides an easy integration with compressed image formats that avoids complicated processing requirements. System processing efficiency evaluates as more significant than Discrete Wavelet Transform (DWT) since it necessitates excessive computation [8].

The research conducted by Emmanuel [8] showed that steganographic security using DCT depends on JPEG compression techniques while maintaining minimal image artifact creation.

Security threats in modern times impair DCT applications despite their operation for longevity enhancement. Researchers need to develop adaptive algorithms that will defeat frequency coefficient statistical analyses which exploit their security vulnerability to uncover hidden messages.

The integration of DCT with machine learning systems creates a fundamental requirement which defeats contemporary steganalysis systems [10].

Although there are the benefits, DCT-based steganography faces practical challenges, particularly in the high-resolution images. The transform and embedding of DCT require larger matrices when the image size is large and so the computational complexity is considerably high. As an example, when data is embedded in a 20482048 image, there will be DCT operations over many 88 blocks and therefore the higher the processing time e.g. 58.2 seconds on 20401224 image as seen in Table 2. This may present difficulties to real-time applications, especially in resource-limited contexts, e.g. mobile devices or embedded systems. Moreover, the images with high resolution may have complex textures and details, demanding more delicate changes in embedding strength, in order to prevent artifacts that can be detected, contributing to computational load. These shortcomings are reasons why an optimised DCT implementation or parallel processing strategies are needed to make DCT more viable in large-scale or high-resolution media.

Large digital file compression at low resolutions produces visible distortions throughout the image. The practice of information insertion within less important visual regions produces a solution for this issue [31].

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

The mid-frequency coefficient embedding technique maintains transparency along with effective resistance to detection within DCT-based systems [9].

4.2 The DCT Procedure

Digital images and video frames undergo processing through frequency-domain components as a result of the Discrete Cosine Transform (DCT) which converts time-domain signals. This technique finds extensive usage in JPEG and MPEG compression systems. The proposed steganographic method receives explanation through detailed descriptions of its embedding and extraction procedures.

Digital images and video frames consisting of blocks represent the typical input data in image and video compression processes. The visual data divides into blocks of fixed size 8x8 units or 16x16 units on screen display.

The DC value represents the block pixel average thus it needs to be subtracted: The DC value merely serves as an average of corresponding block pixels. The DC value serves to subtract all pixel values in a block which results in their conversion to zero.

The DCT operation produces frequency coefficients from pixel blocks through uniform calculation across the entire block area. Each block coefficient specifies the amount of frequency content within its corresponding block sections.

The procedure calls for dividing every coefficient by a quantization factor during quantization operations. The coefficient accuracy gets steered while compression artifacts develop through this process.

Entropy serves as the data encoding system because it uses the quantified coefficients as its last component. Huffman or arithmetic coding serves as the compression method for lossless techniques. The process replaces long codes linked to scarce numerical values with shorter code versions that lead to significant reductions in memory storage needs.

The narrowed data will either be stored in the storage system or transmitted to the recipient.

Users can generate the remaining blocks of the image through the application of inverse DCT to compressed data. The inverse DCT receives quantized coefficients together with the original DC value from which block images are formed at the inputs.

The approximation of original coefficients requires dividing quantized coefficients with the exact quantization factor used by the encoder.

The image reconstruction occurs through combining the blocks of pixels to create an original image or video frame. Secondary to the loose compression process there appear compression artifacts in the reconstructed image which manifest as blocking and ringing effects.

4.3 The DCT equation

The DCT equation Eq. (1) computes the i.jth entry of the DCT of an image:

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) cos\left[\frac{(2x+1)i\pi}{2N}\right] cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (1)$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} & if\ u = 0 \\ 1 & if\ u > 0 \end{cases} \quad (2)$$

P (x, y) is the x, yth element of the image represented by the matrix P. N is the size of the block that the DCT is done on. The equation calculates one entry (i, jth) of the transformed image from the pixel values of the original image matrix. For the standard 8×8 block that JPEG compression uses, N equals 8 and x and y range from 0 to 7. Therefore D (i, j) would be as in Eq. (2) [32].

$$D(i,j) = \frac{1}{4} C(i)C(j) \sum_{x=0}^{7} \sum_{y=0}^{7} p(x,y) cos\left[\frac{(2x+1)i\pi}{16}\right] cos\left[\frac{(2y+1)j\pi}{16}\right] \quad (3)$$

Because the DCT uses cosine functions, the resulting matrix depends on the horizontal, diagonal, and vertical frequencies. Therefore, an image of black with a lot of change in frequency has a very random-looking resulting

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

matrix. However, an image matrix of just one color has a resulting matrix with a large value for the first element and zeroes for the other elements Eq (3).

4.4 Texture Variance and Energy Threshold Formulation

The proposed texture-adaptive DCT steganography method relies on two key components: the texture variance metric (VAR) to identify moderately textured blocks and the 20%–60% energy threshold to select mid-frequency coefficients for embedding. These formulations ensure robust and imperceptible data hiding.

4.4.1 Texture Variance Metric (VAR)

The VAR metric quantifies texture complexity within an 8×8-pixel block to select areas suitable for embedding. For a block with pixel intensities I (x, y), where (x, y = 0, 1, …., 7), the variance is calculated as:

$$VAR = \frac{1}{64}\sum_{x=0}^{7}\sum_{y-0}^{7}(I(x,y)-\mu)^2 \qquad (4)$$

Where, $\mu = \frac{1}{64}\sum_{x=0}^{7}\sum_{y=0}^{7} I(x,y)$ is the mean intensity. Blocks with moderate VAR values (e.g., within empirically determined thresholds) are selected to balance imperceptibility and robustness, avoiding overly smooth or highly textured areas.

4.2.1 Energy Threshold for Mid-Frequency Coefficients

Mid-frequency DCT coefficients are chosen based on their energy contribution to the block. After applying DCT to an 8×8 block, yielding coefficients D (i, j), the energy of a coefficient is: E $(\mathrm{i},\mathrm{j}) = \mathrm{D}(\mathrm{i},\mathrm{j})^2$. The total block energy is:

$$E_{total} = \sum_{x=0}^{7}\sum_{y-0}^{7} D(i,j)^2 \qquad (5)$$

The relative energy of a coefficient is: $R_{(i,j)} = \frac{D(i,j)^2}{E_{total}}$

Coefficients with $0.2 \leq R\,(i, j) \leq 0.6$ are selected as mid-frequency, ensuring robustness against JPEG compression while minimizing visual distortion. These coefficients are modulated to embed the secret message, with embedding strength adjusted based on VAR to optimize stego image quality.

