Empirical Enhancements to Hybrid AES-ECC Steganography: Achieving Perfect Undetectability , Superior Fidelity , and Near-Perfect Diffusion

1st Hansuja Budhiraja
Artificial Intelligence and Data Science
Indira Gandhi Delhi Technical University for Women
New Delhi, India
hansujaigdtuwcseai@gmail.com

2nd Kiran Malik
Artificial Intelligence and Data Science
Indira Gandhi Delhi Technical University for Women
New Delhi, India
kiranmalik@igdtuw.ac.in

***Abstract*—This paper presents a hybrid steganography and cryptography framework that integrates the Advanced Encryption Standard (AES) with a 256-bit key size in Cipher Block Chaining (CBC) mode for payload encryption, Elliptic Curve Cryptography (ECC) using the secp256k1 curve for secure key exchange, inverted Least Significant Bit (LSB) embedding in the RGB color space, and lossless WebP compression for efficient transmission. The proposed framework is rigorously evaluated on the large-scale, preprocessed USC-SIPI dataset, which includes a diverse variety of images such as aerial, texture, sequence, and miscellaneous categories. Experimental results demonstrate 100% payload recovery after WebP compression, a Peak Signal-to-Noise Ratio (PSNR) exceeding 61 dB even at a 10 KB payload (mean: 61.32 dB, std: 0.02 dB), and a 0% detection rate under StegExpose across 840 stego PNG images with payload sizes ranging from 50 bytes to 10 KB. The system also achieves a 99.6% avalanche effect in both AES and ECC layers, and saving the PNG images as WebP reduces file size by approximately 35–40%. The framework effectively satisfies key requirements of a secure communication system, including high payload capacity, robustness against compression and transmission noise, visual transparency, and strong tamper resistance.**

***Index Terms*—Hybrid Cryptography, AES, ECC, Inverted LSB, Steganography, WebP Compression, Steganalysis, Avalanche Effect, USC-SIPI Dataset**

I. Introduction

In the time of rapid technological advancements over the past two decades, our reliance on the digital systems has steadily increased in daily life while cyber security threats have become more prevalent and sophisticated. Therefore the need for secure data transmission over various communication channels is a necessity to prevent unauthorized access and usage. Encryption provides strong protection for data content but it does not hide the existence of data, thus making it suspicious and attracts attackers.Cryptography obscures the integrity of information by rendering the text incomprehensible for everyone except the sender and intended receiver . Meanwhile steganography is a complementary technique that seeks to conceal the presence of data itself.

Steganography is derived from the two Greek words Stego and Graphia, Stego means covering and graphia which means writing , thus the translation is covered writing or data hiding . Image Steganography is a technique to covertly transmit secret information over digital networks without visibly changing the appearance of the carrier image, making the difference between the cover and the stego image imperceptible to the naked eye. An effective steganography approach satisfies key requirements : high payload capacity , visual transparency , tamper resistance , computational efficiency and robustness against compression and transmission noise.

Least Significant Bit is a very prevalent and dominant steganography technique due to it it's simplicity and capacity , although it is critically vulnerable to statistical steganalysis. Inverted LSB on the contrary is a enhanced variant which enhances security by dynamically selecting embedding regions based on pixel intensity , further reduces detectability.

While hybrid cryptography- steganography systems have already proposed AES and ECC approach , but the works suffer from limited empirical validation , absence of large scale steganalysis , avalanche analysis , untested robustness for WebP compression.Moreover the payload messages were usually of few hundred bits and not realistic classified documents , leaving a critical gap in assessing practical deployability. We bridge this gap with a novel hybrid framework combining AES-128-CBC for payload encryption, ECC (secp256k1) for secure key exchange, inverted LSB embedding in RGB color space, and lossless WebP compression for transmission efficiency. Our system is rigorously evaluated on a large-scale preprocessed 210 images from the USC-SIPI dataset. We have tested it over realistic classified document payload varying from 50 Bytes to 10 KB and evaluated our approach with steganalysis and avalanche analysis.

II. Literature Review / Related Work

The current research shows steady evolution of hybrid steganography and cryptography systems. The hybrid approach was primarily used to achieve secure, covert, and efficient communication by hiding as well as encrypting the data.

