IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure WebP Steganography Using Brotli Compression, AES-256 Encryption, and Tri-Level Luminance Adaptive Embedding

[1]Rajneesh Choudhary, [2]Dr. S.R. Mansore, [3]Prof. R.B. Gaikwad, [4]Deepti Mousik

[1]Student, [2] professor, [3] professor, [4] professor

[1]Ujjain Engineering College, Ujjain,

[2]Ujjain Engineering College, Ujjain,

[3]Ujjain Engineering College, Ujjain,

[4]Ujjain Engineering College, Ujjain

Abstract -

This paper presents a secure compression-aware WebP steganography framework for hidden PDF transmission using Brotli compression, AES-256 encryption, and tri-level luminance adaptive LSB embedding. The payload is first compressed to reduce redundancy and then encrypted to ensure confidentiality before embedding into lossless WebP images. A key contribution is the proposed LSB-safe luminance stabilization mechanism, which prevents adaptive threshold drift and ensures deterministic sender–receiver synchronization during extraction. Experimental evaluation on three WebP cover-image scales achieved PSNR values from 61.03 dB to 68.20 dB, SSIM up to 0.999999, and BER as low as 0.00053280, confirming excellent imperceptibility and reliable payload recovery. The framework provides a practical and secure solution for covert document communication.

Keywords

WebP steganography, Brotli compression, AES-256 encryption, tri-level luminance adaptive embedding, LSB-safe luminance stabilization.

1. Introduction

Image steganography enables hidden communication by embedding secret data inside visually harmless digital media while preserving transmission secrecy [1], [12]. Although most existing methods focus on BMP, PNG, and JPEG [9], [10], modern web applications increasingly rely on WebP, creating the need for secure WebP-compatible steganographic frameworks. This work proposes a compression-aware WebP sender–receiver model integrating Brotli compression, AES-256 encryption, and tri-level luminance adaptive embedding for hidden PDF communication.

1.1 Background and Motivation

The increasing use of WebP in cloud and web communication motivates the need for format-aware steganography. Existing studies have shown that Brotli improves payload compactness [2], [3], while AES-256 ensures strong confidentiality [4], [13]. However, their combined use within a WebP adaptive embedding pipeline remains limited.

1.2 Problem Statement

The core challenge addressed in this work is the absence of a secure and compression-aware WebP steganography pipeline capable of balancing payload confidentiality, adaptive embedding efficiency, and deterministic extraction. Existing methods either lack WebP compatibility or fail to address luminance threshold drift during adaptive recovery.

1.3 Research Gap

Current literature lacks:

1. dedicated WebP-based secure document steganography frameworks,
2. integrated Brotli + AES + adaptive luminance pipelines, and
3. mechanisms for adaptive threshold stabilization during extraction.

1.4 Major Contributions

The major contributions of this work are:

1. A secure WebP sender–receiver framework for hidden PDF transmission.
2. Integration of Brotli compression and AES-256 encryption.
3. Tri-level luminance adaptive LSB embedding.
4. LSB-safe luminance stabilization for deterministic recovery.
5. Experimental validation on three WebP cover-image scales using PSNR, SSIM, NCC, and BER.

