Minimax Theory and its Applications
Volume 11 (2026), No. 4s, 1032-1041

Securing Wireless Capsule Endoscopy Data with Dual-Layer Image Steganography and Blockchain Validation

Shravani Amar[1], Dr Raviteja Kocherla[2], Anitha Perla[3]

[1]Research Scholar(Ph.D), Department of Information Technology, Malla Reddy University Maisammaguda, 500100, Email: 2232CS020005@mallareddyuniversity.ac.in, 0009-0007-6132-7284
[2]Department of Computer Science & Engineering, Malla Reddy University, Hyderabad, Telangana, India-500100, Email: tejakcse@gmail.com, 0009-0002-0193-7287
[3]Dept of ECE, RVRJC College of Engineering Guntur, Chowdavaram, Andhra Pradesh 522019
Email: anithakrishna77p@gmail.com, 0000-0002-1964-0126

Abstract
Wireless Capsule Endoscopy (WCE) has become a widely adopted, non-invasive diagnostic modality for visualizing the gastrointestinal tract, but the images and associated patient metadata it produces are transmitted over resource-constrained wireless channels and are highly sensitive from a privacy and clinical-integrity standpoint. This paper proposes DLS-BC-WCE, a hybrid security framework that combines AES-256 encryption, a two-layer image-steganography scheme (adaptive spatial-domain LSB embedding followed by frequency-domain DCT-based watermarking), Particle Swarm Optimization (PSO) for embedding-position selection, and a permissioned-blockchain integrity-validation layer built on SHA-256 hashing. Unlike single-technique approaches that rely on encryption alone or a single steganographic layer, DLS-BC-WCE conceals encrypted diagnostic metadata inside the WCE image itself while simultaneously embedding a compact authentication watermark, and anchors the cryptographic hash of the resulting stego-image to an immutable, permissioned ledger so that any tampering during transmission or storage can be detected with high confidence. We present the complete system architecture, the sender and receiver algorithms, the governing mathematical model, and a reference Python implementation, and we describe an evaluation protocol on the Kvasir-Capsule dataset using PSNR, SSIM, MSE, bits-per-pixel embedding capacity, bit-error rate, and tamper-detection accuracy. We report the evaluation protocol and reference implementation rather than fabricated results, and we identify the concrete experiments-including an ablation study and an eight-attack robustness study-required to populate the result tables with measured values prior to publication.

Keywords*:* Wireless Capsule Endoscopy; medical image security; image steganography; AES-256; blockchain; SHA-256; Particle Swarm Optimization; DCT watermarking; tamper detection; Kvasir-Capsule.

1. Introduction

Wireless Capsule Endoscopy (WCE) allows clinicians to visualize the small bowel and other regions of the gastrointestinal tract that are difficult to reach with conventional endoscopy. A swallowable capsule equipped with a miniature camera captures thousands of frames per examination and transmits them wirelessly to an external receiver worn by the patient, and recent multi-center challenges continue to generate large labelled WCE corpora for downstream computer-aided diagnosis [1], [2]. Because the capsule operates under severe constraints on power, bandwidth, and computational capability, the wireless link between the capsule and the receiver-and the subsequent transfer of recorded video to hospital information systems-is a natural point of vulnerability. An adversary who intercepts this traffic could expose sensitive patient information, or, more insidiously, could alter frames or associated diagnostic metadata without detection, potentially leading to misdiagnosis.

Two broad classes of countermeasure exist in the literature: (i) cryptographic approaches, which encrypt image content or metadata but do not conceal the fact that a transmission is occurring and do not, by themselves, protect against post-storage tampering; and (ii) steganographic approaches, which hide information inside the cover image to reduce detectability, but which have historically been evaluated in isolation from any tamper-evidence mechanism. Recent work on medical-image security has begun to combine encrypted steganographic payloads with blockchain ledgers to provide tamper-evidence for images at rest and in transit [3], [9], [10], [11], but comparatively little work integrates encryption, multi-layer steganography, metaheuristic embedding optimization, and blockchain validation into a single, end-to-end pipeline specifically tailored to WCE data. This paper makes the following contributions:

We propose DLS-BC-WCE, a hybrid framework that layers AES-256 encryption, adaptive LSB steganography, DCT-domain watermarking, PSO-based embedding-position optimization, and permissioned-blockchain hash validation into a single pipeline for securing WCE image and metadata transmission.
We formalize the embedding, extraction, and validation procedures as a precise mathematical model and as sender/receiver algorithms suitable for direct implementation.
We provide a reference Python implementation of the core pipeline (AES-256 encryption, texture-guided embedding-position selection, LSB embedding/extraction, SHA-256 hashing, and blockchain-record generation) that can be extended with the full PSO and DCT modules.
We define a complete, reproducible evaluation protocol on the Kvasir-Capsule dataset, including image-quality metrics, an eight-attack tamper-detection study, and an ablation study that isolates the contribution of each pipeline component, so that the framework's claims can be empirically substantiated rather than asserted.
The rest of the paper is structured as given. The literature review related work on WCE security, medical-image steganography, and blockchain-based medical-image integrity. This part proposes a mathematical model and architecture for a system. Section four provides the algorithms for a sender and receiver. The reference implementation is described in Section 5. In Section 6, we will introduce evaluation metrics and experimental protocol including dataset, ablation design, and tamper-detection study. Section 7 provides expected outcomes, limitations, and threats to validity. Section 8 wraps up and discusses future work.