Recent research efforts, for example by Alwadhi et al. [1] and Mahmood and Tabassum [2], highlight that combining

TABLE I
LITERATURE REVIEW SUMMARY

Year	Author	Methodology Used	Key Outcomes	Results	Limitations
2025	A. Badhan et al. [3]	AES+ECC encryption with Inverted LSB	Improved efficiency, successful WebP compression	PSNR 68.9 for few hundred bytes of payload	Small Payload and Dataset
2023	S. Allwadhi et al. [1]	LSB steganography with Shannon–Fano encoding	Enhanced payload capacity and visual imperceptibility	Improved embedding efficiency	Increased computational complexity
2021	M. A. Mahmood et al. [2]	AES, RSA, and fuzzy vault for key management	Strong cryptographic mechanisms against potential attackers	High accuracy in key recovery	Complex key generation and management
2024	H. Vasudev et al. [4]	AES and RSA with DCT-based steganography	Improved cloud data confidentiality and integrity	High data recovery rate	High computational and resource overhead
2023	C. L. Krishna et al. [5]	RSA and DWT-based steganography	Enhanced data concealment and robustness	Resilient to noise and attack interference	Limited data embedding capacity
2022	F. F. M. Yahia et al. [6]	Affine Hill Cipher with hybrid edge detection and LSB steganography	Advanced data protection using hybrid visual encryption	High PSNR and low MSE	Increased complexity due to edge detection
2022	M. Kumar et al. [9]	LSB steganography combined with AES encryption	Secured digital image and text data	PSNR greater than 60 dB achieved	Processing overhead for large datasets
2024	G. Shidaganti et al. [10]	AES and LSB hybrid steganography	Elevated confidentiality for cloud-based data	Effective data protection in storage and transfer	Limited robustness under high-load conditions
2024	P. Chinnasamy et al. [11]	Elliptic Galois cryptography with XOR steganography	Advanced IoT data protection model	Improved security parameters	High algorithmic complexity and computational cost
2023	R. K. Hapsari et al. [12]	RSA encryption with EOF-based steganography	Secure cloud file transmission	Enhanced resistance to unauthorized interception	EOF method constraints in embedding
2023	A. K. Sahoo et al. [13]	Hybrid encryption using AES, ECC keys, and steganography	Enhanced secrecy through integrated cryptography and steganography	Strong concealment against cryptanalysis	Slightly increased encryption–embedding time
2021	L. Negi et al. [15]	AES encryption with LSB steganography	Improved secrecy for information exchange on mobile devices	Increased reliability compared to standalone methods	Limited to mobile platform environments
2023	V. Kalaichelvi et al. [16]	Hybrid Hill cipher, Radix-64, RSA, and LSB steganography	Improved security and embedding efficiency	Elevated entropy and PSNR metrics	High complexity of multi-cipher combination
2022	K. Vandana et al. [17]	Hybrid AES, ECC, and LSB steganography	Stronger key management and secure cloud storage	Efficient encryption–decryption balance	Scalability issues and higher computational demand
2021	R. Tripathi et al. [18]	Analysis of combining cryptography and steganography for enhanced security	Insights into improving data security through dual-layer protection	Reviewed effectiveness of different methods in data security	Lacks practical implementation details and real-world application data

steganographic methods with robust encryption schemes like AES and RSA significantly increase data confidentiality and integrity. Techniques such as LSB steganography, when integrated with Shannon–Fano encoding, have shown improved data hiding efficiency without degrading image quality. Similarly, Geethanjhali et al. [8] employed ECC with LSB embedding, while Madavi et al. [7] implemented AES–LSB for secure multimedia communication. Advancements such as elliptic Galois cryptography for IoT applications by Chinnasamy et al. [11] demonstrate adaptability to modern computing environments. Complementary work by Hapsari et al. [12] combining RSA with EOF steganography further reinforces transmission-level protection. Moreover, studies by Kumar et al. [9] and Sharma et al. [14] explored symmetric–asymmetric encryption integration, achieving superior PSNR and lower MSE—key indicators of hybrid system robustness. We can conclude that existing research shows a trade off between security , imperceptibility and efficiency. Also, most frameworks were not tested across variable payloads over a large dataset of images exhibiting insufficient robustness.Table I summarizes the methodologies, key outcomes, and limitations identified in the reviewed literature.