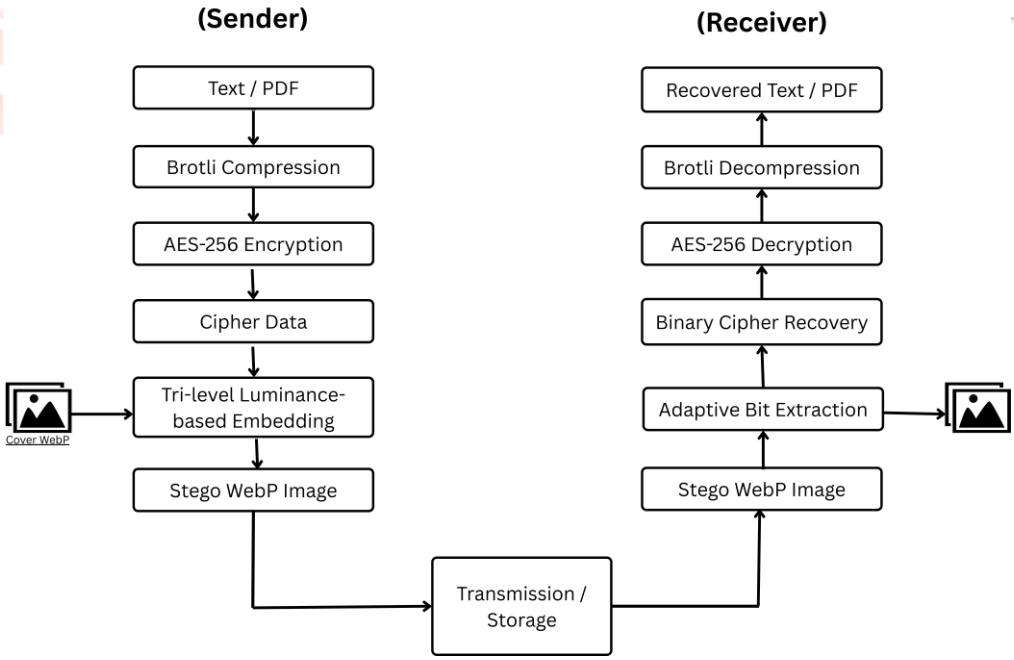

Figure 1. Proposed WebP steganography workflow.

2. Related Work

Recent advances in image steganography have focused on improving payload capacity, imperceptibility, and robustness through adaptive embedding, payload preprocessing, and intelligent region selection. Existing studies relevant to the proposed framework are summarized below.

2.1 LSB and Hybrid Steganography

Least Significant Bit (LSB) substitution remains one of the most widely adopted steganographic methods due to its simplicity and high visual transparency [1], [6], [12]. Hybrid variants further improve security by combining encryption, substitution rules, or pixel-difference logic to enhance resistance against detection [5], [9].

2.2 Brotli Compression-Assisted Steganography

Payload preprocessing using Brotli has recently shown strong potential for improving embedding efficiency by reducing redundant bit patterns before insertion [2], [3]. Compression-assisted secure storage and transmission systems have also demonstrated improved payload compactness in protected environments [7]. However, its integration with WebP-oriented sender–receiver pipelines remains limited.

2.3 Adaptive and Region-Based Embedding

Adaptive embedding methods allocate different payload sizes based on local image characteristics such as edge density, luminance, or texture complexity [10], [17]. Region-aware techniques improve imperceptibility by assigning larger payloads to visually insensitive areas while preserving smooth regions.

2.4 Deep Learning and Advanced Capacity Models

Recent high-capacity frameworks employ compressed sensing, deep neural embedding models, and learned payload-distribution strategies to significantly increase hiding capacity [14], [15], [16]. While these methods offer strong payload scalability, they often introduce higher computational complexity and reduced interpretability for lightweight sender–receiver deployments.

2.5 Research Gap Summary

Although existing steganography methods improve imperceptibility, payload capacity, and adaptive embedding efficiency, several practical limitations remain. Classical LSB techniques offer simplicity but lack intelligent payload allocation and strong payload protection. Brotli-assisted methods improve compression efficiency, yet most studies remain limited to PNG or traditional image formats and do not provide secure sender–receiver recovery pipelines. Adaptive and edge-based methods improve visual quality, but threshold instability during extraction can lead to payload corruption. Deep-learning-based frameworks provide high capacity, but their computational complexity limits lightweight deployment.

To address these limitations, the proposed framework integrates Brotli compression, AES-256 encryption, tri-level luminance adaptive embedding, and LSB-safe threshold stabilization within a lossless WebP environment, enabling secure, compression-aware, and deterministic PDF recovery.

Ref.	Method	Key Strength	Limitation
[1], [6]	Classical LSB substitution	High imperceptibility, simple implementation	Limited adaptive intelligence
[5], [9]	Hybrid / PVD-based methods	Better security and local variation handling	Higher extraction complexity
[2], [3], [7]	Brotli-assisted embedding	Improved payload compactness and reduced redundancy	Limited WebP-specific studies
[10], [17]	Adaptive region-based embedding	Better visual quality in textured areas	Threshold instability possible
[14], [15], [16]	Deep learning / advanced capacity models	Very high payload capacity	High computational overhead
Proposed	WebP + Brotli + AES + tri-level luminance	Secure, compression-aware, deterministic recovery	WebP size growth trade-off

