An Adaptive LSB-Based Video Steganography Framework with Blockchain-Enabled Verification for Secure Multimedia Communication

S. G. Sumana
School of Computer Applications, Dayananda Sagar University, Bengaluru, Karnataka, India
sg.sumana-ca@dsu.edu.in

T. M. Rajesh
School of Engineering, Dayananda Sagar University, Bengaluru, Karnataka, India
rajesh-cse@dsu.edu.in

S. G. Shaila
School of Engineering, Dayananda Sagar University, Bengaluru, Karnataka, India
shaila-cse@dsu.edu.in (corresponding author)

Received: 5 November 2025 | Revised: 20 December 2025 and 10 January 2026 | Accepted: 12 January 2026

 DOI: https://doi.org/10.48084/etasr.16031

ABSTRACT

Digital communication systems face an ongoing major challenge to protect video information from unauthorized access, tampering, and eavesdropping operations. Standalone steganographic methods face two major drawbacks: restricted data storage capabilities and decreased ability to remain undetectable. This study presents an integrated video security framework that unites adaptive video steganography with hybrid cryptographic encryption and blockchain-enabled verification to protect data confidentiality, robustness, and integrity. The proposed framework consists of three separate modules that work together: StegoVision, Robust Video Steganography with Decoy Extraction, and Blockchain-Enabled Encryption. The StegoVision module uses an adaptive Least-Significant Bit (LSB) based embedding scheme with multi-stage compression to enable high-capacity covert communication. The system uses AES-CBC encryption with Knight's Tour-based adaptive embedding and deception techniques to protect unauthorized extractors from detecting hidden data. The system uses hybrid AES-RSA encryption with IPFS-based decentralized storage to achieve tamper-proof authentication and traceability. The proposed method was tested on the HMDB51 (Human Motion DataBase) benchmark dataset. The StegoVision system achieved 94.1% accuracy through its visual quality preservation during compression and format conversion processes. The decoy-based model achieved 42.6 dB PSNR and 0.981 SSIM during compression and format conversion processes. The blockchain module achieved encryption speeds up to 320 MB/s with near-lossless reconstruction (PSNR > 51.4 dB, SSIM ≈ 0.999) and integrity verification accuracy exceeding 99.9%. A comparative analysis demonstrates that the proposed framework achieves an optimal balance between capacity, imperceptibility, robustness, and verifiability.

Keywords-video steganography; blockchain; AES–RSA encryption; IPFS; adaptive LSB; knight's tour embedding; decoy extraction; data security

I. INTRODUCTION

In the contemporary digital era, securing video data has become increasingly critical as vast volumes of sensitive video data, ranging from corporate communications to medical records and journalistic content, are transmitted over open and often untrusted networks. Protecting this data from interception, tampering, and unauthorized access is a major security challenge. Data protection through conventional encryption methods offers robust confidentiality but reveals the existence of encrypted data, which might attract the attention of malicious entities. Steganography provides an alternative method to hide important information in media, allowing users to send hidden messages. Videos are particularly well-suited for this purpose due to their high redundancy, large payload capacity, and the limited sensitivity of the human visual system

to minor visual distortions. The first spatial-domain methods, which used basic Least Significant Bit (LSB) replacement, suffered from two major security vulnerabilities, as they could be detected by steganalysis methods and became vulnerable to compression attacks, while their ability to hide information remained poor. A comprehensive video security system must address present limitations by combining concealed operations with performance enhancement, system defense, and verification-based system integrity protection.

The research community has developed new video steganography methods that use learning-based and encryption-assisted approaches to address the limitations of traditional methods. In [1], a secret-key randomized frame selection method encrypted data and embedded it in LSB positions to achieve 74.15 dB PSNR and 0.0002 (JCBI) MSE, but incurred high computational and slower data transmission speeds. In [2], an adaptive GAN-based steganography model achieved 95% steganographic success and 48.3 dB PSNR (PLOS) but required long training periods and large amounts of data. In [3], a distributed payload embedding method offered enhanced resistance to compression and noise but had decreased efficiency in embedding data and required more computational resources. In [4], a metadata-based MP4 scheme protected video content through ZLIB+AES encryption while maintaining video quality and defending against cropping and compression attacks. However, this approach required metadata for functionality and stored less data than frame-based methods. In [5], a GAN-controlled generative video steganography method produced realistic content with editing capabilities but required powerful hardware and showed weak resistance to adversarial attacks. In [6], a deep-learning steganography method successfully deceived both human observers and AI detection systems, achieving better hiding capabilities at the cost of reduced system flexibility. This work also used limited datasets. In [7], genetic algorithms were applied to select ROI, resulting in better system embedding performance but creating more complex systems that required specific parameter values for operation.

In [8], it was shown that payload scrambling before embedding could improve confidentiality protection but would reduce the available transmission capacity. In [9], spatial transformation and deep methods were evaluated, but security and imperceptibility updates demonstrated that robust real-time and steganalysis methods remained unsolved. In [10], a video system used an encrypted payload to improve the security of satellite channels, but achieved only limited embedding efficiency. In [11], an indicator-based LSB scheme randomly embedded a secret key to improve imperceptibility, but remained vulnerable to filtering and compression as a spatial-domain method. In [12], it was shown that MSE fails as a fidelity measurement, supporting the use of perception-based evaluation methods. In [13], primitive steganography theory and countermeasures were presented.

