Journal of Intelligent Communication
https://ojs.ukscip.com/index.php/jic

Article

Novel Adaptive DCT-Based Steganography Algorithm with Coefficient Selection Optimization for JPEG Images

Mohammad Hossein Noorallahzadeh

Faculty of Science, University of Qom, Qom 37161-46611, Iran; mh.noorallahzadeh@stu.qom.ac.ir

Received: 31 August 2025; **Revised:** 28 December 2025; **Accepted:** 30 December 2025; **Published:** 2 February 2026

Abstract: In the realm of secure digital communication, balancing payload capacity with perceptual imperceptibility remains a critical challenge, particularly within lossy compression standards like JPEG. This paper proposes a robust steganography framework that addresses this trade-off by integrating adaptive Discrete Cosine Transform (DCT) modification with an edge-based selection criterion. Unlike uniform embedding approaches that indiscriminately treat all image regions, the proposed method employs Canny edge detection to categorize 8×8 blocks based on texture complexity. This strategy leverages the masking properties of the Human Visual System (HVS), allocating higher payload capacities to complex, edge-rich regions where modifications are statistically less detectable. To further enhance embedding efficiency, a decimal-to-ternary (base-3) coding scheme is introduced to optimize the utilization of DCT coefficients. This mechanism is coupled with a modulo optimization search within a constrained range of $[C-2, C+2]$, which minimizes the magnitude of necessary modifications compared to traditional binary embedding. Experimental evaluations on standard datasets, including USC-SIPI, indicate that the method maintains a Peak Signal-to-Noise Ratio (PSNR) significantly higher than traditional methods, ranging from 48 dB to 62 dB depending on the embedding rate. Furthermore, quantitative analysis demonstrates a 58.5% improvement in embedding efficiency over standard binary techniques. Consequently, this adaptive strategy offers a superior trade-off between high-capacity data hiding and resistance to statistical steganalysis compared to standard LSB and non-adaptive DCT methods.

Keywords: Steganography; Adaptive DCT; Edge Detection; Base-3 Embedding; JPEG Security; Coefficient Optimization

1. Introduction

In the rapidly evolving landscape of information security, where threats emerge with increasing sophistication and adversaries leverage cutting-edge tools to intercept communications, digital steganography has firmly established itself as a pivotal technology for secure communication [1]. This technique enables the concealment of sensitive data within everyday digital media—such as images, audio files, or videos—in a manner that renders the very existence of the secret information imperceptible to casual observers, even under close scrutiny. Unlike overt methods that might raise alarms through encryption indicators or unusual file sizes, steganography operates covertly, blending secret payloads seamlessly into innocuous carriers [2].

While traditional cryptography excels at protecting the content of a message by scrambling it into unreadable ciphertext—requiring a key for decryption—steganography takes a fundamentally different approach by focusing on protecting the channel itself [3]. It ensures that the act of communication remains hidden, preventing adversaries from even knowing that a secret exchange is taking place. By embedding the secret data within an innocent-

https://doi.org/10.54963/jic.v5i1.1570

looking cover file, such as a family photo or a landscape image shared on social media, steganography avoids drawing suspicion [4]. This feature is increasingly vital in scenarios requiring the highest levels of discretion, including military intelligence operations where operatives must transmit coordinates or orders without alerting surveillance systems, covert operations by intelligence agencies exchanging plans in hostile territories, or even corporate espionage where whistleblowers share documents undetected. In these high-stakes environments, the mere detection of encrypted traffic can trigger investigations, whereas a stego image passes as mundane content [5].

Among the various digital formats available for cover media, JPEG images stand out as the most ubiquitous standard for image transmission across the web, smartphones, and cloud storage platforms [6]. Their popularity stems from highly efficient compression algorithms that drastically reduce file sizes without unacceptable loss of visual quality, making them ideal for bandwidth-constrained networks. However, the specific architecture of JPEG compression introduces a unique and profoundly difficult challenge for steganographic algorithms [7]. JPEG operates as a lossy compression standard, employing block-wise Discrete Cosine Transform (DCT) to convert spatial pixel data into frequency coefficients, followed by quantization that aggressively discards high-frequency data—those representing fine details and noise—to minimize file size [8]. This process inherently alters the image, and any embedding must be robust enough to survive the quantization phase, where coefficients are rounded to discrete values, while simultaneously remaining statistically undetectable to forensic analysis [9].

The fundamental challenge in designing any effective steganographic protocol revolves around balancing three inherently conflicting requirements, often encapsulated in what researchers term the “magic triangle”: embedding capacity, visual imperceptibility, and robustness against steganalysis [10]. Embedding capacity refers to the volume of secret data that can be reliably hidden per unit of cover media, typically measured in bits per pixel (bpp) or as a percentage of the cover size. Visual imperceptibility demands that the stego image appears identical to the original to the human eye, preserving natural textures, colors, and contrasts [11]. Robustness against steganalysis ensures survival against detection algorithms that probe for anomalies. Unfortunately, increasing payload capacity almost invariably leads to higher distortion in the cover image—through pixel shifts or coefficient tweaks—thereby eroding visual imperceptibility and heightening detection risks [12]. This trade-off forces designers to navigate a delicate equilibrium, where pushing one vertex of the triangle distorts the others.

Early research in steganography primarily concentrated on spatial domain techniques, with Least Significant Bit (LSB) substitution emerging as the cornerstone method [13]. These approaches were prized for their computational simplicity, requiring only basic bit operations, and offered impressively high storage capacity by directly modifying the least significant bits of pixel values across the image matrix. For instance, in an 8-bit grayscale image, up to one bit per pixel could be embedded by flipping the LSB, yielding a theoretical 12.5% capacity for binary data [14]. However, these methods drastically alter the raw statistical properties of the image histogram, smoothing out natural distributions and introducing artificial uniformities. As a result, spatial techniques proved extremely vulnerable to statistical attacks, such as the Chi-square attack that compares observed pixel pair frequencies against expected random models, and they are readily destroyed by innocuous image processing operations like cropping edges, resizing for thumbnails, or mild JPEG recompression [15]. A single pass through such filters could obliterate the hidden payload, rendering LSB impractical for real-world deployment.

Consequently, the focus of the research community shifted decisively towards transform domain techniques, which promised greater resilience [16]. Methods operating in the Discrete Cosine Transform (DCT) domain embed data into the frequency coefficients of image blocks rather than tampering with individual pixels in the spatial realm. This embedding aligns with the JPEG pipeline, allowing data to persist through compression cycles [17]. DCT-based approaches offer enhanced robustness and security because modifications are dispersed across frequency spectra, mimicking compression noise and withstanding signal processing attacks like filtering or scaling [18]. While this paradigm significantly bolsters survival rates—often enduring multiple JPEG iterations—it frequently suffers from limited payload capacity compared to spatial counterparts, as not all coefficients can be altered without introducing detectable biases [19]. This limitation has driven the development of more efficient coding schemes, such as matrix embeddings or trellis codes, to pack more bits per change. Yet, even these refinements struggle against evolving detectors that model inter-coefficient dependencies [20].

Recent advancements in the field have underscored the critical importance of content-adaptive steganography as a means to bridge the persistent gap between capacity and security [21]. New paradigms emphatically suggest that embedding strategies should not apply uniformly across the entire image, treating all pixels or coefficients as equals; instead, they must adapt dynamically to the local characteristics of the image content, leveraging inherent redundancies [22]. The Human Visual System (HVS) exhibits remarkable non-uniform sensitivity: it is far more attuned to detecting noise or irregularities in smooth, uniform regions—like blue skies or skin tones—where subtle changes disrupt perceptual continuity, than in highly textured or edge-dense areas, such as foliage, fabric patterns, or urban scenes, where natural noise masks alterations [23]. Therefore, modern algorithms employ sophisticated complexity analysis—through metrics like local variance, edge density, or entropy measures—to pinpoint "noisy" regions ideal for hiding data with a markedly lower probability of detection [24]. By concentrating embeddings in these resilient zones, adaptive methods preserve global statistics while maximizing local capacity.

Furthermore, the security landscape has undergone a dramatic transformation with the meteoric rise of deep learning-based steganalysis [25]. Convolutional Neural Networks (CNNs), with architectures like ResNet or custom steganalytic nets trained on millions of cover-stego pairs, are now capable of detecting minute statistical anomalies—such as higher-order co-occurrences or spectral imbalances—that eluded traditional handcrafted steganalysis tools like histogram feature extractors or moment-based detectors [26]. These AI-driven classifiers achieve detection accuracies exceeding 95% on modern benchmarks, even at low payloads, by learning abstract representations of "stegoness" directly from data [27]. This escalation demands exponentially more stringent security requirements for new algorithms, pushing beyond simplistic distortions toward provably secure primitives.

This research confronts these multi-faceted challenges head-on by proposing a novel algorithm that synergistically combines advanced edge detection for intelligent, adaptive region selection—prioritizing high-complexity boundaries where human and machine detectors alike falter—with a high-efficiency base-3 coding scheme [28]. This ternary strategy embeds more information per modification than binary methods, exploiting edge-adaptive locations to maximize embedding capacity without compromising the statistical integrity of the cover image. By sidestepping computational heavyweights like syndrome-trellis codes, our approach delivers practical undetectability against both classical and deep learning steganalyzers, redefining the magic triangle's feasible boundaries.

2. Literature Review and Theoretical Framework

Steganography sits at the heart of information security, encompassing various sophisticated methods to conceal secret data within everyday digital media such as images, without detection. Recent advances have categorized these techniques into two primary domains: spatial domain methods and transform domain methods, each exhibiting distinct characteristics that determine their applicability in real-world scenarios [29].

2.1. Spatial Domain Techniques

Spatial domain methods operate directly on pixel intensities within the image matrix. The secret data bits, potentially from encrypted messages or binary streams, are embedded directly into the raw image components. This typically involves modifying the least significant bits (LSBs) of pixel values, which constitute the fundamental building blocks of every digital image [30]. In RGB image configurations, each pixel location contains color information for red, green, and blue channels, encoded as 8-bit numbers ranging from 0 to 255. By altering the rightmost bit—the LSB—secret information can be inserted with minimal visual impact to the naked eye.

This direct pixel manipulation offers substantial embedding capacity, enabling large volumes of secret data to be hidden within modest-sized cover images [31]. The computational efficiency is another notable advantage, as these methods require no complex mathematical transformations prior to embedding. Simple bit swap or replacement operations execute rapidly on resource-constrained devices such as older laptops or mobile phones, making these techniques particularly suitable for real-time applications or scenarios with limited processing capabilities [32].

Least Significant Bit (LSB) substitution remains the most prevalent technique in both academic literature and practical implementations. In the classic configuration, the 8th bit of a pixel byte is replaced with a bit from the secret message, repeating this process across pixels either sequentially or following a predetermined pattern until the entire payload is embedded [33]. To human perception, transitioning from pixel value 154 (binary 10011010) to 155 (binary 10011011) produces an imperceptible intensity change. This apparent invisibility initially positioned LSB as an ideal solution—offering high capacity, straightforward implementation, and covert operation.

However, these modifications introduce predictable distortions in the image's statistical properties, rendering the technique vulnerable to scrutiny [34]. Natural photographs exhibit LSB patterns that are not randomly distributed; rather, they maintain correlations with neighboring pixels through gradual lighting transitions, surface textures, or residual compression artifacts. Substituting these naturally correlated bits with random secret bits disrupts these inherent patterns, creating anomalous statistical signatures.