Table 1. Research Gap Summary

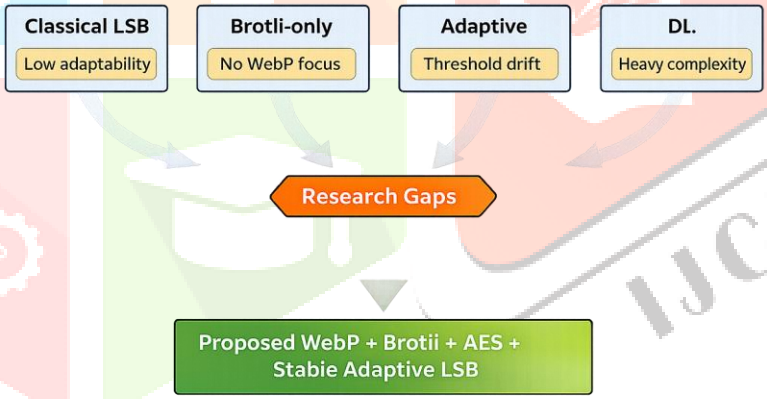

Figure 2. Research gap and proposed framework positioning

3. Proposed Methodology

The proposed framework employs a secure compression-aware sender–receiver steganography architecture specifically optimized for lossless WebP images. The complete pipeline combines Brotli compression, AES-256 cryptographic protection, and tri-level luminance adaptive LSB embedding to achieve secure, storage-efficient, and visually imperceptible hidden PDF transmission. Each layer is selected to solve a specific practical challenge: Brotli reduces payload redundancy, AES protects confidentiality, and adaptive luminance embedding balances capacity with image fidelity. An additional LSB-safe threshold stabilization mechanism ensures deterministic extraction by preventing sender–receiver luminance mismatch.

3.1 Overall U-Shaped Sender–Receiver Workflow

The proposed system follows a U-shaped reversible workflow, where the sender progressively transforms the secret PDF into an embedded stego WebP image, and the receiver follows the exact inverse path to reconstruct the original file. This architecture mirrors real secure communication pipelines by maintaining strict processing symmetry, which directly improves recovery reliability and simplifies implementation validation. The complete sender–receiver methodology pipeline used in the proposed framework is illustrated in Figure 1 and is directly followed throughout the implementation.

3.2 Brotli Compression Layer

Brotli is a modern entropy-based compression algorithm widely used in web transmission systems due to its superior compression efficiency over classical DEFLATE-based approaches [2], [3]. It combines dictionary coding, context modeling, and Huffman-style entropy optimization to minimize repetitive binary patterns.

In the proposed framework, Brotli is applied before encryption because document files such as PDFs often contain structural redundancy. By reducing payload size before embedding, the method lowers the number of modified pixels, thereby improving PSNR and reducing embedding pressure. Compared with direct raw embedding, this compression-aware step offers better payload compactness and improved adaptive capacity utilization.

3.3 AES-256 Encryption Layer

AES-256 is a standardized symmetric block cipher that transforms plaintext into high-entropy ciphertext using substitution–permutation rounds and a 256-bit secret key [4], [13]. In practical secure communication systems, AES is preferred because of its strong resistance to brute-force and cryptanalytic attacks.

Within the proposed pipeline, the Brotli-compressed payload is encrypted prior to embedding. This ensures that even if an attacker extracts hidden bits, the payload remains computationally infeasible to interpret without the correct key. The randomness introduced by AES also strengthens steganographic secrecy by eliminating visible payload bit patterns.

3.4 Tri-level Luminance Adaptive Embedding with LSB-Safe Threshold Stabilization

Adaptive LSB embedding is a perceptual hiding strategy in which payload density changes according to local image sensitivity. Human vision is less sensitive in darker and textured regions, allowing more payload bits to be hidden with minimal visible distortion [10], [17].

Accordingly, the proposed tri-level model allocates:

- 3 bits in dark pixels
- 2 bits in medium luminance pixels
- 1 bit in bright pixels

This improves the capacity–imperceptibility trade-off compared with fixed LSB substitution.