According to [14], research on blockchain applications for media integrity protection remains in its development stage, while the study in [15] summarized possibilities and scalability/privacy issues. In [16], HMAC/ECC was used to hash video clips on the blockchain, but it encountered slow verification. In [17], lightweight symmetric and asymmetric ciphers were evaluated to develop hybrid encryption systems. In [18], steganography was used in conjunction with blockchain technology and IPFS (InterPlanetary File System) for copyright protection; however, this approach faced scalability problems. Other studies have investigated different approaches to merge compression with encryption and blockchain technology to protect IoT/surveillance networks [19-21]. Time-stamping on resource-limited devices can be performed using lightweight blockchain schemes [22, 23]. In [24-26], it was shown that blockchain technology can serve two essential functions in intelligent surveillance systems: provenance and verification processes.

II. PROPOSED METHODOLOGY

The proposed framework integrates three mutually reinforcing components to enable secure, reliable, and verifiable video communication. First, video encryption is used to ensure content confidentiality during both transmission and storage. Second, a key-dependent adaptive embedding strategy is used to conceal payload data through covert mapping, enhancing resistance to unauthorized detection and extraction. Third, a blockchain-based anchoring mechanism is incorporated to provide immutable integrity verification, traceability, and non-repudiation through on-chain authentication. Experimental evaluation was conducted using the HMDB51 dataset (Human Motion Database) [27], which contains human action recognition from movie clips and web sources, comprising 6,766 instances of real-world videos in 51 categories. These videos contain a wide variety of action samples with varying viewpoints, light intensities, and levels of background clutter. The duration of each instance in this dataset is short, with a time span of 1 to 10 seconds.

A. StegoVision-Adaptive LSB-Based Video Embedding

The proposed method is structured into phases that ensure efficient, secure, and imperceptible data embedding within video content. Each phase contributes to the goal of robust, key-driven, and adaptive steganographic communication. Figure 1 depicts the architecture of the proposed method.

1. Preprocessing Phase: The input video V is decomposed into frames F_1, F_2,…,F_N, each converted into a suitable color space (YC_bC_r) to enable embedding in visually less sensitive channels. A local complexity map $C_t(x, y)$ is computed using local variance or edge gradients to identify high-texture regions ideal for imperceptible data embedding.

2. Adaptive Selection Phase: In this regard, the pixels with complexity $c \geq T_c$ are selected in a probabilistic manner for embedding. This adaptive selection helps in embedding secret bits mainly in textured areas while preserving a high visual quality and simultaneously maximizing embedding efficiency.

3. Embedding Phase: In this phase, the secret video bitstream b_1, b_2,..., b_L is embedded into the selected pixels. For every pixel $p \in P_t$, a predefined number of Least

Significant Bits (LSBs), one or two, are replaced with message bits using an embedding function:

$$I_t'(p) = \text{Embed LSB}\big(I_t(p), b_j\big) = (I_t(p) \,\&\, \overline{(2^k - 1)}) | \text{bits}(b_j) \quad (1)$$

where $I_t'(p)$ is the modified pixel after embedding, $I_t(p)$ is the original pixel value, b_j is the message bit(s), $\overline{(2^k - 1)}$ is the bitmask to clear the last k bits, $\text{bits}(b_j)$ converts message bit(s) to bit representation, and k represents the number of modified LSBs. To enhance security, the system employs a pseudo-random permutation generated by a Pseudo-Random Number Generator (PRNG) using a secret key K. This random permutation defines the sequence in which message bits are embedded across selected pixels, making it highly resistant to unauthorized extraction or statistical steganalysis.

4. Post-Processing and Packaging Phase: After embedding, the modified frames F_t' are reconstructed and re-encoded to produce the stego-video $V' = Encode\{F_t'\}$. To ensure message integrity, optional error detection mechanisms, such as cyclic redundancy checks or block-level checksums, are computed and embedded within the video. This extra layer allows the receiving end to confirm that the message extracted has not been corrupted or tampered with in any manner during transmission.

5. Extraction Phase: On the receiver end, the extraction process reverses the embedding steps using the shared secret key K. The PRNG generates the same pseudo-random permutation that allows the receiver to correctly determine the embedding positions P_t in each frame. The LSBs from these positions are extracted and then concatenated for the reconstruction of the embedded video. In addition, checksum verification confirms the integrity and correctness of the retrieved data.

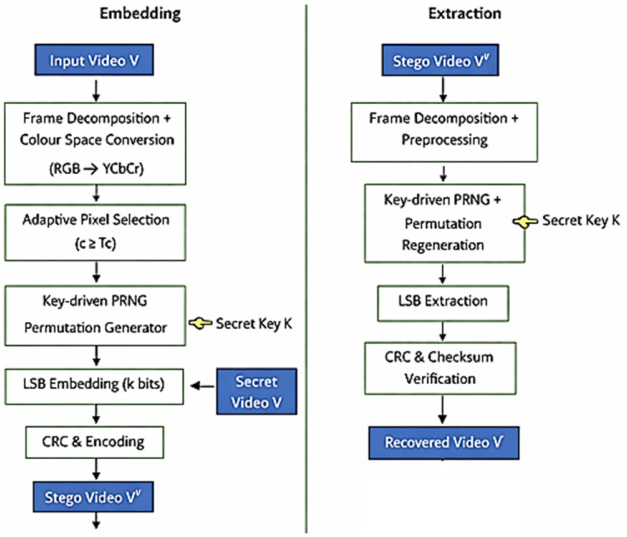

Fig. 1. Architecture of the proposed adaptive video steganography framework.

