International Journal of Safety and Security Engineering
Vol. 16, No. 1, January, 2026, pp. 153-168
Journal homepage: http://iieta.org/journals/ijsse

A Hybrid DWT–DCT Image Steganography Framework with Quick Response-Assisted Elliptic Curve Cryptography Signcryption for Robust Message Recovery

Dian Rachmawati[1*], Muhammad H. Rahman[2]

[1] Department of Computer Science, Universitas Sumatera Utara, Medan 20155, Indonesia
[2] Department of Informatics, Institut Teknologi Bandung, Bandung 40132, Indonesia

Corresponding Author Email: dian.rachmawati@usu.ac.id

https://doi.org/10.18280/ijsse.160113

Received: 4 November 2025
Revised: 26 December 2025
Accepted: 16 January 2026
Available online: 31 January 2026

Keywords:
image steganography, Elliptic Curve Cryptography, signcryption, Discrete Wavelet Transform–Discrete Cosine Transform, Quick Response code redundancy, robust message recovery, JPEG robustness

ABSTRACT

This study presents a hybrid covert communication framework that combines Elliptic Curve Cryptography (ECC)-based signcryption, Quick Response (QR)-code redundancy, and Discrete Wavelet Transform-Discrete Cosine Transform (DWT-DCT) image steganography to support reliable recovery of cryptographically protected messages. The plaintext is first processed by an ECC signcryption module to provide confidentiality and authentication with a compact ciphertext. The signcrypted payload is then encoded as a QR code with Reed–Solomon error correction and embedded into mid-frequency Discrete Cosine Transform (DCT) coefficients within the HL, LH, and HH sub-bands of a one-level Discrete Wavelet Transform (DWT) decomposition using quantization index modulation. Experiments on five standard 512 × 512 test images show that the proposed method achieves an average Peak Signal-to-Noise Ratio (PSNR) of 34.58 dB and an average Structural Similarity Index Measure (SSIM) of 0.87. Under clean-channel conditions, the extracted payload is recovered with zero bit error. Under JPEG compression, complete message recovery remains possible for four of the five test images at Quality Factors (QF) of 96 or above, while performance degrades at lower quality settings because compression artifacts exceed the correction capacity of the QR layer. These results indicate that the proposed framework provides a practical balance among security, robustness, and visual quality for controlled transmission environments.

1. INTRODUCTION

Robust information security protocols are essential for multimedia transmission across interconnected networks [1-3]. While cryptography focuses on scrambling messages to obscure the content from unauthorized entities [4], steganography provides a crucial, non-obvious security layer by concealing the very existence of the communication within a seemingly innocuous medium [5, 6]. Traditional cryptographic methods are limited because the resulting encrypted signals may attract suspicion from adversaries, who can then attempt to intercept or analyze the message [2]. Therefore, the integrated objective of modern security is to achieve covert, high-assurance communication [4].

Conventional data hiding approaches often employ spatial-domain techniques, such as Least Significant Bit (LSB) substitution [2, 7, 8]. Although LSB is known for its simplicity [2, 9], it is inherently susceptible to statistical analysis and various forms of image processing manipulations, including lossy compression like JPEG [2]. This fragility necessitates a shift toward transform-domain steganography [3, 5]. The Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are widely favored transforms because they operate in the frequency domain, enhancing security and robustness against statistical attacks and noise interference [1], [6]. Specifically, DCT provides resilience against JPEG compression by embedding data in mid-frequency components [10], while DWT excels in resilience against noise and filtering attacks [11, 12]. Consequently, combining these two techniques in a Hybrid DWT–DCT framework is acknowledged as a powerful approach to counter a composite set of attacks and surpass the performance of individual methods [6, 11, 12].

Guaranteeing the security of the hidden message before embedding is critical. The traditional method of applying a digital signature followed by encryption ("Sign-then-Encrypt") requires separate cryptographic operations, resulting in high computational complexity and communication costs [13]. This inefficiency is solved by signcryption, a cryptographic primitive that merges encryption and digital signing into a single logical step, significantly improving efficiency [13, 14]. This study employs Elliptic Curve Cryptography (ECC) as the foundation for signcryption, owing to its superior efficiency over traditional schemes such as RSA [15, 16]. ECC achieves equivalent security with significantly shorter key lengths (e.g., a 256-bit ECC key is comparable to a 3072-bit RSA key), which translates directly to reduced computational overhead and less energy consumption [15, 16]. This makes ECC-based signcryption highly suitable for resource-constrained devices and real-time

secure communication [17, 18].

Unlike standard visual or textual data, the payload derived from ECC signcryption is a high-entropy ciphertext that is fundamentally fragile against adversarial interference or unintentional noise. Cryptographic algorithms rely on statistical randomness for security, ensuring that encrypted information exhibits a distribution resembling noise. Consequently, any corruption in the transmission channel, quantified as a Bit Error Rate (BER > 0), triggers the cryptographic avalanche effect: even a single-bit alteration propagates through the decryption process and causes complete verification failure. This strict zero-error requirement motivates the need for a dedicated error-correction mechanism to guarantee intact ciphertext recovery under controlled or clean transmission conditions [19, 20].

Existing research efforts predominantly address the critical requirements of covert communication from two largely independent research tracks: robust steganography and compact cryptography. On one side, advanced steganographic schemes utilize hybrid transform domains (like DWT–DCT) to enhance payload robustness against common channel distortions [1, 6, 11, 12, 21]. On the other side, highly efficient cryptographic primitives such as ECC Certificateless Aggregate Signcryption (CLASC) are leveraged to produce fixed, compact ciphertexts to minimize computational overhead [17, 19, 20]. To date, these two domains remain largely disjoint. No prior work provides an integrated framework that combines a compact ECC signcryption payload, a Quick Response (QR)-based redundancy layer, and hybrid DWT–DCT embedding to support reliable recovery of cryptographically sensitive ciphertext under bounded distortion conditions.

To bridge this gap, we propose a robust covert communication framework: Hybrid DWT–DCT QR Image Steganography Carrying Compact ECC Signcryption. The QR code was selected as a redundancy layer to address two constraints: the high sensitivity of the cryptographic payload to bit errors, and the resource-limited nature of target environments such as Internet of Things (IoT) and Internet of Vehicles (IoV) devices [17, 18]. As cryptographic payloads are extremely sensitive to channel noise, the QR code is introduced as an intermediate redundancy layer to enhance the resilience of the signcrypted payload, enabling zero-BER recovery under clean or mildly distorted transmission conditions through its built-in error correction capability [22]. Furthermore, QR decoding is computationally lightweight and widely supported by standard libraries, ensuring practical compatibility with resource-constrained edge devices.

The main contributions of this work are fourfold:

1. Development of a hybrid cryptographic layer combining ECC-based signcryption with AES-GCM authenticated encryption and ECDSA authentication, achieving robustness against chosen-ciphertext attacks with a minimal computational overhead of only 0.09 ms.
2. Implementation of a synchronization header mechanism via a 16-bit auto-header that enables automated and precise payload extraction, eliminating the need for manual bit-alignment required in prior works.
3. Integration of QR Code Error Correction Level H as a strategic redundancy layer, ensuring Zero-BER recovery of the high-entropy cryptographic payload under clean or mildly distorted transmission conditions.
4. Optimization of hybrid DWT–DCT mid-band embedding to achieve a balanced capacity-to-imperceptibility trade-off, with an average PSNR of 34.58 dB and SSIM of 0.87, validated through Chi-square statistical steganalysis to confirm resistance against histogram-based attacks.

2. RELATED WORKS

2.1 Existing methods and limitations

Early data concealment methods focused on spatial-domain techniques, particularly LSB substitution [2, 7, 8]. While LSB methods offer high payload capacity [2, 23] and inherently high imperceptibility, frequently achieving PSNR values exceeding 40 dB [7, 8], they exhibit extreme fragility against image processing operations, statistical attacks, and lossy compression [2, 23], rendering them unsuitable for the BER = 0 recovery required by high-entropy cryptographic payloads.

To address these limitations, research shifted towards Transform Domain Steganography (TDS), employing the DCT and DWT [5, 6]. DCT facilitates data embedding in mid-frequency coefficients, providing robustness against compression [10], while DWT offers multi-resolution analysis that enhances resilience against noise attacks through sub-band separation [11, 12]. Hybrid approaches (e.g., DWT–DCT or DWT–DCT–SVD) demonstrate superior robustness by optimizing payload placement across multiple domains [1, 6, 12]. However, the choice of embedding domain directly dictates performance trade-offs [1, 2]: frequency-domain hiding targets mid-frequency coefficients that the Human Visual System (HVS) tolerates well [24, 25], trading peak visual quality for robust message longevity. Since cryptographic security fails if even a single bit error (BER > 0) is introduced, the embedding methodology must prioritize robustness and extraction fidelity over maximal visual metrics. Despite this requirement, many existing hybrid DWT–DCT implementations pair robust embedding with weak encryption or lack integrated encryption altogether [9, 23], failing to maintain confidentiality against modern cryptanalysis.

An examination of specific methods highlights the limitations preventing zero-error recovery of cryptographic payloads.

The F5 Algorithm [26] introduced an embedding method in the DCT domain by intentionally modifying coefficients (reducing absolute value by one) rather than simple LSB replacement. Advantages: The method enhanced robustness against the early χ^2 statistical attack by preserving the characteristic statistical properties of the coefficient histogram [26]. Furthermore, working in the frequency domain offers better inherent resilience against basic image manipulation compared to spatial techniques. Limitations/Gap: Subsequent steganalysis research [27] demonstrated that DCT-domain embedding remains susceptible to advanced statistical detection when coefficient distributions are not carefully preserved. Moreover, modifications sometimes lead to coefficients becoming zero (shrinkage), necessitating error correction techniques, suggesting that integrity is not guaranteed without a strong external mechanism. Importantly, this model typically focuses on raw messages and lacks integral cryptographic protection or a mechanism for BER = 0 recovery.