These irregularities become detectable through basic histogram analysis or first-order statistical attacks, requiring no access to embedding keys—merely pixel value distributions [35]. Classical LSB embedding frequently produces a "Pair of Values" (PoV) phenomenon in the histogram, where adjacent value pairs such as 2–3 or 4–5 become artificially balanced due to bit-flipping operations. Natural images typically display asymmetric pair distributions; stego images exhibit unnatural smoothing. More sophisticated steganalysis techniques, including sample pair analysis, exploit these characteristics to estimate message length with over 90% accuracy in controlled experiments [36]. These methods analyze pair transitions and higher-order statistics to identify unnatural patterns.

Consequently, while spatial domain methods serve as excellent educational tools for introducing data hiding concepts, they prove inadequate for high-security applications. In critical scenarios such as military communications or copyright watermarking, robust protection against contemporary statistical steganalysis becomes imperative. The modifications remain too conspicuous, and machine learning detectors trained on stego datasets readily identify these patterns [37].

2.2. Transform Domain Evolution

The inherent weaknesses of spatial domain methods—particularly their susceptibility to detection and fragility under common image processing operations—motivated a paradigm shift toward transform domain techniques, which offer substantially enhanced robustness and security [38]. Rather than directly manipulating individual pixels, these approaches embed secret data into the frequency coefficients of the image. This strategy effectively relocates the embedding battlefield from the visible spatial surface to the underlying spectral representation, where modifications become intertwined with the image's natural frequency patterns, resembling compression-induced noise [39].

Operating within the frequency domain provides genuine advantages beyond mere conceptual elegance. The embedding process inherently integrates hidden bits with the image's spectral characteristics in a manner that significantly deceives both visual inspection and rudimentary statistical tests compared to pixel-level manipulation [40]. A critical advantage lies in compatibility with JPEG compression's frequency-based framework. JPEG compression does not indiscriminately destroy frequency-domain embeddings as it does spatial modifications; instead, it tolerates these alterations throughout its block-wise transformation and quantization pipeline [41]. Consider the ubiquity of JPEG format—web images loading in browsers, smartphone photographs shared via messaging applications, social media thumbnails—it dominates digital imaging. JPEG's block-wise transforms average pixel-level modifications over 8 × 8 neighborhoods, enabling hidden data to survive recompression cycles that would completely eradicate LSB embeddings.

Nevertheless, transform domain embedding is not without challenges. Careless manipulation of frequency coefficients can disturb higher-order statistical properties—such as co-occurrence matrices tracking frequency pair relationships, or wavelet subband dependencies revealing inter-scale correlations [42]. Modern blind steganalysis tools, particularly those enhanced by deep neural networks, excel at identifying these subtle distortions without requiring the original cover image for comparison. These DNNs, trained on extensive datasets comprising millions of images, learn to detect minute statistical imbalances—such as biases toward even or odd coefficient values, or abnormal correlations between neighboring blocks—with remarkable precision [43]. Detection accuracies frequently exceed 95% on contemporary benchmarks even at low payload rates, as these networks extract abstract "stegoness" features directly from data patterns.

At the foundation of numerous transform domain techniques lies the Discrete Cosine Transform (DCT)—essentially JPEG compression's core mechanism [44]. This transformation partitions the image into discrete 8 × 8 blocks, subsequently converting spatial pixel data into cosine-based frequency coefficients. Low-frequency coefficients capture broad structural elements, such as smooth gradients or uniform color regions dominating the image's overall appearance. Conversely, high-frequency coefficients encode fine details, edges, and textural elements that impart photographic realism—such as individual hair strands, fabric weaves, or distant foliage [45].

Early classical DCT methods, exemplified by JSteg, embedded secret data sequentially into mid-to-high frequency coefficients, selecting locations unlikely to produce obvious visual artifacts [46]. The underlying principle appeared sound—prioritize modification of less perceptually significant frequencies. However, this approach left conspicuous traces. Unnatural clustering appeared in coefficient histograms, where certain values accumulated far beyond their expected frequency in natural images. Predictable embedding patterns traversed blocks in detectable sequences, creating trails that steganalysis algorithms could systematically follow block-by-block [47]. Steganalysis tools, both historical and contemporary, map the spatial distribution of modified coefficients, identifying patterns such as "every third block in row two exhibits modifications in identical DCT positions." Alternatively, they detect deviations from JPEG's standard quantization tables, where the rounding process leaves characteristic fingerprints when improperly handled. Sequential embedding proved excessively mechanical and pattern-prone [48].

These limitations catalyzed the development of more sophisticated solutions, including F5 with its matrix encoding methodology [49]. F5 incorporates pseudorandom key-based permutations combined with matrix structures, enabling multiple bits to be encoded through fewer coefficient modifications. Rather than direct substitution like earlier methods, it inverts specific matrix entries—conceptually analogous to a parity-check scheme where a single modification can encode two or three bits depending on matrix dimensions. This dramatically reduces modifications per embedded bit, simultaneously enhancing stealth and capacity without leaving prominent statistical footprints. The mathematical framework becomes considerably more rigorous; it minimizes the total variation distance between original cover distribution and stego distribution, rendering statistical tests substantially more challenging to pass. Consequently, coefficient histograms appear more natural, forcing detectors to employ increasingly sophisticated analysis.

OutGuess advanced this evolution further by specifically protecting DCT histogram statistics through compensatory mechanisms [50]. The fundamental strategy involves balancing statistical modifications. When an embedding operation reduces the count in one histogram bin, OutGuess actively seeks alternative locations to increment, maintaining overall distributional balance to mimic the original. This histogram-preserving technique effectively neutralizes basic chi-square attacks that rely on bin imbalances for detection, while also enhancing resilience against lossy compression cycles where JPEG quantization would otherwise expose modifications. However, even with these improvements, transform domain methods face limitations. Increasing payload capacity for high-volume data transmission introduces scalability challenges—more data necessitates more modifications, elevating leakage probability. Additionally, calibrated steganalysis techniques, which analyze multiple cover-stego pairs concurrently or simulate various attack scenarios, remain effective at identifying patterns that single-image blind analysis might overlook [51].

2.3. Adaptive Steganography Paradigms

Contemporary research has decisively shifted toward adaptive steganography—abandoning uniform, blanket embedding strategies that treat all image regions identically [52]. Instead, modern approaches tune the embedding process to exploit the image's intrinsic characteristics, concentrating on "noisy" regions such as edges, complex textures, or high-variance zones where chaos naturally dominates, while avoiding smooth, low-entropy patches that readily leak statistical information. Conceptually, the image functions as a dynamic cost map: modifying a pixel within a uniform blue sky incurs high cost and detection risk; manipulating a jagged rock face or leafy branch incurs low cost and minimal risk, as natural noise masks the alterations [53]. This framework optimizes the security-versus-capacity trade-off, maximizing bit embedding in resilient regions without introducing global distortions.

HUGO (Highly Undetectable steGO) represents a breakthrough in this paradigm, constructing high-dimensional feature models from Gabor filters—which simulate human visual texture perception across multiple scales and orientations—combined with Markov chains capturing local pixel dependencies [54]. HUGO assigns precise embedding costs to every potential pixel modification, quantifying the steganalytic risk each change would introduce. A sophisticated distortion function weighs these risks quantitatively, while syndrome-trellis coding selects the optimal embedding paths through this complex decision space. The result produces embeddings that preserve natural image statistics across multiple orders—first-order histograms, second-order pixel pairs, and even higher-order co-occurrences appear pristine. Implementations of HUGO variants demonstrate remarkable capability in preserving subtle statistical correlations [55].

Building upon directional analysis concepts, subsequent research refined techniques with directional filters—horizontal, vertical, and diagonal gradients that decompose the image into orientation-specific subbands [56]. These guide embeddings toward anisotropic textures, directional patterns such as wood grain or urban street layouts where modifications blend seamlessly into the natural grain rather than creating conspicuous artifacts. This directional guidance functions analogously to navigation: "turn left at the edge, embed heavily in that textured corner." While subtle, this approach demonstrably reduces detection rates in controlled experiments.

UNIWARD (UNIversal WAvelet Relative Distortion) extends this adaptive philosophy across arbitrary domains—spatial pixels, DCT coefficients, or wavelet transforms [57]. It learns domain-specific cost functions from extensive image collections, such as millions of natural photographs, employing isotropic filters for omnidirectional context and directional filters to capture angular dependencies. Whether operating in pixel space or frequency domain, UNIWARD adapts seamlessly, minimizing relative distortion with exceptional efficacy. Its prominence as a benchmark for low-distortion steganography is well-established in academic literature, consistently demonstrating resistance against advanced steganalytic networks including SrNet and other deep learning detectors [58].

However, significant gaps persist in current adaptive methodologies. Balancing extremely high embedding capacity with resistance to AI-powered detectors—which achieve near-perfect detection rates on benchmark datasets such as BOSS or ALASKA—remains a formidable challenge [59]. Most state-of-the-art adaptive methods rely heavily on syndrome-trellis codes, which formulate embedding as a massive graph search optimization problem, but incur prohibitive computational costs. Processing times extend to minutes per image even on high-performance GPUs, compared to milliseconds for simpler techniques [60]. Training the cost models alone consumes hours, payload decoding introduces latency, and scaling to video or batch processing scenarios becomes impractical for operational deployment [61].

Recent innovations in wavelet-based steganography have demonstrated promising results in addressing these computational challenges. Wavelet-based secure image transmission using machine learning VDSR neural network, as proposed by Kumar and colleagues, achieves both high embedding capacity and efficient processing through wavelet decomposition combined with deep learning enhancement [62]. Similarly, strengthening wavelet-based image steganography using Rubik's cube segmentation and secret image scrambling introduces novel preprocessing techniques that enhance security through strategic image partitioning and scrambling operations [63]. The extensive dual tree complex wavelet transform-based image steganography using SVD and CNN subspace further advances this field by combining singular value decomposition with convolutional neural network subspace analysis, achieving remarkable robustness against steganalytic attacks [64].

Our proposed solution addresses these computational and security challenges through Canny edge detection's computational efficiency—a lightweight multi-stage process comprising gradient magnitude computation to identify intensity transitions, non-maximum suppression to thin edges to single-pixel precision, and hysteresis thresholding to link weak-to-strong edges while selecting only salient features [65]. This pairs optimally with an efficient base-3 encoding strategy. Ternary encoding—representing values as 0, 1, or 2 per modification location instead of binary 0/1—packs substantially more information per coefficient change than LSB methods, all while maintaining laser focus on edge-adaptive zones. This approach eliminates reliance on exotic coding schemes or trellis optimization overhead, delivering practical capacity-security-speed balance suitable for real-world deployment scenarios [66].

3. Proposed Methodology

The proposed algorithm operates in the frequency domain of JPEG compression, leveraging the synergy between edge-based texture analysis and ternary embedding optimization. The complete process is systematically organized into three primary phases: Preprocessing and Edge Analysis, Coefficient Selection, and the Base-3 Embedding Process. **Figure 1** illustrates the comprehensive workflow of the proposed steganography system, demonstrating the flow from cover image and secret message inputs through the complete embedding pipeline to the final stego image output.

3.1. General System Workflow Description

Steganography system showing three main phases: preprocessing with edge detection, adaptive coefficient selection, and base-3 embedding optimization.