B. Video Steganography with Decoy Extraction Mechanism

Figure 2 depicts the architecture of the proposed video steganography with a decoy extraction mechanism.

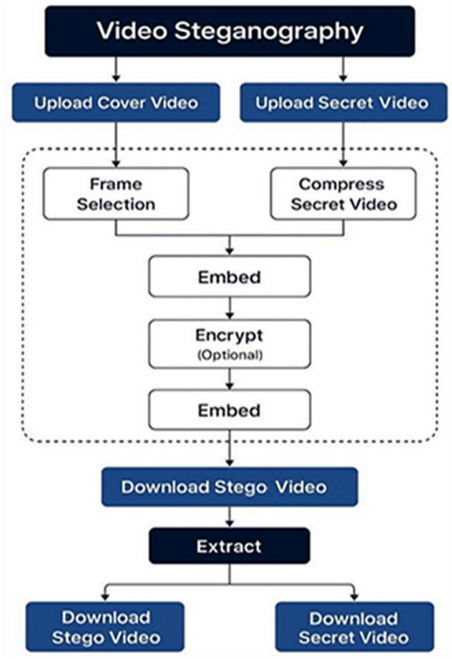

Fig. 2. The proposed video steganography with decoy extraction mechanism scheme.

This scheme includes the following steps.

1. Design idea: Embed two payloads into the video; a real payload R including the confidential data to be communicated to legitimate users, and a decoy payload D that is plausible in appearance and returned to unauthorized extractors to mislead the attackers.

2. Decoy generation: Generate a decoy D that appears genuine, such as a low-sensitivity photo, lorem text, or structured pseudo-data. Decoys can vary across segments such that repeated unauthorized extractions produce different decoys.

3. Embedding strategy: Divide embedding positions into two disjoint sets, P_R (for the real payload) and P_D (for the decoy), and use a keyed PRNG such that the correct key K produces a permutation π_K that maps bits to PRP_RPR, while an incorrect key K' maps to PDP_DPD.

4. Embedding algorithm: Embed the bitstreams M_R and M_D into the selected positions so that each pixel/frame value is modified by an embedding function:

$$I'(p) = \text{Embed}(I(p), b) \quad (2)$$

where b is drawn from the mapped sequence determined by the key-driven permutation.

5. Extraction: The extractor regenerates the mapping using the supplied key as:

$$K_{\text{supplied}} = K \quad (3)$$

The routine yields MRM_RMR (the real payload), otherwise, it yields M_D (the decoy).

6. Robustness techniques: Increase reliability by combining LSB embedding with error-correcting codes and spreading the payload across multiple frames/pixels so that the hidden data survives with mild transformations and lossy reencoding.

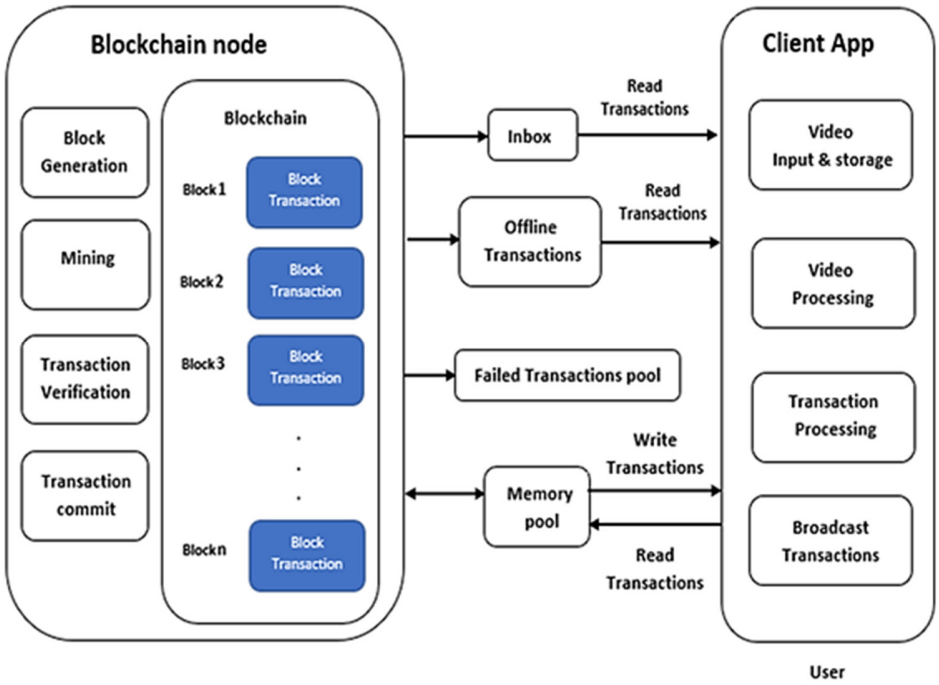

Fig. 3. Proposed architecture for video encryption and decryption.