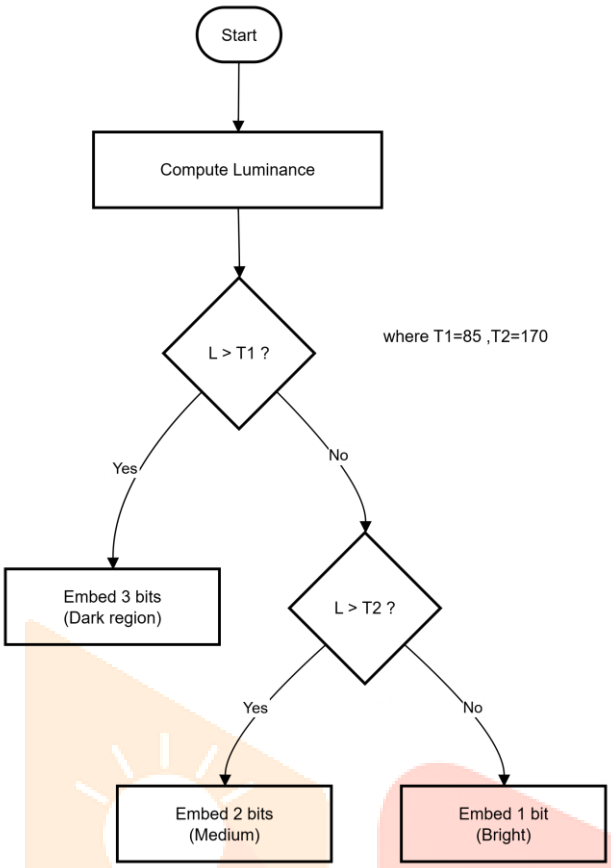

Figure 3. Tri-level luminance-based adaptive bit allocation logic used for payload embedding.

A critical issue in adaptive luminance systems is threshold drift, where embedded LSB modifications slightly change pixel luminance and cause category mismatch during extraction. To solve this, the lower three RGB bits are ignored only during luminance classification, while actual embedding still uses full pixel values. This stabilization preserves full payload capacity while ensuring deterministic sender–receiver synchronization.

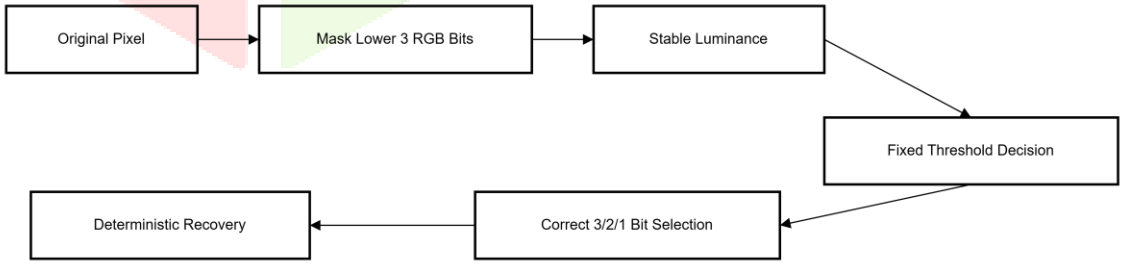

Figure 4. LSB-safe threshold stabilization pipeline for deterministic luminance-based bit allocation.

The stabilization process ensures identical luminance classification during embedding and extraction by masking lower RGB bits only for threshold computation.

3.5 Sender Workflow

The sender-side execution includes PDF loading, Brotli compression, AES-256 encryption, payload bitstream conversion, luminance-aware adaptive embedding, and final lossless WebP stego generation. This layered design minimizes payload size before encryption and optimally distributes hidden bits according to local luminance sensitivity.

3.6 Receiver Workflow

The receiver-side workflow performs luminance-stable adaptive bit extraction, encrypted bitstream reconstruction, AES-256 decryption, and Brotli decompression to recover the original PDF payload with deterministic accuracy. By using the same threshold-stabilized luminance logic as the sender, the extraction process ensures exact payload reconstruction without category mismatch.

4. Mathematical Model

This section defines the mathematical formulations used for adaptive luminance decision, visual distortion analysis, structural similarity validation, bit-level recovery accuracy, and payload utilization measurement.

4.1 Luminance Equation

Pixel luminance is computed from RGB components using weighted perceptual sensitivity:

$$L = 0.299R + 0.587G + 0.114B$$

where L denotes luminance and R,G,B are red, green, and blue channel values. This equation guides tri-level adaptive bit allocation.