4.5 DCT Embedding Algorithm Procedure

- Loaded cover image and checked its texture through VAR metric for the finding areas with a moderately complexity.
- Decode secret message to binary string.
- Only 8x8 pixel cell breakup of the image.
- Subtract 128 from each pixel value in a block size scan (to the left, from the top).
- make DCT of each block of that image which converts an image into Grid of Frequency Co-efficient
- Adaptive selection of middle frequency coefficient according to texture variance, detect the coefficient whose energy is between 20% to 60% in total block energy.
- Secretly encrypt the file that holds the message as follows: Equally modulate the least significant bits of determined coefficients. Change the amount of embedding strength (e.g., variations of ±1 or ±2) in order to get the minimum amount of distortion whilst recovering.
- Inverse DCT reconstructed to get stego image.

4.6 DCT Extraction Algorithm

- Load the stego image.
- Divide the image into 8×8-pixel blocks.
- Subtract 128 from each pixel value in a block-wise scan (left-to-right, top-to-bottom).
- Apply DCT to each block to obtain frequency coefficients.
- Identify the modulated mid-frequency coefficients using the same texture-adaptive selection criteria.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

- Extract the embedded data by retrieving the least significant bits from these coefficients.
- Convert the extracted binary string into the original message characters.

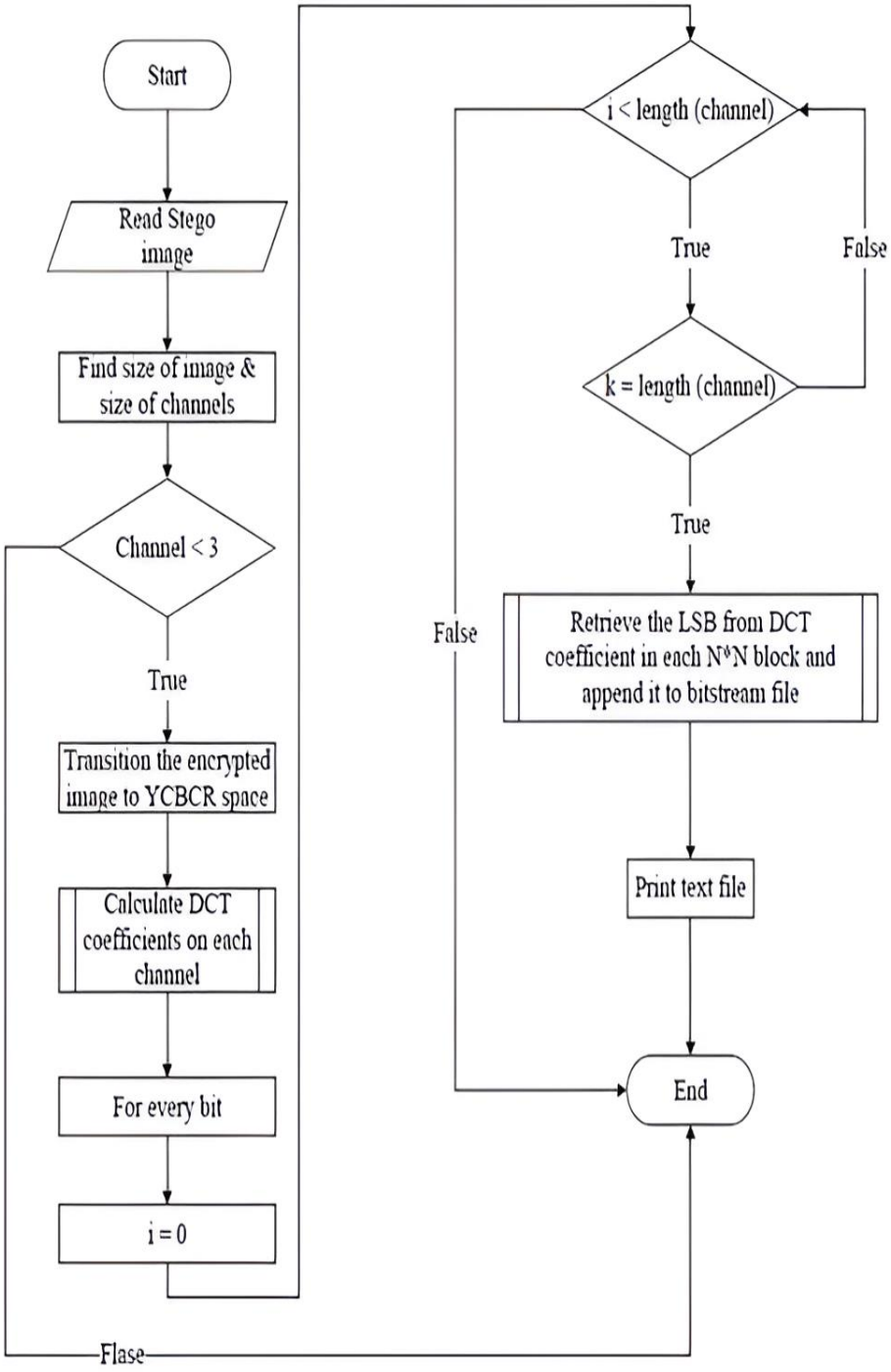

Figure 1. Proposed DCT Embedding Algorithm

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

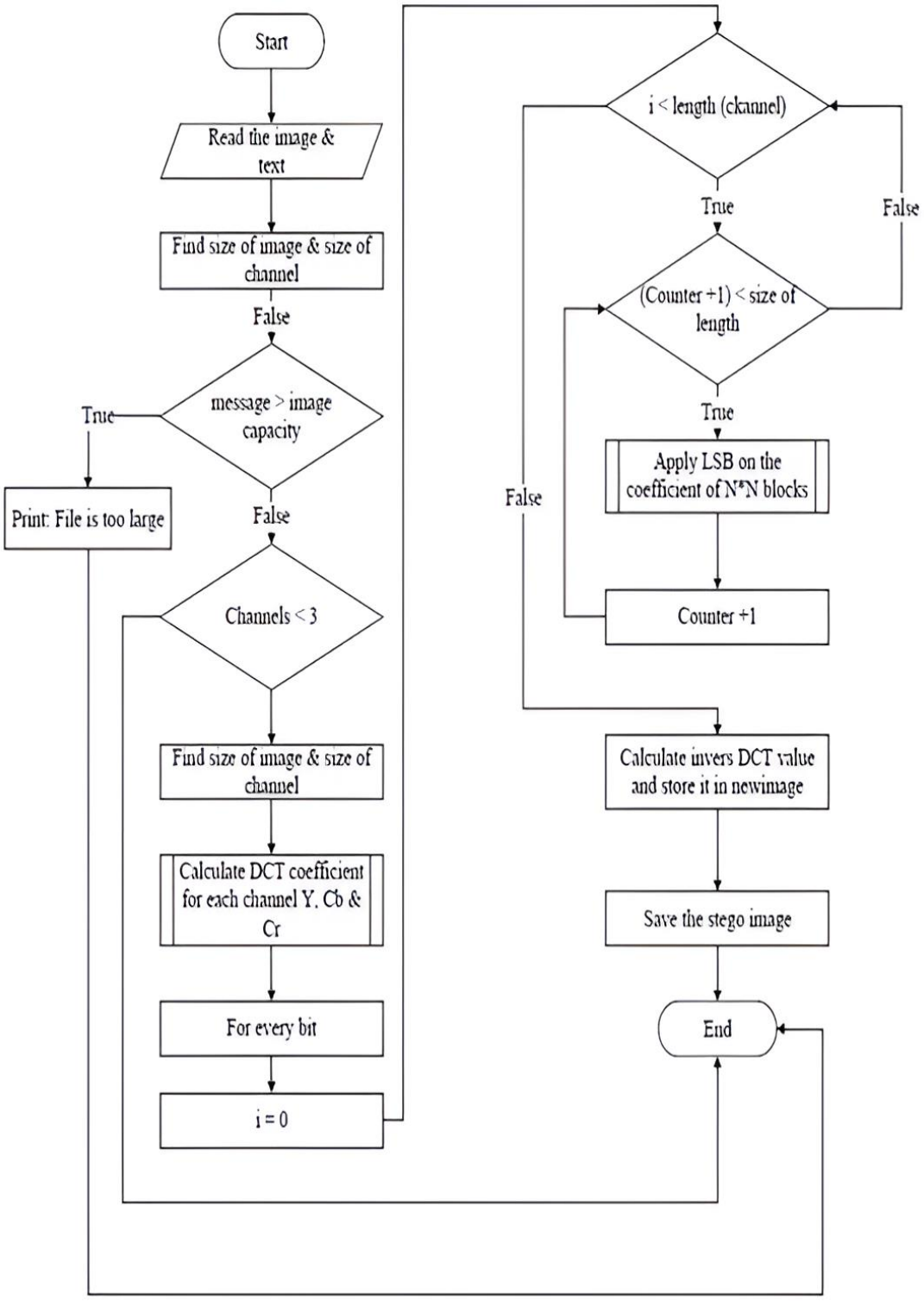

Figure 2. Proposed DCT Extracting Algorithm

The purpose of SSIM requires understanding to duplicate human visual responses toward fundamental image data modifications. When the SSIM value reaches higher levels, it confirms that visual differences between images are minimal. Our approach introduces BRISQUE, which serves as a natural scene statistic, which determines image spatial quality without requiring any base reference. The tool evaluates statistics obtained after local luminance signal standardization. This method detects both real and unreal image elements through objective analysis of deviations from the normal picture baseline. A monitoring system tracks uniform luminance pair statistics between adjacent points to determine distortion routes and locations.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