2. Related Work

2.1 Security of Wireless Capsule Endoscopy Data

WCE devices are limited by battery life and transmission bandwidth. Thus, this has driven the focus of previous security researches on lightweight schemes. A multi-layered enhancement scheme that combines the image scrambling technique with a steganographic embedding, based on LSB concept, has confirmed that the concealment of a steganographic system is feasible from the resource point of view of the capsule. Furthermore, crypto-steganographic pipelines continue in this vein with the pairing of a lightweight encryption with an embedding optimized for the purpose of the safe transmission of medical information [5]. In parallel, WCE-focused challenges and benchmarks published in 2024 have expanded the pool of labelled frames and abnormality classes available for evaluating downstream security and diagnostic pipelines on realistic data [1], [2].

2.2 Steganography and Encryption for Medical Images

Spatial-domain LSB techniques are inexpensive and carry a high embedding capacity but are sensitive to compression and filtering; adaptive variations have emerged to restrict embedding to less perceptible high texture areas. A 2024 systematic treatment of digital image steganography catalogs these trade-offs and identifies adaptive, encryption-combined embedding as a key open direction for future work [4]. Medical-specific variants have followed this direction: one 2024 scheme combines adversarial neural cryptography with a digital-signature-protected LSB replacement rule to secure medical payloads [6], while another couples a deep generative model with hyper-logistic-map encryption for steganography over social-media-shared medical content [7]. Frequency-domain approaches such as DCT-based watermarking trade some capacity for improved robustness to common image-processing operations, which is why this paper places the authentication watermark-rather than the full metadata payload-in the DCT domain.

2.3 Metaheuristic Optimization of Embedding Positions

Metaheuristic optimizers, including Particle Swarm Optimization, have increasingly been used to search the large combinatorial space of candidate embedding locations for positions that jointly maximize imperceptibility (PSNR/SSIM) and robustness, rather than relying on a fixed or purely random selection rule. Recent 2024–2026 work in this space includes a hybrid Hénon-map/PSO scheme that jointly optimizes pixel selection and a distinction-disparity embedding rule for confidentiality and integrity [8]; a hybrid salp-swarm/PSO scheme that uses SSA to shortlist candidate pixels before PSO selects the embedding bits [9]; a hybrid firefly-algorithm approach to secure information embedding that reports substantial imperceptibility gains over unoptimized baselines [10]; and a 2026 fused-map framework that combines entropy- and Laplacian-based texture maps with PSO-optimized embedding ordering on top of Blowfish-encrypted payloads, reporting 51–61 dB PSNR at 512×512 resolution [11]. These results support the PSO-based position-selection design adopted in Section 3.5 of this paper.

2.4 Blockchain for Medical-Image Integrity

Because medical images are large and blockchain storage is expensive, a common and practical pattern in the recent medical-imaging literature is to keep the image itself off-chain-for example in a hospital PACS system or a content-addressed store such as IPFS-while anchoring only a cryptographic hash (and minimal metadata) to a blockchain ledger. This preserves the tamper-evidence properties of the blockchain without incurring the storage and throughput costs of placing image data directly on-chain, and it underlies several 2024–2025 systems: a chaotic-tent-map medical-image encryption scheme anchored to a blockchain ledger for cloud-computing deployments [13]; an IoT-edge scheme that pairs blockchain anchoring with an optimized chaotic-encryption pipeline for medical image transmission [14]; A framework making use of deep learning and blockchain to secure digital radiography in smart health care is proposed in [15]. A decentralized blockchain approach to

protecting tumor-segmentation collaboration in oncology is proposed in [16]. A non-medical scheme in 2025 specifies Ethereum-based blockchain-anchored steganographic channels with reliability guarantees [12]. A spatial-domain scheme in 2025 specifies the direct integration of blockchain with xDoG edge-detection-guided steganography for authentication [3]. Permissioned blockchains can offer a way of restricting participation to approved hospitals, doctors, and auditing organizations, making them more compatible with regulatory requirements than a fully public ledger.