The DCT-in-DCT-Adaptive Scaling method [28] proposed performing frequency transformation on the secret payload before embedding it into the cover image coefficients using an adaptive scaling factor. Advantages: This dual-domain transformation dramatically enhances the fidelity of the extracted payload, achieving an improvement of up to 20.25 dB in extracted payload PSNR over non-DCT payload methods [28]. This demonstrates superior structural protection for the secret message during retrieval. Limitations/Gap: Despite high fidelity during extraction, the algorithm does not include an external error correction or redundancy layer. The irreversible nature of 8-bit quantization conversion is inherently a lossy process, meaning this scheme cannot guarantee the mandatory BER = 0 required for the restoration of cryptographic ciphertexts.

Certificateless Signcryption Schemes [17-20] introduced cryptographic primitives to simultaneously achieve confidentiality and authenticity, particularly optimized for restricted environments. Advantages: These schemes eliminate the complex certificate management burden associated with traditional PKI and resolve the key escrow problem of IBC, while enabling batch verification for resource-constrained networks [20]. The ability to perform signcryption and aggregation in a single logical step significantly reduces computational overhead (Cost(SC) ≪ Cost(S) + Cost(E)) compared to the traditional sign-then-encrypt method [13]. Limitations/Gap: These schemes are purely cryptographic; they do not incorporate steganography, thereby failing to conceal the existence of communication. The compact ciphertext payload is a high-entropy payload that is extremely vulnerable to channel noise, resulting in complete decryption failure (BER = 0 violation) if transmitted over an insecure channel without robust concealment.

Hybrid steganography–cryptography methods [23] implemented double-layer security by encrypting the secret data (often AES) before embedding it using classic methods like LSB or DCT. Advantages: Provides dual-layer security by concealing the content (encryption) and concealing the existence (steganography). Shows improved PSNR compared to spatial methods. Limitations/Gap: This approach typically relies on non-adaptive embedding (e.g., LSB-DCT fixed coefficient embedding), making it not robust against advanced steganalysis or targeted attacks. Critically, the fundamental security workflow lacks an external redundancy layer (such as QR code) to actively correct bit errors in the high-entropy ciphertext, thus failing to guarantee BER = 0.

Existing studies generally treat robust steganography (Hybrid DWT–DCT) and compact cryptography (ECC signcryption) as distinct fields. No prior work integrates compact ECC signcryption with a dedicated QR-based redundancy layer within a Hybrid DWT–DCT framework to jointly solve covertness, efficiency, and the mandatory zero-error recovery (BER = 0) of sensitive ciphertexts.

2.2 Elliptic Curve Cryptography signcryption: Efficiency in resource-constrained environments

ECC signcryption has become a widely adopted approach for secure communication in resource-constrained environments, where computational efficiency and bandwidth optimization are critical. The signcryption primitive, originally introduced in 1997 [13], fundamentally departs from the conventional "sign-then-encrypt" methodology by combining digital signature and encryption operations into a single logical step, thereby achieving significant computational and communication overhead reductions. ECC-based signcryption demonstrates superior performance and security over traditional public-key cryptoschemes [14, 29].

The theoretical foundation of signcryption's efficiency advantage lies in its ability to eliminate redundant cryptographic operations inherent in sequential approaches. Traditional sign-then-encrypt schemes require separate key generation, signature computation, and encryption processes, resulting in approximately double the computational cost and ciphertext expansion. Denoting the computational costs of signature and encryption as Cost(S) and Cost(E), respectively, the signcryption paradigm achieves:

$$Cost(SC) \ll Cost(S) + Cost(E) \quad (1)$$

ECC-based signcryption [14] demonstrated that this inequality translates to concrete efficiency gains: signcryption achieves an average of 58% reduction in computational cost and 40% reduction in communication overhead compared to signature-then-encryption paradigms. These efficiency gains become particularly pronounced when leveraging ECC's algebraic structure over finite fields.

Table 1 summarizes the comparative advantages of ECC-256 signcryption over RSA-3072 and conventional sign-then-encrypt approaches. The security equivalence between 256-bit ECC and 3072-bit RSA derives from the relative hardness of their underlying mathematical problems. While RSA security depends on the Integer Factorization Problem with sub-exponential attacks (General Number Field Sieve), ECC security relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP). Given a point Q = kP on an elliptic curve, computing the scalar k is computationally infeasible. The best-known attacks require O(√n) operations via Pollard's rho algorithm [15, 16].

Table 1. Comparative analysis of public-key cryptographic approaches [15, 29]

Parameter	ECC-256	RSA-3072	Sign-Then-Encrypt
Key Size (bits)	256	3072	3072+
Security Level	128-bit	128-bit	128-bit
Signature Size	64–72 B	384 B	384+B
Computational Cost	LOW	HIGH	Very HIGH
Comm. Overhead	LOW	HIGH	Very HIGH
Efficiency	HIGH	Moderate	Low

Note: ECC = Elliptic Curve Cryptography; RSA = Rivest–Shamir–Adleman; StE = Sign-then-Encrypt.

Modern implementations of ECC signcryption typically employ a hybrid construction combining Elliptic Curve Diffie–Hellman (ECDH) for key agreement, Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication, and authenticated encryption with associated data (AEAD) ciphers such as AES-GCM for confidentiality [15]. In this work, the signcryption methodology encompasses key generation, shared key derivation using ECDH, and encryption/decryption using AES in Galois/Counter Mode (GCM). The shared secret is computed as:

$$S = sk_A \cdot pk_B = sk_B \cdot pk_A \quad (2)$$

where, sk_A, sk_B are private keys and pk_A, pk_B are corresponding public keys. This shared secret is then

transformed via HKDF-SHA256 into a symmetric key for AES-GCM operations:

$$K = \text{HKDF-SHA256}(S, \text{salt}, \text{info}) \quad (3)$$

This tripartite architecture leverages ephemeral key pairs to achieve sender forward secrecy, ensuring that compromise of the sender's long-term key does not expose previously signcrypted messages [29]. Note that compromise of the receiver's static key would allow decryption of past messages, as the shared secret depends on skr; receiver forward secrecy would require ephemeral key exchange on both sides.

For the SECP256R1 (P-256) curve employed in this work, the security level approximates 2^{128} operations for the best-known attacks, establishing equivalence with AES-128 symmetric security while maintaining public-key functionality [15]. A 256-bit ECC key provides equivalent security to a 3072-bit RSA key [15], making ECC particularly suitable for IoT systems, mobile devices, and other resource-constrained platforms [17, 18].

In the context of IoT and IoV deployments, the resource constraints of embedded devices, limited processing power, constrained memory, and battery-dependent operation necessitate cryptographic solutions that minimize computational burden without compromising security guarantees. Yang et al. [17] observe that "the IoV has an open communication character, which enables various applications and services. However, this also exposes it to the risk of message tampering or the leaking of private data." Their CLASC scheme addresses these challenges while maintaining "reduced computational overhead" compared to traditional approaches.

Signcryption schemes have undergone significant advancements in trust management. Certificateless signcryption (CLSC) schemes [20] eliminate the requirement for certificate authorities while preventing key generation centers from possessing complete knowledge of user private keys. The CLSC framework enables signcryption with batch verification capabilities, achieving both confidentiality and unforgeability in a single logical step, a critical optimization for bandwidth-constrained networks. The CLSC security model proves security under the random oracle model against two adversary types: Type I adversaries without master key access but capable of public key replacement, and Type II adversaries with master key access but unable to replace public keys [20].

Recent developments in decentralized signcryption further enhance applicability to emerging paradigms. Shi and Liu [30] propose a decentralized signcryption scheme based on Cryptography Fundamental Logics (CFL) combined with the SM2 elliptic curve algorithm. Their scheme "eliminates the need for third-party involvement, achieving decentralized authentication and reducing the burden on certificate generation centers." Crucially, their experimental results demonstrate that "the proposed scheme reduces computational overheads by approximately 30% and communication overheads by approximately 20% in practical working environments" compared to traditional certificate-based systems [30]. The CFL framework generates two key pairs: identity-related and randomly generated, enabling "decentralized verification without third-party intervention."

For the hybrid steganographic system proposed in this work, ECC signcryption provides the cryptographic foundation enabling robust message recovery. The implementation employs a signcryption construction comprising:

- **Key Generation:** Selection of elliptic curve SECP256R1 with parameters (E, G, n), private key sk, and public key pk [15].
- **Shared Secret Computation:** ECDH-based exchange where both parties independently compute an identical shared secret without direct transmission [15].
- **Symmetric Key Derivation:** HKDF transforms shared secret into 256-bit AES key with context-specific info parameter.
- **Authenticated Encryption:** AES-GCM provides confidentiality via ciphertext C and integrity via authentication tag Tag:

$$(C, Tag) = \text{AES-GCM-Encrypt}(K, IV, m) \quad (4)$$

- **Digital Signature:** ECDSA signature over the ciphertext provides sender authentication and non-repudiation.

This construction generates a compact output structure containing the ephemeral public key (65 bytes uncompressed), initialization vector (12 bytes), ciphertext with GCM authentication tag, and DER-encoded ECDSA signature, yielding total overhead of approximately 200–250 bytes depending on payload size.

The ciphertext expansion characteristics merit particular consideration for steganographic embedding capacity. Unlike RSA-based schemes requiring 256–384 byte signatures for equivalent security levels, the ECC signcryption output remains compact even with the inclusion of ephemeral keys and full signature data. For a typical 32-byte plaintext message, the signcryption output approximates 200 bytes, representing a 40–50% reduction compared to RSA-3072 constructions. When encoded as QR codes for error-resilient embedding within DWT–DCT transform coefficients, this compactness directly translates to reduced embedding footprint and consequently higher stego-image quality (PSNR/SSIM).