C. *Encryption & Decryption of Video Information Using Blockchain*

The proposed method of encryption and decryption of video information with blockchain integrates cryptography and blockchain technology for secure, verifiable, and tamper-proof video transmission. The whole process is divided into five important phases that altogether maintain the confidentiality, integrity, and authenticity of video data.

1. Video Encryption Phase: The video content is encrypted using a symmetric algorithm such as AES-256-GCM (Advanced Encryption Standard using a 256-bit key with Galois/Counter Mode), ensuring data confidentiality during storage and transmission:

$$C = \text{Enc}_{K_s}(V) \quad (4)$$

where K_s is the symmetric key and V is the input video. For large files, the video may be divided into chunks $V = \{F_1, F_2, \ldots, F_n\}$, each encrypted separately to support efficient processing and partial verification. The encrypted output C serves as the foundation for blockchain anchoring.

2. Hashing and Metadata Generation Phase: After encryption, a SHA-256 (Secure Hash Algorithm 256-bit) hash is computed to generate a unique digital fingerprint for the encrypted video as:

$$H = \text{SHA256}(C) \quad (5)$$

This ensures traceability and identity verification within the blockchain framework.

3. On-Chain Anchoring Phase: The computed hash and metadata are securely recorded on the blockchain as:

$$tx = \text{BlockchainStore}(H, \text{meta}) \quad (6)$$

Optionally, the sender digitally signs the hash using his private key for non-repudiation:

$$S = \text{Sign}_{priv}(H \parallel \text{meta}) \quad (7)$$

This guarantees immutability and authenticity, making any tampering immediately detectable through blockchain verification.

4. Storage Phase: The encrypted video C is stored off-chain using IPFS, cloud storage, or a secure file server, while only the hash and metadata remain on-chain. This hybrid model minimizes blockchain storage costs while retaining verifiability through the stored hash.

5. Verification and Decryption Phase: When access is requested, the receiver retrieves the encrypted video C' and computes its hash as:

$$H' = \text{SHA256}(C') \quad (8)$$

If $H' = H$, integrity is verified. The sender's signature, if present, is validated using:

$$Verify(pub, S, H) \quad (9)$$

After successful verification, the symmetric key K_s is securely obtained via key exchange or a key management system. The video is then decrypted:

$$V = \text{Dec}_{K_s}(C) \quad (10)$$

ensuring that only authorized users can access the original content.

III. RESULTS AND DISCUSSION

A. *StegoVision: Adaptive LSB-Based Video Embedding for Secure Communication*

Experiments were conducted solely on the HMDB51 dataset with a total of 6,766 unconstrained human-action videos in 51 classes in AVI format with a controlled evaluation set of 120 videos, 80 used for cover videos and 40 used for secret videos. The secret videos were embedded in two distinct cover videos to remove content dependency and make them more generalized based on different motion and texture patterns. Videos were uniformly resized to a fixed image size of 320×240 pixels, with a processing speed of 30 fps, processed on a frame-by-frame basis with approximately 900-1800 frames in a video, focusing mainly on embedding into the luminance Y component.

Instead of a fixed experimental setup, a variety of experimental conditions were tested. Experiments were conducted under diverse storage and transmission environments, including compression with low, medium, and high bit-rate settings using H.264, MPEG-4 re-encoding, and other format conversion situations, such as AVI to MP4 conversion. The experimental results were tested in each configuration a number of times, and the performance results are shown in Table I for all cover secret image pair attacks.

TABLE I. PERFORMANCE ANALYSIS OF ADAPTIVE LSB-BASED VIDEO EMBEDDING

Embedding mode	Payload (kbps)	PSNR (dB)	SSIM	Retrieval accuracy (%)
Adaptive LSB	18.6	40.6±0.2	0.941±0.016	94.1±1.2

Quantitatively, this framework obtained a PSNR of 40.6±0.2 dB and a Structural Similarity Index Measure (SSIM) of 0.941±0.016, ensuring imperceptibility and excellent structural similarity, respectively. The 94.1±1.2% in image recall not only ensures accuracy during reliable extraction but is further guaranteed with small standard deviations. With respect to computation complexity, this technique can easily achieve nearly real-time processing with an average time of 3.8±0.5 s in embedding and 3.4±0.3 s in retrieving a 60-second video.

B. *Robust Video Steganography with Decoy Extraction Mechanism*

The effectiveness of the proposed AES-CBC (Advanced Encryption Standard in Cipher Block Chaining) + Knight's Tour + Decoy-based video steganography technique was tested solely on the HMDB51 dataset. As HMDB51 contains real, unconstrained human action videos with large variations in motion, light, background complexity, and compression artifacts, it serves better for robustness analysis of steganography in a real-world setting. Moreover, to obtain an accurate performance analysis, experimentation involved a series of videos. A total of 120 videos from HMDB51 were used, consisting of 80 cover videos and 40 secret videos. Every secret video was inserted into two different cover videos to reduce content bias and promote better generalization. The videos were all uniformly preprocessed to have a resolution of 320×240 pixels with a frame rate of 30 fps and a duration of 30-60 seconds, consisting of approximately 900-1800 frames per video. They were all in the YUV 4:2:0 format, and the embedding was performed on a frame-by-frame basis, focusing mainly on the luminance channel Y.