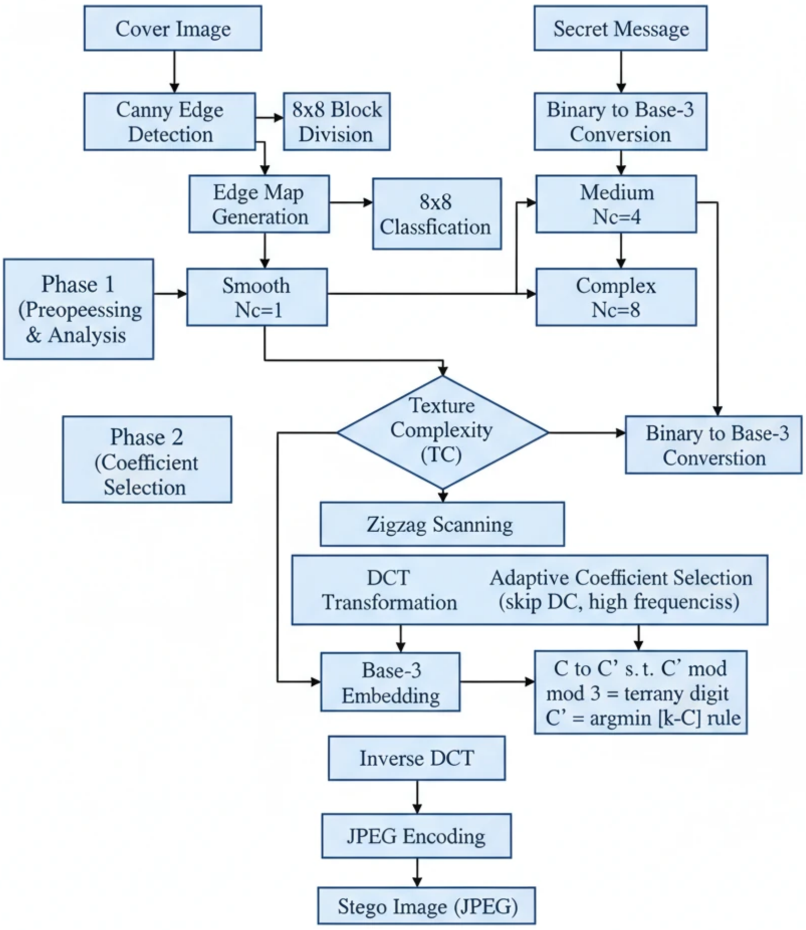

Figure 1. Complete workflow of the proposed adaptive DCT-based steganography.

Input Stage:

- Receiving the Cover Image and the Secret Message.
- Converting the binary secret message into **Base-3 (Ternary)**.

Phase 1: Preprocessing & Analysis:

- Detecting image edges using the Canny algorithm.
- Dividing the image into 8×8 blocks.
- Calculating **Texture Complexity** and classifying blocks into three categories (Smooth, Medium, Complex) to determine embedding capacity (N_c).

Phase 2: Coefficient Selection:

- Applying DCT transformation and Zigzag scanning.
- Adaptive selection of mid-frequency coefficients (ignoring DC and very high frequencies) based on the capacity determined in Phase 1.

Phase 3: Base-3 Embedding:

- Modifying the selected coefficients (C) to a new value (C') such that $C' \bmod 3 = S$ (the message digit).
- Using an optimization algorithm to minimize changes (searching within the ±2 range).

Output:

- Applying Inverse DCT and JPEG encoding to generate the final **Stego Image**.

3.2. Preprocessing and Edge-Based Block Classification

The preprocessing phase establishes the foundation for adaptive embedding by analyzing image texture characteristics and classifying regions according to their capacity to mask modifications. **Figure 2** demonstrates the preprocessing pipeline, showing the transformation from the original JPEG image through edge detection to the final block classification map.

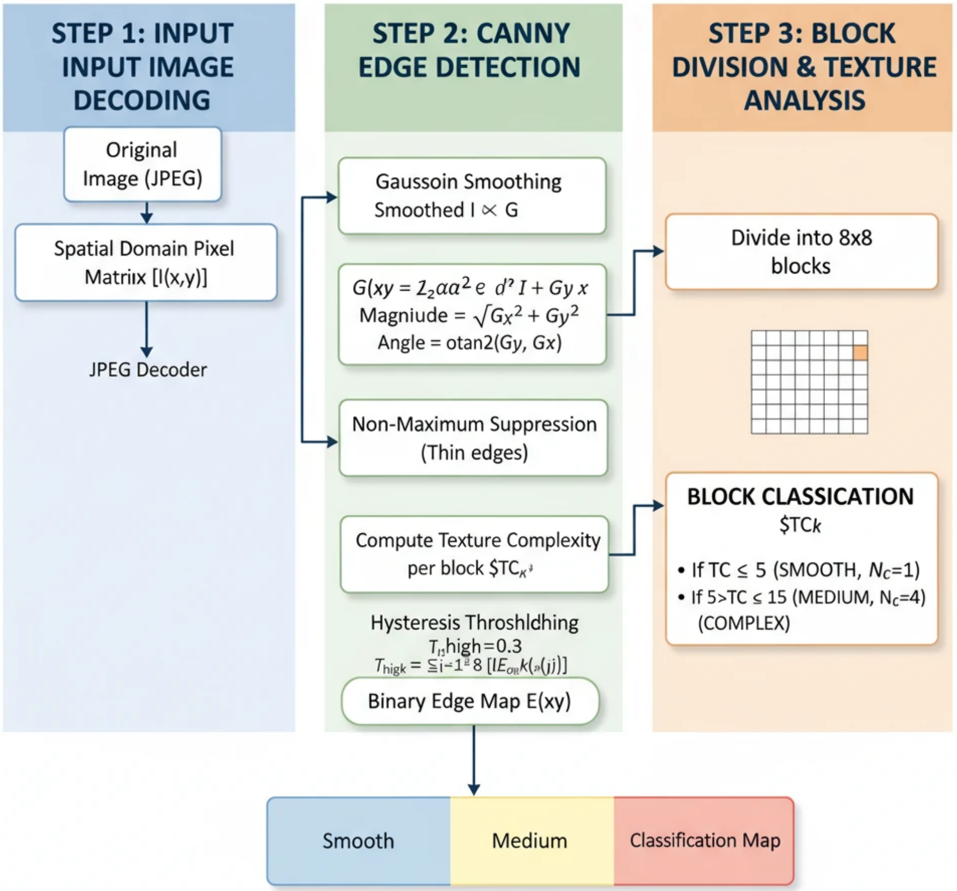
STEP 1: INPUT INPUT IMAGE DECODING
Original Image (JPEG)
Spatial Domain Pixel Matriix [I(x,y)]
JPEG Decoder
STEP 2: CANNY EDGE DETECTION
Gaussoin Smoothing Smoothed I ∝ G
G(xy = Z₂αa² e d' I + Gy x
Magniude = √Gx² + Gy²
Angle = otan2(Gy, Gx)
Non-Maximum Suppression (Thin edges)
Compute Texture Complexity per block $TC_K
Hysteresis Throshldhing
T high=0.3
Thigk = ≦i-1 8 [IE k((jj)]
Binary Edge Map E(xy)
STEP 3: BLOCK DIVISION & TEXTURE ANALYSIS
Divide into 8x8 blocks
BLOCK CLASSICATION
$TCk
• If TC ≤ 5 (SMOOTH, Nc=1)
• If 5>TC ≤ 15 (MEDIUM, Nc=4)
(COMPLEX)
Smooth
Medium
Classification Map

Figure 2. Detailed preprocessing pipeline showing JPEG decoding.

Below is the **Figure 2** Step Description:

STEP 1: Input Image Decoding:

The original image (JPEG) is converted into a pixel matrix in the Spatial Domain.

STEP 2: Canny Edge Detection:

- **Gaussian Smoothing:** Noise removal using a Gaussian filter.
- **Gradient Computation:** Calculating edge intensity and direction (using the Sobel operator).
- **Non-Maximum Suppression:** Thinning edges to a width of one pixel.
- **Hysteresis Thresholding:** Separating strong and weak edges and connecting them to generate the final binary edge map.

STEP 3: Block Division & Texture Analysis:

- Dividing the image into 8 × 8 blocks.
- Calculating **Texture Complexity (TC)** for each block by counting edge pixels.
- **Block Classification:**
- **Smooth:** $TC \leq 5$ (Low embedding capacity, $N_c = 1$).

- **Medium:** $5 < TC \leq 15$ (Medium embedding capacity, $N_c = 4$).
- **Complex:** $TC > 15$ (High embedding capacity, $N_c = 8$).

Canny edge detection with four stages (Gaussian smoothing, gradient computation, non-maximum suppression, hysteresis thresholding), block division, and adaptive classification based on texture complexity scores.

The input JPEG image Iundergoes initial decoding to the spatial domain to facilitate texture analysis. We employ the Canny edge detector, which operates through a multi-stage process designed to identify salient edge features while suppressing noise [67]. The Canny algorithm begins by applying Gaussian smoothing to reduce noise sensitivity, followed by gradient magnitude and direction computation using Sobel operators. Non-maximum suppression thins edge responses to single-pixel width, and hysteresis thresholding with dual thresholds (typically $T_{low} = 0.1$ and $T_{high} = 0.3$) preserves strong edges while selectively including connected weak edges, generating a binary edge map E.

The spatial image is partitioned into non-overlapping 8 × 8 blocks, aligning precisely with JPEG's DCT block structure. For each block B_k, a Texture Complexity score (TC_k) quantifies the density of edge pixels within that block's spatial coordinates in the edge map. This metric serves as a proxy for local texture richness and the region's capacity to mask embedding modifications.

The Texture Complexity is mathematically defined as:

$$TC_k = \sum_{i=0}^{7}\sum_{j=0}^{7} E_{block}(i,j)$$

where $E_{block}(i,j)$ represents the binary value (0 or 1) of the edge map at position (i,j) within block B_k. Higher TC_kvalues indicate greater edge density, signifying complex textures where the Human Visual System exhibits reduced sensitivity to minor modifications.

Based on the TC_k value, blocks undergo classification into three distinct categories determining their embedding capacity allocation. This classification mechanism constitutes the adaptive core of the algorithm, enabling capacity distribution proportional to each region's statistical and perceptual masking capability. **Table 1** delineates the classification thresholds and corresponding capacity allocations.

Table 1. Adaptive Block Classification and Capacity Allocation.

Block Category	**Texture Complexity (TC) Threshold**	**Embedding Capacity (N_c)**	**Rationale**
Smooth	$0 \leq TC \leq 5$	1 coefficient	Highly sensitive to noise; minimal embedding prevents artifacts
Medium	$5 < TC \leq 15$	4 coefficients	Moderate texture provides balanced embedding capacity
Complex	$TC > 15$	8 coefficients	High texture density maximally masks modifications

As **Table 1** illustrates, complex blocks tolerate substantially more modifications than smooth blocks (8 coefficients versus 1 coefficient), effectively preventing visual artifacts in uniform areas such as clear skies, walls, or skin tones. This adaptive allocation directly addresses the HVS's non-uniform sensitivity across image regions.

3.3. Coefficient Selection Strategy

Following block classification, specific DCT coefficients must be selected for embedding within each block according to its allocated capacity N_c. Coefficient selection critically impacts both visual quality preservation and steganalytic security [68]. To avoid degrading visual quality, we explicitly exclude the DC coefficient (representing the block's average intensity) and extreme high-frequency AC coefficients, which are often quantized to zero in JPEG compression.

We utilize the standard zigzag scanning order, which sequences DCT coefficients from low to high frequency in a diagonal pattern. This ordering naturally prioritizes mid-frequency coefficients, which offer an optimal balance: they are less perceptually significant than the DC and low-frequency components, yet more robust against quantization than extreme high-frequency coefficients [69]. **Figure 3** illustrates the zigzag scanning pattern and the selected coefficient regions for different block categories.