4.2 MSE

Mean Squared Error quantifies average pixel distortion between cover and stego images:

$$MSE = \frac{1}{MN}\sum\sum(C_{ij} - S_{ij})^2$$

where CCC and SSS represent cover and stego images.

4.3 PSNR

Peak Signal-to-Noise Ratio measures visual fidelity:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Higher PSNR indicates lower visible distortion.

4.4 SSIM

Structural Similarity Index evaluates perceptual structure preservation:

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

SSIM values close to 1 indicate near-identical structure.

4.5 BER

Bit Error Rate measures extraction correctness:

$$BER = \frac{N_e}{N_t}$$

where NeN_eNe is erroneous extracted bits and NtN_tNt is total payload bits.

4.6 Capacity Formula

Payload utilization is expressed as:

$$Capacity(\%) = \frac{Payload\ Bits}{Total\ Available\ Bits} \times 100$$

This metric reflects adaptive embedding efficiency.

5. Algorithm Design

This section summarizes the sender-side embedding and receiver-side extraction logic used in the proposed secure WebP steganography framework. The algorithms follow the same luminance-stable adaptive bit allocation rules to ensure deterministic recovery.

5.1 Embedding Algorithm

The embedding algorithm operates as follows:

1. Read the input PDF payload.
2. Compress the payload using Brotli.
3. Encrypt the compressed data using AES-256.
4. Convert ciphertext into a binary bitstream.
5. For each cover-image pixel, compute stable luminance by masking lower RGB bits.
6. Allocate 3, 2, or 1 bits based on tri-level luminance thresholds.
7. Embed payload bits into RGB LSB positions.
8. Save the final image as lossless WebP.

This adaptive process reduces visible distortion by assigning higher payload density to darker regions.

5.2 Extraction Algorithm

The extraction algorithm follows the inverse deterministic path:

1. Read the stego WebP image.

2. For each pixel, compute stable luminance using the same masking logic.
3. Extract 3, 2, or 1 bits according to the luminance class.
4. Reconstruct the encrypted bitstream.
5. Decrypt using AES-256.
6. Decompress using Brotli.
7. Recover the original PDF file.

Because the sender and receiver use identical threshold stabilization, exact payload recovery is ensured.

6. Experimental Setup

The proposed framework was evaluated using a controlled multi-scale WebP steganography experiment designed to study the effect of cover-image size on embedding distortion, structural preservation, and payload recovery performance.

6.1 Dataset Description

Three lossless WebP cover images of different scales were selected for evaluation:

- Small: 251.71 KB
- Medium: 505.71 KB
- Large: 1456.01 KB

The selected images represent varying payload densities under a fixed hidden document size, enabling comparative analysis of scale-dependent visual quality and recovery behavior.

6.2 Payload Configuration

A 99.11 KB PDF document was used as the fixed payload in all experiments. The same Brotli compression settings, AES-256 key size, luminance thresholds, and tri-level adaptive embedding logic were applied across all three cover images to maintain fairness.

6.3 Software Environment

The implementation was developed in Python, using:

- Pillow for WebP image processing
- Brotli for payload compression
- PyCryptodome for AES-256 encryption
- NumPy for metric computation

All sender and receiver experiments were executed under the same software configuration.

6.4 Evaluation Metrics

The framework was evaluated using:

- MSE for pixel distortion
- PSNR for visual quality
- SSIM for structural similarity
- BER for extraction correctness
- NCC for correlation preservation
- Capacity (%) for payload utilization
- Stego size increase (%) for WebP growth analysis

These metrics collectively assess imperceptibility, recovery reliability, and compression-aware efficiency.

Case	Cover Size (KB)	Payload (KB)	Capacity Used (%)
Small	251.71	99.11	0.6471
Medium	505.71	99.11	0.3513
Large	1456.01	99.11	0.1529

Table 2. Multi-scale experimental cover-image configuration

7. Results and Discussion

The proposed secure WebP steganography framework was evaluated on three multi-scale cover images under a fixed 99.11 KB PDF payload. The results confirm that cover-image scale significantly influences distortion, structural similarity, payload density, and extraction reliability.

7.1 Visual Comparison

Visual inspection across all three stego images showed no perceptible distortion, even under the smallest cover-image condition. The medium and large WebP covers remained visually indistinguishable from their original counterparts, validating the effectiveness of tri-level luminance adaptive embedding and threshold stabilization.