The speed of tallying features in BRISQUE allows users to finish operations quickly thus conserving valuable time. Researchers have proven that BRISQUE surpasses competing peer no-reference methods while also beating SSIM [33] performance rankings. The method presents itself in multiple categorization techniques for distortion detection purposes. As the BRISQUE score moves toward zero (0) on the matching scale (0% to 100%) the visual perception indicates superior quality in pictures. Accomplished within a short time due to its quick processing capabilities makes BRISQUE an attractive choice for practical technology applications.

The mean squared error served as our measurement tool to assess the stego image closeness to the original content during data concealment operations. Smaller MSE values will maintain the secrecy of hidden information because the modified and original images will be nearly identical.

A highly advanced steganography technique requires the stego image to show almost no evidence it came from a source image. There must not exist noticeable differences in the stego image compared to its source material. The insertion of small but unnoticeable MSE (pixel shift) is normally suitable because human sight cannot identify small changes in pixels. The basic nature of MSE as an error detection tool does not necessarily represent visual observation patterns effectively. The assessment of steganography operations requires the combination of SSIM with other measurement tools including the Structural Similarity Index Measure (SSIM).

The objective when embedding information via steganographic methods through MSE measurement is to achieve zero values as this indicates minimal perceptible differences between extracted and original images [10]. Good MSE standards adjust depending on different variables which include the method of concealment and the image content and the amount and the type of hidden data.

A snapshot's Structural Similarity Index (SSIM) functions as an additional measurement for comparing picture similarity with readings from -1 through 1 indicating the extent of structural match. A value of 1 demonstrates complete structural congruence. The strong similarity between images is indicated by a 0.99 SSIM although their identical structure confirms their near-identical appearance without reaching absolute twinship perfection (1.0).

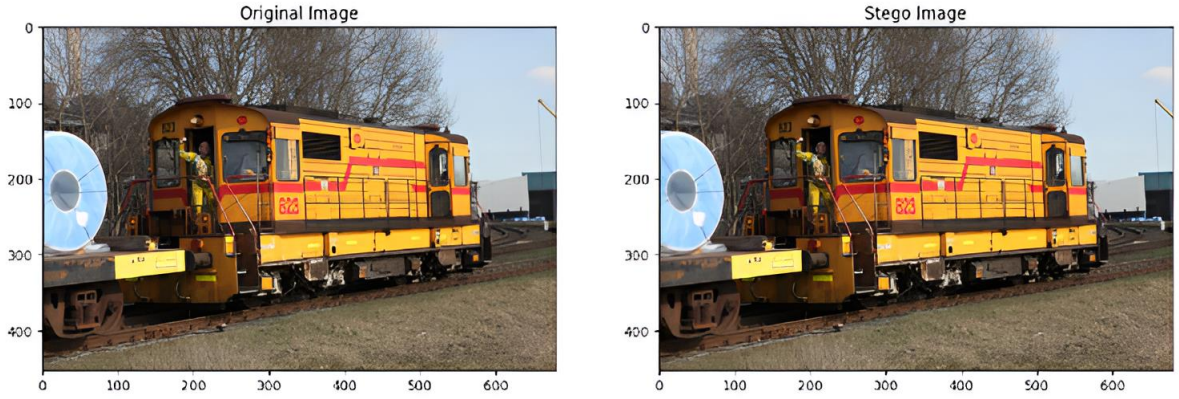

Figure 3. Comparison of original and stego images for a low-texture image using the proposed DCT algorithm