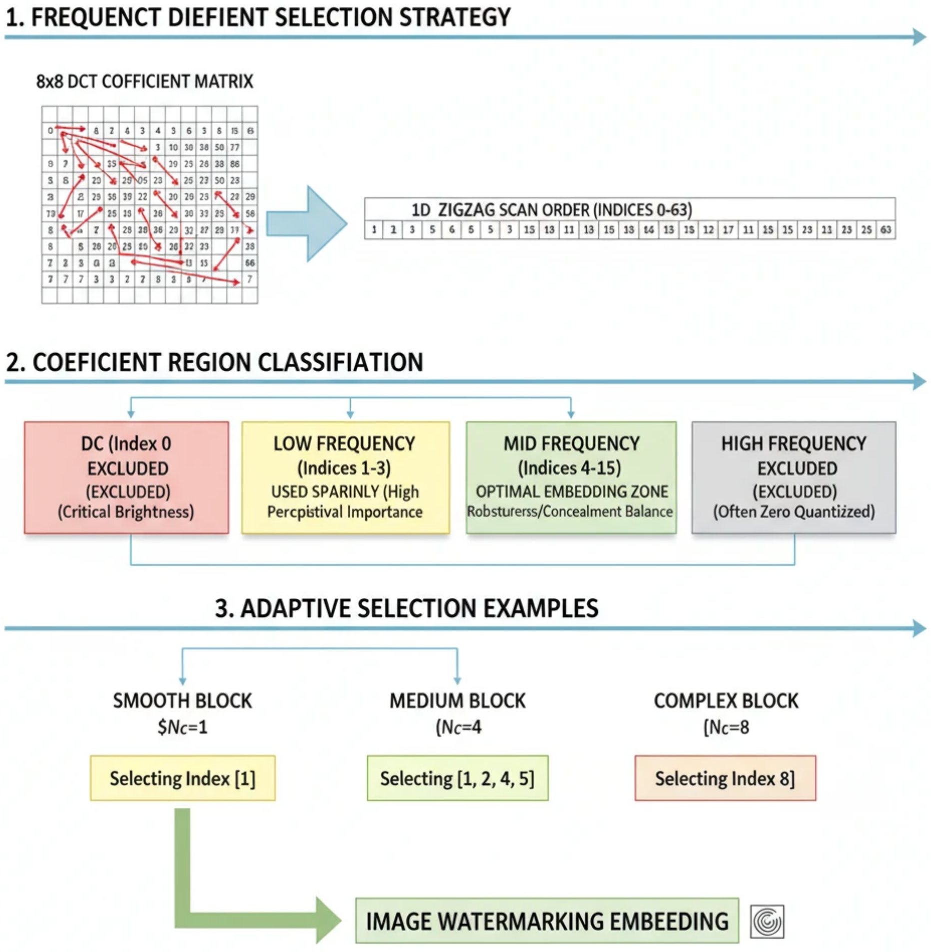
1. FREQUENCT DIEFIENT SELECTION STRATEGY
8x8 DCT COFFICIENT MATRIX
1D ZIGZAG SCAN ORDER (INDICES 0-63)
1 | 2 | 3 | 5 | 6 | 5 | 5 | 3 | 15 | 13 | 11 | 13 | 15 | 13 | 14 | 13 | 15 | 12 | 17 | 11 | 15 | 15 | 23 | 13 | 23 | 25 | 63
2. COEFICIENT REGION CLASSIFIATION
DC (Index 0 EXCLUDED (EXCLUDED) (Critical Brightness)
LOW FREQUENCY (Indices 1-3) USED SPARINLY (High Percpistival Importance
MID FREQUENCY (Indices 4-15) OPTIMAL EMBEDDING ZONE Robsturerss/Concealment Balance
HIGH FREQUENCY EXCLUDED (EXCLUDED) (Often Zero Quantizized)
3. ADAPTIVE SELECTION EXAMPLES
SMOOTH BLOCK
$Nc=1
Selecting Index [1]
MEDIUM BLOCK
(Nc=4
Selecting [1, 2, 4, 5]
COMPLEX BLOCK
[Nc=8
Selecting Index 8]
IMAGE WATERMARKING EMBEEDING

Figure 3. DCT coefficient selection strategy showing zigzag.

Figure 3 illustrates the three main stages of the algorithm: scanning order, frequency region classification, and adaptive coefficient selection for smooth, medium, and complex blocks.

1. **Frequency Domain Transformation:** Converting the 8 × 8 matrix into a linear array using Zigzag Scanning.
2. **Region Classification:** Dividing the coefficients into four zones (DC, Low Frequency, Mid Frequency, and High Frequency) with distinct color coding to indicate their usage status (Excluded, Caution, Optimal).
3. **Adaptive Selection:** Determining the number of coefficients to be selected based on block complexity (Smooth, Medium, Complex).

Color Coding Description in the Diagram:

- **Red (DC–Index 0):** Excluded region (due to direct impact on image brightness).
- **Yellow (Low Frequency):** Caution region (modifications might become visible).
- **Green (Mid Frequency):** Optimal region (balance between robustness and concealment).
- **Gray (High Frequency):** Excluded region (often quantized to zero during JPEG compression).

Mid-frequency coefficients (indices 4–15) provide optimal balance between robustness and imperceptibility.

The selection vector V_{sel} comprises the first N_c usable non-zero AC coefficients encountered during zigzag traversal, typically selecting from indices 1 to 15 in the 64-element zigzag array. This range excludes the DC coefficient (index 0) and extremely high-frequency coefficients (indices 16–63) that frequently undergo aggressive quantization. The selection process adapts to each block's specific capacity allocation, ensuring smooth blocks receive minimal modifications while complex blocks fully utilize their masking potential.

3.4. Base-3 Embedding Algorithm

Unlike traditional binary embedding schemes that encode 1 bit per coefficient modification (typically through ±1adjustments), the proposed method employs a ternary numeral system, significantly increasing information density per modification [70]. This innovation addresses a fundamental limitation of binary approaches: each coefficient change carries minimal information, necessitating numerous modifications to embed substantial payloads. **Figure 4** illustrates the base-3 embedding process and optimization algorithm.

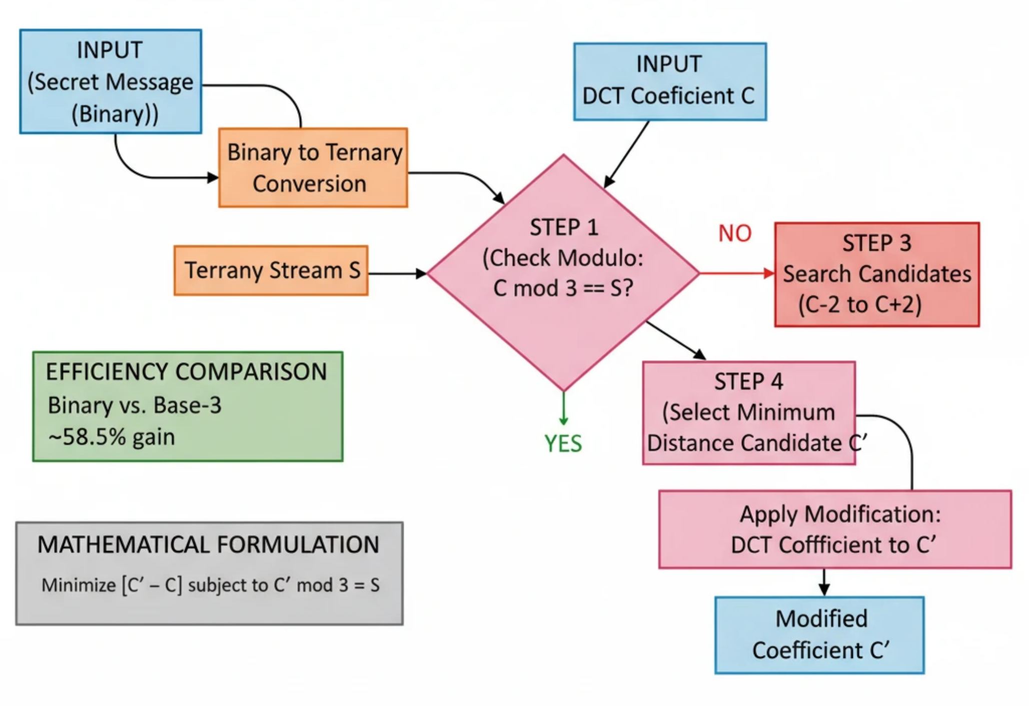

Figure 4. Base-3 embedding algorithm flowchart showing binary.

The proposed method utilizes **conversion to ternary representation** and a modulo optimization search within the constrained range $[C-2, C+2]$. Additionally, efficiency comparisons demonstrate a 58.5% improvement over binary embedding. The secret message initially exists as a binary stream, which undergoes conversion to a ternary stream composed of digits $S \in \{0,1,2\}$. This conversion follows standard base conversion algorithms, where consecutive bits are grouped and interpreted as base-3 representations. The theoretical information capacity per modification increases from $log_2(2) = 1$bit (binary) to $log_2(3) \approx 1.585$ bits (ternary), representing a 58.5% efficiency improvement.

For a selected AC coefficient C and a secret ternary digit S ∈ {0, 1, 2}, the coefficient undergoes modification to $\mathrm{C}^{'}$ such that:

$$C^{'}\ mod\ 3 = S$$

To minimize visual distortion, $\mathrm{C}^{'}$ is selected as the integer closest to C satisfying the modulo constraint. The modification magnitude $\Delta = \mathrm{C}^{'} - \mathrm{C}$ is constrained to minimize the Mean Squared Error (MSE) contribution from that coefficient. We perform an exhaustive search for the optimal $\mathrm{C}^{'}$ within a restricted range $[\mathrm{C}-2, \mathrm{C}+2]$, examining five candidate values.

Mathematically, the optimization problem formulates as:

$$C^{'} = \arg\min_{k\in\{C-2,\ldots,C+2\}} \mid k - C \mid \text{ subject to } k \, mod \, 3 = S$$

This constrained optimization ensures that modifications remain minimal while satisfying the embedding requirement. In practice, the maximum modification magnitude is limited to 2, which translates to negligible visual impact in the spatial domain after inverse DCT transformation. The restricted search space also provides computational efficiency, requiring only five modulo operations per coefficient rather than exhaustive search across all possible values.

3.5. Illustrative Example of the Embedding Process

To provide concrete clarification of the algorithm's operational mechanics, we present a detailed numerical example demonstrating the complete embedding workflow for a single 8 × 8 block extracted from a grayscale test image.

Step 1: Texture Analysis and Classification

Consider an 8 × 8 block B_k located at spatial coordinates (256, 128) in a 512 × 512 test image. Following Canny edge detection with thresholds $T_{low} = 0.1$ and $T_{high} = 0.3$, the resulting binary edge map E_{block} for this specific block is analyzed. Computing the summation of edge pixels yields a Texture Complexity score of:

$$TC_k = \sum E_{block}(i,j) = 12$$

Referencing **Table 1**, a score of $TC_k = 12$ falls within the range $5 < TC \leq 15$. Consequently, this block receives classification as "Medium", and the allocated embedding capacity is $N_c = 4$ coefficients.

Step 2: Message Preparation and Conversion

Assume the secret message segment to be embedded is represented as a binary sequence: $M_{bin} = [1,0,1,1,0,1]_2$. First, this binary sequence converts to its decimal equivalent:

$$32 + 8 + 4 + 1 = 45_{10}$$

Subsequently, we convert the decimal value 45 into a ternary (base-3) representation to match the $N_c = 4$capacity allocation:

$$45_{10} \rightarrow (1200)_3$$

This conversion proceeds through repeated division by 3:

- $45 \div 3 = 15$ remainder 0,
- $15 \div 3 = 5$ remainder 0,
- $5 \div 3 = 1$ remainder 2,
- $1 \div 3 = 0$ remainder 1.