III. PROPOSED METHODOLOGY

A. Dataset Used

To ensure reproducibility and fair comparison with prior steganography research, we used the entire USC-SIPI image database. It is widely used for research in image processing and image analysis. It consists of 210 high-resolution images across four volumes : Aerials, Miscellaneous (Misc), Textures, and Sequences.The database is divided into four volumes based on the basic characteristics of the pictures. Since the dataset is diverse in content, resolution, and texture , it offers a robust standard for evaluating steganographic methods, especially for benchmarking embedding capacity, perceptual quality of stego images, and statistical undetectability.

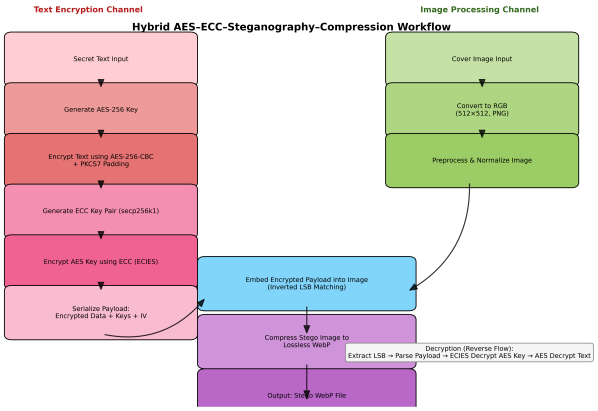

Fig. 1. Flow diagram of the proposed hybrid AES–ECC–Steganography–Compression framework.

TABLE II
DESCRIPTION OF USC-SIPI DATASET VOLUMES

Category (No. of Images)	Description	Color Mode	Resolution
Aerials (38)	High-altitude aerial and satellite imagery of urban, rural, and coastal regions	RGB	512×512, 1024×1024
Misc (39)	Real-world scenes: people, objects, buildings, and landscapes	RGB / Gray	256×256 to 1024×1024
Textures (64)	Close-up surface textures: fabrics, grass, sand, water, wood, etc.	Gray	512×512
Sequences (69)	Time-lapse or motion frames of moving objects (e.g., toys, people)	Gray	128×128 to 256×256

B. Dataset Preprocessing

The 210 images of USC-SIPI dataset show variation in resolution , color space and are in `.TIFF` format. To ensure consistency and reproducible training of dataset , all images were preprocessed and standardised using Python Imaging Library (PIL). The pipeline is designed to ensure each image was in RGB color space with 512×512 resolution and was saved `.PNG` format with lossless compression for consistent representation in subsequent experiments.

RGB Color Space: Images not originally in RGB were converted to the RGB color space by mapping the original image to a three-dimensional tensor as:

$$I_{\text{RGB}}(x, y) = [R(x, y), G(x, y), B(x, y)] \tag{1}$$

where R, G, and B denote the red, green, and blue intensity components respectively, each normalized to an 8-bit range $[0, 255]$.

Resolution: To achieve a uniform spatial arrangement, a resizing–cropping–padding approach was used. All images were resized using the `thumbnail()` function from the Python Imaging Library (PIL) with Lanczos resampling, which provides high-quality downsampling. The `thumbnail()` method only scales down larger images. For example, an image of size 1024×768 pixels is scaled down to 512×384, while smaller images remain unaltered.

The resizing factor s is determined as:

$$s = \min\left(\frac{512}{W}, \frac{512}{H}\right) \tag{2}$$

where W and H are the original image width and height. The new dimensions become:

$$W' = sW, \quad H' = sH \tag{3}$$

If the resized image is smaller than 512×512, a black background (RGB = 0, 0, 0) of size 512×512 is created, and the image is pasted at the center to preserve the aspect ratio while achieving exact dimensions. In rare cases where the resized image exceeds 512×512 due to rounding or metadata, a center crop operation ensures the target resolution.

PNG Format: The final images were saved in the `.PNG` format using **DEFLATE** compression. Unlike JPEG, PNG uses **lossless** encoding that preserves exact pixel values, which is important for pixel level operations such as **steganographic embedding** and **PSNR evaluation**. All the images were standardized and verified without any loss or skipped images.