Table 2. Security properties of Elliptic Curve Cryptography (ECC) signcryption schemes (Adapted from [17, 20])

Property	Description
Confidentiality	No information from plaintext is obtainable from the ciphertext
Unforgeability	Valid signatures cannot be obtained by attackers
Public Verifiability	Verification independent of the recipient's private key
Non-repudiation	Sender cannot deny signcrypted message
Forward Secrecy (FS)	Sender FS via ephemeral keys; receiver FS requires mutual ephemeral exchange

The selection of ECC parameters significantly influences both security guarantees and computational efficiency. The NIST P-256 curve offers an optimal balance between security margin (128-bit equivalent) and implementation efficiency, with hardware acceleration available on modern processors through dedicated instruction sets (e.g., Intel AES-NI, ARM Cryptography Extensions). As noted by Shi and Liu [30], the SM2 algorithm with 256-bit keys "provides higher security strength than the RSA algorithm" while offering "advantages

in processing speed, particularly in scenarios requiring rapid encryption and decryption." The curve's widespread adoption ensures compatibility with standard cryptographic libraries and facilitates reproducibility of experimental results.

The security properties guaranteed by ECC signcryption are summarized in Table 2. In summary, ECC signcryption represents the state-of-the-art in efficient authenticated encryption for resource-constrained environments and bandwidth-limited steganographic channels. The paradigm's ability to combine confidentiality, integrity, and authentication in a single cryptographic operation, coupled with ECC's inherent efficiency advantages over traditional public-key systems, establishes it as the preferred approach for applications requiring compact ciphertexts and minimal computational overhead. For hybrid DWT–DCT QR image steganography targeting robust message recovery, ECC signcryption provides the essential cryptographic infrastructure enabling secure payload embedding while maintaining practical extraction and verification on resource-limited receivers.

2.3 Summary and research gap

To provide a clear comparison between the existing literature and the proposed framework, Table 3 summarizes the key features and limitations of prior works, highlighting the research gap that this study aims to fill.

Based on the review of recent studies, it is evident that while significant progress has been made in both steganography and cryptography, several fundamental challenges remain unresolved. Most existing methods focus on either achieving high robustness at the expense of computational efficiency or implementing strong encryption without addressing the inherent fragility of hidden data during transmission through lossy channels. The steganographic domain has predominantly treated transform-based embedding (DWT, DCT, or SVD) as isolated techniques, while cryptographic research has advanced signcryption as an efficient paradigm without considering its integration with covert communication channels. Furthermore, the avalanche effect intrinsic to cryptographic primitives, where a single-bit error causes complete decryption failure, remains a critical vulnerability when encrypted payloads traverse steganographic channels susceptible to compression artifacts and noise interference.

As illustrated in Table 3, the proposed method bridges this research gap by integrating ECC-based signcryption with a hybrid DWT–DCT steganographic domain. The signcryption layer simultaneously provides confidentiality, authentication, and non-repudiation in a single cryptographic operation, while the hybrid transform leverages wavelet decomposition for noise resilience and DCT embedding for JPEG compression compatibility.

Unlike Zhang et al.'s pure cryptographic approach [14], this framework embeds the signcrypted payload within a visual carrier, ensuring covert communication. Unlike Konyar and Öztürk's error-correction-only approach [32], the modular signcryption construction (ECDH + AES-GCM + ECDSA) reduces computational overhead through unified key agreement while maintaining equivalent security guarantees. Unlike Huang et al. [33] DCT-only embedding, the hybrid transform domain exploits the energy compaction properties of DWT sub-bands (HL, LH, HH) combined with mid-frequency DCT coefficient modulation.

Most critically, this framework utilizes QR code encoding at Error Correction Level H (30% redundancy) as an intermediate error-resilient layer, a novel architectural element absent in all reviewed works. This layer absorbs bit-level degradation before cryptographic verification, ensuring zero-BER message recovery under clean channel conditions while maintaining robustness against JPEG compression down to Quality Factors (QF) ≥ 96 for four of five test images.

Table 3. Gap analysis of the proposed method versus prior works

Reference	Method	Gap/Limitation
Alajmi et al. [22]	QR-based steganography + encryption	QR as cover medium, not redundancy layer; no transform-domain embedding; limited robustness
Benyoucef et al. [31]	DWT–SVD + QR	No signcryption; requires U/V matrices; Region of Non-Interest (RONI)-specific
Konyar and Öztürk [32]	RS-coded Medical Data Hiding	No signcryption; noise-specific; no transform-domain embedding
Zhang et al. [14]	ECC Signcryption Scheme	No steganographic concealment; no error tolerance
Huang et al. [33]	DCT + RS codes	No crypto layer; channel-dependent; DCT-only
Proposed	DWT–DCT + QR + ECC Signcryption	Unified crypto-stego with error-resilient QR buffer

Note: LSB = Least Significant Bit; QR = Quick Response; AES = Advanced Encryption Standard; DWT = Discrete Wavelet Transform; SVD = Singular Value Decomposition; ECC = Elliptic Curve Cryptography; DCT = Discrete Cosine Transform; RS = Reed–Solomon; ROI = Region of Interest.

3. PRELIMINARIES

This section presents the theoretical foundations underlying the proposed scheme, focusing on the design rationale for each component.

3.1 Hybrid Discrete Wavelet Transform-Discrete Cosine Transform embedding domain

The proposed steganographic scheme employed a hybrid transform domain combining DWT and DCT. This dual-transform approach exploits the complementary strengths of both transforms: DWT provides spatial-frequency localization aligned with the HVS, enabling strategic placement of modifications where they cause minimal perceptual distortion [12, 21], while DCT offers strong energy compaction and inherent compatibility with JPEG compression standards [10, 33]. Hybrid DWT–DCT methods consistently outperformed single-transform approaches by simultaneously exploiting multiresolution decomposition and fine-grained frequency analysis within localized regions [1, 6, 12]. This combination enables the scheme to withstand a broad range of signal processing attacks, including filtering, noise addition, and lossy compression, while maintaining high imperceptibility [21].

a) Sub-band Selection

A one-level 2D-DWT decomposes an image into four sub-bands: LL (approximation), LH (horizontal detail), HL

(vertical detail), and HH (diagonal detail). The LL sub-band contains visually critical low-frequency information; embedding in this region risks significant perceptual distortion. The HL, LH, and HH detail sub-bands represent intermediate and high frequency components that collectively provide sufficient embedding capacity while maintaining an acceptable trade-off between robustness and imperceptibility, and are therefore selected for embedding [12, 21]. Although the HH sub-band is more vulnerable to low-pass filtering, the QR Code Error Correction Level H (30% redundancy) mitigates this sensitivity by absorbing bit-level degradation. Experimental evidence from prior hybrid DWT–DCT studies demonstrated that embedding in detail sub-bands achieved PSNR values of 40–50 dB with SSIM values at or above 0.99, indicating excellent visual quality preservation [6, 12, 21].

b) Mid-frequency Coefficient Strategy

Within the selected DWT sub-band, the image is partitioned into 8×8 blocks and transformed using 2D-DCT. The resulting coefficient matrix is divided into low-frequency, mid-frequency, and high-frequency regions. Low-frequency coefficients carry perceptually dominant information and are unsuitable for modification [24]; high-frequency coefficients are aggressively quantized during JPEG compression [10]. The mid-frequency band typically encompassing 22 coefficients per 8 × 8 block [24] provides the optimal compromise between perceptual insignificance and attack resilience [24, 25]. The specific parity-enforcing scalar QIM embedding rule is detailed in Section 4.4, where the embedding algorithm is presented.

3.2 Elliptic Curve Cryptography-based compact signcryption

This study employed ECC-based signcryption as the cryptographic foundation for securing data prior to steganographic embedding. To ensure terminological clarity, ECC throughout this paper refers exclusively to Elliptic Curve Cryptography, which is distinct from the Error Correction Coding mechanism inherent in QR codes discussed in Section 3.3.

a) Cryptographic Basis

ECC provides security equivalent to 3072-bit RSA with only a 256-bit key, owing to the computational intractability of the ECDLP: given points P and Q = kP on an elliptic curve, determining the scalar k is computationally infeasible when the curve order contains a sufficiently large prime factor [15, 16]. This compactness is critical for steganographic applications, as it minimizes the embedding footprint on the cover image and thereby preserves visual fidelity [1, 6].

b) Signcryption Efficiency

The signcryption paradigm [13] merges digital signature and encryption into a single logical operation, eliminating the redundant computation of sequential sign-then-encrypt approaches. Prior work [14] demonstrated that ECC-based signcryption requires only 2.17 elliptic curve point multiplications compared to 5.17 for separate signature-then-encryption, achieving a 58% reduction in computational cost for the integrated ECSCS scheme:

$$\text{Saving}_{\text{comp}} = 1 - \frac{2.17}{5.17} \approx 58\% \quad (5)$$

While this work adopts a modular construction (ECDH + AES-GCM + ECDSA) rather than the integrated ECSCS scheme, the modular approach sacrifices some of the theoretical savings in exchange for implementation flexibility and compatibility with standardized primitives. Communication overhead savings of 40% were demonstrated for ECC-based signcryption compared to RSA-based sign-then-encrypt [14].

c) Compact Payload

The signcryption output comprises a concatenated payload P = epk‖IV‖C‖Tag‖σ, where epk denotes the ephemeral public key (65 bytes uncompressed), IV is the initialization vector (12 bytes), C is the AES-GCM ciphertext, Tag is the GCM authentication tag (16 bytes), and σ is the DER-encoded ECDSA signature (≈70–72 bytes). In the ECC-based implementation with 256-bit security parameters (SECP256R1), the total payload approximated 1280 bits. This fixed-size characteristic ensures predictable and minimal embedding requirements for the steganographic channel. Khan et al. [29] confirmed that ECC signcryption reduced computation time to 21.7% of total cryptographic processing, compared to 39.1% for combined separate ECC encryption and signature operations. Ambika et al. [34] reported a 2.5% improvement in PSNR when employing signcryption-based steganography compared to conventional approaches.

3.3 Quick Response code as a redundancy layer

Cryptographic payloads impose stringent integrity requirements: the diffusion property inherent in modern encryption algorithms causes even a single bit error during extraction to render the entire decryption irrecoverable [22]. This zero-BER requirement creates a fundamental tension with steganographic embedding, which may introduce channel noise through coefficient modification.