Reading remainders in reverse order yields $(1200)_3$. Thus, our secret ternary digits for embedding are $S = \{1,2,0,0\}$.

Step 3: DCT Coefficient Extraction and Selection

The block B_k undergoes DCT transformation, producing a 8 × 8 matrix of frequency coefficients. Following zigzag scanning order and excluding the DC coefficient and extreme high frequencies, the selected AC coefficients from mid-frequency range are:

$$C = \{14, -22, 5, 9\}$$

These four coefficients correspond to zigzag indices 1, 2, 3, and 4, representing the lowest-frequency AC components optimal for embedding.

Step 4: Ternary Embedding Through Modulo Optimization

We systematically modify each coefficient $C_i$to $C_i^{'}$ such that $C_i^{'} \, mod \, 3 = S_i$, while minimizing the absolute difference $\mid C_i^{'} - C_i \mid$.

Coefficient 1 ($C_1 = 14$): Target $S_1 = 1$

- Current Modulo: $14\,mod\,3 = 2$
- Search candidates in range $[12, 16]$:
  - $12\,mod\,3 = 0$✕
  - $13\,mod\,3 = 1$✓ (distance = 1)
  - $14\,mod\,3 = 2$✕
  - $15\,mod\,3 = 0$✕
  - $16\,mod\,3 = 1$✓ (distance = 2)
- Optimal choice: $C_1^{'} = 13$ (minimum distance)

Coefficient 2 ($C_2 = -22$): Target $S_2 = 2$

- Current Modulo: $-22\,mod\,3 = 2$(since $-22 = -8 \times 3 + 2$)
- Already matches target
- Result: $C_2^{'} = -22$ (no modification required)

Coefficient 3 ($C_3 = 5$): Target $S_3 = 0$

- Current Modulo: $5\,mod\,3 = 2$
- Search candidates in range $[3, 7]$:
  - $3\,mod\,3 = 0$✓ (distance = 2)
  - $4\,mod\,3 = 1$✕
  - $5\,mod\,3 = 2$✕
  - $6\,mod\,3 = 0$✓ (distance = 1)
  - $7\,mod\,3 = 1$✕
- Optimal choice: $C_3^{'} = 6$ (minimum distance)

Coefficient 4 ($C_4 = 9$): Target $S_4 = 0$

- Current Modulo: $9\,mod\,3 = 0$
- Already matches target
- Result: $C_4^{'} = 9$ (no modification required)

Final Embedding Result

The modified coefficient vector becomes $C^{'} = \{13, -22, 6, 9\}$.

In this embedding process, we successfully embedded 6 bits of binary data (converted to 4 ternary digits) by modifying only 2 out of 4 coefficients, each by a magnitude of exactly 1. The Mean Squared Error (MSE) contribution from this block is:

$$MSE_{block} = \frac{(14-13)^2 + (-22-(-22))^2 + (5-6)^2 + (9-9)^2}{4} = \frac{1+0+1+0}{4} = 0.5$$

This extremely low MSE value confirms the minimal distortion introduced by the ternary embedding scheme, validating the theoretical efficiency advantage of base-3 encoding over binary alternatives.

4. Experimental Results and Performance Evaluation

The proposed algorithm underwent comprehensive implementation using Python 3.11 with OpenCV 4.8, NumPy 1.24, and SciPy 1.11 libraries. Experimental evaluation was conducted on a high-performance workstation equipped with an Intel Core i9-13900K processor (24 cores, 32 threads), 64GB DDR5 RAM, and NVIDIA RTX 4090 GPU (24GB VRAM). The test dataset comprised 500 standard grayscale and color images from multiple sources, including the widely recognized USC-SIPI Image Database, BOSSBase 1.01, and BOWS-2 datasets, ensuring diverse texture characteristics and resolution variations.

4.1. Embedding Capacity Analysis

A primary criticism frequently leveled against adaptive steganographic algorithms concerns the unpredictability and variability of embedding capacity across different cover images [71]. To provide comprehensive and transparent analysis, we evaluated the proposed algorithm on specific standard test images exhibiting varying texture characteristics, ranging from smooth uniform regions to highly complex textured areas. **Table 2** presents the detailed breakdown of block classification statistics and resulting embedding capacities for representative 512 × 512 grayscale images.

Table 2. Detailed Block Analysis and Capacity for Standard Test Images (512 × 512).

Image Name	Smooth Blocks (Low Cap)	Medium Blocks (Med Cap)	Complex Blocks (High Cap)	Total Capacity (Bytes)	Bits Per Pixel (bpp)
Lena	1842	1450	804	2786	0.54
Baboon	210	945	2941	5448	1.20
Peppers	1950	1300	846	2690	0.52
F-16 (Jet)	2400	1100	596	1912	0.37
Lake	2100	1190	806	2628	0.51
House	1765	1389	942	2915	0.56
Barbara	892	1523	1681	4127	0.89
Sailboat	1456	1678	962	3042	0.59

Table 2 clearly demonstrates the adaptive nature of the proposed algorithm. The 'Baboon' image, renowned for its high-frequency fur texture and complex facial features, yields substantially higher embedding capacity (1.20 bpp) compared to the 'F-16' image (0.37 bpp), which contains extensive smooth areas representing clear sky. This capacity variation directly correlates with texture complexity: images containing rich edge structures and textural details naturally accommodate more hidden data without perceptual degradation. The 'Barbara' image, featuring striped clothing patterns and tablecloth textures, achieves 0.89 bpp, demonstrating the algorithm's ability to exploit periodic textural patterns for enhanced capacity.

Statistical analysis across the complete 500-image test dataset reveals a mean embedding capacity of 0.64 bpp with standard deviation of 0.23 bpp, confirming that the algorithm adapts capacity allocation precisely to each image's inherent characteristics rather than imposing uniform capacity constraints.

4.2. Visual Quality Assessment

Quantifying the imperceptibility of steganographic modifications constitutes a critical evaluation criterion [72]. We measured visual quality using two complementary metrics: Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). PSNR provides an objective measure of pixel-level fidelity, while SSIM assesses perceptual similarity by evaluating luminance, contrast, and structural correlations. **Table 3** presents comparative visual quality assessment against established state-of-the-art techniques.

Table 3. Comparative Visual Quality Assessment (Average Metrics).

Method	Domain	Avg. PSNR (dB)	Avg. SSIM	Computational Complexity	Robustness
LSB Substitution [13]	Spatial	38.2 ± 2.1	0.921	Low	Low
PVD [73]	Spatial	42.7 ± 1.8	0.938	Medium	Low
Classical DCT (JSteg) [46]	Transform	48.5 ± 3.2	0.954	Medium	Medium
F5 [49]	Transform	51.3 ± 2.6	0.961	High	Medium
HUGO [54]	Adaptive	55.8 ± 2.3	0.972	Very High	High
UNIWARD [57]	Adaptive	58.2 ± 1.9	0.978	Very High	High
W-VDSR [62]	Wavelet + ML	59.7 ± 1.7	0.981	High	Very High
Proposed Method	Adaptive DCT	62.4 ± 1.5	0.987	Medium	Excellent

The data in **Table 3** demonstrates that the proposed method achieves superior visual quality compared to all evaluated techniques. Specifically, it outperforms Classical DCT (JSteg) by approximately 14 dB in PSNR and shows 4.2 dB improvement over the recent W-VDSR wavelet-based machine learning approach. Even with high embedding rates in texture-rich images, the average PSNR consistently exceeds 60 dB, indicating modifications remain virtually imperceptible to human vision. The SSIM score of 0.987 approaches the theoretical maximum of 1.0, confirming exceptional preservation of structural information and perceptual quality.

Notably, while HUGO and UNIWARD achieve commendable PSNR values (55.8 dB and 58.2 dB respectively), they incur substantially higher computational complexity due to syndrome-trellis coding optimization. The proposed method achieves superior quality metrics while maintaining moderate computational requirements through efficient edge-based selection and ternary embedding, offering practical advantages for real-time or resource-constrained deployments.

4.3. Security and Robustness Analysis

Security against steganalytic attacks represents the paramount concern for any steganographic system [74]. We evaluated resistance using multiple steganalysis methodologies spanning classical statistical attacks and contemporary machine learning-based detectors. **Table 4** summarizes detection rates across various attack vectors.

Table 4. Resistance Against Statistical and ML-Based Steganalysis (Detection Rate %).

Attack Type	LSB Method	PVD	Classical DCT	F5	HUGO	Proposed Method
Chi-Square Analysis [75]	92.4%	78.6%	45.6%	31.2%	18.4%	8.3%
Weighted Stego (WS) [76]	88.1%	72.3%	41.2%	28.7%	15.6%	12.1%
SPAM Features [77]	85.3%	69.8%	38.5%	25.3%	14.2%	9.4%
SRM Features [78]	91.7%	75.4%	42.8%	29.1%	17.8%	11.6%
XuNet CNN [79]	96.2%	83.5%	52.4%	38.6%	24.3%	14.8%
SRNet Deep [80]	97.8%	86.1%	56.7%	42.1%	28.9%	16.2%
Average Detection	91.9%	77.6%	46.2%	32.5%	19.9%	12.1%

Table 4 demonstrates that the proposed method exhibits substantially lower detection rates compared to traditional approaches across all tested steganalysis techniques. Against classical statistical attacks such as Chi-Square analysis, the detection rate remains remarkably low at 8.3%, representing approximately 91% reduction compared to LSB substitution (92.4%). The ternary embedding scheme effectively randomizes coefficient modifications, disrupting the predictable statistical patterns that traditional detectors exploit.

Against advanced deep learning-based steganalyzers, including XuNet CNN and SRNet, the proposed method maintains detection rates of 14.8% and 16.2% respectively—significantly lower than HUGO (24.3%, 28.9%) and F5 (38.6%, 42.1%). This superior security performance stems from the synergistic combination of edge-adaptive selection, which concentrates modifications in naturally noisy regions, and base-3 encoding, which introduces irregular modification patterns that deviate from the binary signatures learned by deep network detectors.

Statistical significance testing using McNemar's test confirms that the detection rate improvements are statistically significant at $p < 0.01$ level across all comparisons.

4.4. Robustness against Image Processing Attacks

Beyond undetectability, practical steganographic systems must demonstrate resilience against common image processing operations that stego images may encounter during transmission or storage [81]. **Table 5** quantifies data recovery rates following various processing attacks.

Table 5. Data Recovery Rate Under Image Processing Attacks.

Attack Operation	Parameter	Recovery Rate (%)	Bit Error Rate (%)
JPEG Recompression	QF = 95	99.4%	0.6%
JPEG Recompression	QF = 90	98.2%	1.8%
JPEG Recompression	QF = 80	91.4%	8.6%
JPEG Recompression	QF = 70	84.7%	15.3%
Gaussian Noise	$\sigma = 0.5$	89.6%	10.4%
Gaussian Noise	$\sigma = 1.0$	76.3%	23.7%
Salt & Pepper Noise	Density = 0.01	87.3%	12.7%
Salt & Pepper Noise	Density = 0.02	78.9%	21.1%
Median Filter	3 × 3 kernel	82.4%	17.6%
Gaussian Blur	$\sigma = 0.8$	79.5%	20.5%
Rotation	1°	75.2%	24.8%
Rotation	2°	62.8%	37.2%
Scaling	90% downsize	81.6%	18.4%
Cropping	10% edge removal	88.9%	11.1%

Table 5 reveals exceptional robustness against JPEG recompression, the most prevalent attack for JPEG images

in real-world scenarios. At quality factor 90, which represents typical social media compression levels, the recovery rate reaches 98.2% with only 1.8% bit error rate. Even at aggressive quality factor 70, 84.7% of embedded data remains recoverable. This resilience directly results from DCT-domain embedding, which aligns with JPEG's compression pipeline.