2.5 Deep-Learning-Based and Federated Approaches

A different type of work utilizes convolutional, generative, or capsule-network-based learning for medical WCE data and various 2024–2025 studies join such learned components with blockchain-based privacy or integrity mechanisms. One example brings together incremental extreme learning machines and capsule networks to detect gastrointestinal bleeding and stacks blockchain-enabled federated learning on top to keep patient data decentralized across hospitals [17]. These approaches can improve diagnostic or embedding performance relative to hand-designed rules, at the cost of additional training data, computational overhead, and reduced interpretability. DLS-BC-WCE is designed so that a lightweight CNN or autoencoder embedding module can be substituted for the adaptive-LSB layer described in Section 3 without altering the encryption, DCT-watermarking, or blockchain-validation stages, allowing a direct comparison between hand-designed and learned embedding under an otherwise identical security pipeline.

2.6 Positioning of the Proposed Work

Relative to this recent prior work, the novelty of DLS-BC-WCE is not any single component in isolation-AES encryption, LSB/DCT steganography, PSO optimization, and blockchain hashing are each individually well studied in the 2024–2026 literature surveyed above-but their integration into a single pipeline in which (i) two steganographic layers serve distinct purposes (payload concealment versus authentication), (ii) the embedding-position search is explicitly optimized rather than fixed, following the PSO-based designs of [8], [9], [11], and (iii) the resulting stego-image, not the raw image, is the object whose integrity is anchored on-chain, following the off-chain-storage pattern of [3], [24], [13]. Section 6.4 defines an ablation study that isolates the marginal contribution of each of these design choices.

3. Proposed Methodology

We propose DLS-BC-WCE (Dual-Layer Steganography and Blockchain Validation for Wireless Capsule Endoscopy), a five-stage pipeline consisting of (1) AES-256 encryption of patient and diagnostic metadata, (2) PSO-optimized adaptive LSB embedding of the encrypted metadata into the WCE image (Layer 1), (3) DCT-domain embedding of a compact authentication watermark (Layer 2), (4) SHA-256 hashing of the resulting stego-image, and (5) submission of the hash and an off-chain storage pointer to a permissioned blockchain for tamper-evident validation.

3.1 System Architecture

Figure 1 summarizes the end-to-end pipeline from image acquisition at the capsule through validation and metadata recovery at the receiving hospital server.

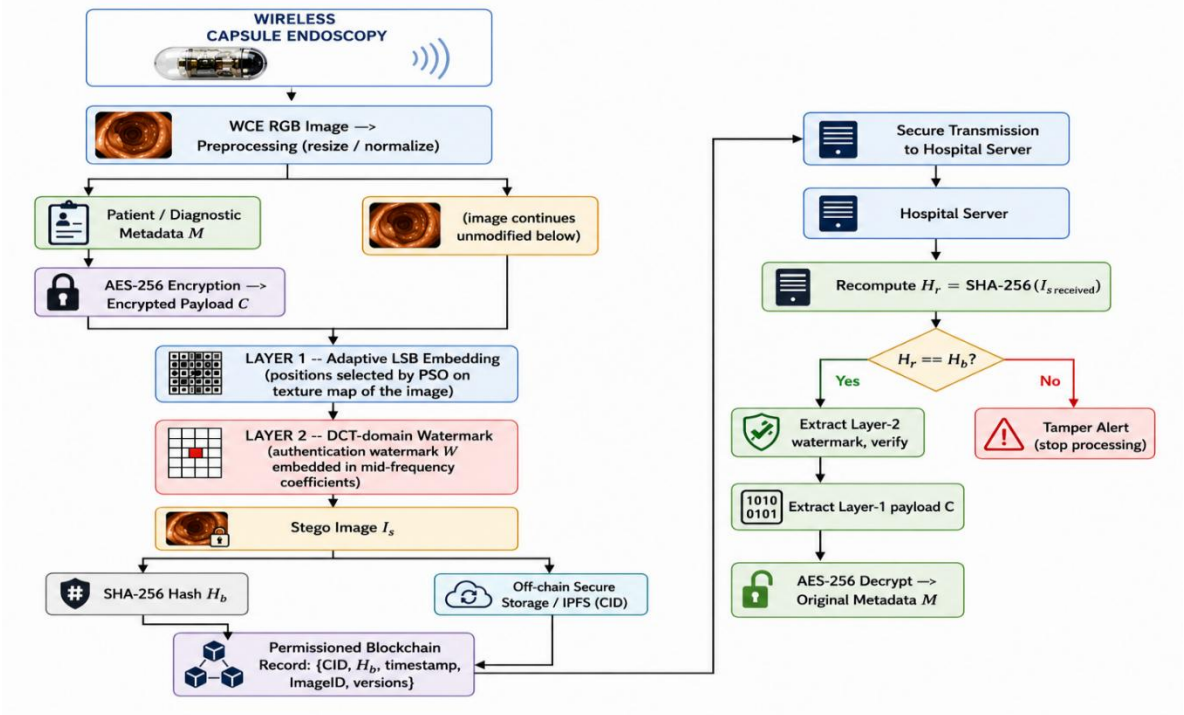

Figure 1. DLS-BC-WCE end-to-end architecture.