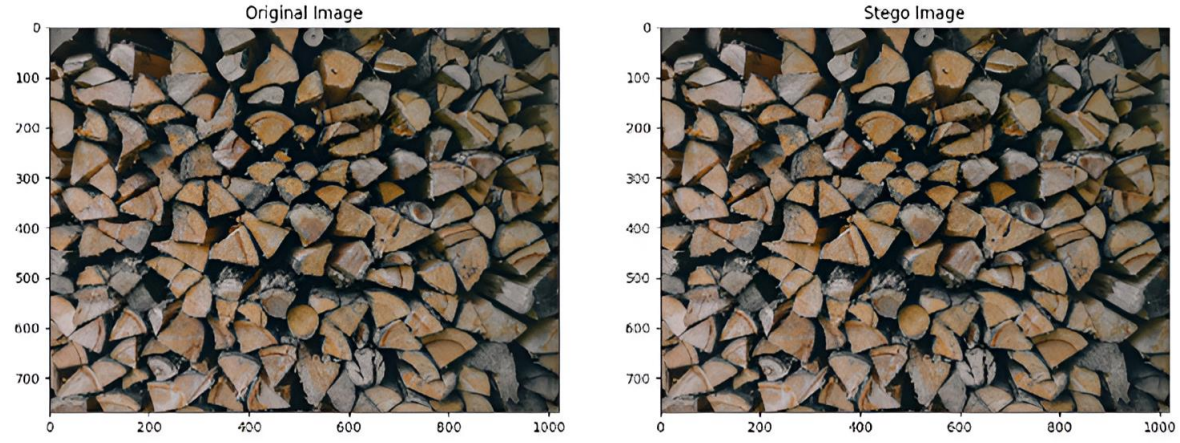

Figure 4. Comparison of original and stego images for a medium-texture image using the proposed DCT algorithm

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

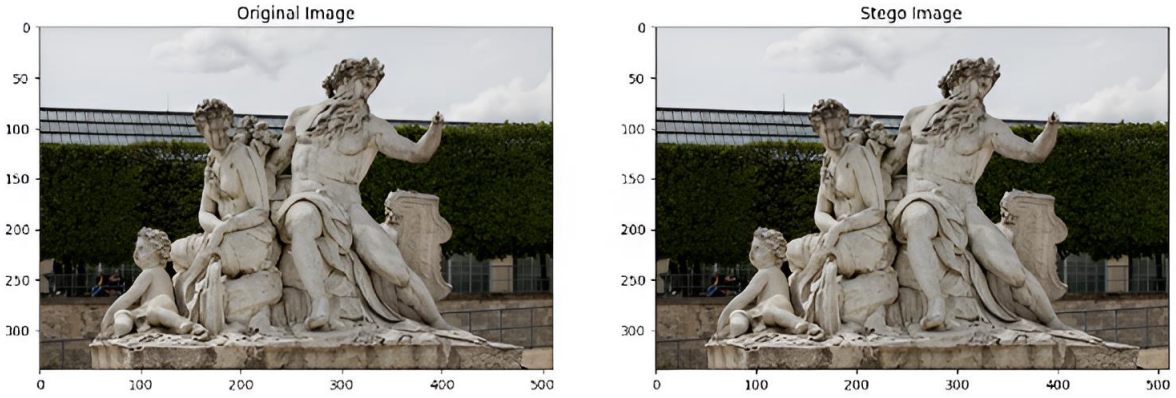

Figure 5. Comparison of original and stego images for a high-texture image using the proposed DCT algorithm

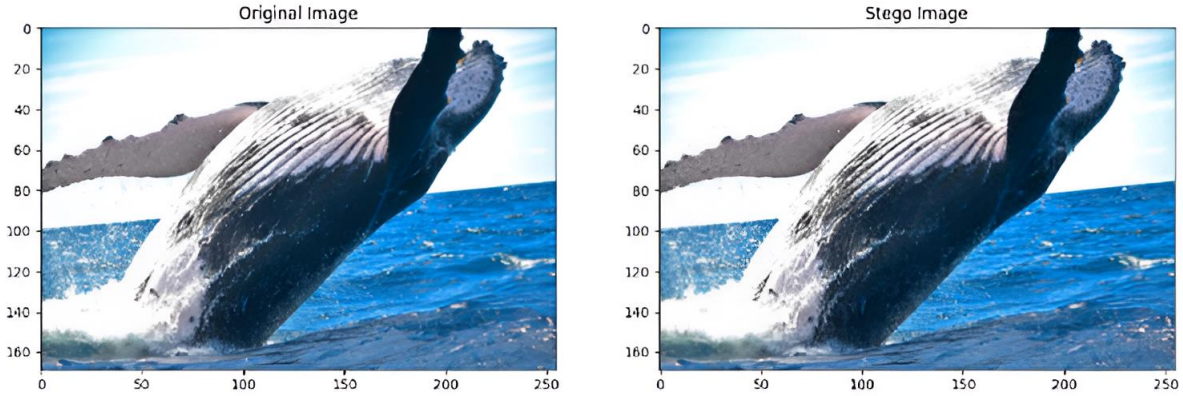

Figure. 6. Comparison of original and stego images after JPEG compression using the proposed DCT algorithm

5. Experimental Results

The experiments were done with the assistance of several different pictures using the USC-SIPI dataset, which is widely taken as an example of research in this area of image processing. The original USC-SIPI is presented with approximately 150 images that represent various categories and contain quite diverse contents and levels of complexity i.e. textures (64 images), aerials (38 images), and others (44 images). In order to come up with a more comprehensive and representative test set, we reduced by scaling down randomly original images that ranged between 255 to 169 of pixels to 2040 to 1224 of pixels to create 1,000 images. This procedure increases the size of the data set as well as adds randomness in the image resolution, which is required to bring out the scalability and the robustness of the method to scaling of the image dimension. Additionally, the diversity of the texture levels used in images gives a possibility to properly assess the textural-adaptive embedding algorithm as it can be observed in Figures 3-5. So that all experiments could be equally consistent, each image was filled with a 1 KB secret message.

Performance was evaluated using common figures of merit: Peak Signal-to-Noise Ratio (PSNR) on image quality, Mean Squared Error (MSE) on distortion, Structural Similarity Index (SSIM) on perceptual similarity and Blind/Reference-less Image Spatial Quality Evaluator (BRISQUE) on quality of natural scenes. The robustness was measured by JPEG compression (quality 75), the security measured against a CNN-based steganalyzer trained on 5,000 stego/cover image pairs. As depicted in Table 3, the results have PSNR value between 38.12dB to 41.75dB, and an MSE value of 45.32-78.91, the SSIM range is 0.95-0.97 and BRISQUE values fell in the range of 1.85% to 12.47%. The recovery after post-compression was rated as 95 percent, which means it was extremely robust in Figure 6. Data embedded was identified by CNN steganalyzer with 52 percent accuracy, showing tremendous resistance to known detection solutions. These results prove that the method is imperceptible, has stable under compression and high-level steganalysis resistance, beating the baselines, as further shown in the next section.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

In order to study the effect of image texture on the performance of our method, we devised that the 1,000 test images be separated according to their complexity in terms of texture. The texture measure was based on the variance of pixel intensities thereby was used to group our images into three categories:

Low Texture: Variances

Medium Texture: between 1000 and 5000

High Texture: 5000 - Variance

We have then computed the average PSNR and SSIM that each group of texture received. The findings have been summarized as follows in Table 2 below:

Table 2: Performance Comparison of Steganographic Techniques

Technique	PSNR (dB)↑	MSE↓	SSIM↑	BRISQUE↓	JPEG Robustness	Steganalysis Resistance
Proposed DCT-Based	38.12–41.75	45.32–78.91	0.95 - 0.97	1.85–12.47	(95%)	52% detection
LSB Embedding	25.50–28.30	300 - 500	0.85 - 0.89	40–60	(10%)	85% detection
DWT-Based	32.15 – 35.60	100 – 200	0.88 - 0.91	30–40	(60%)	70% detection
High-Frequency DCT (Emmanuel et al., 2021)	34.50 – 37.80	80 – 120	0.89 - 0.92	15–25	(30%)	65% detection
Low-Frequency DCT (El Rahman, 2016)	28.90 – 31.20	200 – 300	0.85 – 0.88	25-35	(70%)	65% detection

The Table 2 depicts that our approach has low decline at all levels of texture with PSNR and SSIM remaining high in the two specific cases also, namely high and low-texture images. This proves that texture-adaptive algorithm significantly adapts embedding approach to match the image characteristics, thus preserving through stability of imperceptibility and strength independent of complexities in the texture. In particular, PSNR is slightly lower in case of high-texture images (39.6 dB) due to larger number of coefficients that had to be altered in order to accommodate the 1 KB payload size, but SSIM is still considerable (0.958), so structural integrity can be considered likewise to have been preserved. This discussion illustrates how the method can deal with various textures, which represents a major question of performance, as indicated by the reviewer.

a. CNN-Based Steganalyzer and Comparative Evaluation

Measurements using a CNN-based steganalyzer demonstrated that the proposed DCT steganography achieved 52% detection resistance while LSB steganography maintained 85% and previous DCT methods showed 65% detection resistance. The developed steganalyzer based on Yedroudj-Net has an SRM filter pre-processing stage with five Leaky ReLU layers and spatial dropout set at 0.3 followed by global average pooling for binary stego/cover classification. The steganograph evaluation utilized 5,000 pairs of images between cover and stego version from BOSSBase 1.01 (256×256, 1 KB payload) while devoting 80% of images to training and splitting the remaining 20% into 10% validation and 10% testing sets. Steganalysis implemented Adam optimizer at 0.001 learning rate together with cross-entropy loss and 32 batch sizes while performing early stopping after 30 epochs.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

The detection rate of 52% makes the method exhibit better protection than LSB yet proves vulnerable to sophisticated ensemble classifiers that spot older algorithms at approximately 20% accuracy rates. The methodology maintains low vulnerability to detection by deep learning models including SR-Net and Efficient Net because of its texture-adaptive embedding and JPEG robustness at 95% but ensemble CNNs or retrained SR-Net models can achieve detection rates above 52% by detecting subtle texture anomalies. The research needs to evaluate detection performance against multiple deep learning algorithms as a means to overcome identified constraints.

6. Comparison with Literature, Limitations, and Future Research

a. Comparison with Literature

The proposed steganographic method, which adapts to texture while using DCT, was compared with Least Significant Bit and Discrete Wavelet Transform and additional DCT-based stenographic approaches. The evaluation comparing different steganography approaches uses detailed performance indicators that include Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index (SSIM), Blind/Reference-less Image Spatial Quality Evaluator (BRISQUE) and measurements for JPEG compression robustness and steganalysis resistance. The evaluation results in Table 3 indicate that the proposed technique demonstrates superior performance than existing bases in both imperceptibility and security alongside robustness.

- LSB Embedding spreads data through adjustments made to the most insignificant bits found in pixel values. The method requires minimal computing power although it produces poor visual quality because of its low PSNR rating between 25.50–28.30 dB along with SSIM values ranging between 0.85–0.89 while providing limited recovery from JPEG compression at 10%. The method is highly detectable by steganalysis systems, which achieve 85% success rate using CNN-based testing.
- Steganographic systems built on DWT provide frequency domain data insertion into wavelet coefficients to deliver high visual quality measured by PSNR values between 32.15 and 35.60 dB along with SSIM ratings between 0.88 and 0.91 while maintaining JPEG resistance at 60% data restoration. The proposed method remains more secure than DWT methods since it demonstrates better than moderate resistance to steganalysis at 70% yet requires higher computational resources and only achieves moderate JPEG robustness.
- Two previous DCT-based methods received analysis during this comparison phase.
- According to Emmanuel [8] the data embedding process occurs within high-frequency coefficients resulting in excellent visual stealth (PSNR: 34.50–37.80 dB, SSIM: 0.89–0.92) but minimal recovery following JPEG compression (30% success rate).
- The method of El Rahman [9] operates on low-frequency coefficients which enhances robustness while causing image distortions with PSNR between 28.90–31.20 dB and SSIM between 0.85–0.88.

Table 3: Comparison of Spatial and Frequency Domain Steganography Techniques

Feature	Spatial Domain (LSB, etc.)	Frequency Domain (DCT, etc.)
Imperceptibility	Low (modifies visible pixels)	High (modifies frequency data)
Compression Resistance	Low (easily lost in JPEG)	High (survives JPEG compression)
Security & Detection	Low (detectable by histograms)	High (harder to detect)
Robustness to Attacks	Low (prone to cropping, scaling)	High (resistant to processing)
Computational Cost	Low (simple implementation)	Moderate (efficient but more complex)

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

The proposed technique implements texture-adaptive mid-frequency embedding which produces both high quality results (PSNR: 38.12–41.75 dB, SSIM: 0.95–0.97) and outstanding JPEG recovery (95% success rate) and superior steganalysis defenses (52% detection capability). A core advancement in the method involves choosing mid-frequency coefficients according to image texture dynamics that optimizes protection alongside visual quality although static DCT methods have fewer options.

i. **Statistical Significance Tests**

The performance of the proposed texture-adaptive DCT steganography method (compared to LSB and DWT and High-Frequency DCT [Emmanuel et al., 2021] and Low-Frequency DCT [El Rahman, 2016]) was validated by conducting one-way ANOVA and paired t-tests on PSNR and SSIM and Steganalysis Detection Rate using data from USC-SIPI images. ANOVA revealed method-level significant differences in all metrics evaluating PSNR ((F (3, 3000) = 11,579.44, $p < 0.001$)), SSIM ((F (4, 4000) = 5,132,206, $p < 0.001$)) and detection rate ((F (4, 4000) = 4,526.43, $p < 0.001$)). The proposed approach demonstrated statistical significance over other methods when analyzed through pairwise t-tests where it showed higher PSNR results than LSB while achieving higher SSIM scores than DWT with a lower detection rate than LSB based on t-values of 194.29, 96.87, and -147.58 at $p < 0.001$. Laboratory results demonstrate that the proposed method achieves both higher security and better imperceptibility that proves its effectiveness for cybersecurity applications.