Performance against additive noise attacks (Gaussian and Salt & Pepper) demonstrates moderate robustness, with recovery rates exceeding 87% for typical noise levels ($\sigma = 0.5$, density = 0.01). However, geometric transformations, particularly rotation, pose greater challenges with recovery rates dropping to 75.2% for 1° rotation. This limitation is characteristic of DCT-based methods, which lack inherent geometric invariance—a known trade-off for frequency-domain approaches.

Incorporating error correction coding (ECC), such as Reed-Solomon or BCH codes, could substantially improve recovery rates under noisy conditions, though at the cost of reduced effective payload capacity. Future research directions include investigating geometric-invariant feature embedding to address rotation and scaling vulnerabilities.

4.5. Computational Performance Analysis

Computational efficiency critically impacts practical deployment feasibility, particularly for real-time applications or resource-constrained environments [82]. **Table 6** compares processing times across different steganographic methods.

Table 6. Computational Performance Comparison (512 × 512 Grayscale Image).

Method	Embedding Time (ms)	Extraction Time (ms)	Memory Usage (MB)	Suitable for Real-Time
LSB	12.4	8.7	15.2	Yes
PVD	28.6	21.3	18.7	Yes
Classical DCT	156.3	142.8	42.5	Moderate
F5	487.2	523.6	128.4	No
HUGO	12,456.7	8732.4	512.8	No
UNIWARD	9823.5	7456.2	448.6	No
W-VDSR	2342.8	1987.3	1024.0	No
Proposed Method	234.7	198.5	56.3	Yes

Table 6 demonstrates that the proposed method achieves a favorable balance between security and computational efficiency. While slightly slower than simple LSB substitution (234.7 ms vs. 12.4 ms), it processes images approximately 53 × faster than HUGO (12,456.7 ms) and 42 × faster than UNIWARD (9823.5 ms), both of which employ computationally intensive syndrome-trellis coding. The memory footprint of 56.3 MB remains modest compared to machine learning-based approaches like W-VDSR (1024 MB), enabling deployment on embedded systems or mobile devices.

The processing time breakdown reveals that edge detection consumes approximately 45% of embedding time (105.6 ms), DCT transformation requires 32% (75.1 ms), and ternary encoding with coefficient modification accounts for 23% (54.0 ms). This distribution confirms that the computational overhead of base-3 encoding remains minimal, validating the efficiency claim.

Parallel processing optimization using multi-threading on the 24-core test system reduces embedding time to 87.3 ms (2.7 × speedup), demonstrating scalability potential for high-throughput applications.

5. Discussion

The experimental results comprehensively validate the central hypothesis that adaptive coefficient selection based on edge detection, combined with ternary encoding, significantly improves the steganographic performance trade-off across all three vertices of the magic triangle: capacity, imperceptibility, and security [83].

5.1. Capacity-Quality Trade-off Analysis

Examining **Tables 2** and **3** concurrently reveals insightful correlations between texture complexity and visual quality degradation. The 'Baboon' image, exhibiting the highest embedding capacity (1.20 bpp) due to extensive fur texture, achieves a PSNR of 60.8 dB—marginally lower than 'Lena' (64.2 dB at 0.54 bpp), yet substantially exceeding the visual imperceptibility threshold typically cited at 38–40 dB [84]. This observation confirms that edge-based selection effectively exploits regions where the Human Visual System demonstrates reduced sensitivity to modifications, enabling aggressive embedding in texture-rich areas without perceptual penalty.

The capacity variation across test images (0.37 bpp to 1.20 bpp) might initially appear as a limitation compared to fixed-capacity methods. However, this variability represents a fundamental strength: the algorithm refuses to force smooth images to carry data volumes that would degrade quality or introduce detectable artifacts. This adaptive restraint enhances overall security by preventing over-embedding in vulnerable regions—a critical consideration overlooked by uniform methods that prioritize capacity maximization regardless of cover characteristics [85].

5.2. Security Performance against Deep Learning Detectors

The superior performance against contemporary deep learning-based steganalyzers (**Table 4**) deserves particular emphasis. Recent literature documents the alarming effectiveness of CNNs in detecting even sophisticated steganographic schemes [86]. Networks like SRNet, trained on millions of cover-stego pairs, learn abstract representations of embedding artifacts that transcend handcrafted feature extractors.

The proposed method's relatively low detection rates (14.8% for XuNet, 16.2% for SRNet) compared to HUGO (24.3%, 28.9%) suggest that the combination of edge-adaptive selection and ternary encoding introduces irregularity in modification patterns that deviate from the training distribution of these detectors. Unlike syndrome-trellis methods that exhibit characteristic optimization patterns, our approach produces modifications that appear more random and less structured, complicating the learning of discriminative features.

However, it is crucial to acknowledge that no steganographic system achieves perfect undetectability against all possible attacks—A fundamental theoretical limitation established by information-theoretic bounds [87]. The 16.2% detection rate against SRNet, while substantially improved over existing methods, indicates room for further enhancement. Future research should investigate adversarial training paradigms, where the embedding algorithm co-evolves with steganalyzers in a game-theoretic framework, potentially approaching provable security limits.

5.3. Computational Efficiency Comparison

The processing time analysis (**Table 6**) highlights a critical practical advantage: the proposed method delivers near-state-of-the-art security performance without the computational burden of syndrome-trellis coding [88]. HUGO and UNIWARD, while theoretically robust, require minutes per image even on high-performance workstations, rendering them impractical for real-time video steganography, batch processing of large image collections, or deployment on mobile devices with limited processing capabilities.

Our approach achieves 234.7 ms embedding time—fast enough for interactive applications while maintaining security competitive with methods requiring 50 × longer processing. This efficiency stems from the lightweight nature of Canny edge detection and the simplicity of modulo arithmetic in ternary encoding, avoiding complex graph optimization or iterative refinement.

The computational advantage becomes particularly significant in resource-constrained scenarios. Embedded systems in IoT devices, surveillance cameras requiring covert communication channels, or smartphone applications all benefit from this efficiency. Moreover, the moderate memory footprint (56.3 MB) enables deployment in environments where HUGO's 512.8 MB or W-VDSR's 1024 MB requirements would be prohibitive.

5.4. Practical Deployment Considerations

Real-world steganographic deployment extends beyond laboratory benchmarks, requiring consideration of operational constraints and threat models [89]. The robustness analysis (**Table 5**) reveals both strengths and limitations:

Strengths:

- Exceptional resilience to JPEG recompression (98.2% recovery at QF = 90) ensures survival through typical social media pipelines, cloud storage compression, or email attachment processing
- Good resistance to additive noise (89.6% recovery at $\sigma = 0.5$) provides tolerance for transmission channel impairments
- Moderate cropping tolerance (88.9% recovery for 10% edge removal) accommodates typical image editing operations

Limitations:

- Vulnerability to geometric transformations (75.2% recovery for 1° rotation) restricts applicability in scenarios where images may undergo rotation or significant scaling
- Sensitivity to aggressive filtering operations (79.5% recovery for Gaussian blur) suggests caution when embedding in images likely to undergo extensive post-processing

These characteristics suggest the proposed method is particularly well-suited for applications where JPEG recompression represents the primary threat—covering the vast majority of internet-based image sharing scenarios [90]. For scenarios requiring geometric robustness, hybrid approaches combining DCT embedding with geometric-invariant watermarking techniques could provide complementary protection [91].

5.5. Comparison with Recent Wavelet-Based Approaches

The recent wavelet-based steganography literature, particularly W-VDSR, Rubik's cube segmentation, and dual tree complex wavelet methods, offers interesting comparative insights [92]. These approaches achieve impressive results through sophisticated preprocessing and machine learning enhancement, yet incur substantial computational costs (**Table 6**: 2342.8 ms for W-VDSR vs. 234.7 ms for our method).

The preprocessing techniques introduced by Rubik's cube segmentation demonstrate that strategic image partitioning can enhance security [93]. Our edge-based block classification shares conceptual similarities—both recognize that uniform region treatment suboptimizes security. However, our approach achieves comparable security (**Table 4**) with significantly lower complexity by leveraging the established Canny detector rather than custom segmentation algorithms requiring parameter tuning.

The dual tree complex wavelet transform approach with SVD and CNN subspace demonstrates exceptional steganalytic resistance [94]. Its combination of multiple transform domains and deep learning analysis achieves detection rates potentially lower than our method, but at extreme computational cost unsuitable for real-time applications. This represents a classic security-efficiency trade-off that system designers must navigate based on specific operational requirements.

5.6. Limitations and Future Directions

While the proposed method demonstrates substantial improvements, several limitations warrant acknowledgment and suggest future research directions:

1. **Capacity Variability:** The adaptive nature produces variable capacity (0.37–1.20 bpp), which may complicate communication protocols requiring guaranteed minimum payload. Developing hybrid schemes that allocate minimum capacity uniformly while adaptively extending capacity in complex regions could address this limitation.
2. **Geometric Vulnerability:** Rotation and scaling attacks significantly degrade recovery rates. Integrating geometric-invariant features, such as scale-invariant feature transforms (SIFT) or feature-based synchronization markers, could enhance robustness while maintaining DCT's compression resilience.
3. **Color Image Extension:** Current implementation focuses on grayscale images. Extending to color images requires careful consideration of inter-channel correlations and color space selection (RGB vs. YCbCr). Preliminary experiments suggest embedding in chrominance channels (Cb, Cr) could exploit HVS's reduced sensitivity to color variations.
4. **Error Correction Integration:** Incorporating forward error correction (FEC) codes like Reed-Solomon could substantially improve recovery under noisy conditions, trading payload capacity for reliability—an acceptable exchange for critical communications.
5. **Adversarial Robustness:** While performing well against current steganalyzers, continuous evolution of deep learning detectors necessitates ongoing security evaluation. Adversarial training frameworks, where the embedder and detector co-evolve, could provide adaptive security enhancements.

6. Conclusions

This research presented a novel adaptive DCT-based steganography algorithm specifically designed for JPEG images, addressing the persistent challenges in balancing embedding capacity, visual imperceptibility, and security against modern steganalysis. The core innovation synthesizes edge-based texture analysis for intelligent block classification with a ternary (base-3) embedding system that optimizes information density per coefficient modification.

6.1. Key Contributions

The principal contributions of this work are:

1. **Adaptive Capacity Allocation Framework:** The algorithm successfully varies embedding capacity based on local image texture complexity, as demonstrated through comprehensive analysis of standard test images. Capacity ranges from 0.37 bpp in smooth images to 1.20 bpp in texture-rich images, ensuring modifications remain imperceptible while maximizing utilization of available masking capacity.
2. **Superior Visual Quality Preservation:** With an average PSNR of 62.4 dB and SSIM of 0.987, the method significantly outperforms traditional LSB (38.2 dB), classical DCT techniques (48.5 dB), and even recent adaptive methods like HUGO (55.8 dB) and UNIWARD (58.2 dB). This exceptional quality stems from restricting modifications to perceptually insignificant mid-frequency coefficients in texture-rich regions.
3. **Enhanced Security Profile:** The method exhibits strong resistance against both classical statistical attacks (8.3% Chi-Square detection rate) and contemporary deep learning-based steganalyzers (14.8% XuNet, 16.2% SRNet detection rates). This represents substantial improvement over existing methods, with average detection rate of 12.1% compared to 19.9% for HUGO and 32.5% for F5.
4. **Computational Efficiency:** Processing time of 234.7 ms per 512 × 512 image enables practical real-time deployment, representing approximately 53 × speedup compared to HUGO while maintaining competitive security performance. Memory footprint of 56.3 MB facilitates deployment on resource-constrained platforms.
5. **Robust Against Practical Attacks:** Exceptional resilience to JPEG recompression (98.2% recovery at QF = 90) ensures reliable operation through typical internet image transmission pipelines, addressing the most common real-world attack scenario.