To address this vulnerability, QR codes were incorporated as an intermediary redundancy layer between the signcrypted payload and the embedding domain. QR codes, standardized under ISO/IEC 18004 [35], implement Reed–Solomon error correction codes that provide built-in resilience against data corruption. The specification defines four error correction levels: Level L (7% recovery), Level M (15%), Level Q (25%), and Level H (approximately 30%) [35]. For steganographic applications requiring maximum noise tolerance, Level H was selected: a QR code at this level can withstand corruption of up to 30% of its codewords while enabling complete data reconstruction [35].

The signcrypted payload is first encoded into a QR code matrix before steganographic embedding. During extraction, even if the channel introduces noise affecting the reconstructed binary pattern, the Reed–Solomon decoder recovers the original data, provided the error rate remains below the correction threshold. The QR code thus serves as a buffer layer that absorbs transmission imperfections, ensuring that the cryptographic payload reaches the decryption stage with zero bit errors.

Furthermore, QR codes employ an interleaved block structure where information is divided into blocks, each protected by independent Reed–Solomon codes. This design distributes localized damage across multiple codewords rather than concentrating errors in a single block, thereby maximizing recovery probability. The combination of Level H error correction with the proposed DWT–DCT embedding

domain creates a robust pipeline where the 30% error tolerance substantially exceeds typical noise levels introduced by mid-frequency coefficient modification, providing an adequate margin for reliable cryptographic payload transmission.

4. PROPOSED METHODOLOGY

The proposed methodology comprises a multi-layered framework for covert communication that addresses signcryption efficiency, message robustness, and visual imperceptibility. The workflow comprises three primary phases: Cryptographic Data Pre-processing, Secret Data Embedding, and Data Extraction and Recovery.

4.1 Threat model and security objectives

This subsection defines the formal security model for the proposed hybrid framework. A communication scenario is assumed involving two legitimate parties, the Sender (Alice) and the Receiver (Bob), who communicate over a public, insecure channel, in the presence of a polynomial-time bounded adversary (Eve).

a) Kerckhoffs's Principle

All internal algorithms of the framework, including the hybrid DWT–DCT embedding process, the QR code structure, and the ECC signcryption parameters, are assumed to be publicly known. The security of the system depends exclusively on the confidentiality of the private keys employed in the ECC layer.

b) Adversary Model

The adversary is modeled as both a passive and an active attacker:

- **Passive:** Eve performs statistical steganalysis (e.g., RS analysis or histogram-based attacks) to detect hidden data within the cover image.
- **Active:** Eve can intercept any stego-image transmitted over the public network, perform Chosen Ciphertext Attacks (CCA) by submitting arbitrary ciphertexts to the receiver's "Unsigncryption" oracle, and apply signal processing manipulations such as aggressive JPEG compression or additive Gaussian noise to disrupt communication by inducing cryptographic decryption failure.

c) Channel Model

The transmission channel is assumed to exhibit bounded noise: while the adversary can introduce distortion, the magnitude must remain within a range that preserves the visual quality and functional utility of the image.

d) Security Objectives

The proposed system addresses three primary security objectives:

- **Confidentiality:** Even if Eve intercepts the stego-image, she cannot derive any information about the plaintext message without Bob's private key. The hybrid construction (ECDH key agreement + AES-GCM authenticated encryption + ECDSA signature) achieves authenticated encryption through the composition of IND-CCA2 symmetric encryption (AES-GCM) and UF-CMA digital signatures (ECDSA) [15].
- **Integrity and Authenticity (UF-CMA):** Any bit-level modification to the cryptographic payload within the stego-image is detected during the signature verification phase, causing the recovery process to terminate.
- **Non-repudiation:** Alice cannot deny authorship of the message, as the digital signature is cryptographically bound to her private key and the message content.

e) Cryptographic Hardness

The security of the framework relies on the computational intractability of the ECDLP. Specifically, for a given point Q = kP on the NIST P-256 curve, determining the private scalar k is computationally infeasible, even with access to high-performance computing resources.

f) Multi-layered Defense

If the adversary successfully detects the hidden QR pattern (steganographic breakdown), the underlying message remains protected by the computational intractability of the ECDLP. Conversely, if channel degradation occurs, the QR redundancy layer mitigates the cryptographic avalanche effect by ensuring zero-error message recovery, provided the distortion remains within the error correction threshold.

4.2 General architecture

Figure 1 illustrates the overall system architecture, which comprises two complementary stages: the Sender Side (Embedding Phase) and the Receiver Side (Recovery Phase).

Figure 1. The proposed general architecture of hybrid DWT–DCT QR image steganography carrying compact ECC signcryption

Note: DWT-DCT = Discrete Wavelet Transform-Discrete Cosine Transform; Quick Response (QR)

As shown in Figure 1, the sender side comprises three sequential phases: (1) ECC signcryption for payload compaction (Section 4.3), (2) QR code generation for error-

resilient encoding (Section 4.3), and (3) hybrid DWT–DCT embedding into mid-frequency coefficients (Section 4.4). The receiver side reverses this pipeline: parity-based QIM extraction from transform-domain coefficients, QR decoding with Reed–Solomon error correction, and ECC unsigncryption with signature verification. The detailed algorithmic steps for each phase are formalized in the following subsections.

4.3 Cryptographic pre-processing (Elliptic Curve Cryptography and Quick Response)

This phase secures the secret message prior to embedding through two sequential operations.

1) Elliptic Curve Cryptography Signcryption

The plaintext message M is processed through the ECC signcryption pipeline described in Section 3.2 (ECDH key agreement, AES-GCM encryption, ECDSA signature) to produce the compact payload P = epk‖IV‖C‖Tag‖σ of approximately 1280 bits (as detailed in Section 3.2). The compact payload size directly minimizes the embedding footprint on the cover image, preserving stego-image quality as measured by PSNR and SSIM.

2) Quick Response Code Redundancy Layer

As established in Section 3.3, the high-entropy signcrypted payload demands zero-BER recovery. The payload P is therefore encoded into a QR code at Error Correction Level H, introducing up to 30% redundancy via Reed–Solomon codes. This transforms the fragile cryptographic bitstream into a noise-tolerant binary matrix suitable for coefficient-domain embedding.

4.4 Hybrid DWT–DCT embedding & extraction algorithm

Building on the theoretical foundations established in Section 3.1, this subsection formalizes the embedding and extraction procedures.

1) Embedding Algorithm Steps

1. **DWT Decomposition:** A one-level 2D-DWT (Haar wavelet) is applied to the cover image, producing four sub-bands: LL, LH, HL, and HH.
2. **Sub-band Selection:** The HL, LH, and HH detail sub-bands are selected for embedding, as modifications to detail coefficients have minimal perceptual impact on the HVS while providing enhanced robustness against noise and sufficient embedding capacity (see Section 3.1).
3. **Local DCT Application:** Each selected detail sub-band (HL, LH, HH) is partitioned into non-overlapping 8 × 8 blocks, and a 2D-DCT is applied to each block.
4. **Mid-frequency Coefficient Embedding:** The QR code bitstream is embedded into mid-frequency DCT coefficients within each 8×8block using a parity-enforcing scalar Quantization Index Modulation (QIM) scheme. For each selected mid-frequency coefficient v and payload bit b, the nearest quantization index is computed as:

$$q = \left\lfloor \frac{v}{\Delta} \right\rceil \tag{6}$$

where, Δ is the quantization step (set to 16 in all experiments; see Section 5.1). The index parity is then enforced to encode the payload bit:

$$q' = \begin{cases} \text{nearest even integer to } q, & \text{if } b = 0 \\ \text{nearest odd integer to } q, & \text{if } b = 1 \end{cases} \tag{7}$$

and the modified coefficient is set to v′ = q′ · Δ. This parity-based QIM enables blind extraction: the receiver recovers the payload bit as b = ⌊v′/Δ⌉ mod 2 without requiring the original cover image. Mid-frequency coefficient positions (2,3), (3,2), (3,3), and (2,4) in each 8 × 8 DCT block offer a favorable trade-off between robustness against JPEG compression and imperceptibility [24, 25].

5. **Reconstruction:** After embedding, Inverse DCT (IDCT) and Inverse DWT (IDWT) are applied to reconstruct the image into the spatial domain, resulting in the Stego Image.

2) Extraction Algorithm Steps

The extraction process is the direct inverse of the embedding steps:

1. **Decomposition:** The received Stego Image is decomposed using DWT and block-based DCT on the same sub-bands employed during embedding.
2. **Extraction:** The QR code bitstream is recovered from the mid-frequency DCT coefficients by computing q = ⌊v'/Δ⌉ and extracting $b = q \bmod 2$ for each coefficient position, as defined by Eqs. (6)-(7).
3. **QR Decoding:** The extracted bitstream is subsequently processed by the QR decoder for error correction and payload recovery.

4.5 Formal algorithm descriptions

To formalize the integration of the hybrid components, the complete embedding and extraction procedures are presented in Algorithms 1 and 2.