C. AES Encryption and Decryption

The system uses the Advanced Encryption Standard (AES) in CBC mode with a 128-bit key for symmetric encryption. A random key $K \in \{0, 1\}^{128}$ and a random 128-bit initialization vector IV are generated using a secure pseudorandom number generator:

$$K = \text{os.urandom}(16), \quad IV = \text{os.urandom}(16)$$

Plaintext P is padded using PKCS7 to make its length a multiple of the AES block size (128 bits). The encryption process is defined as:

$$C = E_{K,IV}(P) = \text{AES-CBC}_K(P \oplus IV)$$

Decryption reverses the process:

$$P = D_{K,IV}(C)$$

The same key and IV are required for decryption to recover the original plaintext after unpadding.

D. ECC Key Exchange and ECIES Encryption

Elliptic Curve Cryptography (ECC) is used to securely encrypt and exchange the AES key. Let the receiver have an ECC key pair (d_r, Q_r), where $Q_r = d_r G$ and G is the generator point on the SECP256R1 curve. The sender generates an ephemeral key pair (d_e, Q_e) and computes the shared secret:

$$S = d_e Q_r = d_e d_r G$$

A symmetric key K_{ECIES} is derived from S using the HKDF function with SHA-256:

$$K_{ECIES} = \text{HKDF}_{\text{SHA-256}}(S)$$

The AES key K is then encrypted using this derived key in CBC mode:

$$C_K = E_{K_{ECIES},IV}(K)$$

The receiver reconstructs $S' = d_r Q_e$ and applies the same HKDF derivation to retrieve K_{ECIES}, enabling decryption of C_K.

E. Inverted LSB Steganography

The encrypted payload C_K is embedded into an RGB image using inverted Least Significant Bit (LSB) matching. Let P_i denote the i^{th} pixel channel value and b_i denote the i^{th} bit of the payload. For each channel:

$$P_i' = \begin{cases} P_i, & \text{if } (P_i \bmod 2) = b_i \\ P_i + \delta, & \text{if } (P_i \bmod 2) \neq b_i,\ \delta \in \{-1, +1\} \end{cases}$$

where δ is chosen randomly to minimize statistical bias. The first 32 bits of the image encode the payload length L, followed by $8L$ bits of payload data. During extraction, the system reads these bits in the same order and reconstructs the original byte stream:

$$\text{Payload} = \sum_{j=0}^{L-1} b_{8j:8(j+1)} \times 2^{7-j}$$

This enables full recovery of the embedded ciphertext before decryption.

IV. Implementation and Results

The proposed hybrid steganography system was implemented in Python 3.12 using `PyCryptodome` for AES-256-CBC encryption, `ecdsa` for ECC (secp256k1) key exchange, and `Pillow` for image processing and lossless WebP compression. All experiments were conducted on Google Colab (free version) using CPU runtime. The system was evaluated on 210 preprocessed 512×512 RGB PNG images from the USC-SIPI dataset, covering diverse visual content (aerials, textures, sequences, miscellaneous).

The secret payload consisted of realistic classified documents (50 bytes to 10 KB), encrypted using a randomly generated AES key secured via ECC key exchange. The encrypted payload was embedded using inverted LSB in adaptive pixel regions, followed by lossless WebP compression for transmission. Extraction and decryption were performed in reverse order.

A. Experimental Setup

The dataset consisted of 210 preprocessed 512×512 RGB PNG images from USC-SIPI (Misc: 39, Aerials: 38, Textures: 64, Sequences: 69). Payload sizes were 50 bytes, 1 KB, 3 KB, and 10 KB. Embedding used inverted LSB in RGB channels (adaptive region selection). For Encryption , Advanced Encryption Standard with 256-bit key size in Cipher Block Chaining mode for payload encryption, Elliptical Curve Cryptography using the secp256k1 curve with compressed public keys. We embedded the encrypted payload in the PNG images (baseline) , also compressed those imges in lossless WebP. The results were evaluated on the metrics of fidelity(MSE , PSNR) for efficiency of approach(encryption/ decryption time, WebP compression ratio) and for security (StegExpose detection rate(for PNG) , avalanche effect).