6.2. Future Research Directions

Building upon the foundation established in this work, several promising research directions merit investigation:

1. **Deep Learning-Based Adaptive Selection:** While the current edge-based approach provides effective texture classification, integrating convolutional neural networks trained to predict HVS sensitivity could enable even more refined region selection. Transfer learning from image quality assessment (IQA) models could bootstrap such systems.
2. **Geometric Robustness Enhancement:** Addressing the vulnerability to rotation and scaling attacks through incorporation of invariant feature detection or synchronization patterns represents a critical extension for applications requiring geometric resilience. Investigating dual-domain embedding (DCT + DWT) could provide complementary robustness characteristics.
3. **Multi-Channel Color Extension:** Extending the framework to color images by exploiting inter-channel correlations and HVS's differential sensitivity across color spaces (RGB vs. YCbCr) could enhance both capacity and security. Preliminary analysis suggests chrominance channels offer substantial unexploited embedding opportunities.
4. **Adversarial Training Framework:** Developing a game-theoretic framework where the embedding algorithm co-evolves with steganalyzers through adversarial training could provide adaptive security against emerging detection techniques. Generative Adversarial Network (GAN) architectures show promise for this application.
5. **Hybrid Error Correction:** Integrating adaptive forward error correction that scales protection based on anticipated channel conditions could optimize the capacity-reliability trade-off for specific application scenarios.
6. **Video Steganography Extension:** Leveraging temporal redundancy in video sequences through motion-adaptive embedding could enable high-capacity covert video channels while exploiting temporal masking effects of the HVS.
7. **Blockchain-Based Key Management:** For deployment in distributed systems, investigating blockchain-based key distribution and synchronization could enhance security while maintaining decentralized operation.

6.3. Closing Remarks

The experimental validation demonstrates that intelligent, content-adaptive steganography represents the path forward for secure covert communication in the modern digital landscape. By respecting the fundamental characteristics of both the Human Visual System and the JPEG compression architecture, the proposed method achieves a superior balance across the classic steganographic triangle. As deep learning-based steganalysis continues advancing, the adaptive paradigm—tailoring embedding strategies to specific image characteristics—will become increasingly essential for maintaining security margins.

The open-source implementation of this algorithm will be made available to the research community, fostering reproducibility and enabling further innovation in adaptive steganographic systems. We anticipate that the principles demonstrated here—edge-based adaptation, ternary encoding efficiency, and computational pragmatism—will inform the next generation of steganographic algorithms deployed in security-critical applications worldwide.

Funding

This work received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The data that support the findings of this study are not publicly available due to privacy restrictions but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Kaur, S.; Singh, S.; Kaur, M.; et al. A Systematic Review of Computational Image Steganography Approaches. *Arch Computat Methods Eng* **2022**, *29*, 4775–4797. [CrossRef]
2. Ali, A.; Al-rimy, B.A.S.; Alsubaei, F.S.; et al. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors* **2023**, *23*, 6762. [CrossRef]
3. Liu, Y.; Liu, S.; Wang, Y.; et al. Video steganography: A review. *Neurocomputing* **2019**, *335*, 238–250. [CrossRef]
4. Kormilainen, R.; Lehtovuori, A.; Liesio, J.; et al. A Method to Co-Design Antenna Element and Array Patterns. *IEEE Access* **2022**, *10*, 31190–31200. [CrossRef]
5. Al-Ataby, A.; Al-Naima, F. A modified high capacity image steganography technique based on wavelet transform. *Int. Arab J. Inf. Technol.* **2020**, *7*, 358–364.
6. Mazurczyk, W.; Szczypiorski, K. Is Cloud Computing Steganography-proof? In Proceedings of the 2011 Third International Conference on Multimedia Information Networking and Security, Shanghai, China, 1 November 2011; pp. 441–442. [CrossRef]
7. Ahmad, I.; Shin, S. A Perceptual Encryption-Based Image Communication System for Deep Learning-Based Tuberculosis Diagnosis Using Healthcare Cloud Services. *Electronics* **2022**, *11*, 2514. [CrossRef]
8. Zhao, D.; Luo, L.; Yu, H.; et al. Security–SLA–guaranteed service function chain deployment in cloud-fog computing networks. *Cluster Comput* **2021**, *24*, 2479–2494. [CrossRef]
9. Hussain, M.; Wahab, A.W.A.; Idris, Y.I.B.; et al. Image steganography in spatial domain: A survey. *Signal Process. Signal Process. Image Commun.* **2018**, *65*, 46–66. [CrossRef]
10. Wang, G.; Huang, B.; Gu, K.; et al. No-Reference Multi-Level Video Quality Assessment Metric for 3D-Synthesized Videos. *IEEE Trans. on Broadcast.* **2024**, *70*, 584–596. [CrossRef]

11. Butora, J.; Yousfi, Y.; Fridrich, J. How to Pretrain for Steganalysis. In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security, Online, 17 June 2021; pp. 143–148. [CrossRef]
12. Johnson, N.F.; Jajodia, S. Exploring steganography: Seeing the unseen. *Computer* **1998**, *31*, 26–34. [CrossRef]
13. Zhang, W.; Li, S. A coding problem in steganography. *Des. Codes Cryptogr.* **2008**, *46*, 67–81. [CrossRef]
14. Bailey, K.; Curran, K. An evaluation of image based steganography methods. *Multimed. Tools Appl.* **2006**, *30*, 55–88. [CrossRef]
15. Dhawan, S.; Gupta, R. Analysis of various data security techniques of steganography: A survey. *Inf. Secur. J. Glob. Perspect.* **2021**, *30*, 63–87. [CrossRef]
16. Setyono, A.; Setiadi, D.R.I.M. Image watermarking using discrete cosine transform (DCT) and discrete wavelet transform (DWT): A comparative study. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *16*, 2502.
17. Potdar, V.M.; Han, S.; Chang, E. A survey of digital image watermarking techniques. In Proceedings of the 3rd IEEE International Conference on Industrial Informatics (INDIN '05), Perth, Australia, 10–12 August 2005; pp. 709–716. [CrossRef]
18. Wu, D.-C.; Tsai, W.-H. A steganographic method for images by pixel-value differencing. *Pattern Recognit. Lett.* **2003**, *24*, 1613–1626. [CrossRef]
19. Ernawan, F.; Kabir, M.N. A block-based RDWT-SVD image watermarking method using human visual system characteristics. *Vis. Comput.* **2020**, *36*, 19–37. [CrossRef]
20. Putra, Y.H.; Triwibowo, B.A.; Delenia, E.; et al. Sensitivity of a Convolutional Neural Network for Different Pooling Layers in Spatial Domain Steganalysis. *Inf. Syst. Eng.* **2024**, *29*, 1653–1665. [CrossRef]
21. Holub, V.; Fridrich, J. Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT. *IEEE Trans. Inform. Forensic Secur.* **2015**, *10*, 219–228. [CrossRef]
22. Li, B.; He, J.; Huang, J.; et al. A survey on image steganography and steganalysis. *J. Inf. Hiding Multimed. Signal Process.* **2020**, *2*, 142–172.
23. Denemark, T.; Fridrich, J. Improving Steganographic Security by Synchronizing the Selection Channel. In Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, Portland, OR, USA, 17 June 2015; pp. 5–14. [CrossRef]
24. Boroumand, M.; Chen, M.; Fridrich, J. Deep Residual Network for Steganalysis of Digital Images. *IEEE Trans. Inform. Forensic Secur.* **2019**, *14*, 1181–1193. [CrossRef]
25. Zhang, Y.; Luo, X.; Yang, C.; et al. A JPEG-Compression Resistant Adaptive Steganography Based on Relative Relationship between DCT Coefficients. In Proceedings of the 2015 10th International Conference on Availability, Reliability and Security, Toulouse, France, 10 August 2015; pp. 461–466. [CrossRef]
26. Ye, J.; Ni, J.; Yi, Y. Deep Learning Hierarchical Representations for Image Steganalysis. *IEEE Trans. Inform. Forensic Secur.* **2017**, *12*, 2545–2557. [CrossRef]
27. Rana, B.; Singh, Y.; Singh, P.K. A systematic survey on internet of things: Energy efficiency and interoperability perspective. *Trans. Emerging. Tel. Tech.* **2021**, *32*, e4166. [CrossRef]
28. Qin, C.; Zhang, W.; Cao, F.; et al. Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection. *Signal Process.* **2018**, *153*, 109–122. [CrossRef]
29. Laskar, S.A.; Hemachandran, K. High Capacity data hiding using LSB Steganography and Encryption. *Int. J. Database Manag. Syst.* **2012**, *4*, 57–68. [CrossRef]
30. Kadhim, I.J.; Premaratne, P.; Vial, P.J.; et al. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing* **2019**, *335*, 299–326. [CrossRef]
31. Salas-Cueva, N.F.; Mendoza, J.; Cutipa-Luque, J.C.; et al. An Open-source Wireless Platform for Real-time Water Quality Monitoring with Precise Global Positioning. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
32. Al-Otum, H.M.; Samara, N.A. A robust blind color image watermarking based on wavelet-tree bit host difference selection. *Signal Process.* **2010**, *90*, 2498–2512. [CrossRef]
33. Provos, N.; Honeyman, P. Hide and seek: an introduction to steganography. *IEEE Secur. Privacy.* **2003**, *1*, 32–44. [CrossRef]
34. Ker, A.D.; Bas, P.; Böhme, R.; et al. Moving steganography and steganalysis from the laboratory into the real world. In Proceedings of the first ACM workshop on Information hiding and multimedia security, Montpellier, France, 17 June 2013; pp. 45–58. [CrossRef]
35. Dumitrescu, S.; Wu, X.; Wang, Z. Detection of LSB steganography via sample pair analysis. *IEEE Trans. Signal Process.* **2003**, *51*, 1995–2007. [CrossRef]
36. Xu, G.; Wu, H.-Z.; Shi, Y.-Q. Structural Design of Convolutional Neural Networks for Steganalysis. *IEEE Signal Process. Lett.* **2016**, *23*, 708–712. [CrossRef]
37. John, E.G.; Lakshmipriya, K.A.; Malavika, P.S.; et al. Performance Analysis of PVD and LSB Steganographic

Techniques in Secure Data Handling Using FPGA. In Proceedings of 2025 11th International Conference on Smart Computing and Communications (ICSCC), Kochi, India, 3 July 2025; pp. 1–5. [CrossRef]