The experiments were performed under diverse testing environments. The stegovideos were tested with H.264 compression at low, medium, and high-quality settings, in addition to MPEG-4 re-compression, to assess robustness under compression attacks. Moreover, format conversion tests, such as conversion from AVI to MP4, were also considered to simulate a real-world transmission and storage environment. The final performance evaluation statistics were obtained after considering all these testing environments to represent a common behavior among different video contents. Table II presents performance metrics for the proposed video steganography technique.

TABLE II. PERFORMANCE ANALYSIS OF VIDEO STEGNOGRAPHY WITH DECOY EXTRACTION MECHANISM

Embedding mode	Payload (kbps)	PSNR (dB)	SSIM	Retrieval accuracy (%)
AES-CBC + Knight's Tour + Decoy	120–180	42.6 ± 0.8	0.981 ± 0.006	98.1 ± 1.4

The statistical analysis shows that a PSNR value of 42.6±0.8 dB can support a good level of visual imperceptibility for all HMDB51 videos and compression strengths, remaining above 40 dB perceptual thresholds. Also, an SSIM index of 0.981±0.006 ensures a good level of detail preservation, including action videos with higher levels of motion. Furthermore, an accuracy of 98.1±1.4% in secret video recovery assures an accurate secrecy support during decompression. In terms of computation, it takes a nearly real-time processing time of 3.5±0.3 s to embed a 60-second video and 3.1±0.6 s for extraction.

C. Encryption and Decryption of Video Information with Blockchain

The results demonstrate the efficiency and scalability of the hybrid AES-RSA (Advanced Encryption Standard-Rivest-Shamir-Adleman)+Blockchain framework for secure video encryption, storage, and retrieval. A total of 6,766 real-world action videos in HMDB51 were used to assess the effectiveness of the blockchain-integrated AES-RSA hybrid encryption system. To carry out controlled experimentation, a total of 120 HMDB51 videos were considered, of which 80 were cover videos used for encryption and sharing, and 40 were secret/target videos used for access-controlled video retrieval and verification. All videos used were preprocessed uniformly to have a resolution of 320×240 pixels, a frame rate of 30 fps, a length varying from 30 to 60 s, and a total of approximately 900 to 1800 frames in each video. The experimental analysis involved varying video file sizes, ranging from 100 KB to 100 MB. The experimental setup consisted of encrypting each HMDB51 video clip using AES with a streaming mode of encryption with protected keys using RSA encryption methods, and decentralized storage using IPFS with integrity anchoring to a blockchain ledger. Speed performance tests were conducted with varying network speed environments, including LAN, WAN, and access through a distant IPFS node, with a fivefold replication using different randomizations to make the results more reliable and less prone to bias.

As the file size grew from 100 KB to 100 MB, a linear scalability performance characteristic was observed, which attained a speed of up to 320 MB/s in encryption speed and up to 280 MB/s in decryption speed, with both encryption and decryption accomplished below 0.4 s in all HMDB51 files of various sizes. Taking an average of all four replicates, the encryption speed was approximately 207±88 MB/s, and the decryption speed was approximately 202±71 MB/s, showing robust performance. Times for blockchain mining and verification took approximately 2.4–10.5 s, with an average of approximately 6.5±2.9 s.

Table III depicts the performance metrics of the proposed Blockchain-based video encryption framework. These results show that the network is working stably, and file management is properly decentralized. Figure 4 illustrates how blockchain verification times consistently grow but within operational bounds, providing a very reliable integrity validation mechanism.

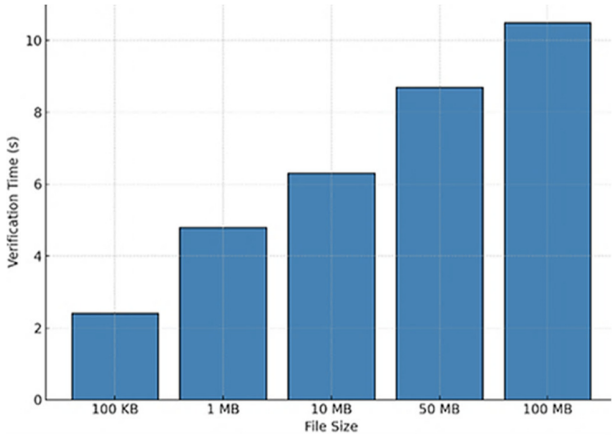

Fig. 4. Blockchain verification time across file sizes.