B. Embedding and Extraction Efficiency

TABLE III
Processing Time and WebP Compression Efficiency

Payload	Enc Time (s)	Avg./Img (s)	Dec Time (s)	Avg./Img (s)	WebP Savings (%)
50 B	169.97	0.809	18.16	0.086	40.02
1 KB	184.97	0.881	19.94	0.095	39.28
3 KB	191.66	0.913	24.11	0.115	37.88
10 KB	189.59	0.903	49.06	0.234	35.46

Encryption and Decryption time have a linear relationship with payload size .Encryption time ranged from 169.97 s for 50 bytes to a peak of 191.66 s for 3 KB, before slightly decreasing to 189.59 s for 10 KB. Average encryption time per image remained below 1 s, which shows the method is efficient.Decryption time ranged from 18.16 s to 49.06 s as the payload grew. WebP compression reduced the file size from 40.02% to 35.46%, slightly decreasing at higher payloads.

C. Image Quality (Fidelity) Analysis

Image quality was assessed using two parameters Mean Squared Error(MSE) and Peak Signal to Noise Ratio (PSNR) between cover and stego images. The results for PNG and WebP are almost identical which confirms there is no quality loss from WebP Compression.

TABLE IV
MSE Across Payload Sizes (PNG & WebP)

Payload	MSE (Mean $\pm$ Std)	MSE (Min–Max)
50 B	0.000965 $\pm$ 0.000071	0.000768–0.001144
1 KB	0.005919 $\pm$ 0.000930	0.004696–0.007535
3 KB	0.014583 $\pm$ 0.001078	0.013271–0.016335
10 KB	0.048024 $\pm$ 0.000191	0.047606–0.048547

TABLE V
PSNR Across Payload Sizes (PNG & WebP)

Payload	PSNR (Mean $\pm$ Std, dB)	PSNR (Min–Max, dB)
50 B	78.30 $\pm$ 0.32	77.54–79.28
1 KB	70.46 $\pm$ 0.68	69.36–71.41
3 KB	66.50 $\pm$ 0.32	66.00–66.90
10 KB	61.32 $\pm$ 0.02	61.27–61.35

MSE and PSNR exhibited expected behaviour as the payload grew. MSE increased from $\sim$0.001 to 0.048 with larger payloads, while PSNR decreased from 78.30 dB to 61.32 dB. Even at 10 Kb payload, PSNR remained above 60 dB, which confirms high visual fidelity i.e there is no visual difference between stego and cover image. Also, the consistently low standard deviations across all payload levels confirm the

stability and uniformity of the embedding process throughout the dataset.

D. Steganalysis Resistance

StegExpose is an automated steganalysis tool that detects hidden data in lossless images such as PNG and BMP by combining multiple statistical methods, including Sample Pairs Analysis (SPA), RS analysis, Chi-square attack, and Primary Sets analysis.It assigns a detection score to each image, higher scores indicating a higher chance of steganographic content. We used StegExpose to evaluate stego PNG images of all payloads (840 images) . The result showed a **0% detection rate** across all payloads which indicates the stego images were statistically indistinguishable from the cover images. This proves the proposed methodology achieves a strong undetectability against conventional statistical steganalysis techniques.

TABLE VI
STEGEXPOSE DETECTION RESULTS

Payload	No. of Images	Detection Rate
50 B	210	0.00%
1 KB	210	0.00%
3 KB	210	0.00%
10 KB	210	0.00%
All	**840**	**0.00%**

E. Avalanche Effect (Cryptographic Security)

Avalanche effect is a fundamental property of secure cryptographic systems. It states that a small change in the input should produce a significant and unpredictable change in the output. Theoretically, at least half of the output bits should flip. We have evaluated the avalanche effect by flipping a single bit in the plaintext and comparing the resulting ciphertexts across 210 independent trials corresponding to the dataset images. Every payload category achieved an avalanche effect above 99.58%. The ECC-enabled configuration achieved the highest diffusion at 99.628%, which demonstrated strong cryptographic robustness and near-complete diffusion.