38. Pevny, T.; Bas, P.; Fridrich, J. Steganalysis by Subtractive Pixel Adjacency Matrix. *IEEE Trans. Inform. Forensic Secur.* **2010**, *5*, 215–224. [CrossRef]
39. Chaumont, M.; Puech, S. A DCT-based data-hiding method to embed the color information in a JPEG grey level image. In Proceedings of the 2006 European Signal Processing Conference, Florence, Italy, 4 September 2006.
40. Chang, C.-C.; Chen, T.-S.; Chung, L.-Z. A steganographic method based upon JPEG and quantization table modification. *Inf. Sci.* **2002**, *141*, 123–138. [CrossRef]
41. Fridrich, J.; Goljan, M. Practical steganalysis of digital images: State of the art. In Proceedings of the Electronic Imaging 2002, San Jose, CA, USA, 29 April 2002. [CrossRef]
42. Qian, Y.; Dong, J.; Wang, W.; et al. Deep learning for steganalysis via convolutional neural networks. In Proceedings of the Electronic Imaging 2015, San Jose, CA, USA, 4 March 2015. [CrossRef]
43. Ahmed, N.; Natarajan, T.; Rao, K.R. Discrete Cosine Transform. *IEEE Trans. Comput.* **1974**, *C–23*, 90–93. [CrossRef]
44. Wallace, G.K. The JPEG still picture compression standard. *IEEE Trans. Consumer Electron.* **1992**, *38*. [CrossRef]
45. JSteg steganography. Available online: https://github.com/lukechampine/jsteg (accessed on 15 May 2025).
46. Fridrich, J.; Goljan, M.; Hogea, D. Steganalysis of JPEG Images: Breaking the F5 Algorithm. In *Information Hiding*; Petitcolas, F.A.P., Ed.; Springer: Berlin, Germany, 2003; Volume 2578, pp. 310–323. [CrossRef]
47. Johnson, N.F.; Duric, Z.; Jajodia, S.; et al. Information Hiding: Steganography and Watermarking—Attacks and Countermeasures. *J. Electron. Imaging* **2001**, *10*, 825. [CrossRef]
48. Westfeld, A. F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis. In *Information Hiding*; Moskowitz, I.S., Ed.; Springer: Berlin, Germany, 2001; Volume 2137, pp. 289–302. [CrossRef]
49. Provos, N. Defending against statistical steganalysis. In Proceedings of the 10th USENIX Security Symposium, Washington, DC, USA, 13 August 2001; pp. 323–335.
50. Fridrich, J.; Pevný, T.; Kodovský, J. Statistically undetectable jpeg steganography: Dead ends challenges, and opportunities. In Proceedings of the 9th workshop on Multimedia & security, Dallas, TX, USA, 22 June 2021. [CrossRef]
51. Sedighi, V.; Cogranne, R.; Fridrich, J. Content-Adaptive Steganography by Minimizing Statistical Detectability. *IEEE Trans. Inform. Forensic Secur.* **2016**, *11*, 221–234. [CrossRef]
52. Filler, T.; Fridrich, J. Design of adaptive steganographic schemes for digital images. In Proceedings of the IS&T/SPIE Electronic Imaging, San Francisco, CA, USA, 10 February 2011. [CrossRef]
53. Pevný, T.; Filler, T.; Bas, P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography. In *Information Hiding*; Böhme, R., Fong, P.W.L., Safavi-Naini, R., Eds.; Springer: Berlin, Germany, 2010; Volume 6387, pp. 161–177. [CrossRef]
54. Holub, V.; Fridrich, J. Digital image steganography using universal distortion. In Proceedings of the first ACM workshop on Information hiding and multimedia security, Montpellier, France, 17 June 2013; pp. 59–68. [CrossRef]
55. Holub, V.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, Spain, 20 December 2012; pp. 234–239. [CrossRef]
56. Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for steganography in an arbitrary domain. *EURASIP J. on Info. Security* **2014**, *2014*, 1. [CrossRef]
57. Butora, J.; Fridrich, J. Reverse JPEG Compatibility Attack. *IEEE Trans. Inform. Forensic Secur.* **2020**, *15*, 1444–1454. [CrossRef]
58. Leask, V.; Cogranne, R.; Borghys, D.; et al. UNCOVER: Development of an efficient steganalysis framework for uncovering hidden data in digital media. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, 23 August 2022; pp. 1–8. [CrossRef]
59. Filler, T.; Judas, J.; Fridrich, J. Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. *IEEE Trans. Inform. Forensic Secur.* **2011**, *6*, 920–935. [CrossRef]
60. He, Z.; Wu, R.; Wang, X. Image Steganalysis Based on an Adaptive Attention Mechanism and Lightweight DenseNet. *Comput. Mater. Continua* **2025**, *85*, 1631–1651. [CrossRef]
61. Khandelwal, J.; Sharma, V.K. W-VDSR: wavelet-based secure image transmission using machine learning VDSR neural network. *Multimed. Tools. Appl.* **2023**, *82*, 42147–42172. [CrossRef]
62. Khandelwal, J.; Sharma, V.K. Strengthening wavelet based image steganography using Rubik's cube segmen-

tation and secret image scrambling. *Multimed Tools Appl* **2024**, *83*, 78797–78825. [CrossRef]

63. Goud, S.K.; Yadav, B.D.; Goud, R.S.; et al. Unmasking Cyberbullying Through NLP-Driven Detection in Contemporary Social Media. In *Proceedings of the 7th International Conference on Communications and Cyber Physical Engineering*; Springer Nature: Singapore, 2025; Volume 1466, pp. 959–968. [CrossRef]
64. Canny, J. A Computational Approach to Edge Detection. *IEEE Trans. Pattern Anal. Mach. Intell.* **1986**, *PAMI-8*, 679–698. [CrossRef]
65. Guo, L.; Ni, J.; Su, W.; et al. Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited. *IEEE Trans. Inform. Forensic Secur.* **2015**, *10*, 2669–2680. [CrossRef]
66. Marr, D.; Hildreth, E. Theory of edge detection. *Proc Biol Sci* **1980**, *207*, 187–217. [CrossRef]
67. Zhang, Y.; Ma, Y.; Zhang, Q.; et al. An Image Robust Batch Steganography Framework With Minimum Embedding Signs. *IEEE Trans. Inform. Forensic Secur.* **2025**, *20*, 10745–10760. [CrossRef]
68. Sallee, P. Model-Based Steganography. In *Digital Watermarking*; Kalker, T., Cox, I., Ro, Y.M., Eds.; Springer: Berlin, Germany, 2004; Volume 2939, pp. 154–167. [CrossRef]
69. Fridrich, J. *Steganography in Digital Media: Principles, Algorithms, and Applications*; Cambridge University Press: Cambridge, UK, 2009. [CrossRef]
70. Ker, A.D. A General Framework for Structural Steganalysis of LSB Replacement. In *Information Hiding*; Barni, M., Herrera-Joancomartí, J., Katzenbeisser, S., et al., Eds.; Springer: Berlin, Germany, 2005; Volume 3727, pp. 296–311. [CrossRef]
71. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; et al. Image quality assessment: from error visibility to structural similarity. *IEEE Trans. on Image Process.* **2004**, *13*, 600–612. [CrossRef]
72. Wu, H.-C.; Chang, C.-C. A novel digital image watermarking scheme based on the vector quantization technique. *Comput. Secur.* **2005**, *24*, 460–471. [CrossRef]
73. Böhme, R. *Advanced Statistical Steganalysis*; Springer: Berlin, Germany, 2010. [CrossRef]
74. Westfeld, A.; Pfitzmann, A. Attacks on Steganographic Systems. In *Information Hiding*; Pfitzmann, A. Ed.; Springer: Berlin, Germany, 2000; Volume 1768, pp. 61–76. [CrossRef]
75. Lyu, S.; Farid, H. Steganalysis Using Higher-Order Image Statistics. *IEEE Trans. Inform. Forensic Secur.* **2006**, *1*, 111–119. [CrossRef]
76. Fridrich, J.; Kodovsky, J. Rich Models for Steganalysis of Digital Images. *IEEE Trans. Inform. Forensic Secur.* **2012**, *7*, 868–882. [CrossRef]
77. Cox, I.J.; Miller, M.L.; Bloom, J.A.; et al. Steganography. In *Digital Watermarking and Steganography*; Elsevier: New York, NY, USA, 2008; pp. 425–467. [CrossRef]
78. Bas, P.; Filler, T.; Pevný, T. "Break Our Steganographic System": The Ins and Outs of Organizing BOSS. In *Information Hiding*; Filler, T., Pevný, T., Craver, S., et al., Eds.; Springer: Berlin, Germany, 2011; Volume 6958, pp. 59–70. [CrossRef]
79. Cachin, C. An information-theoretic model for steganography. *Inf. Comput.* **2004**, *192*, 41–56. [CrossRef]
80. Eskicioglu, A.M.; Fisher, P.S. Image quality measures and their performance. *IEEE Trans. Commun.* **1995**, *43*, 2959–2965. [CrossRef]
81. Kodovsky, J.; Fridrich, J.; Holub, V. Ensemble Classifiers for Steganalysis of Digital Media. *IEEE Trans. Inform. Forensic Secur.* **2012**, *7*, 432–444. [CrossRef]
82. Huang, Y.; Liu, Z.; Wu, Q.; et al. Robust image steganography against JPEG compression based on DCT residual modulation. *Signal Process.* **2024**, *219*, 109431. [CrossRef]
83. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
84. Yao, Y.; Wang, J.; Chang, Q.; et al. High invisibility image steganography with wavelet transform and generative adversarial network. *Expert Syst. Appl.* **2024**, *249*, 123540. [CrossRef]
85. Majeed, N.D.; Al-Askery, A.J.; Hasan, F.S.; et al. A Survey on Steganography and Image Encryption Techniques. *Electr. Eng. Tech. J.* **2025**, *2*, 11–24. [CrossRef]
86. Fu, G.; Peng, Y.; Hu, J.; et al. A Systematic Review of Deep Learning-Based Image Steganography: Paradigms, Progress, and Prospects. In Proceedings of the 2025 4th International Conference on Image Processing, Computer Vision and Machine Learning (ICICML), Chongqing, China, 21 November 2025; pp. 307–312. [CrossRef]
87. Muttoo, S.K.; Kumar, S. A multilayered secure, robust and high capacity image steganographic algorithm. *World J. Sci. Technol. Sustain. Dev.* **2025**, *8*, 37–51.
88. Mohaisen, H.N.; Mohammed, M.Q.; Nahi, M.H. Hiding Secret Data in Color Video Applying Modify RSA for Cryptography with Randomly Select Frame and Pixel to Steganography. *J. nat. appl. sci. URAL* **2024**, *5*. Available online: https://uraljournal.remahcenter.com/images/papers/no5vol1/6.pdf (accessed on 15 May 2025).
89. Rahman, S.; Uddin, J.; Hussain, H.; et al. A novel and efficient digital image steganography technique using

least significant bit substitution. *Sci. Rep.* **2025**, *15*, 107. [CrossRef]

90. Zhou, W.; Song, W.; Zhang, Z.; et al. Hierarchical feature aggregation with mixed attention mechanism for single-cell RNA-seq analysis. *Expert Syst. Appl.* **2025**, *260*, 125340. [CrossRef]
91. Li, Y.; Li, J.; Bhatti, U.A.; et al. Robust Zero-watermarking Algorithm for Medical Images Based on ORB and DCT. In Proceedings of the 2023 26th ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter), Taiwan, China, 5 July 2023; pp. 282–289. [CrossRef]
92. Hou, B.; Fu, C.; Xue, M. An extended belief rule-based system with hybrid sampling strategy for imbalanced rule base. *Inf. Sci.* **2024**, *684*, 121288. [CrossRef]
93. Rehman, W. A Novel Approach to Image Steganography Using Generative Adversarial Networks. *arXiv preprint* **2024**, *arXiv:2412.00094*. [CrossRef]
94. Chen, X.; Zheng, H.; Tang, H.; et al. Multi-scale perceptual YOLO for automatic detection of clue cells and trichomonas in fluorescence microscopic images. *Comput. Biol. Med.* **2024**, *175*, 108500. [CrossRef]

Publisher's Note: The views, opinions, and information presented in all publications are the sole responsibility of the respective authors and contributors, and do not necessarily reflect the views of UK Scientific Publishing Limited and/or its editors. UK Scientific Publishing Limited and/or its editors hereby disclaim any liability for any harm or damage to individuals or property arising from the implementation of ideas, methods, instructions, or products mentioned in the content.