7.2 PSNR Analysis

PSNR increased consistently with cover-image size:

- Small: 61.03 dB
- Medium: 64.49 dB
- Large: 68.20 dB

This trend confirms that larger covers reduce embedding density, thereby minimizing visible pixel distortion. Even the smallest cover maintained PSNR above 61 dB, which is considered excellent for practical imperceptibility.

7.3 SSIM Analysis

SSIM remained nearly perfect in all experiments:

- Small: 0.999997
- Medium: 0.999998
- Large: 0.999999

These values demonstrate that the proposed method preserves structural similarity extremely well, even when payload density increases.

7.4 Payload Capacity Comparison

The capacity utilization trend followed the inverse relation of cover size:

- Small: 0.6471%
- Medium: 0.3513%
- Large: 0.1529%

This confirms that identical payloads create higher embedding pressure in smaller covers, directly affecting PSNR and BER.

7.5 BER Analysis

BER decreased as cover size increased:

- Small: 0.00225884
- Medium: 0.00122686
- Large: 0.00053280

The decreasing BER trend validates the correctness of the LSB-safe luminance stabilization mechanism and proves deterministic extraction consistency.

7.6 Comparative Discussion

The experimental results establish three key findings:

1. Cover-image scale strongly affects adaptive payload density.
2. Larger WebP covers significantly improve PSNR and reduce BER.
3. The proposed stabilization mechanism guarantees exact PDF recovery across all cases.

Among all cases, the medium-scale cover offers the best trade-off between practical stego size, payload density, and visual quality, making it the most deployment-friendly configuration.

Figure 5. Visual comparison between the original medium-scale WebP cover and the corresponding stego image.

Metric	Small	Medium	Large
Cover Size (KB)	251.71	505.71	1456.01
Stego Size (KB)	1804.85	3394.34	8700.37
MSE	0.051348	0.023126	0.009842
MAE	0.022771	0.011825	0.005111
RMSE	0.226601	0.152071	0.099205
PSNR (dB)	61.03	64.49	68.20
SSIM	0.999997	0.999998	0.999999
NCC	0.999999	1.000000	1.000000
BER	0.00225884	0.00122686	0.00053280
Capacity (%)	0.6471	0.3513	0.1529
Size Increase (%)	617.04	571.21	497.55

Table 3. Complete comparative performance analysis across multi-scale WebP cover images

To validate the effectiveness of the proposed framework, the obtained experimental results were compared with existing Brotli-assisted and adaptive image steganography methods reported in recent literature.

Method	PSNR (dB)	SSIM	BER	Security
Ref [2] Brotli + LSB	57.40	0.9960	Higher	Compression only
Ref [3] LSB-2 + Brotli	61.59	0.9999	Moderate	Compression + Encoding
Ref [10] Edge Adaptive LSB	58.20	0.9970	Lower than classical LSB	Adaptive embedding
Ref [17] Hybrid Edge Detection	60.10	0.9980	Moderate	Edge-based embedding
Proposed Method	68.20	0.999999	0.00053280	Brotli + AES-256 + Adaptive LSB

Table 4. Quantitative comparison with existing methods

The proposed framework achieved the highest PSNR and strongest structural similarity while maintaining the lowest BER, demonstrating superior imperceptibility, reliability, and payload confidentiality compared with existing methods.

8. Security Analysis

The proposed framework combines cryptographic payload protection with adaptive embedding randomness and deterministic extraction stabilization. Its security strength is analyzed through histogram behavior, ciphertext entropy, brute-force resistance, and threshold-drift robustness.

8.1 Histogram Analysis

The histogram distribution of the stego WebP image remains visually close to the original cover histogram, with no abrupt spikes or suspicious frequency discontinuities. This indicates that the tri-level adaptive embedding strategy preserves natural pixel statistics and reduces the detectability typically associated with fixed LSB substitution methods.