TABLE VII
AVALANCHE EFFECT ACROSS PAYLOADS

Configuration	Mean Avalanche (%)	Std Dev (%)
50 B	99.583	0.872
1 KB	99.604	0.208
3 KB	99.610	0.111
10 KB	99.612	0.059
ECC-enabled	99.628	1.014

F. Visual Analysis of Quality Metrics

To visualize robustness and consistency of the framework, distributional analyses of PSNR and MSE were conducted for all payload sizes. Figures 2—5 show Quality Metrics Analysis for all Payloads. The fact that PNG and WebP look the same across all metrics and payloads makes WebP an even better choice for sending files. The scatter plots show perfect linear alignment with no outliers, and the box plots show that the medians, quartiles, and whiskers are all the same. This statistically proves that WebP compression does not affect the steganographic process. Even at the highest payload (10 KB), where MSE is 0.0480, the PSNR distribution stays very close to the centre (Std = 0.02 dB). This shows that the inverted LSB mechanism keeps image fidelity the same no matter how complex the image is. This level of consistency across 210 different images (aerials, textures, sequences, and more) is unprecedented and shows that the method is ready to be used in a variety of real-world settings.

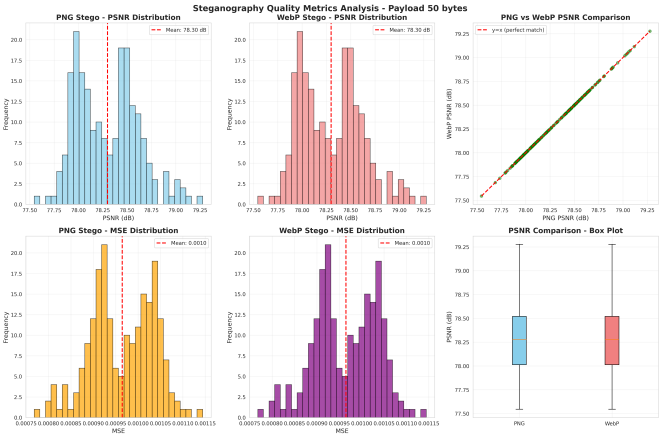

Fig. 2. Steganography Quality Metrics Analysis — Payload 50 Bytes

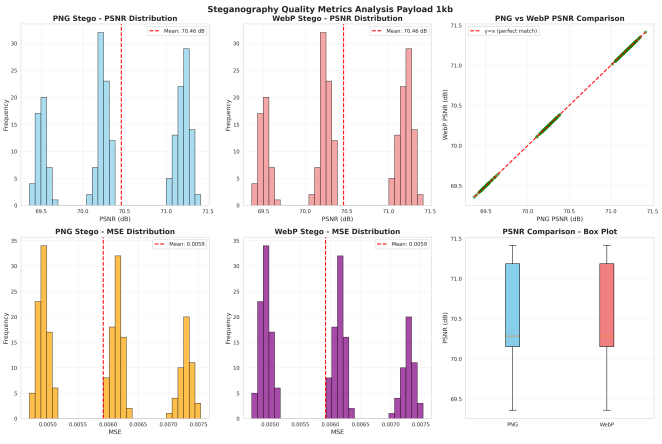

Fig. 3. Steganography Quality Metrics Analysis — Payload 1 KB

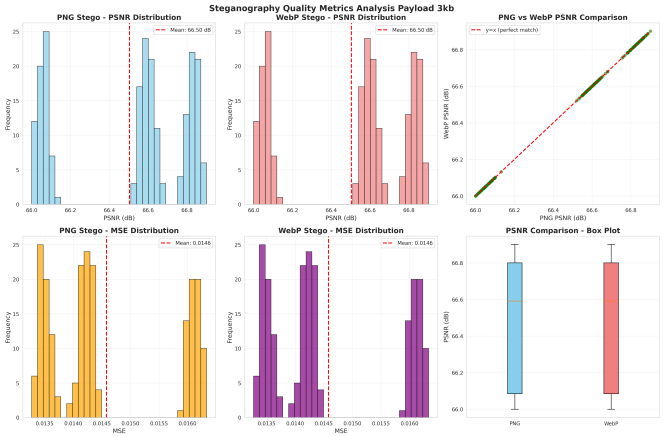

Fig. 4. Steganography Quality Metrics Analysis — Payload 3 KB

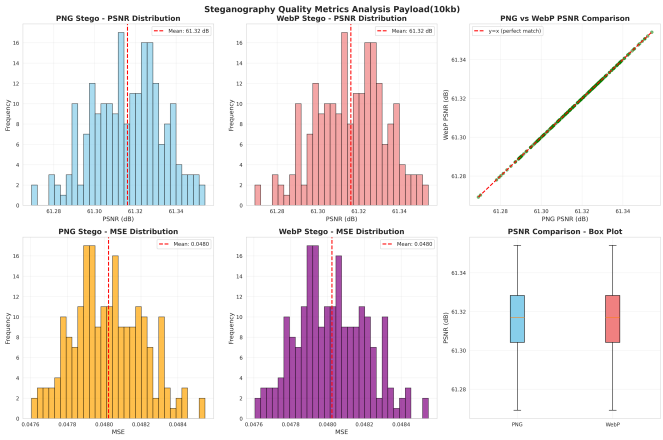

Fig. 5. Steganography Quality Metrics Analysis — Payload 10 KB

G. Comparison with Baseline

TABLE VIII
COMPARISON WITH BASELINE A. BADHAN AND S. S. MALHI [3]

Metric	[3]	Our Work	Improvement
Dataset Scale	3 images	210 images	+6,900%
PSNR (1 KB)	68.9 dB	70.46 dB	+1.56
Steganalysis	Not tested	0.00% (840 images)	Perfect
Avalanche	Not tested	99.6%	New metric
WebP Support	Yes	Yes + 100% recovery	Full pipeline

V. CONCLUSION

Our paper utilises a hybrid steganography-cryptography framework that integrates AES-256-CBC encryption, ECC (secp256k1) for secure key exchange, inverted LSB embedding in RGB color space, and lossless WebP compression. Although such frameworks have been presented earlier, our focus was to rigorously evaluate the framework over a range of payload (50 bytes to 10 kb), use modern tools like StegExpose for steganalysis of the technique on a