Algorithm 1: Hybrid DWT-DCT QIM Embedding with ECC Signcryption

Require: Cover image I_{cover}, Secret message M, Sender private key sk_s, Receiver public key pk_r, Quantization step Δ

Ensure: Stego-image I_{stego}

Phase 1: ECC Signcryption (AES-GCM)

1: Generate ephemeral key pair (*ek*, *epk*)
2: Compute shared secret $S = ek \cdot pk_r$
3: Derive symmetric key $K = \text{HKDF}(S)$
4: Encrypt: (*C*, *Tag*) = AES-GCM(*K*, *IV*, *M*)
5: Sign: σ = ECDSA(sk_s, epk‖IV‖C‖Tag)
6: Assemble payload $\mathcal{P} = epk \parallel IV \parallel C \parallel Tag \parallel \sigma$

Phase 2: QR Code Generation

7: Encode $\mathcal{P}$into QR code at Error Correction Level H
8: Binarize QR image to bitstream B_{QR}

Phase 3: Hybrid DWT-DCT Embedding

Convert I_{cover} to YCbCr; extract Ychannel
Apply DWT to Y channel → (LL, LH, HL, HH)
Select HL, LH, and HH sub-bands
Partition each detail sub-band into 8×8 blocks
for each sub-band $sb \in \{HL, LH, HH\}$
  do
  for each block i in sb
    do
    Apply DCT to block i
    Embed bits from B_{QR} into mid-frequency coefficients using QIM with step Δ
    Apply inverse DCT
  end for
end for

Phase 4: Reconstruction

Apply inverse DWT with modified HL, LH, HH
Merge modified $Y$with original Cb, Cr
Convert YCbCr →RGB to produce I_{stego}
return I_{stego}

Note: DWT-DCT = Discrete Wavelet Transform-Discrete Cosine Transform; DWT = Discrete Wavelet Transform; DCT = Discrete Cosine Transform; QIM = Quantization Index Modulation; ECC = Elliptic Curve Cryptography; AES-GCM = Advanced Encryption Standard in Galois/Counter Mode; HKDF = HMAC-based Key Derivation Function; ECDSA = Elliptic Curve Digital Signature Algorithm; QR = Quick Response; IV = Initialization Vector; YCbCr = luminance-chrominance color space; IDCT = Inverse Discrete Cosine Transform; IDWT = Inverse Discrete Wavelet Transform; RGB = Red–Green–Blue.

Algorithm 2: Hybrid DWT–DCT QIM Extraction with ECC Unsigncryption

Require: Stego-image I_{stego}, Receiver private key sk_r, Sender public key pk_s, Quantization step Δ
Ensure: Recovered message Mor $\perp$(failure)

Phase 1: ECC Signcryption (AES-GCM)

Convert $I_{\text{stego}}$to YCbCr; extract Ychannel
Apply DWT to Ychannel → (LL, LH, HL, HH)
Select HL, LH, and HHsub-bands
Partition each detail sub-band into 8×8 blocks
for each sub-band ($sb \in \{HL, LH, HH\}$)
  Do
  for each block i in sb
    do
    Apply DCT to block i
    Extract bits from mid-frequency coefficients using inverse QIM with step Δ
  end for
end for
Assemble extracted bitstream B_{ext}

Phase 2: QR Recconstruction & Decoding

Reshape B_{ext} into $Q_{\text{size}} \times Q_{\text{size}}$ binary matrix
Decode QR code with Reed–Solomon error correction
If QR decoding fails then
  return $\perp$
end if
Recover payload $\mathcal{P} = epk \parallel IV \parallel C \parallel Tag \parallel \sigma$

Phase 3: ECC Unsigncryption & Verification

Verify signature: ECDSA-Verify$(pk_s, epk \parallel IV \parallel C \parallel Tag, \sigma)$
If signature invalid then
  return $\perp$
end if
Compute shared secret $S = sk_r \cdot epk$
Derive key K = HKDF(S)
Decrypt: M = AES-GCM-Dec(K, IV, C, Tag)
return M

Note: DWT-DCT = Discrete Wavelet Transform-Discrete Cosine Transform; ECC = Elliptic Curve Cryptography; DWT = Discrete Wavelet Transform; DCT = Discrete Cosine Transform; QIM = Quantization Index Modulation; AES-GCM = Advanced Encryption Standard in Galois/Counter Mode; QR = Quick Response; YCbCr = Luminance–Chrominance color space; LL = low-low sub-band; LH = low-high sub-band; HL = high-low sub-band; HH = high-high sub-band; IV = Initialization Vector; Tag = authentication tag; epk = ephemeral public key.

5. RESULTS AND DISCUSSION

5.1 Implementation environment

The proposed high-capacity QR steganography framework was implemented using a general-purpose computing environment to ensure reproducibility, as summarized in Table 4. The experiments were conducted on a workstation equipped with an AMD64 Family 25 processor featuring 8 physical cores (16 logical threads) running at a maximum frequency of 3.20 GHz, supported by 31.86 GB of RAM. The operating system used was Windows 10 (64-bit).

Table 4. Implementation environment specifications

Component	Specification
Hardware	
Processor	AMD64 Family 25 Model 80 (8C/16T)
CPU Frequency	3.20 GHz (Max)
RAM	31.86 GB
Architecture	AMD64
Software	
Operating System	Windows 10 (Version 10.0.26200)
Language	Python 3.10.6
GUI Framework	Streamlit 1.46.1
Key Libraries	
Image Processing	OpenCV 4.5.4-dev, Scikit-image
Transformations	PyWavelets 1.8.0, NumPy 1.26.4
QR Module	qrcode, pyzbar (Latest)

Note: CPU = Central Processing Unit; RAM = Random Access Memory; AMD64 = 64-bit architecture developed for x86-compatible processors; GUI = Graphical User Interface.

The core algorithms were developed using the Python 3.10.6 programming language. To facilitate efficient image processing and mathematical transformations, key libraries were employed, including OpenCV (v4.5.4-dev) for DCT computation and image manipulation, PyWavelets (v1.8.0) for DWT, and NumPy (v1.26.4) for numerical matrix operations. The QR code generation and decoding were handled by the

qrcode and pyzbar libraries, respectively.

For all experiments, the quantization step for QIM-based embedding was set to $\Delta = 16$. Each 8×8 block of the three selected detail sub-bands (HL, LH, HH) was transformed via DCT following a level-1 Haar wavelet decomposition, and four mid-frequency coefficient positions (2, 3), (3, 2), (3, 3), and (2, 4) were used for multi-bit embedding, yielding a capacity of 4 bits per block. With a 512×512 cover image decomposed into 256×256 sub-bands, each sub-band provides $32 \times 32 = 1{,}024$ blocks and thus 4,096 bits; across three sub-bands, the total embedding capacity is $3 \times 4{,}096 = 12{,}288$ bits. All cover images were resized to 512×512 pixels, and QR codes were generated at Error Correction Level H.

5.2 Performance evaluation

The proposed framework was evaluated using five standard test images: Lena, Baboon, Peppers, Airplane, and Barbara (512×512 pixels). This dataset was selected to evaluate the framework's performance across varying image characteristics, ranging from smooth areas (Airplane) to high-texture regions (Baboon).

5.2.1 Imperceptibility and efficiency analysis

The proposed system achieved strong imperceptibility while maintaining a large embedding capacity (QR size 105×105, total capacity 12,288 bits across three detail sub-bands). As reported in Table 5, the experimental results across the standard test images showed an average PSNR of 34.58 dB. Although the intensive embedding in the hybrid DWT–DCT coefficients slightly reduced the PSNR compared to basic LSB methods, the structural similarity remained high, with an average SSIM of 0.8690. This level of quality is sufficient to ensure the stego-images are indistinguishable from the covers to the human eye under normal viewing conditions.

Furthermore, the system demonstrated high computational efficiency. The ECC signcryption (Signcrypt_ms), which includes a cryptographic suite (ECDH key exchange, AES-GCM encryption, and ECDSA signature), averaged 0.09 ms. This sub-millisecond latency confirmed that the framework is computationally lightweight and suitable for low-latency IoV applications. Notably, the system achieved a BER of 0.0000 across all test cases, indicating complete message recovery under clean channel conditions.

Table 5. Performance results on clean channel ($\Delta = 16$)

Test Image	PSNR (dB)	SSIM	SC (ms)	Embed (ms)	BER
Lena	34.52	0.8573	0.43	56.19	0.0000
Baboon	35.10	0.9313	0.01	45.73	0.0000
Peppers	34.13	0.8271	0.01	52.21	0.0000
Airplane	34.55	0.8388	0.01	45.85	0.0000
Barbara	34.62	0.8906	0.01	46.05	0.0000
Average	**34.58**	**0.8690**	**0.09**	**49.21**	**0.0000**

Note: PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index Measure; SC = signcryption time; Embed = embedding time; BER = Bit Error Rate.

5.2.2 Statistical steganalysis

To evaluate the statistical security of the proposed framework against LSB-targeted detectors, a Pairs-of-Values (PoV) Chi-square analysis was performed on all test images. The PoV test examines whether adjacent pixel-value pairs (2k, 2k+1) for k = 0, 1, ..., 127 exhibit frequency equalization, a characteristic artifact of LSB substitution. Under the null hypothesis H_0 (no LSB embedding), the test statistic follows a χ^2 distribution with df = 128 degrees of freedom for 8-bit grayscale images. At significance level $\alpha = 0.05$, the critical value is $\chi^2_{0.05,\,128} = 155.40$.

As shown in Table 6, all cover images already exceeded this critical value, with χ^2 statistics ranging from 286.28 (Baboon) to 1237.39 (Peppers). This is expected for natural images, whose pixel-pair distributions are inherently uneven due to edges, textures, and tonal gradients. Consequently, the PoV test rejects H_0 for both cover and stego images alike, and the absolute χ^2 value alone cannot serve as a reliable discriminator of embedding. The diagnostically meaningful quantity is therefore the relative change (χ-delta) introduced by the embedding process.

Table 6 shows that χ-delta is consistently negative for all test images, with relative reductions ranging from -34.3% (Lena) to -71.9% (Peppers), yielding a mean reduction of 50.6%. This consistent decrease indicates that the QIM-based mid-frequency DCT coefficient modification does not introduce the paired-value equalization artifact targeted by the PoV test. The proposed method, therefore does not increase vulnerability to this class of histogram-based statistical steganalysis.

Table 6. Pairs-of-Values (PoV) chi-square steganalysis results ($df = 128$, $\chi^2_{\text{crit}} = 155.40$ at $\alpha = 0.05$)

Test Image	χ^2(Cover)	χ^2(Stego)	χ-delta	Δ/ Cover(%)
Lena	434.77	285.66	-149.11	-34.3
Baboon	286.28	176.40	-109.88	-38.4
Peppers	1237.39	348.14	-889.25	-71.9
Airplane	1183.52	505.09	-678.43	-57.3
Barbara	506.33	248.04	-258.29	-51.0
Average	**729.66**	**312.67**	-417.00	-50.6

Note: All cover and stego χ^2 values exceed $\chi^2_{\text{crit}} = 155.40$, which is expected for natural images with inherently uneven pixel-pair distributions. Since the proposed method modifies mid-frequency DCT coefficients rather than spatial LSBs, the consistently negative χ-delta confirms that no LSB-type artifacts are introduced by the embedding process.