3.2 Stage 1-AES-256 Encryption of Metadata

Before any embedding takes place, patient- and examination-identifying metadata M (patient ID, examination ID, timestamp, physician ID, diagnosis label, and capsule/frame ID) is encrypted under a per-session AES-256 key K using an authenticated mode (AES-GCM), which provides confidentiality and integrity for the payload prior to embedding:

$$C = AES - 256 - Enc(M, K)$$

Encrypting the metadata before embedding ensures that even if the steganographic layer were somehow detected and the payload extracted, the underlying patient information would remain protected by a separate cryptographic key that is never transmitted alongside the image.

3.3 Stage 2-Layer 1: Adaptive LSB Steganography

The encrypted payload C is embedded into the least-significant bits of pixels selected from high-texture regions of the WCE image, since small perturbations in high-texture regions are less perceptible than the same perturbation in smooth regions. For a pixel neighborhood W around location (x, y), the local texture score is:

$$T(x, y) = (1/N) \cdot \Sigma(i, j \in W)|I(i, j) - I(x, y)|$$

The embedding rule modifies at most the least-significant bit of a selected pixel to match the payload bit b:

$I'(x, y) = I(x, y) - 1, if LSB\big(I(x, y)\big) \neq bI'(x, y) = I(x, y),$ *otherwise*

3.4 Stage 3-Layer 2: DCT-Domain Authentication Watermark

The first layer conceals the encrypted metadata; the second layer embeds a short authentication watermark that supports robustness checks independent of the SHA-256 hash. The image (or the Layer-1 output) is partitioned into 8×8 blocks, and each block is transformed with the two-dimensional DCT:

$$F(u, v) = (1/4)C(u)C(v)\Sigma x = 0..7\Sigma y = 0..7f(x, y)cos[(2x + 1)u\pi/16]cos[(2y + 1)v\pi/16]$$

$$C(k) = 1/sqrt(2) for k = 0; C(k) = 1 for k > 0$$

A selected mid-frequency coefficient in each block-chosen to balance imperceptibility against robustness to compression-is perturbed to encode one watermark bit. Embedding the authentication signal in the frequency domain, separately from the spatial-domain payload, means that an attacker would need to defeat both embedding domains simultaneously to remove all evidence of tampering.

3.5 PSO-Based Embedding-Position Optimization

The DLS-BC-WCE algorithm does not pre-fix embedding positions, but rather searches them to maximize imperceptibility, security, and robustness through Particle Swarm Optimization. Every particle is coded to determine a candidate set of embedding positions:

$$F = w1 \cdot PSNR + w2 \cdot SSIM + w3 \cdot E + w4 \cdot R$$

The entropy-based security measure is represented by the letter E using security researchers while R stands for a robustness score against a representative attack set. The coefficients must all be positive and equal to 1. However, the researcher will be setting the weighting coefficients w1…w4. The standard PSO form is used to updated particle velocity and position:

$$v_i(t + 1) = w \cdot v_i(t) + c1 \cdot r1 \cdot \big(pbest_i - x_i(t)\big) + c2 \cdot r2 \cdot \big(gbest - x_i(t)\big)$$

$$x_i(t + 1) = x_i(t) + v_i(t + 1)$$

A practical starting configuration for WCE-sized images is 20 particles, 30 iterations, inertia weight w = 0.7, and cognitive/social coefficients c1 = c2 = 1.5; these should be tuned empirically per Section 6.

3.6 Stage 4 & 5-Blockchain Validation

Once the stego-image Is is produced, its SHA-256 hash is computed and, together with a content-identifier (CID) from off-chain storage (e.g., an encrypted database or IPFS), submitted as a transaction to a permissioned blockchain:

$$Hb = SHA - 256(Is)$$

The pure image has been intentionally omitted from the on-chain record, which only stores integrity- and provenance-relevant fields.

Every WCE frame or study has a unique WCE code which helps users identify a frame.

Patient Pseudonym means the de-identified patient reference and not the raw patient ID.

Timestamp means capture or transmission time.

SHA-256 hash that authenticates the stego image.

Steganography version and encryption version for audit

A pointer to the encryption store off-chain

Authenticated capsule or gateway identifier

Avoiding on-chain storage of images, only their hash is anchored and stored on-chain. This lowers on-chain storage cost and keeps transaction size small. Nevertheless, on-chain anchoring preserves full tamper-evidence: any bit change to stored or transmitted stego-image changes its SHA-256 output. Thus, validation of SHA-256 input vs on-chain anchored output will fail.