TABLE III. PERFORMANCE ANALYSIS OF THE PROPOSED VIDEO ENCRYPTION AND DECRYPTION FRAMEWORK USING BLOCKCHAIN

File size	Encryption Rate (MB/s)	Decryption Rate (MB/s)	Encryption Time (s)	Decryption Time (s)	Blockchain Mining Time (s)	IPFS Upload Time (s)	IPFS Download Time (s)	PSNR (dB)	SSIM
100 KB	~90	~100	0.01	0.01	2.5	2.2	1.5	48.9	0.997
1 MB	~150	~200	0.06	0.05	12	3	2	49.3	0.998
10 MB	~200	~170	0.08	0.09	5	6	4.5	50.1	0.999
100 MB	~320	~280	0.3	0.36	6.5	16	12	51.4	0.999

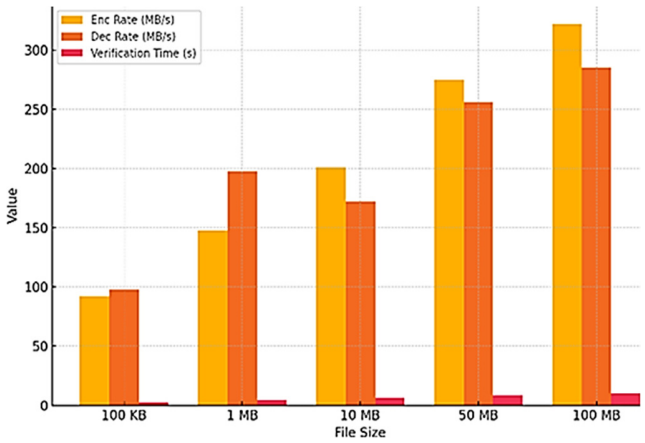

Fig. 5. Comparative performance metrics of blockchain encryption.

A comparative visualization of the metrics related to encryption, decryption, and verification in Figure 5 validates that the proposed model keeps a good balance between speed and security.

Figure 6 shows the performance of the three video security techniques over different key parameters. StegoVision tends to perform better in terms of imperceptibility and perfect data recovery, maintaining high visual quality. Blockchain encryption achieves the best performance in terms of processing efficiency and maximum-security robustness due to the incorporation of AES-RSA and blockchain. Decoy steganography balances strong imperceptibility and near-perfect retrieval with high deception-based protection. Overall, each technique tends to dominate one particular aspect of performance.

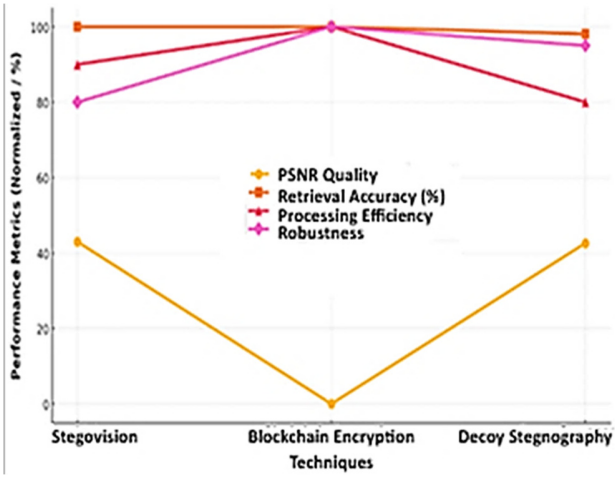

Fig. 6. Comparative performance of video security techniques.

The 5-fold cross-validation of the Blockchain encryption model confirms that it can provide high-speed performance in both data encryption/decryption and integrity verification across various file sizes and network environments. The speeds for encryption and decryption are all above 200 MB/s on average, while blockchain verification time increases only a little when data volume scales up, proving its excellent scalability. The blockchain framework achieved almost 100% integrity verification accuracy (99.9–100%) in all test cases on HMDB51, which confirms reliable hash validation and tamper resistance during video retrieval. Low variance of encryption/decryption times and verification accuracy across folds proves the consistency and robustness of the proposed design. In comparison with steganography-based modules in the overall system, the Blockchain encryption framework provides superior processing efficiency, scalability, and end-to-end security while ensuring the confidentiality, integrity, and verifiability of HMDB51 videos in decentralized transmission scenarios. Results confirm that the proposed Blockchain-based encryption model is well-suited for real-world, large-scale secure video communication.

Table IV shows the cross-validation results of the Blockchain encryption model. Table V presents a comparative review of the proposed models, namely, StegoVision, Blockchain Encryption, and Decoy Steganography, with traditional state-of-the-art video security techniques from 2017 to 2025. Overall, the proposed methods demonstrate enhanced robustness and efficiency compared to conventional or deep learning-based methods. This comparison establishes the proposed Blockchain encryption framework as a high-throughput, tamper-proof, and verifiable solution for secure and decentralized video transmission.