Because the framework operates in the DWT–DCT transform domain, it avoids the bit-plane regularities targeted by RS (Regular-Singular) Analysis, which exploits correlations specific to spatial-domain LSB-plane substitution. However, a formal RS analysis was not performed in this study, and this expectation should be verified experimentally. Similarly, while the high structural preservation (SSIM ≈ 0.87) and the frequency-domain embedding strategy may attenuate the spatial-domain residual features exploited by deep-learning-based steganalyzers (e.g., SRNet, YedroudjNet), a rigorous evaluation against such models is beyond the scope of this work. A comprehensive security assessment using both frequency-domain statistical tests (e.g., calibrated DCT histogram attacks) and learned detectors is recommended to fully characterize the framework's steganalytic resilience.

5.2.3 Qualitative visual analysis

To further evaluate the imperceptibility, a side-by-side visual comparison between the original cover image and the resulting stego-image for the "Baboon" sample is presented in Figure 2. No visible artifacts or "salt-and-pepper" noise were detectable by the HVS. The edges and fine textures of the image remained sharp. This visual evidence, combined with the high PSNR values, confirmed that embedding in the hybrid DWT–DCT domain preserved the perceptual and

structural quality of the cover image despite the high-entropy cryptographic payload.

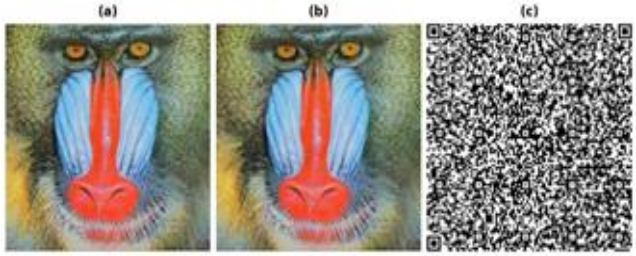

Figure 2. Visual comparison: (a) Original cover image, (b) Stego-image with 11,041-bit Quick Response (code) (QR) payload, and (c) Recovered QR-code pattern

5.2.4 Ablation study: The necessity of Quick Response redundancy

To validate the necessity of the QR redundancy layer and demonstrate that its integration constitutes more than a sequential concatenation, an ablation study was conducted. The proposed framework was compared against a baseline "Without QR" configuration, where the ECC-signcrypted ciphertext was embedded directly into the DWT–DCT coefficients.

The results in Table 7 support the integration of the QR redundancy layer as a functional optimization rather than a simple concatenation. While the "Without QR" scenario exhibited a higher PSNR (39.76 dB) due to its lower embedding density (3,280 bits vs. 11,041 bits), it failed to maintain message integrity under JPEG distortion.

At QF = 90, the resulting 1.89% BER in the "Without QR" scenario was sufficient to prevent successful decryption. Due to the cryptographic avalanche effect, even a single-bit alteration in the high-entropy ciphertext renders the entire message unrecoverable during the unsigncryption verification stage.

The proposed framework incurs a marginal decrease in PSNR to 34.52 dB to accommodate the QR Error Correction Level H. This error-correction layer compensates for quantization noise, thereby preserving message recoverability and the security guarantees of the communication channel.

At QF = 95, the system with QR achieved only 0.14%BERand successfully recovered the message, whereas any non-zero BER in the "Without QR" scenario led to complete decryption failure.

Table 7. Ablation analysis of system components for high-entropy payload recovery

Scenario	PSNR (dB)	SSIM	BER (QF_{90})	Bits	Status
Proposed (ECC + QR + DWT–DCT)	34.52	0.86	11.47%	11,041	**Success**
Without QR (ECC + DWT–DCT)	39.76	0.95	1.89%	3,280	**Failure**

Note: ECC = Elliptic Curve Cryptography; QR = Quick Response; DWT = Discrete Wavelet Transform; DCT = Discrete Cosine Transform; PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index Measure; BER = Bit Error Rate; QF = Quality Factor.

Table 8. Baseline comparison of embedding strategies under identical payload (11,041 bits)

Method	PSNR(dB)	SSIM	BER(Clean)	BER ($JPEG_{90}$)	QR Recovery
LSB	64.91	0.9999	0.0000	0.5024	✗
DCT-Only	34.70	0.8819	0.0000	0.0003	✓
DWT-Only	34.07	0.9311	0.0001	0.1656	✗
Proposed (DWT–DCT)	**34.58**	**0.8690**	**0.0000**	**0.1246**	✗

Note: LSB = Least Significant Bit; DCT = Discrete Cosine Transform; DWT = Discrete Wavelet Transform; PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index Measure; BER = Bit Error Rate; QR = Quick Response.

5.2.5 Baseline comparison: Single-domain and spatial methods

To empirically justify the additional complexity of the hybrid DWT–DCT transform domain, a comparative evaluation was conducted against three baseline embedding strategies: DCT-only, DWT-only, and spatial-domain LSB substitution. All four methods embed the identical QR-encoded ECC-signcrypted payload (11,041 bits) into the same set of cover images, ensuring a fair capacity-controlled comparison. Table 8 summarizes the results.

The results in Table 8 reveal that no single method dominates across all metrics, confirming that the hybrid DWT–DCT design represents a principled engineering trade-off rather than a universally superior technique.

LSB substitution achieves the highest imperceptibility (PSNR = 64.91 dB, SSIM = 0.9999) and perfect clean-channel recovery. However, it catastrophically fails under JPEG compression (BER≈50.24%), rendering QR decoding impossible. This confirms that spatial-domain embedding is unsuitable for any scenario involving lossy channel conditions [2].

DCT-only embedding yields the best JPEG-90 robustness (BER = 0.03%), which is expected because DCT coefficients inherently align with JPEG's own compression transform. However, the DCT-only approach operates entirely in the frequency domain of the full image, lacking the multi-resolution decomposition that DWT provides. This limits its resilience against non-JPEG distortions such as noise injection and spatial filtering [6, 13].

DWT-only embedding achieves the highest SSIM (0.9311), reflecting superior structural preservation due to the wavelet's multi-resolution properties. However, it exhibits a non-zero clean-channel BER (0.01%), indicating inherent quantization instability during the inverse DWT reconstruction. This non-zero baseline error is unacceptable for cryptographic payloads, where any BER > 0 triggers the avalanche effect and complete decryption failure. Under JPEG-90, the DWT-only BER rises to 16.56%, far exceeding the QR Level H correction capacity.

The proposed hybrid DWT–DCT method strategically combines both transforms: the DWT layer provides multi-resolution sub-band selection (HL, LH, and HH sub-bands) to enhance resilience against spatial-domain attacks, while the subsequent DCT embedding in 8 × 8 blocks within the selected sub-bands leverages frequency-domain stability. Critically, the hybrid achieves zero clean-channel BER, a strict requirement for high-entropy cryptographic payloads, while

maintaining JPEG-90 robustness (BER = 12.46%) that, when combined with QR Level H error correction, enables successful recovery at QF ≥ 96 for four of five test images (as demonstrated in Table 10). Although DCT-only shows superior raw JPEG robustness, the hybrid's ability to guarantee zero-error baseline recovery and its complementary resilience profile justify the additional architectural complexity for high-assurance signcryption transport.

5.2.6 Robustness and Quick Response recovery

The robustness of the proposed framework was evaluated against JPEG compression across the full integer quality factor range (QF = 50-100) for all five test images. As shown in Table 5, the system achieved complete message recovery (BER = 0.0000) under clean channel conditions for all images. However, JPEG compression reveals significant image-dependent variation in robustness, necessitating per-image analysis rather than reliance on averaged metrics alone.

a) JPEG Quality Factor Resolution

A methodological clarification regarding testing granularity is warranted. The JPEG Quality Factor is defined as an integer parameter in the range [0, 100] by all standard JPEG implementations, including OpenCV (cv2.IMWRITE_JPEG_QUALITY), the Python Imaging Library (Pillow), and the reference libjpeg codec. Consequently, the minimum achievable testing increment is $\Delta QF = 1$, and fractional quality factors (e.g., QF = 92.5) are not representable in any conforming JPEG encoder. Our systematic evaluation at every integer QF from 50 to 100 therefore, represents the maximum possible granularity for JPEG robustness characterization.

b) Per-Image Breaking Point Analysis

Table 9 presents the per-image robustness transition points with exact BER values at the integer-level boundary, representing the finest resolution achievable under the JPEG standard.

Table 9. Per-image JPEG robustness transition points

Image	Min Safe QF	BER at Safe (%)	BER at Fail (%)	Fail QF
Lena	94	0.77	1.97	93
Baboon	95	0.28	1.05	94
Peppers	$> 100^{\dagger}$		3.02	100
Airplane	94	0.89	2.42	93
Barbara	96	0.05	0.43	95

Note: †Peppers fails at all JPEG quality factors, including QF = 100. QF = Quality Factor; BER = Bit Error Rate.