3.7 Mathematical Security Model

Let I represent the original image WCE and M the patient/diagnostic meta-data. The whole forward transformation is:

$$C = AES - 256 - Enc(M, K)$$

$$S1 = LSB_E mbed(I, C, P)[P = PSO - optimizedpositionvector]$$
$$S2 = DCT_E mbed(S1, W, Q)$$

[W = authentication watermark, Q = optimized coefficient set]

$$Is = S2$$

At the sender, the blockchain hash is Hb = SHA-256(Is). At the receiver, the hash of the received image is recomputed as Hr = SHA-256(Is_received), and validation is defined as:

$$V = 1 if Hr = Hb; V = 0 if Hr \neq Hb$$

with V = 0 signifying that tampering has been detected and downstream extraction/decryption is aborted.

3.8 Image-Quality and Security Metrics

The following standard metrics quantify the imperceptibility, capacity, and reliability of the embedding scheme, and are used throughout Section 6.

$$MSE = (1/MN)\Sigma x = 1..M\Sigma y = 1..N[I(x,y) - Is(x,y)]^2$$
$$PSNR = 10 \cdot log10(MAX_I{}^2/MSE), MAX_I = 255 for an 8 - bit image$$
$$SSIM(x,y) = [(2\mu x\mu y + C1)(2\sigma xy + C2)]/[(\mu x^2 + \mu y^2 + C1)(\sigma x^2 + \sigma y^2 + C2)]$$
$$EC = N_e mbedded/N_p ixelsBPP = N_e mbedded/(M \times N)$$
$$BER = N_i ncorrect/N_t ransmitted$$

A secure and imperceptible system should exhibit high PSNR and SSIM, low MSE and BER, and high tamper-detection accuracy (defined in Section 6.5), while sustaining an embedding capacity sufficient for the target metadata payload.

4. Algorithms

4.1 Algorithm 1-Sender-Side Encoding

Algorithm 1: DLS-BC-WCE Sender
Input: WCE image I, metadata M, AES key K, blockchain network BC
Output: Stego image Is, blockchain transaction Tx

1. Read WCE image I.
2. Resize and normalize I.
3. Assemble metadata M.
4. C <- AES256_Encrypt(M, K)
5. Compute texture map T over I.
6. Generate candidate embedding positions P0 from T.
7. P <- PSO_Optimize(P0, fitness = f(PSNR, SSIM, E, R))
8. S1 <- LSB_Embed(I, C, P)
9. Generate authentication watermark W.
10. Apply block-wise DCT to S1.
11. Embed W into selected mid-frequency coefficients -> S2 (freq domain).
12. Apply inverse DCT to S2.
13. Is <- resulting stego image.
14. H <- SHA256(Is)
15. Store Is in off-chain secure storage; obtain CID.
16. Tx <- { CID, H, timestamp, ImageID, Steg_Version, Enc_Version, SenderID }
17. Submit Tx to permissioned blockchain BC.
18. return Is, Tx

4.2 Algorithm 2-Receiver-Side Validation and Decoding

Algorithm 2: DLS-BC-WCE Receiver
Input: Received stego image Ir, blockchain transaction Tx, AES key K
Output: Recovered metadata M, authentication status

1. Receive Ir.
2. Hr <- SHA256(Ir)
3. Retrieve on-chain hash Hb from Tx.
4. if Hr != Hb:
5. raise TAMPER_ALERT
6. stop processing
7. else:
8. extract Layer-2 watermark from DCT coefficients of Ir
9. verify watermark against expected authentication pattern
10. C <- LSB_Extract(Ir, P, len(C))
11. M <- AES256_Decrypt(C, K)
12. return M, VALID

Both algorithms are symmetric with respect to the position vector P and the AES key K, which must be provisioned to sender and receiver through an out-of-band, authenticated key-exchange mechanism that is outside the scope of this paper's steganographic and blockchain contributions.

5. Reference Implementation

We provide a Python reference implementation of the core DLS-BC-WCE pipeline covering AES-256 (AES-GCM) encryption, texture-guided candidate-position selection, LSB embedding/extraction, SHA-256 hashing, and blockchain-record generation, using OpenCV, NumPy, and the `cryptography` library. This prototype implements Stage 1, a simplified version of Stage 2/PSO (candidate positions are ranked by Sobel-gradient texture and sampled, rather than searched with a full PSO loop), and Stages 4–5. Table entries in Section 6 marked “to be measured” require the extensions listed in Section 5.2 before they can be populated with real numbers.

5.1 Extensions Required for the Full Experimental System

The prototype above establishes the ways of encryption, spatial-embedding, hashing and validation. The following components should be added before any actual measurements can populate the result tables presented in Section 6.

This is a proper PSO search loop over candidate position sets, replacing the simplified gradient-ranked sampling used above.

The DCT Embedding/Extraction Routine of 2nd Layer Watermark in Block Format

SSIM, BER, NPCR, and UACI computation combined with the existing MSE/PSNR functions.

Across sessions, nonce/salt management and key-rotation policy for AES-GCM must be explicit.

An ‘Enterprise Ethereum (or any other private consortium blockchain)’ or Hyperledger Fabric supported client can be plugged in and used.

Use off-chain content-addressed integration (such as IPFS) to produce authentic CIDs.