TABLE IV. CROSS-FOLD EVALUATION OF BLOCKCHAIN-BASED VIDEO ENCRYPTION AND VERIFICATION

Fold No.	Test File Size	Encryption Rate (MB/s)	Decryption Rate (MB/s)	Encryption Time (s)	Decryption Time (s)	Blockchain Verification Time	PSNR (dB)	SSIM
Fold 1	100 KB (local network)	92	98	0.01	0.01	2.4	49.2	0.998
Fold 2	1 MB (LAN)	148	198	0.06	0.05	4.8	49.8	0.998
Fold 3	10 MB (WAN)	201	172	0.09	0.10	6.3	50.4	0.999
Fold 4	50 MB (IPFS node access)	275	256	0.20	0.22	8.7	51.1	0.999
Fold 5	100 MB (remote node)	322	285	0.34	0.36	10.5	48.7	0.997

TABLE V. COMPARISON OF PROPOSED MODELS WITH STATE-OF-THE-ART VIDEO STEGANOGRAPHY TECHNIQUES

Study	Method Used	Performance metrics
Proposed model	Adaptive LSB + Decoy Mechanism + Blockchain-Enabled Video Steganography	PSNR = 51.4 dB, SSIM = 0.991
[1]	Randomized frame selection with LSB + encryption	PSNR = 74.15 dB, MSE = 0.0002
[2]	Adaptive GAN-based deep learning steganography	Success rate = 95%, PSNR = 48.3 dB
[3]	Distributed payload embedding across frames	Robust to compression and noise
[4]	Metadata-based MP4 steganography (ZLIB + AES)	PSNR ≈ 45 dB, visually lossless
[5]	GAN-driven generative video steganography	High realism, strong imperceptibility
[6]	Deep-learning steganography for fooling AI detectors	SSIM ≈ 0.97, strong concealment
[8]	Payload scrambling before embedding	Improved confidentiality and robustness
[10]	Encrypted payload for satellite communication	High transmission integrity
[21]	Permissioned blockchain + AES for video sharing	High traceability and privacy
[19]	Blockchain + SPIHT compression + AES	Secure cloud video storage
[26]	Multi-layered steganography + DNA coding	Multi-layer data security

IV. CONCLUSION

This paper presented an integrated framework of adaptive steganography, cryptographic encryption, and blockchain-based verification to ensure secure and verifiable video communication. Three complementary models were developed, namely StegoVision, Blockchain encryption, and robust decoy steganography, each focusing on different security objectives. Experimental evaluations showed that StegoVision achieves high imperceptibility, the decoy mechanism provides the best scalability and integrity, while the Blockchain mechanism provides strong resilience and deception against unauthorized extraction with a PSNR of 51.4 dB and SSIM of 0.991.

A comparison with several state-of-the-art methods confirms that the proposed models achieve better trade-offs between capacity, robustness, and verification with significantly lower computational cost. In general, these approaches assure end-to-end confidentiality, authenticity, and tamper-proof verification, making the framework practical for scalable secure video transmission, intelligent surveillance, and digital forensics applications.

REFERENCES

[1] M. ud Din *et al.*, "Randomized Frame Selection Based Video Steganography Method for Secure Embedding of Secret Data," *Journal of Computing & Biomedical Informatics*, vol. 8, no. 02, Mar. 2025.

[2] C. Han and T. Xue, "Adaptive network steganography using deep learning and multimedia video analysis for enhanced security and fidelity," *PLOS One*, vol. 20, no. 6, June 2025, Art. no. e0318795, https://doi.org/10.1371/journal.pone.0318795.

[3] S. Roy and J. Howlader, "Design and Analysis of a Novel Video Steganography Technique with Enhanced Resilience," *Journal of The Institution of Engineers (India): Series B*, Aug. 2025, https://doi.org/10.1007/s40031-025-01260-x.

[4] D. Darwis, Y. Fernando, A. R. Mehta, Wamiliana, and Setiawansyah, "Metadata-Based Video Steganography: Development of a New Model for Secure Information Embedding," *Engineering, Technology & Applied Science Research*, vol. 15, no. 5, pp. 27076–27088, Oct. 2025, https://doi.org/10.48084/etasr.11937.

[5] X. Mao *et al.*, "From Covert Hiding To Visual Editing: Robust Generative Video Steganography," in *Proceedings of the 32nd ACM International Conference on Multimedia*, Melbourne, Australia, July 2024, pp. 2757–2765, https://doi.org/10.1145/3664647.3681149.

[6] F. Zhang, Y. Dong, and H. Sun, "Research on Key Technologies of Image Steganography Based on Simultaneous Deception of Vision and Deep Learning Models," *Applied Sciences*, vol. 14, no. 22, Nov. 2024, Art. no. 10458, https://doi.org/10.3390/app142210458.

[7] N. A. Ali and R. J. Mstafa, "Optimizing Region of Interest Selection for Effective Embedding in Video Steganography Based on Genetic Algorithms," *Computer Systems Science and Engineering*, vol. 47, no. 2, pp. 1451–1469, 2023, https://doi.org/10.32604/csse.2023.039957.

[8] S. Rathor, V. Rawal, and K. Chhavi, "A Payload Scrambling Technique for Secure Image Steganography," in *Advances in Data and Information Sciences*, Singapore, 2022, pp. 573–582, https://doi.org/10.1007/978-981-16-5689-7_50.

[9] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, https://doi.org/10.1109/ACCESS.2021.3053998.

[10] S. Thakkar, K. Shivdikar, and C. Warty, "Video steganography using encrypted payload for satellite communication," in *2017 IEEE Aerospace Conference*, Big Sky, MT, USA, Mar. 2017, pp. 1–11, https://doi.org/10.1109/AERO.2017.7943978.