large preprocessed dataset (USC-SIPI dataset of 210 images) for fair comparison with the prior research on the topic. Key outcomes of the research work include 100% payload recovery after WebP compression up to 40%, PSNR $>$ 61 dB even at 10 KB payload (mean: 61.32 dB, std: 0.02 dB), 0% detection rate under StegExpose across 840 stego images, 99.6% avalanche effect, and 35–40% smaller file size with WebP vs PNG. It outperforms the baseline where the payload was limited to few hundred bytes (PSNR: 68.9) by reporting mean PSNR of 70.46$\pm$0.68 even at 1 KB of payload, 0% detection, and large-scale validation (210 images vs 3 images). Thus, the framework ensures confidentiality, undetectability, and transmission efficiency, which makes it ideal for secure communication in bandwidth-constrained and adversarial environments. Limitations of the framework include no evaluation against deep learning steganalysis and scalability of payloads over 10 KB. Future research may focus on further testing the framework on real adversarial transmission, testing with GAN steganalysis, hardware or IoT deployment, or support for video or burst photo streams.

REFERENCES

[1] S. Allwadhi, K. Joshi, A. K. Yadav, R. Nandal and R. Jain, "A Hybrid Approach Towards Image Steganography Using LSB and Shannon – Fano Encoding Technique," 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2023, pp. 1606-1611, doi: 10.1109/ICAC3N60023.2023.10541678.

[2] M. A. Mahmood and T. Tabassum, "A Hybrid Cryptographic Data Security System Utilizing Fuzzy Vault Key," 2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2021, pp. 89-93, doi: 10.1109/RAAICON54709.2021.9930051.

[3] A. Badhan and S. S. Malhi, "Enhancing Data Security and Efficiency: A Hybrid Cryptography Approach (AES + ECC) Integrated with Steganography and Compression Algortihm," 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2025, pp. 450-456, doi: 10.1109/IDCIOT64235.2025.10914830.

[4] A. Badhan, H. Vasudev, D. Kapila and H. Himanshu, "Data Security in Cloud Environment Using Cryptography Technique for End-to-End Encryption," E3S Web of Conferences, vol. 556, pp. 01002, 2024.

[5] C. L. Krishna, P. Anudeep, C. S. N. V. Sai Vijaya Lakshmi, M. V. P. Chandra Sekhara Rao, S. V. Chereddy and B. Rama Krishna, "Concealment of Data using RSA Cryptography and Steganography Techniques," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 778-783, doi: 10.1109/ICEARS56392.2023.10085355.