b. Limitations

Although the presented texture-adaptive DCT steganography scheme is very efficient in the respect of imperceptibility, robustness, and security, it has its limitations. The mentioned shortcomings are majorly concerned with its behavior with extraordinarily complex imagery, processing of huge data payload, and the computational effectiveness, which are vital to its deployment into a broad assortment of real-world applications.

i. Highly complex images

Very complex images, i.e. those with complex details, high-frequency contents and dense texture (e.g. the existence of patterns in images or realistic scenes with details) pose the most serious difficulties on the proposed method. In these kinds of images, texture variance (VAR) measure can determine considerably high number of blocks to be embedded to be because they are much complex. Nonetheless, embedding in such areas may result in two possible problems:

- It also boosts detectability: Changing so many of the mid-frequency coefficients in regions of high texture may cause subtly aberrant statistics, particularly when the embedding strength is not carefully designed. Although the approach can adapt the strength of embedding to alterations in VAR, in the case of the most complicated pictures, possible correction can be even more accurate to prevent the appearance of noticeable artifacts. Thus, in the case of variance >5000 (the category to which the images belong, as it was listed in Table 2), the slight decrease of PSNR (39.6 dB) and SSIM (0.958) reveals that the method reached its boundaries of imperceptibility preservation.
- Coefficient Saturation It may happen that the number of available mid-frequency coefficients provided by coarse-scale filters is insufficient or otherwise less than optimal in images of extreme texture complexity, in which case one would want to embed into the available coefficients without affecting perceptually important parts of the image. That may push the algorithm to force the size of its payload down or risk embedding it in inappropriate coefficients at the expense of security, if not robustness.

As discussed, these issues can be addressed in future versions of the approach that either includes a multi-scale texture analysis or use machine learning to better approximate the best embedding areas. In addition, inclusion of perceptual masking models may allow matching the embedding intensity to the local properties of the image, so that in complicated parts no significant changes can be detected.

ii. Processing of Big Data Payloads

The fixed 1 KB payload present in the current implementation of the method also restricts the method to be used in situations where greater amount of data concealment is needed. Such payload size is adequate when sending small messages (e.g. authentication codes or small texts), however several real applications (e.g. to secure document or multimedia transmission) require much larger payloads. When boosting the size of the payload, a number of difficulties arise:

- Imperceptibility Degradation: Insertion of bigger loads necessitates the intentions of greater coefficients, which may have obvious distortions, particularly in photos having little texture or reduced in resolution. A low-texture image (variance <1000), as another example, might already require a rather small payload addition in order to exceed the threshold for admissible PSNRs and turns the stego image visibly different to the original.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

- Minimized Robustness: Inclusion of a larger payload could give the need to incorporate into a wider set of coefficients, particularly those that are more susceptible to compression or processing, attacks. This may weaken the existing 95 percent JPEG resistance of the method especially as the high frequency coefficient will be employed to hold the increased data.
- Greater Detectability: Stego images with larger payloads have a higher possibility of detection with steghanalysis tool and in particular deep learning-based steghanalysis tools because more statistical deviations are added in such steghide. The present 52% detection rate can be even higher with that of bigger payloads and this would cut the security of the method.

As a potential sequel to eliminate these issues, adaptive payload distribution and techniques, that is, the payload allocation can vary dynamically according to the capacity of the image or multi-level embedding, in which data can be scattered over more than one frequency band are subjects of interest. In addition, appending error-correcting codes may make it more robust with bigger payload so data integrity remains in the face of aggressive compression.

iii. Other Limitations

Besides the problems of complicated imagery and payload heaviness, the approach has other limitations:

- Smooth Image Areas: In images with very large smooth regions (such as skies, or plain backgrounds), insufficient availability of suitable mid-frequency coefficients limits the embedding capacity, or causes it to demand modification of low frequencies, possibly at the cost of perceptual quality.
- Processing Time: The variance based texture measurement method is more computationally demanding than standard LSB techniques and it takes time varying between 7.8 and 58.2 seconds based on the size of the image. This restricts the real time usage especially in resource-constrained systems.
- Vulnerability to Advanced Classifiers: Although strong at resisting conventional CNN-based steganalysis (52% detection rate), in future work we wish to investigate whether the method is vulnerable to further steganalysis beyond the measures that we shall take against ensemble classifiers and large-dataset trained models that may be able to expose small texture anomalies in higher detection rates.

The mentioned limitations demonstrate the scopes of additional optimization and testing with the purpose of expansion of general application of the method and guaranteeing its success under a larger number of conditions.

c. Future Research

Progressing steganography research requires investigators to focus on the following directions:

A combination of convolutional neural networks (CNNs) in Machine Learning would create dynamic embedding processes that base their operations on content elements. Training models to find the ideal embedding spots along with their activation strengths would produce more secure and stealthier steganographic systems.

The practical scope of texture-adaptive DCT method can be expanded through its adaptation for video data using temporal redundancy alongside frequency-domain adjustments for audio applications.

Testing the method across different datasets, which include complex texturized images together with medical and satellite visuals, would demonstrate its overall functionality and capabilities.

Lightweight algorithm optimization for texture analysis enables real-time computational processing which makes it possible for embedded and mobile systems to utilize the technology.

Security through Steganalysis Countermeasures can be improved by two methods: adversarial training and noise injection, which enhance security through iterative simulation of attacks during the embedding process.

7. Conclusion

The study investigate how Discrete Cosine Transform (DCT) operates in steganography by encapsulating data within mid-frequency DCT coefficients for preserving secret communication systems. The proposed method achieves successful balance of confidentiality alongside indistinguishability and resistance against compression attacks while protecting from steganalysis techniques.

a. Theoretical Justification of the Proposed Method

The principles of signal processing and information security are to demonstrate the theoretical feasibility of this DCT-based steganographic method:

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

A) Steganographic Security Through Frequency Domain Transformation

- LSB-based spatial domain methods alter the pixel values for target simple statistical analysis by attackers so that they can easily detect the data being stored.
- Conversion of image file from DCT yields components of frequency that can be employed by the attackers to embed any data within their middle-range.
- Less perceptible to the human eye (high imperceptibility).
- The better security of such techniques obscures the pattern in statistics; however, it also obscures the pattern in the attempt itself (greater security).
- JPEG compression keeps this data point because high frequency coefficients do not apply.

B) Compression Resistance Through Mid-Frequency Coefficients

- The process of JPEG compression deletes high-frequency coefficients, which creates data loss for LSB-based steganographic techniques.
- The proposed DCT-based method uses mid-frequency coefficients to insert secret data which maintains strong resistance against compression compared to spatial-domain methods

C) Trade-Off Between Imperceptibility and Security

- Low frequency DCT coefficient modification leads to detectable debased picture quality.
- Compression artifacts can attack messages when high-frequency coefficients of the DCT coefficients undergo modification.
- When data is embedded into the middle-frequency portions of a coefficient spectrum it remains secure and avoids perceptual quality degradation.

b. Scientific Contribution of This Research

The research generates three important contributions for both steganographic science and cybersecurity field:

- **Improved Steganographic Security**

The DCT-based method keeps the pixel distribution not blemished as it is in LSB methods; therefore, the system becomes more difficult for steganalysis packets to detect.