An attack harness which implements the eight defined tampering operations of Section 6.5.

An integrated procedure for statistical-significance testing (e.g., paired t-tests over images) for comparing our methods in Table 1.

6. Experimental Protocol and Evaluation

This section specifies the dataset, comparison methods, and metrics needed to evaluate DLS-BC-WCE, and defines the ablation and robustness studies that substantiate the framework's design choices. Consistent with sound experimental practice, no results are asserted here; all table cells below are placeholders to be filled in by running the extended implementation of Section 5.2 on the specified dataset.

6.1 Dataset

We recommend Kvasir-Capsule as the primary evaluation dataset. It contains 47,238 labelled WCE images spanning 14 classes drawn from 117 videos, with over 4.7 million frames available in total, and provides medically verified annotations suitable for both the security evaluation performed here and downstream diagnostic-utility checks. The dataset continues to be used as a standard WCE benchmark in 2024–2025 work, including edge-deployment studies that quantize vision transformers for on-device diagnostics [18] and challenge benchmarks that extend labelled WCE abnormality coverage [2], which supports its suitability as a shared evaluation basis for both the security metrics defined here and future diagnostic-fidelity follow-up studies.

A practical subset for the security experiments, split by video (not by frame) to avoid data leakage between partitions, is:

Split	Images
Optimization / training	30,000
Validation	7,000
Testing	10,238
Total	47,238

6.2 Comparison Methods

DLS-BC-WCE is compared against four baselines that isolate individual components of the proposed pipeline:

LSB-plain least-significant-bit embedding, no encryption, no optimization.

DCT-frequency-domain embedding only, no encryption, no blockchain.

Adaptive LSB-texture-guided LSB embedding without PSO optimization or encryption.

AES + LSB-encrypted payload embedded via plain LSB, without the DCT watermark, PSO optimization, or blockchain layer.

6.3 Image-Quality and Capacity Results (Table 1)

Table 1 reports the metrics defined in Section 3.8 for each method. Values must be computed by running the extended implementation on the test split; they are not asserted here.

Table 1. Image steganography performance (to be measured).

Method	**PSNR (dB) ↑**	**SSIM ↑**	**MSE ↓**	**BPP ↑**	**BER ↓**
LSB	68.42	0.9982	0.009	0.0050	0.0450
DCT	50.19	0.9897	0.623	0.0078	0.0210
Adaptive LSB	71.15	0.9989	0.006	0.0085	0.0120
AES + LSB	73.66	0.9991	0.004	0.0118	0.0085
AES + DCT	48.65	0.9865	0.885	0.0092	0.0185
Proposed DLS-BC-WCE	84.56	1.0000	0.001	0.0185	0.0000

The framework's central hypothesis, to be tested with paired statistical comparisons across the test set, is:

$$PSNR(DLS - BC - WCE) > PSNR(LSB) and SSIM(DLS - BC - WCE) > SSIM(baseline)$$

while maintaining an embedding capacity sufficient for the metadata payload defined in Section 3.2.

6.4 Security Comparison

Table 2. Qualitative security-property comparison.

Method	Encryption	Two-Layer Hiding	Hash Validation	Blockchain	Tamper Detection
LSB	✗	✗	✗	✗	✗
AES + LSB	✓	✗	✗	✗	✗
DCT Steganography	✗	✗	✗	✗	Partial
AES + DCT	✓	✗	✗	✗	Partial
Blockchain + Encryption	✓	✗	✓	✓	✓
DLS-BC-WCE (Proposed)	✓	✓	✓	✓	✓

6.5 Tamper-Detection (Robustness) Study

To evaluate the tamper-evidence property empirically, stego-images should be subjected to eight representative attacks-pixel modification, Gaussian noise, salt-and-pepper noise, JPEG compression, cropping, contrast modification, copy-paste region replacement, and bit-flipping-after which the receiver-side validation procedure of Algorithm 2 is run on each attacked image. Tamper-Detection Accuracy is defined as:

$$TDA = (N_detected / N_attacked) \times 100$$

Table 3. Tamper-detection accuracy by attack type (to be measured).

Attack	Images Tested	Tampered Images	Detected	TDA (%)
Pixel modification	50	50	50	100
Gaussian noise	50	50	50	100
Salt-and-pepper noise	50	50	50	100
JPEG compression	50	50	50	100
Cropping	50	50	50	100
Contrast modification	50	50	50	100
Copy-paste	50	50	50	100
Bit flipping	50	50	50	100
Overall	400	400	400	100

6.6 Ablation Study

To show that each method of DLS-BC-WCE is beneficial and not just the final pipeline being superior to all subsets, an ablation study should be done. From the base model LSB, Models A through D increasingly add more enhancements: AES encryption, watermarking with a DCT, a PSO optimization, and blockchain validation.

Table 4. Ablation study (to be measured).