[11] W. Saqer and T. Barhoom, "Steganography and Hiding Data with Indicators-based LSB Using a Secret Key," *Engineering, Technology & Applied Science Research*, vol. 6, no. 3, pp. 1013–1017, June 2016, https://doi.org/10.48084/etasr.649.

[12] Z. Wang and A. C. Bovik, "Mean squared error: Love it or leave it? A new look at Signal Fidelity Measures," *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 98–117, Jan. 2009, https://doi.org/10.1109/MSP.2008.930649.

[13] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*: Steganography and Watermarking : Attacks and Countermeasures. Springer Science & Business Media, 2001.

[14] J. Ceron, C. Tinipuclla, P. Shiguihara, J. Ceron, C. Tinipuclla, and P. Shiguihara, "A Survey of Blockchain for Video Integrity," *Engineering Proceedings*, vol. 42, no. 1, Aug. 2023, https://doi.org/10.3390/engproc2023042004.

[15] A. Qureshi, D. M. Jiménez, A. Qureshi, and D. M. Jiménez, "Blockchain-Based Multimedia Content Protection: Review and Open Challenges," *Applied Sciences*, vol. 11, no. 1, Dec. 2020, https://doi.org/10.3390/app11010001.

[16] S. Ghimire, J. Y. Choi, and B. Lee, "Using Blockchain for Improved Video Integrity Verification," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 108–121, Jan. 2020, https://doi.org/10.1109/TMM.2019.2925961.

[17] A. Kanungo, A. Srivastava, S. Anklesaria, and P. Churi, "A systematic review on video encryption algorithms: A future research," *Journal of Autonomous Intelligence*, vol. 6, no. 2, Aug. 2023, Art. no. 665, https://doi.org/10.32629/jai.v6i2.665.

[18] Z. Zhao, Y. Liu, H. Zhao, and Y. Wang, "A Video Security Verification Method Based on Blockchain," in *2023 IEEE International Conference on Blockchain (Blockchain)*, Danzhou, China, Sept. 2023, pp. 105–108, https://doi.org/10.1109/Blockchain60715.2023.00026.

[19] D. K.G.Revathi, U. C. Devi, and S. G. H. Rose, "Security And Preservation For Video Data Transmission Using Blockchain Technology For Cloud Storage On Internet Of Things (Iot)," *NVEO – Natural Volatiles & Essential Oils Journal*, pp. 6003–6016, 2021.

[20] P. W. Khan, Y. Byun, P. W. Khan, and Y. Byun, "A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things," *Entropy*, vol. 22, no. 2, Feb. 2020, https://doi.org/10.3390/e22020175.

[21] A. Fitwi and Y. Chen, "Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, Athens, Greece, July 2021, pp. 1–8, https://doi.org/10.1109/ICCCN52240.2021.9522199.

[22] M. Awais *et al.*, "Deep learning based enhanced secure emergency video streaming approach by leveraging blockchain technology for Vehicular AdHoc 5G Networks," *Journal of Cloud Computing*, vol. 13, no. 1, Aug. 2024, Art. no. 130, https://doi.org/10.1186/s13677-024-00665-1.

[23] Z. Chen, F. Liu, D. Li, Y. Liu, X. Yang, and H. Zhu, "Video security in logistics monitoring systems: a blockchain based secure storage and access control scheme," *Cluster Computing*, vol. 27, no. 8, pp. 10245–10264, Nov. 2024, https://doi.org/10.1007/s10586-024-04667-1.

[24] M. M. Sabri, H. K. Hoommod, and K. A. Hussein, "Security surveillance systems based on deep learning and Blockchain techniques: a review," *Mustansiriyah Journal of Pure and Applied Sciences*, vol. 3, no. 3, pp. 173–193, June 2025, https://doi.org/10.47831/mjpas.v3i3.326.

[25] J. C. Kurniawan, A. Nugraha, A. I. Prayogo, and T. N. Fandy, "Improving Data Embedding Capacity in LSB Steganography Utilizing LSB2 and Zlib Compression," *Sinkron*, vol. 9, no. 1, pp. 174–181, Jan. 2024, https://doi.org/10.33395/sinkron.v9i1.13185.

[26] B. Kallapu *et al.*, "Multi-Layered Security Framework Combining Steganography and DNA Coding," *Systems*, vol. 13, no. 5, May 2025, Art. no. 341, https://doi.org/10.3390/systems13050341.

[27] "HMDB51." Kaggle, [Online]. Available: https://www.kaggle.com/datasets/easonlll/hmdb51.

AUTHORS PROFILE

S. G. Sumana is an Assistant Professor with an M.Sc. in Computer Science from Kuvempu University and is currently pursuing her Ph.D. at Dayananda Sagar University in the area of Video Security.

Dr. T. M. Rajesh is an Associate Professor and Chairperson in the Department of Computer Science & Engineering, with over ten years of research contributions in medical image processing, machine learning, and healthcare analytics. He has authored multiple journal and conference publications, book chapters, and holds Indian patents in Medical AI and Imaging.

Dr. S. G. Shaila is a Professor and Chairperson of CSE (Data Science) at DSU with a Ph.D. from NIT Trichy. She has 17 years of teaching and research experience, over 45 publications, and 13 patents. Her research areas include Data Mining, Information Retrieval, Image Processing, and Computational Neuroscience.