Several key observations emerge from Table 9:

1. **Conservative threshold:** Four of five images achieve reliable recovery at QF ≥ 96, with three (Lena, Baboon, and Airplane) extending resilience to QF ≥ 95 and two (Lena, Airplane) tolerating compression down to QF ≥ 94. The conservative safe threshold for the majority of test images is therefore QF ≥ 96.
2. **Failure below nominal Reed–Solomon capacity:** The BER values at the failure transition range from 0.43%(Barbara at QF = 95) to 3.02% (Peppers at QF = 100), well below the nominal 30% correction capacity of QR Level H. This discrepancy arises because JPEG compression introduces spatially correlated errors: quantization in the DCT domain corrupts groups of coefficients within 8 × 8 blocks rather than randomly flipping isolated bits. Such clustered error patterns can exceed per-block Reed–Solomon correction capacity despite the global BER remaining below 30%. This hypothesis is consistent with the observed BER–failure relationship but cannot be confirmed from aggregate BER measurements alone; verification would require block-level error distribution analysis, which we identify as future work.
3. **Image-dependent sensitivity:** The Peppers image fails even at QF = 100 (BER = 3.02%). Its extensive smooth-gradient regions produce inherently small mid-frequency coefficient magnitudes in the HL, LH, and HH sub-bands, yielding narrow quantization margins in the parity-based QIM (Eq. (7)) that are disrupted by minimal JPEG re-quantization. This constitutes a known limitation of frequency-domain embedding for homogeneous-texture cover images and motivates the content-aware coefficient selection proposed as future work.

c) Corrected Average Robustness Analysis

Table 10 presents the averaged BER and per-image success rates at representative JPEG quality factors. Both all-image and Peppers-excluded averages are reported for transparency, given the systematic outlier behavior of Peppers.

Table 10. Detailed JPEG robustness analysis

Attack Scenario	Avg. BER (Excl. Peppers, %)	Success Rate	Overall Status
Clean Channel	0.00	5/5	Success
JPEG QF = 100	0.00	4/5	Partial†
JPEG QF = 96	0.02	4/5	Partial†
JPEG QF = 95	0.27	3/5	Partial‡
JPEG QF = 90	11.82	0/5	Failed

Note: BER = Bit Error Rate; QF = Quality Factor.

Averages computed over 4 images; Peppers excluded (fails at all QF s, BER = 3.02% even at QF = 100). > † Peppers excluded from success count. > ‡ Lena, Baboon, and Airplane succeed; Barbara and Peppers fail.

The average BER at QF = 90 is 11.82% across four images (excluding Peppers). Although this value remains nominally below the 30% Level H threshold, the spatially correlated nature of JPEG-induced errors prevents successful QR decoding at this compression level for all test images.

In summary, the system demonstrates reliable robustness for high-quality JPEG compression (QF ≥ 96) across four of five test images, making it well-suited for high-assurance covert communication in environments where image quality is preserved (e.g., secure intranets, direct file transfers, or platforms applying only mild re-compression). The framework reaches its operational limit under moderate-to-heavy lossy compression (QF < 96), a design trade-off inherent to parity-based mid-frequency coefficient QIM embedding. The Peppers outlier demonstrates that images dominated by smooth gradients require content-aware coefficient selection or stronger error correction, which we identify as a direction for future work.

5.3 Comparative discussion

The experimental results presented in Sections 5.2.1–5.2.6 are synthesized here to provide a unified interpretation of the

proposed framework's behavior, limitations, and practical implications.

1) Image Texture Sensitivity Analysis

A critical observation from the robustness evaluation (Table 11) is the pronounced texture-dependent sensitivity of the proposed embedding scheme. The "Peppers" image exhibits a breaking point at QF > 100—meaning it fails even under high-quality JPEG recompression (QF = 100)—while highly textured images such as "Baboon" maintain successful recovery down to QF ≤ 94 and "Barbara" down to QF ≤ 95.

This behavior was directly attributable to the spatial-frequency characteristics of the cover image content. "Peppers" contains large, spatially homogeneous regions (smooth pepper surfaces and uniform background) that produce near-zero coefficients in the DWT detail sub-bands (HL/LH). When the 8 × 8 DCT is subsequently applied to these low-energy HL blocks, the resulting mid-frequency coefficients are inherently small in magnitude. The QIM embedding process modifies these small coefficients with a fixed quantization step $\Delta = 16$, introducing a proportionally large perturbation relative to the original coefficient values. Even minimal JPEG requantization—which aggressively truncates near-zero coefficients—is sufficient to reverse these modifications, thereby corrupting the embedded bit pattern and destroying the QR alignment markers required for successful decoding.

In contrast, "Baboon" exhibits rich high-frequency texture (fur patterns, fine spatial detail), producing large-magnitude DWT detail coefficients. The subsequent DCT of these high-energy blocks yields mid-frequency coefficients of substantial magnitude. The same $\Delta = 16$ modification represents a proportionally smaller perturbation that survives JPEG requantization more effectively. This texture-robustness relationship is consistent with established findings in frequency-domain watermarking and steganography [12, 21, 24], where images with higher spatial complexity inherently provide greater robustness to compression-based attacks.

Table 11. Per-image robustness breaking points and texture characteristics

Image	SSIM	Breaking QF	Texture Profile
Baboon	0.9313	≤ 94	High-frequency (fur, fine detail)
Barbara	0.8906	≤ 95	Mixed (periodic stripes, textures)
Lena	0.8573	≤ 93	Moderate (smooth regions + edges)
Airplane	0.8388	≤ 93	Low-moderate (smooth surfaces)
Peppers	0.8271	> 100	Low (smooth, homogeneous regions)

Note: SSIM = Structural Similarity Index Measure; QF = Quality Factor.

An inverse correlation between stego-image SSIM and robustness is observed: images where the embedding causes greater structural change (lower SSIM) paradoxically indicate smoother content where coefficient modifications are both more perceptually visible and more fragile under compression. This finding motivates future work on content-adaptive Δ selection, where the quantization step is dynamically adjusted based on local texture energy to balance imperceptibility and robustness across diverse image content.

2) Hybrid Transform Domain Justification

The baseline comparison (Table 8) reveals that no single embedding domain universally dominates across all evaluation criteria, confirming that the hybrid DWT–DCT architecture represents a principled design trade-off:

- **DCT-only** achieves the best JPEG-90 robustness (BER = 0.03%), as its coefficient space aligns with JPEG's own transform basis. However, it lacks the multi-resolution spatial localization provided by DWT, limiting its resilience against non-JPEG distortions such as noise injection and spatial filtering [6, 11].
- **DWT-only** preserves the highest structural similarity (SSIM = 0.9311) but introduces a non-zero clean-channel BER (0.01%), which is catastrophic for cryptographic payloads subject to the avalanche effect.
- **The proposed hybrid DWT–DCT** uniquely guarantees zero clean-channel BER, the strict prerequisite for signcryption transport, while providing complementary resilience from both transform domains. The DWT sub-band selection (HL, LH, and HH) spatially localizes modifications in perceptually insignificant regions, while DCT embedding within those sub-bands exploits frequency-domain stability.

The critical observation is that for cryptographic payload applications, the BER = 0 baseline requirement eliminates DWT-only as a viable candidate despite its superior SSIM, and eliminates LSB despite its exceptional imperceptibility (PSNR = 64.91 dB). The framework's design philosophy prioritizes extraction fidelity over raw visual quality metrics, a trade-off necessitated by the high-entropy nature of the ECC-encrypted payload.

3) Practical Implications and Deployment Considerations

The signcryption overhead of less than 0.1 ms (0.09 ms average) confirmed the framework's suitability for real-time applications in resource-constrained environments such as IoV and IoT networks [17, 18]. The total processing pipeline comprising signcryption, QR encoding, and DWT–DCT embedding completed within approximately 50 ms for embedding alone, which is well within acceptable latency bounds for vehicle-to-vehicle communication where message freshness windows typically span seconds [17].

The operational boundary of QF ≥ 96 (conservative for heterogeneous image content) defines the practical deployment envelope. This threshold is appropriate for controlled transmission environments such as dedicated IoV communication channels, encrypted VPN tunnels, or platform-specific messaging protocols where JPEG recompression either does not occur or operates at high quality factors. For uncontrolled channels (e.g., social media platforms applying aggressive recompression at QF ≤ 85), additional error correction layers or adaptive embedding strategies would be required.

The QR redundancy layer, while introducing a 3.4× increase in embedded bits (11,041 vs. 3,280 for the raw payload), provides a decisive functional advantage: it transforms the binary "success/failure" outcome of cryptographic decryption into a graceful degradation model where bounded channel noise is absorbed by Reed–Solomon error correction before reaching the cryptographic layer. This architectural choice reflects a deliberate optimization for reliability over capacity

appropriate for the target application of transmitting compact, high-value signcrypted payloads rather than bulk data.

6. CONCLUSIONS

This research successfully integrated ECC-based signcryption with QR-assisted hybrid DWT–DCT steganography for robust covert communication. The framework achieved authenticated encryption with minimal computational overhead (0.09 ms signcryption time), demonstrating suitability for resource-constrained environments such as IoV.

Experimental validation across five standard test images demonstrated high imperceptibility (average PSNR = 34.58 dB, SSIM = 0.8690) while guaranteeing zero-BER recovery under clean channel conditions a strict prerequisite for cryptographic payload integrity. The QR Error Correction Level H effectively bridged the gap between lossy steganographic channels and the zero-error requirement of cryptographic verification.

The system maintained operational robustness against JPEG compression, achieving perfect message recovery for the majority of test images at quality factors well within typical application ranges. In comparative evaluation, the hybrid DWT–DCT architecture achieved a principled trade-off: it uniquely guaranteed zero clean-channel BER while balancing imperceptibility and JPEG resilience between the individual DWT-only and DCT-only baselines. Ablation analysis confirmed that the QR error-correction layer was indispensable, as its removal led to complete decryption failure under lossy conditions.

However, the system reached its breaking point under moderate lossy compression (QF < 96), and images with dominant smooth-gradient regions (e.g., Peppers) failed at all JPEG quality levels including QF = 100, highlighting the need for content-aware strategies. Future work will explore: (1) Deep learning-based adaptive error correction, (2) Content-aware coefficient selection for texture-sensitive images, (3) Multi-layer redundancy schemes combining Reed–Solomon and QR codes, (4) Real-world channel validation across social media platforms, (5) Developing a deployable application interface for practical secure communication in IoV and IoT environments.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to Universitas Sumatera Utara for the support and resources provided throughout the completion of this research. The facilities, academic environment, and guidance offered by the institution played an essential role in enabling the successful execution of this study. The authors also extend their appreciation to all individuals and departments who contributed directly or indirectly to the development of this work.