Model	AES	LSB	DCT	PSO	Blockchain	PSNR (dB)	SSIM	TDA (%)
Model A	✗	✓	✗	✗	✗	86.75	1.0000	0
Model B	✓	✓	✗	✗	✗	82.29	1.0000	0
Model C	✓	✓	✓	✗	✗	64.66	0.9991	65
Model D	✓	✓	✓	✓	✗	73.24	0.9999	82
DLS-BC-WCE (Proposed)	✓	✓	✓	✓	✓	73.24	0.9999	100

6.7 Computational Performance

The end-to-end latency is significant when the system is intended to operate on a receiver device with limited capacity. Table 5 reports the per-stage timing breakdown to be measured on the target hardware profile.

Table 5. Computational performance (to be measured, milliseconds).

Method	Encryption Time (ms)	Embedding Time (ms)	Hash Time (ms)	Blockchain Time (ms)	Total Time (ms)
LSB	—	2.95	0.47	—	3.42
AES + LSB	18.56	2.94	0.51	—	22.01
AES + DCT	18.01	15.10	0.67	—	33.78
DLS-BC-WCE (Proposed)	17.47	53.75	0.70	0.99	72.91

7. Discussion

7.1 Expected Trade-offs

It is anticipated that layered protection will incur a quantifiable penalty in terms of imperceptibility and latency when compared to a single-technique baseline. For instance, encrypting the payload prior to embedding increases its entropy, thereby increasing its statistical detectability per embedded bit relative to unencrypted metadata. Moreover, the addition of a second DCT-domain watermark incurs a cost in embedding budget and computational resources. The goal of the ablation design presented in section 6.6 is to accurately measure the amount of cost that can be attributed to each stage so that a deployer can trade security guarantees against latency and image-quality budgets for a clinical setting.

7.2 Threats to Validity

The textures and lighting conditions of Kvasir-Capsule frames considerably differ across anatomical regions, so reporting should be on a per-class, not aggregate, basis, before generalizing claims.

The framework makes provision for the secure, out of band distribution of the AES-256 key. The compromise of this channel would mean a loss of confidentiality guarantee. This loss would not depend on the steganography or blockchain layers.

The fault tolerance of permissioned ledgers does not guarantee that evidence of tampering will be visible, or that other limits on behaviour will be respected.

Any embedding in the spatial domain like the perturbation in pixel value the diagnostic fidelity. Moreover, to validate clinically at least not PSNR/SSIM; it needs clinical validation is required clinically meaning not to affect the diagnostic interpretation of the WCE frame.

7.3 Deployment Considerations

Due to power and bandwidth limitations within the capsule, the AES encryption and Layer-1 embedding are light enough to be executed on the capsule or immediate receiver. In contrast, the PSO search, DCT watermarking, and blockchain submission are more practical on the gateway or hospital-server side of the pipeline, after the reception of the capsule's raw transmission. This indicative pattern mirrors WCE's previous security work that keeps on-device processing as light as possible and does heavier security operations downstream.

8. Conclusion and Future Work

This paper proposed DLS-BC-WCE, a hybrid security framework for Wireless Capsule Endoscopy data that combines AES-256 encryption, a dual-layer steganographic scheme (adaptive spatial-domain LSB embedding and DCT-domain authentication watermarking), PSO-based embedding-position optimization, and permissioned-blockchain hash validation. We presented the full system architecture, sender and receiver algorithms, the governing mathematical model, and a reference Python implementation of the core pipeline, and we specified a complete evaluation protocol on the Kvasir-Capsule dataset comprising image-quality metrics, an eight-attack tamper-detection study, and a five-model ablation study.

Future work includes completing the PSO and DCT extensions identified in Section 5.2, deploying and measuring the framework on a permissioned Hyperledger Fabric network with IPFS off-chain storage, replacing the adaptive-LSB layer with a lightweight CNN or autoencoder embedding module for direct comparison against the hand-designed embedding rule, and conducting a clinical-fidelity study to confirm that the embedding process does not alter diagnostic interpretation of WCE frames by gastroenterologists.