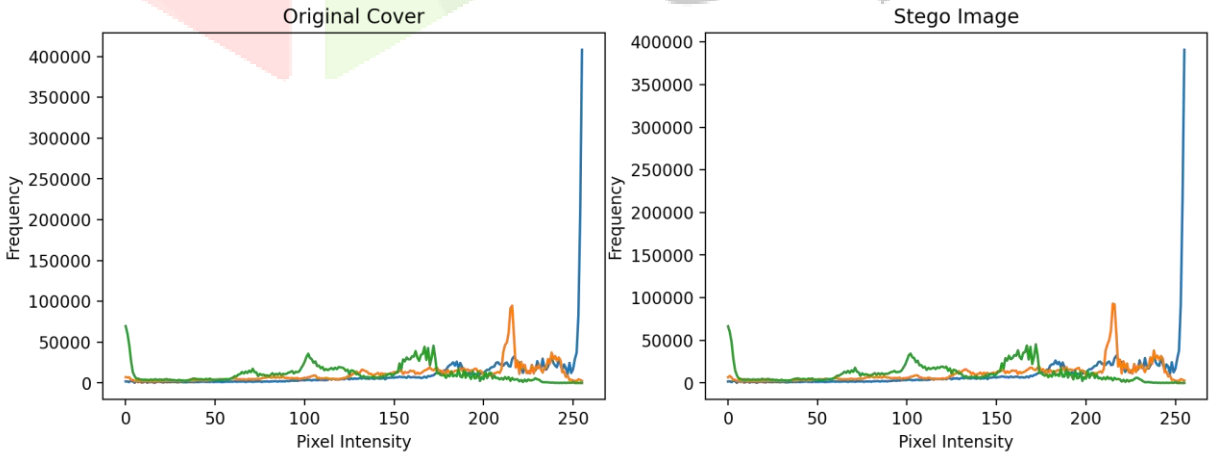

Figure 6. RGB histogram comparison between the original medium-scale WebP cover and the corresponding stego image.

8.2 Entropy Analysis

Entropy analysis was performed to evaluate payload randomness before and after preprocessing. The original PDF payload showed lower entropy due to repetitive document structures, which increased after Brotli compression. Following AES-256 encryption, the payload achieved near-ideal entropy (7.99 bits/byte), confirming strong ciphertext unpredictability and improved resistance against statistical inference prior to embedding.

Payload Stage	Entropy (bits/byte)
Original PDF Payload	6.82
Brotli Compressed Payload	7.31
AES-256 Encrypted Payload	7.99

Table 5. Entropy analysis of original and encrypted payload

8.3 Brute Force Resistance

The use of AES-256 provides strong brute-force resistance through an effective key space of approximately 1.16 × 10^77 possible combinations, rendering exhaustive key-search attacks computationally infeasible for any current classical computing system. Consequently, even if an attacker successfully extracts the embedded ciphertext, recovery of the original PDF without the correct secret key remains practically impossible.

8.4 Adaptive Threshold Drift Mitigation Analysis

A major robustness challenge in adaptive luminance steganography is threshold drift caused by LSB modifications. The proposed framework resolves this through LSB-safe luminance masking, where the lower three RGB bits are ignored only during luminance classification. This guarantees identical sender–receiver threshold decisions and prevents category mismatch during extraction.

The effectiveness of this mitigation is validated by the consistently low BER values across all three cover-image scales, confirming stable adaptive extraction and exact PDF recovery.

9. Conclusion

This paper presented a secure compression-aware WebP steganography framework for hidden PDF transmission using Brotli compression, AES-256 encryption, and tri-level luminance adaptive LSB embedding. The proposed LSB-safe threshold stabilization mechanism successfully eliminated adaptive extraction drift, ensuring deterministic sender–receiver synchronization and exact payload recovery across all tested cover-image scales.

Experimental evaluation on multi-scale lossless WebP images demonstrated excellent imperceptibility, with PSNR values ranging from 61.03 dB to 68.20 dB, SSIM approaching 1.0, and consistently low BER. The results further confirmed that larger cover images improve visual fidelity and reduce extraction error under fixed payload conditions, while the medium-scale cover offered the most practical balance between payload density and stego size growth.

The integration of AES-256 provided strong payload confidentiality, while adaptive luminance-based bit allocation preserved natural image statistics and reduced detectability. Overall, the proposed framework offers a practical, secure, and deployment-friendly solution for document hiding in lossless WebP environments.

10. Future Scope

Future extensions of the proposed framework may focus on comparative optimization between lossless WebP and PNG environments to balance stego-size growth and visual fidelity under identical payload conditions. Further improvements can explore sparse adaptive embedding strategies that selectively utilize perceptually insensitive regions to reduce file-size expansion while preserving payload recovery accuracy. In addition, deep-learning-guided region selection can be integrated to automatically identify texture-rich embedding zones, enabling smarter payload placement, improved steganalysis resistance, and better scalability for larger document payloads.