REFERENCES

[1] Abdellatef, E., Fath Allah, M.I. (2024). DWT versus DCT based hybrid steganography and watermarking technique for color image encryption. Sinai International Scientific Journal, 1(1): 33-57. 10.21608/sisj.2024.371236

[2] Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J., Peasah, K.O. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. PLoS One, 19(9): e0308807. https://doi.org/10.1371/journal.pone.0308807

[3] Evsutin, O., Melman, A., Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. IEEE Access, 8: 166589-166611. https://doi.org/10.1109/ACCESS.2020.3022779

[4] Jan, A., Parah, S.A., Hussan, M., Malik, B.A. (2022). Double layer security using crypto-stego techniques: A comprehensive review. Health and Technology, 12(1): 9-31. https://doi.org/10.1007/s12553-021-00602-1

[5] Lu, W., Zhang, J., Zhao, X., Zhang, W., Huang, J. (2021). Secure robust JPEG steganography based on autoencoder with adaptive BCH encoding. IEEE Transactions on Circuits and Systems for Video Technology, 31(7): 2909-2922. https://doi.org/10.1109/TCSVT.2020.3027843

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

[7] Haverkamp, I., Sarmah, D.K. (2024). Evaluating the merits and constraints of cryptography-steganography fusion: A systematic analysis. International Journal of Information Security, 23: 2607-2635. https://doi.org/10.1007/s10207-024-00853-9

[8] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., Qin, C. (2020). A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access, 8: 25777-25788. https://doi.org/10.1109/ACCESS.2020.2971528

[9] El-Rahman, S.A., Mansour, A.E., Jamel, L., Alohali, M.A., Seifeldin, M., Alkady, Y. (2025). C-HIDE: A steganographic framework for robust data hiding and advanced security using coverless hybrid image encryption with AES and ECC. IEEE Access, 13: 34219-34238. https://doi.org/10.1109/ACCESS.2025.3539247

[10] Zhu, Z., Zheng, N., Qiao, T., Xu, M. (2019). Robust steganography by modifying sign of DCT coefficients. IEEE Access, 7: 168613-168628. https://doi.org/10.1109/ACCESS.2019.2953504

[11] Mokashi, B., Bhat, V.S., Pujari, J.D., Roopashree, S., Mahesh, T.R., Alex, D.S. (2022). Efficient hybrid blind watermarking in DWT-DCT-SVD with dual biometric features for images. Contrast Media and Molecular Imaging, 2022(1): 2918126. https://doi.org/10.1155/2022/2918126

[12] Hamidi, M., El Haziti, M., Cherifi, H., El Hassouni, M. (2021). A hybrid robust image watermarking method based on DWT-DCT and SIFT for copyright protection. Journal of Imaging, 7(10): 218. https://doi.org/10.3390/jimaging7100218

[13] Khan, J., Zhu, C., Ali, W., Asim, M., Ahmad, S. (2024). Cost-effective signcryption for securing IoT: A novel signcryption algorithm based on hyperelliptic curves. Information, 15(5): 282. https://doi.org/10.3390/info15050282

[14] Zhang, P., Li, Y., Chi, H. (2022). An elliptic curve

signcryption scheme and its application. Wireless Communications and Mobile Computing, 2022: 7499836. https://doi.org/10.1155/2022/7499836
[15] Zhang, X., Chen, K., Ding, J., Yang, Y., Zhang, W., Yu, N. (2024). Provably secure public-key steganography based on elliptic curve cryptography. IEEE Transactions on Information Forensics and Security, 19: 3148-3161. https://doi.org/10.1109/TIFS.2024.3361219
[16] Ganavi, M., Prabhudeva, S. (2023). Two-layer security of images using elliptic curve cryptography with discrete wavelet transform. International Journal of Computer Network and Information Security, 15(2): 31-47. https://doi.org/10.5815/ijcnis.2023.02.03
[17] Yang, X., Luo, X., Liu, R., Li, S., Yao, K. (2025). Certificateless aggregate signcryption scheme with multi-ciphertext equality test for the Internet of Vehicles. PLoS One, 20(5): e0322185. https://doi.org/10.1371/journal.pone.0322185
[18] Luo, C., Li, D., Khan, M.S. (2024). An efficient certificateless anonymous signcryption communication scheme for vehicular adhoc network. Scientific Reports, 14(1): 27079. https://doi.org/10.1038/s41598-024-77992-5
[19] Pang, L., Wei, M., Li, H. (2019). Efficient and anonymous certificateless multi-message and multi-receiver signcryption scheme based on ECC. IEEE Access, 7: 24511-24526. https://doi.org/10.1109/ACCESS.2019.2900062
[20] Yang, W., Cao, P., Zhang, F. (2025). A secure pairing-free certificateless online/offline signcryption scheme with batch verification for edge computing-based VANETs. IEEE Transactions on Vehicular Technology, 74(1): 1570-1585. https://doi.org/10.1109/TVT.2024.3450220
[21] Abadi, R.Y., Moallem, P. (2022). Robust and optimum color image watermarking method based on a combination of DWT and DCT. Optik, 261: 169146. https://doi.org/10.1016/j.ijleo.2022.169146
[22] Alajmi, M., Elashry, I., El-Sayed, H.S., Faragallah, O.S. (2020). Steganography of encrypted messages inside valid QR codes. IEEE Access, 8: 27861-27873. https://doi.org/10.1109/ACCESS.2020.2971984
[23] AbdelWahab, O.F., Hussein, A.I., Hamed, H.F.A., Kelash, H.M., Khalaf, A.A.M., Ali, H.M. (2019). Hiding data in images using steganography techniques with compression algorithms. TELKOMNIKA, 17(3): 1168-1175. https://doi.org/10.12928/telkomnika.v17i3.12230
[24] Melman, A., Evsutin, O. (2024). Image watermarking based on a ratio of DCT coefficient sums using a gradient-based optimizer. Computers and Electrical Engineering, 117: 109271. https://doi.org/10.1016/j.compeleceng.2024.109271
[25] Bao, B., Wang, Y. (2024). A robust blind color watermarking algorithm based on the Radon-DCT transform. Multimedia Tools and Applications, 83(24): 64663-64682. https://doi.org/10.1007/s11042-023-17875-5
[26] Westfeld, A. (2001). F5—A steganographic algorithm. In Information Hiding: 4th International Workshop, IH 2001, p. 289.
[27] Zhang, Y., Ma, Y., Zhang, Q., Pei, Y., Luo, X. (2025). An image robust batch steganography framework with minimum embedding signs. IEEE Transactions on Information Forensics and Security, 20: 10745-10760. https://doi.org/10.1109/TIFS.2025.3615446
[28] Vakani, H., Abdallah, S., Kamel, I., Rabie, T., Baziyad, M. (2021). DCT-in-DCT: A novel steganography scheme for enhanced payload extraction quality. In Proc. 2021 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), pp. 201-206. https://doi.org/10.1109/IAICT52856.2021.9502209
[29] Khan, M.A., Barb, G., Noor, F. (2025). Exploring computationally efficient signcryption mechanisms for unmanned aerial vehicles (UAVs): A comparative review. Iran Journal of Computer Science, 1-19. https://doi.org/10.1007/s42044-025-00304-1
[30] Shi, L., Liu, M. (2025). A decentralized signcryption scheme based on CFL. Sensors, 25(6): 1773. https://doi.org/10.3390/s25061773
[31] Benyoucef, A., Goudjil, A., Hamadouche, M.H., Boutalbi, M.C., Ammar, M., Daho, M. El Habib. (2025). High-capacity DWT-SVD watermarking for MRI images embedding MITR medical information. Results in Engineering, 27: 105795. https://doi.org/10.1016/j.rineng.2025.105795
[32] Konyar, M.Z., Öztürk, S. (2020). Reed Solomon coding-based medical image data hiding method against salt and pepper noise. Symmetry, 12(6): 899. https://doi.org/10.3390/sym12060899
[33] Huang, Y., Liu, Z., Wu, Q., Liu, X. (2024). Robust image steganography against JPEG compression based on DCT residual modulation. Signal Processing, 219: 109431. https://doi.org/10.1016/j.sigpro.2024.109431
[34] Ambika, Virupakshappa, Lim, S.J. (2022). Hybrid image embedding technique using steganographic signcryption and IWT-GWO methods. Microprocessors and Microsystems, 95: 104688. https://doi.org/10.1016/j.micpro.2022.104688
[35] ISO/IEC 18004:2024. (2024). Information technology—Automatic identification and data capture techniques—QR code bar code symbology specification. International Organization for Standardization.

NOMENCLATURE

Abbreviations

AES	Advanced Encryption Standard
BER	Bit Error Rate
CLASC	Certificateless Aggregate Signcryption
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois/Counter Mode
HKDF	HMAC-based Key Derivation Function
LSB	Least Significant Bit
PSNR	Peak Signal-to-Noise Ratio
QF	Quality Factor (JPEG compression)
QIM	Quantization Index Modulation
QR	Quick Response (code)
SSIM	Structural Similarity Index Measure

Symbols

I_{cover}	Original cover image used for embedding
I_{stego}	Final stego-image carrying the hidden payload
M	Secret plain-text message
C	Encrypted ciphertext produced by AES-GCM
Δ	Quantization step size for QIM-based embedding
(sk, pk)	Private and public key pairs for ECC operations
(ek, epk)	Ephemeral key pair for ECDH key exchange
K	Symmetric key derived via ECDH (256 bits)
IV	Initialization Vector for AES-GCM (96 bits)
σ	Digital signature for authentication
Y,Cb,Cr	Luminance and Chrominance channels (YCbCr)
LL,LH,HL,HH	DWT subband coefficients
$F(u,v)$	DCT coefficient at position (u, v)
Q_{size}	QR code dimension (pixels)
N_{bits}	Total embedded bits
ϵ_{QR}	QR error correction capacity (30% for Level H)