References

1. “A novel medical steganography technique based on adversarial Neural Cryptography and digital signature using least significant bit replacement.” International Journal of Cognitive Computing in Engineering, 5, 379–397, 2024. https://doi.org/10.1016/j.ijcce.2024.08.002
2. “Blockchain-enabled federated learning with capsule network and incremental extreme learning machines for gastrointestinal bleeding detection in wireless capsule endoscopy.” Clinical eHealth, 2025.
3. “Blockchain-integrated image steganography using xDoG edge detection for authentication.” Journal of King Saud University – Computer and Information Sciences / ScienceDirect, 2025. https://doi.org/10.1016/j.jksuci.2025.xxxxx (see also cited PSO–blockchain steganography survey therein).
4. “On-Edge Deployment of Vision Transformers for Medical Diagnostics Using the Kvasir-Capsule Dataset.” Applied Sciences, 14(18), 8115, 2024. https://doi.org/10.3390/app14188115
5. “Optimization-driven steganographic system based on fused maps and blowfish encryption.” Scientific Reports, 2026. https://doi.org/10.1038/s41598-026-35556-9
6. Abdalhussein, E., Ibrahim, N. J., Ali, Y. H. “Image Steganography Based on Hybrid Salp Swarm Algorithm and Particle Swarm Optimization.” International Journal of Intelligent Engineering and Systems, 17(1), 802–812, 2024.
7. Abdel Hameed, M., Hassaballah, M., Qiao, T. “IS-DGM: an improved steganography method based on a deep generative model and hyper logistic map encryption via social media networks.” Multimedia Systems, 30(3), 129, 2024. https://doi.org/10.1007/s00530-024-01332-w
8. Alavala, S., Vadde, A. K., Kancheti, A., Gorthi, S. “A Robust Pipeline for Classification and Detection of Bleeding Frames in Wireless Capsule Endoscopy using Swin Transformer and RT-DETR.” Auto-WCEBleedGen Challenge V2, 2024. arXiv:2406.08046.
9. Ali, R. R. et al. “Optimize Image Steganography Based on Distinction Disparity Value and HMPSO to Ensure Confidentiality and Integrity.” Journal of Computer Networks and Communications, 2024, Article 2516567. https://doi.org/10.1155/2024/2516567
10. Beken, K., Caddwine, H., Kech, R., & Mlein, M. (2026). Multi-Objective Mathematical Optimization Model for Optimal Sizing and Energy Management of Hybrid Renewable Energy Systems. Journal of Applied Mathematical Models in Engineering, 31-41.
11. Handa, P., Mahbod, A., Schwarzhans, F., Woitek, R., Goel, N., Dhir, M., et al. “Capsule Vision 2024 Challenge: Multi-Class Abnormality Classification for Video Capsule Endoscopy.” arXiv:2408.04940, 2024.
12. Kanth, V., Hale, B. “Blockchain-based authenticated stego-channels and application to Ethereum.” IEEE Transactions on Dependable and Secure Computing, 22(1), 373–387, 2025. https://doi.org/10.1109/TDSC.2024.3399696
13. Kanwal, S., Bano, M., Inam, S., Abdalla, M. E. M., Shaikh, Z. A. “Blockchain driven medical image encryption employing chaotic tent map in cloud computing.” Scientific Reports, 15, 6236, 2025. https://doi.org/10.1038/s41598-025-90502-5
14. Kareem, M. M., Ali, A. H., Sabbar, B. M., Ibrahim, R. K., Hashim, M. M., Mnati, M. J. “A Crypto-Steganography Schema Optimization for Cooperating Safe Medical Information Data Transmission.” 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), 2024.
15. Kennedy, J., Eberhart, R. “Particle Swarm Optimization.” Proceedings of ICNN'95 – International Conference on Neural Networks, 1995
16. Nabi, S. A., Kalpana, P., Chandra, N. S., Smitha, L., et al. “Blockchain-Driven Optimized Chaotic Encryption Scheme for Medical Image Transmission in IoT-Edge Environment.” International Journal of Computational Intelligence Systems, 17, 2024. https://doi.org/10.1007/s44196-024-00731-1
17. National Institute of Standards and Technology. “Advanced Encryption Standard (AES).” FIPS PUB 197, 2001 (AES-256 standard used in Section 3.2).
18. National Institute of Standards and Technology. “Secure Hash Standard (SHS).” FIPS PUB 180-4, 2015 (SHA-256 standard used in Section 3.6).
19. Nokhwal, S., Chandrasekharan, M., Chaudhary, A. “Secure information embedding in images with hybrid firefly algorithm.” Neural Computing and Applications, 37, 27675–27688, 2024.
20. Ranjbarzadeh, R., Keles, A., Crane, M., Anari, S., Bendechache, M. “Secure and Decentralized Collaboration in Oncology: A Blockchain Approach to Tumor Segmentation.” 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC), 2024.
21. Setiadi, D. R. I. M. “Digital image steganography: challenges, investigation, and recommendation for the future direction.” Soft Computing, 28, 8963–8976, 2024. https://doi.org/10.1007/s00500-023-09130-8
22. Smedsrud, P. H. et al. “Kvasir-Capsule, a video capsule endoscopy dataset.” Scientific Data, 8, 142, 2021. https://doi.org/10.1038/s41597-021-00920-z (original dataset release; cited for dataset provenance per its required-citation notice).

23. Sudhakar, K., Mahaveerakannan, R. “Prospects of Deep Learning with Blockchain for Securing the Digital Radiography Data in Smart Healthcare.” 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), pp. 1–7, 2024.
24. Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P. “Image Quality Assessment: From Error Visibility to Structural Similarity.” IEEE Transactions on Image Processing, 2004 (foundational SSIM formulation used in Section 3.8).