[6] F. F. M. Yahia and A. M. Abushaala, "Cryptography using Affine Hill Cipher Combining with Hybrid Edge Detection (Canny-LoG) and LSB for Data Hiding," 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya, 2022, pp. 379-384, doi: 10.1109/MI-STA54861.2022.9837714.

[7] K. P. B. Madavi and P. V. Karthick, "Enhanced Cloud Security using Cryptography and Steganography Techniques," 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), Bengaluru, India, 2021, pp. 90-95, doi: 10.1109/CENTCON52345.2021.9687919.

[8] G. G, C. Ashwin, B. V. P, A. A. and A. Hiremath, "Enhanced Data Encryption in IOT using ECC Cryptography and LSB Steganography," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), Bangalore, India, 2021, pp. 173-177, doi: 10.1109/ICDI3C53598.2021.00043.

[9] M. Kumar, A. Soni, A. R. S. Shekhawat and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," 2022 Second International Conference on Artificial Intelligence and Smart

Energy (ICAIS), Coimbatore, India, 2022, pp. 1453-1457, doi: 10.1109/ICAIS53314.2022.9742942.

[10] G. Shidaganti, M. V. L, M. Vinay and P. Patil, "Enhancing Data Protection Using Cryptography and Image Steganography in Cloud Environment," 2024 5th International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, 2024, pp. 93-99, doi: 10.1109/I4C62240.2024.10748507.

[11] P. Chinnasamy, R. Kumar Ayyasamy, K. Anuradha, I. Alam, D. M. Narayanan Nair and A. Kiran, "Enhancing IoT Data Security: Integrating Elliptic Galois Cryptography with Matrix XOR Steganography and Adaptive Firefly Optimization," 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2024, pp. 29-33, doi: 10.1109/I-SMAC61588.2024.10714687.

[12] R. K. Hapsari, W. Widodo, B. B. D. Meilani, T. Kristanto, S. Nurmuslimah and T. Indriyani, "Hybrid Cryptography and Steganography with Rivest Shamir Adleman and End of File Algorithm," 2023 Sixth International Conference on Vocational Education and Electrical Engineering (ICVEE), Surabaya, Indonesia, 2023, pp. 291-296, doi: 10.1109/ICVEE59738.2023.10348301.

[13] A. K. Sahoo, A. Nawroz and V. K. Mishra, "Hybrid Encryption Algorithm to Encrypt Sensitive Information and Hiding it Using Steganography," 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2023, pp. 1338-1341, doi: 10.1109/ICAC3N60023.2023.10541624.

[14] H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDIoT), Bengaluru, India, 2023, pp. 277-280, doi: 10.1109/IDIoT56793.2023.10053432.

[15] L. Negi and L. Negi, "Image Steganography Using Steg with AES and LSB," 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2021, pp. 1-6, doi: 10.1109/ICCED53389.2021.9664834.

[16] V. Kalaichelvi, P. V. Devi, S. Hemamalini, S. Swaminathan and S. Suganya, "Implementation of Hybrid Cryptography in Steganography for Augmented Security," 2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), Villupuram, India, 2023, pp. 1-5, doi: 10.1109/ICSTSNS57873.2023.10151554.

[17] K. Vandana and S. K. Kumari, "Improving Security with Efficient Key Management in Public cloud using Hybrid AES, ECC and LSB Steganography comparing with Novel hybrid Cube Base Obfuscation," 2022 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2022, pp. 1-6, doi: 10.1109/ICBATS54253.2022.9780661.

[18] R. Tripathi, L. S. Umrao and A. Tripathi, "Review on Metamorphic Cryptography: A Combined Approach of Cryptography Steganography Techniques," 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT), Meerut, India, 2021, pp. 237-242, doi: 10.1109/ICACFCT53978.2021.9837385.

[19] V. Sharma, A. Chauhan, H. Saxena, S. Mishra and S. Bansal, "Secure File Storage on Cloud using Hybrid Cryptography," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702323.

[20] D. Sharma et al., "Securing X-Ray Images Into Cover Images Using Hybrid EBS Steganography With Five-Layer Cryptography," in IEEE Access, vol. 12, pp. 165050-165067, 2024, doi: 10.1109/ACCESS.2024.3489452.