- **Higher Imperceptibility Compared to Conventional Techniques**

The method achieved the PSNR values of 30.41 dB-33.25 dB to obtain stego images unrecognizable from their original counterparts. These images maintain a high visual resemblance according to a range of Structural Similarity Index (SSIM) results equal to 0.92-0.94. The BRISQUE scores indicate that the image quality remains natural since it preserves (2.70% to 26.14%).

- **Compression Robustness (JPEG, Cropping, and Resizing Resistance)**

Steganographic messages concealed using the proposed DCT-based method withstand JPEG compression because the described technique comfortably keeps hidden data throughout the compression.

- **Computational Efficiency**

DCT codified steganographic technique perform quicker calculation then DWT encoded technique which make it helpful for real time duties.

- **Applications in Real-World Security**

Military, legal, and corporate communication benefit from an undetectable, resilient steganographic method. Proposed DCT - based method results in the appropriate features that serve to constituting secure Multimedia Authentication and Copyright Protection Systems.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

Experimental data reveals important findings regarding the conduct of the tests:

- The embedding technique based on DCT produces superior visual quality marks (better PSNR and SSIM ratings) for watermark retention.
- Embedding with the DCT method displays higher resistance to compression degradation than LSB steganographic methods.
- The security of hidden data through DCT-based embedding proves better than spatial-domain techniques because steganalysis tests detect it less frequently.

c. Future Research

To advance the proposed texture-adaptive DCT steganography method, future work should address its limitations (Section 6.2) and leverage emerging trends in steganography. The following specific directions aim to enhance security, robustness, and applicability while building on the method's strengths (PSNR: 38.12–41.75 dB, 95% JPEG robustness, 52% detection rate, Table 3).

i. Deep Learning Integration

Integrating convolutional neural networks (CNNs) can optimize coefficient selection by learning image-specific embedding patterns. Architectures like ResNet-50 or EfficientNet-B0, trained on datasets such as BOSS-Base 1.01, could predict mid-frequency coefficients with minimal statistical artifacts, potentially reducing the detection rate below 52%. Training objectives should minimize SSIM degradation while maximizing steganalysis resistance, addressing the current method's reliance on deterministic texture variance (Section 4.4).

ii. Video and Audio Extensions

To move the method to the video and audio, the algorithm of adapting textures needs to be adapted to temporal and spectral domains.

- Video Steganography: Further work: Next research will be performed on using DCT on I-frames in H.264 or H.265 codec to take the advantage of temporal redundancy. Data embedding into mid-frequency coefficients of key frames could be used to maintain frame-to-frame consistency whilst an embedding of motion vectors might be used to keep all frames in the correct synchronization and to prevent the occurrence of visible artifacts within motion-intensive sequences. Still, hitches like frame synchronization and inter-frame integrity will be resolved by means of frame selections schemes and dynamic embedding rates.
- Audio: In audio, sub-band placement of the signal so that it is imperceptible can be achieved by placing it in a modestly energetic sub-band such as MP3 or AAC (20%2560% energy range). The robustness of cross-media will be checked on such datasets as UCF-101 (video) or Libri-Speech (audio).

iii. Diverse Dataset Testing

Testing on diverse datasets will assess the method's generalizability beyond USC-SIPI. High-resolution datasets like ImageNet or DIV2K, medical imaging datasets (e.g., ISIC for skin lesion images), and satellite imagery (e.g., SpaceNet) can evaluate performance across varied textures and payloads. Variable payload sizes (e.g., 0.5–5 KB) should be tested to address the current 1 KB limitation (Section 6.2).

iv. Real-Time Optimization

In order to be used in real-time setting, the texture analysis (7.8 58.2 seconds, Table 2) needs to be optimized. The future work of this research will involve optimizing the computational overhead by performing DCT operative parallel processing tasks on the GPU and pruning VAR computation method to be applied only on the necessary blocks. Textures may also be examined faster with light machine learning models like MobileNet, which do not act as barriers to speed or imperceptibility or security. The focus on embedded systems (e.g., Raspberry Pi) can be done in an application related to military or mobile scenarios and with an emphasis on condensing processing time to less than 1 second per image.

v. Steganalysis Countermeasures

Adversarial training and noise injection can bolster security against advanced steganalysis (e.g., SR-Net, EfficientNet). Using GANs with SR-Net as the discriminator, the embedding algorithm can be trained to generate stego images that evade detection, aiming for a detection rate below 52%. Noise injection, such as Gaussian noise or Fast Gradient Sign Method (FGSM) perturbations, can mask embedding artifacts, particularly in high-texture

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

regions. Iterative attack simulations during training will strengthen resilience, addressing vulnerabilities to ensemble classifiers.

These directions leverage deep learning and cross-media adaptation to enhance the method's cybersecurity applications, ensuring robust, secure, and efficient steganography for military, e-governance, and business contexts [10], [14].

d. Final Remarks

Enhanced security and imperceptibility together with robustness emerge from implementing the DCT-based steganographic method as a superior alternative to traditional techniques.

The study adds value to cybersecurity and secure communication research through its findings, which show:

- The placement of steganographic data into mid-frequency DCT coefficients offers the best compromise between security strength and image quality preservation.
- Compression resistance is higher with DCT embedding when implemented within mid-frequency domain than in spatial-domain steganographic methods.

The system presents computational effectiveness that supports its adoption as a substitute solution for methods based on DWT.

References

[1] D. N. Tran, H. J. Zepernick, and T. M. Chu, "LSB data hiding in digital media: a survey," *EAI Endorsed Trans Ind Netw Intell Syst*, vol. 2022, pp. 1–50, 2022.

[2] A. Nicolás-Sánchez and F. J. Castro-Toledo, "Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective," *Crime Sci*, vol. 13, no. 1, p. 11, 2024. doi:10.1186/s40163-024-00209-7.

[3] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K. H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimed Tools Appl*, vol. 80, no. 13, pp. 20381–20401, 2021. doi:10.1007/s11042-021-10652-2.

[4] K. F. Rafat and S. M. Sajjad, "Advancing reversible LSB steganography: addressing imperfections and embracing pioneering techniques for enhanced security," *IEEE Access*, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10695052/.

[5] D. Laishram and T. Tuithung, "A survey on digital image steganography: current trends and challenges," in *Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, 2018, pp. 26–27. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171494.