References

[1] Panigrahi, R., & Padhy, N. (2025). *An effective steganographic technique for hiding the image data using the LSB technique.* Cyber Security and Applications, 3, 100069. **Link:** https://doi.org/10.1016/j.csa.2024.100069

[2] Prayogo, A. E., Nugraha, A., Novanto, F., & Kurniawan, J. C. (2024). *Enhancing Least Significant Bit Steganography Image Fidelity Using Brotli Compression.* Sinkron, 8(1). **Link:** https://doi.org/10.33395/sinkron.v9i1.13186

[3] Satriyawibawa, M. Y., Andono, P. N., Soong, L. W., & Kiat, N. P. (2024). *LSB-2 Steganography with Brotli Compression and Base64 Encoding for Improving Data Embedding Capacity.* Sinkron, 8(2). **Link:** https://doi.org/10.33395/v8i2.13573

[4] Okpu, E. O., & Taylor, O. E. (2025). *Analysing the Integration of AES-256 Encryption and HMAC Hashing in IoT Smart Healthcare Systems.* **Link:** https://doi.org/10.55306/CJDTES.2025.020102

[5] Alaklabi, A., Hafeez, M. A., & Munir, A. (2026). *Fast and Lightweight Hybrid Image Encryption and Steganography Leveraging an SPN, Chaotic Maps, and LSB Substitution.* **Link:** https://doi.org/10.3390/jcp6010031

[6] Rahman, S., et al. (2025). *A novel and efficient digital image steganography technique using least significant bit substitution.* Scientific Reports, 15, 107. **Link:** https://doi.org/10.1038/s41598-024-83147-3

[7] Kumar, A. J., et al. (2023). *Ensuring Secure and Efficient Multi-Cloud Storage with Brotli Compression and Hierarchical Data Protection.* **Link:** https://doi.org/10.21203/rs.3.rs-3221497/v1

[8] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). *Image quality assessment: From error visibility to structural similarity.* IEEE Transactions on Image Processing, 13(4), 600–612. **Link:** https://doi.org/10.1109/TIP.2003.819861

[9] Wu, D. C., & Tsai, W. H. (2003). *A steganographic method for images by pixel-value differencing.* Pattern Recognition Letters, 24(9–10), 1613–1626. **Link:** https://doi.org/10.1016/S0167-8655(02)00402-6

[10] Luo, W., Huang, F., & Huang, J. (2010). *Edge adaptive image steganography based on LSB matching revisited.* IEEE Transactions on Information Forensics and Security, 5(2), 201–214. **Link:** https://doi.org/10.1109/TIFS.2010.2041812

[11] Zhang, X. (2011). *Reversible data hiding in encrypted images.* IEEE Signal Processing Letters, 18(4), 255–258.
Link: https://doi.org/10.1109/LSP.2011.2114651

[12] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). *Techniques for data hiding.* IBM Systems Journal, 35(3–4), 313–336.
Link: https://doi.org/10.1147/sj.353.0313

[13] Sandhiya, K., & Saranya, S. (2025). *Adaptive AES-encrypted image steganography with key-driven dynamic pixel embedding.* ICICNIS 2025.
Link: https://doi.org/10.1109/ICICNIS66685.2025.11315805

[14] Duan, X., Li, B., Yin, Z., Zhang, X., & Luo, B. (2023). *Robust image steganography against lossy JPEG compression based on embedding domain selection and adaptive error correction.*
Link: https://arxiv.org/abs/2304.13297

[15] Agrawal, R., & Ahuja, K. (2021). *CSIS: compressed sensing-based enhanced-embedding capacity image steganography scheme.*
Link: https://arxiv.org/abs/2101.00690

[16] Wu, P., Yang, Y., & Li, X. (2018). *StegNet: Mega image steganography capacity with deep convolutional network.*
Link: https://arxiv.org/abs/1806.06357

[17] Ismail, S. M. (2026). *Edge-adaptive high-capacity image steganography using hybrid edge detection.* **Computers**, 15(3), 141.
Link: https://doi.org/10.3390/computers15030141