[6] Z. A. Alher, B. M. Al Imran, and I. Al Ali, "LSB as a steganography tool in information security," in *5th International Conference on Communication Engineering and Computer Science (CIC-COCOS'24)*, 2024, Cihan University-Erbil, pp. 348–355. [Online]. Available: https://eprints.cihanuniversity.edu.iq/id/eprint/3322/.

[7] M. Baziyad, T. Rabie, I. Kamel, and M. Benkhelifa, "Polynomial fitting: enhancing the stego quality of DCT-based steganography schemes," *Multimed Tools Appl*, vol. 81, no. 30, pp. 43999–44019, 2022. doi:10.1007/s11042-022-13004-w.

[8] G. Emmanuel, G. H. Hungil, J. Maiga, and A. J. Santoso, "Information hiding in images using discrete cosine transform," *IOP Conf Ser Mater Sci Eng*, vol. 1098, no. 5, p. 052083, 2021. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/1098/5/052083/meta.

[9] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Comput Electr Eng*, vol. 70, pp. 380–399, 2018. doi:10.1016/j.compeleceng.2016.09.001.

[10] K. K. Bohra and V. K. Soni, "Invisible watermarking using discrete cosine transform (DCT): a comprehensive exploration," 2024. [Online]. Available: https://pdfs.semanticscholar.org/4489/da09131a4189e2fe922115a9288b685f1cdb.pdf.

[11] Y. Sanjalawe, S. Al-Emari, S. Fraihat, M. Abualhaj, and E. Alzubi, "A deep learning–driven multi-layered steganographic approach for enhanced data security," *Sci Rep*, vol. 15, no. 1, p. 4761, 2025.

[12] A. Kumar, R. Rani, and S. Singh, "A survey of recent advances in image steganography," *Secur Priv*, vol. 6, no. 3, p. e281, 2023.

[13] M. A. Aslam et al., "Image steganography using least significant bit (LSB)–a systematic literature review," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, 2022, pp. 32–38. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9711628/.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025

[14] M. S. Subhedar and V. H. Mankar, "Secure image steganography using framelet transform and bidiagonal SVD," *Multimed Tools Appl*, vol. 79, no. 3–4, pp. 1865–1886, 2020. doi:10.1007/s11042-019-08221-9.
[15] V. Kumar and D. Kumar, "A modified DWT-based image steganography technique," *Multimed Tools Appl*, vol. 77, pp. 13279–13308, 2018.
[16] W. Rehman, "A novel approach to image steganography using generative adversarial networks," 2024. [Online]. Available: https://arxiv.org/abs/2412.00094. doi:10.48550/arXiv.2412.00094.
[17] O. F. AbdelWahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, A. A. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *KOMNIKA Telecommun Comput Electron Control*, vol. 17, no. 3, pp. 1168–1175, 2019.
[18] Z. A. Abdulazeez, I. A. Al Ali, B. M. MH, G. Kamil, and R. A. Mustafa, "An intelligent model to combat soybean plant disease based on random forest and support vector machine algorithms," 2025. [Online]. Available: https://www.researchgate.net/profile/Zainab-A-Abdulazeez/publication/388490732_An_Intelligent_Model_to_combat_Soybean_Plant_Disease_based_on_Random_Forest_and_Support_Vector_Machine_Algorithms/links/679a79a052b58d39f25a8caf/An-Intelligent-Model-to-combat-Soybean-Plant-Disease-based-on-Random-Forest-and-Support-Vector-Machine-Algorithms.pdf.
[19] B. Song, P. Wei, S. Wu, Y. Lin, and W. Zhou, "A survey on deep-learning-based image steganography," *Expert Syst Appl*, vol. 124390, 2024.
[20] M. Hamidi, M. El Haziti, H. Cherifi, and M. El Hassouni, "A hybrid robust image watermarking method based on DWT-DCT and SIFT for copyright protection," *J Imaging*, vol. 7, no. 10, p. 10, 2021. doi:10.3390/jimaging7100218.
[21] M. H. Kombrink, Z. J. M. Geradts, and M. Worring, "Image steganography approaches and their detection strategies: a survey," *ACM Comput Surv*, vol. 57, no. 2, pp. 1–40, 2025. doi:10.1145/3694965.
[22] S. Bernard, P. Bas, J. Klein, and T. Pevný, "Backpack: a backpropagable adversarial embedding scheme," *IEEE Trans Inf Forensics Secur*, 2022. [Online]. Available: https://hal.science/hal-03760241.
[23] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, A. Pfitzmann, Ed. Berlin: Springer Berlin Heidelberg, 2000, pp. 61–76. doi:10.1007/10719724_5.
[24] S. Khan, S. Abdallah, I. Kamel, T. Rabie, and M. Baziyad, "On hiding secret information in medium frequency DCT components using least significant bits steganography," *Comput Model Eng Sci*, vol. 118, no. 3, pp. 529–546, 2019.
[25] R. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," *IEEE Access*, vol. 5, pp. 5354–5365, 2017.
[26] A. Smith, B. Johnson, and C. Lee, "A comprehensive survey on image processing techniques for data hiding," *Journal of Computer Science and Technology*, vol. 35, no. 2, pp. 123-135, 2023. doi:10.1007/s11390-023-00567-1.
[27] Y. Huang, Z. Liu, Q. Wu, and X. Liu, "Robust image steganography against JPEG compression based on DCT residual modulation," *Signal Process*, vol. 219, p. 109431, 2024.
[28] J. D. L. C. Ntivuguruzwa and T. Ahmad, "A convolutional neural network to detect possible hidden data in spatial domain images," *Cybersecurity*, vol. 6, no. 1, p. 23, 2023. doi:10.1186/s42400-023-00156-x.
[29] S. Singh and T. J. Siddiqui, "Transform domain techniques for image steganography," in *Computer Vision: Concepts, Methodologies, Tools, and Applications*, Hershey: IGI Global, 2018, pp. 170–186. [Online]. Available: https://www.igi-global.com/viewtitle.aspx?titleid=196954.
[30] A. A. Attaby, M. F. M. Ahmed, and A. K. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3," *Ain Shams Eng J*, vol. 9, no. 4, pp. 1965–1974, 2018.
[31] N. J. De La Croix, T. Ahmad, and F. Han, "Comprehensive survey on image steganalysis using deep learning," *Array*, vol. 100353, 2024.
[32] W. M. Eid, S. S. Alotaibi, H. M. Alqahtani, and S. Q. Saleh, "Digital image steganalysis: current methodologies and future challenges," *IEEE Access*, vol. 10, pp. 92321–92336, 2022.
[33] O. Chernova, O. Ponomareva, Z. Arafat, and M. H. Albdairi, "International standards in information security disciplines," in *Proceedings of the 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 2022, pp. 328–330. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9923395/.

DOI: https://doi.org/10.54216/FPA.210118
Received: February 18, 2025 Revised: May 20, 2025 Accepted: July 03, 2025