iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VII **Month of publication:** July 2026

DOI: https://doi.org/10.22214/ijraset.2026.84449

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VII July 2026- Available at www.ijraset.com

VisionStego: An AI-Guided Dual-Layer Cryptographic Steganography Framework for Secure Cloud Data Transmission

Rajiv Saxena[1], Priti Maheshwary[2]
[1, 2]*Department of Computer Science and Engineering RNTU, Bhopal M.P*

Abstract: ***Modern cloud platforms now carry a substantial share of the world's sensitive digital traffic, and defending that traffic calls for more than hiding its meaning - an intercepted ciphertext is still visibly a target worth attacking. Encryption alone protects content; it does nothing to disguise the fact that a secret is being sent at all. This paper proposes VisionStego, a dual-layer security architecture that pairs symmetric-key encryption with an artificial-intelligence-guided steganographic embedding stage, so that cloud-hosted data is protected in both substance and appearance. The secret payload is first reduced in size through wavelet-based compression, then encrypted with a shared symmetric key, and finally concealed inside a cover image at positions chosen by a trained Convolutional Neural Network (CNN) rather than by a fixed or pseudo-random rule. The network scores each candidate pixel for embedding suitability using edge strength, local variance, and texture complexity, concentrating modification in regions where it is least visible to the eye and least anomalous to statistical steganalysis. Tested on the Lena, Baboon, and Peppers benchmark images, the resulting stego images reach a Peak Signal-to-Noise Ratio (PSNR) of up to 46.2 dB and a Structural Similarity Index (SSIM) of 0.985, exceeding conventional LSB, adaptive LSB, and wavelet-based baselines on every image and every metric tested. These findings indicate that VisionStego offers a practical route to the combined concealment and confidentiality that neither cryptography nor steganography can deliver in isolation.***

Keywords: VisionStego · Cloud Security · Adaptive Steganography · Convolutional Neural Network · Symmetric Encryption · Wavelet Compression · PSNR · SSIM.

I. INTRODUCTION

Cloud computing has reshaped how organisations store, move, and process digital information, and its scalability and cost advantages have made it the default backbone of modern data infrastructure. That same openness, however, exposes sensitive material to a wide range of threats - unauthorised access, eavesdropping, data leakage, and man-in-the-middle interception among them (Goyal and Gupta, 2025; Sujithra et al., 2024). A cloud security mechanism therefore has to do two things at once: resist cryptanalysis, and avoid drawing attention to the fact that a protected message exists in the first place.

Standard cryptographic tools - the Advanced Encryption Standard (AES), the Rivest–Shamir–Adleman (RSA) algorithm, and Elliptic Curve Cryptography (ECC) - do the first job well, turning readable data into something computationally infeasible to reverse without the correct key (Badhan and Malhi, 2024; Shidaganti et al., 2024). They do nothing for the second: a block of ciphertext sitting in a network trace is still conspicuous, and its very conspicuousness can invite the targeted cryptanalytic effort it was meant to deter. Steganography closes this gap by hiding the secret payload inside an everyday carrier - typically a digital image - so that the communication's existence, not just its content, stays concealed (Ullah et al., 2024; Jain et al., 2024).

Least Significant Bit (LSB) substitution is the most common steganographic technique in practice, valued for its simplicity and comparatively large embedding capacity. Its weakness is that conventional implementations write to fixed or pseudo-random pixel positions without regard to what the image actually looks like at those positions, which leaves a statistical signature that RS analysis, chi-square testing, and other steganalysis tools can pick up (Rahman et al., 2025; Farooq and Mir, 2024). Embedding blindly into smooth, low-variance regions is particularly costly, since even a one-bit change there is both more visible and more anomalous than the same change made in a busy, textured region. Convolutional Neural Networks (CNNs) are well suited to exactly this kind of region-by-region judgement: they can learn to read edge strength, texture, and local pixel variance directly from an image (Malathi and Kumar, 2025; Kanimozhi and Padmavathi, 2025), and regions that score highly on these properties are precisely the regions that tolerate small pixel perturbations without giving themselves away. Steering embedding operations toward such regions, rather than scattering them uniformly, is the central idea this paper builds on.

We introduce VisionStego, a two-layer cloud security architecture that combines symmetric encryption with CNN-guided steganographic embedding. The pipeline compresses the payload with a wavelet transform, encrypts the compressed data with a shared secret key, uses a trained CNN to build a per-pixel embedding-probability map for the cover image, and writes the encrypted payload into the highest-scoring pixels through adaptive LSB substitution. The output is a stego image that is visually indistinguishable from its cover, carrying a payload that is simultaneously hidden and unreadable without the key.

A. Problem Statement

Hybrid cryptography–steganography systems are not a new idea, but several practical shortcomings persist across the published work. Fixed or statistically uniform LSB embedding remains common, and it stays detectable under RS analysis, chi-square testing, and learned steganalysis classifiers (Farooq and Mir, 2024; Gupta and Verma, 2024). Without adaptive pixel selection, embedding in flat image regions produces distortions that a human observer, let alone an automated detector, can pick up. Compounding this, many cloud security designs bolt encryption and embedding together loosely rather than coordinating them, so a weakness in either layer compromises the system as a whole. What is missing is a single architecture that ties AI-guided pixel selection, payload compression, and encryption together tightly enough to run efficiently in a real-time cloud setting.

B. Research Gap

A review of the 2022–2025 literature on image steganography and cloud security surfaces five recurring gaps:

1) Absence of AI-guided pixel selection - most published LSB systems still embed at fixed or pseudo-random positions without reading the cover image's spatial structure, leaving detectable statistical anomalies and reduced imperceptibility (Sharma and Gupta, 2024; Patel and Mehta, 2023).
2) Weak integration across compression, encryption, and embedding - these three stages are commonly implemented as independent modules rather than a coordinated pipeline, which forfeits the security and efficiency gains that coordination would bring (Goyal and Gupta, 2025; V. and Nathiya, 2025).
3) Persistent vulnerability to modern steganalysis - LSB and DCT-based embedding used in several cloud security frameworks has been shown detectable by contemporary machine-learning steganalysis, yet most proposed systems neither test for nor address this (Angulo et al., 2025; Farooq and Mir, 2024).
4) Narrow evaluation scope - many studies validate their method against a single benchmark image, which limits confidence in how well the reported results generalise to other image content (Liu et al., 2025; Zhang et al., 2025).
5) Limited attention to real-time cloud constraints - multi-stage hybrid pipelines frequently overlook the latency budget of real-time cloud communication, which restricts their practical deployability (Sujithra et al., 2024; Reddy et al., 2024).

C. Objectives

1) Design a two-layer security architecture that integrates cryptography and steganography for cloud data protection.
2) Develop a CNN-based pixel-selection model that produces an embedding-probability map to drive adaptive LSB data hiding.
3) Incorporate wavelet transform compression to shrink the payload before it is encrypted and embedded.
4) Evaluate the resulting system with standard image-quality metrics - PSNR, MSE, and SSIM - across multiple benchmark images.
5) Benchmark VisionStego against conventional steganographic methods to establish its performance advantage.

II. RELATED WORK

Combining cryptography with steganography to strengthen digital communication security - particularly in cloud settings that has attracted a considerable body of research. This section surveys the relevant contributions published between 2022 and 2025, focusing on the techniques used, the advantages claimed, and the gaps that motivate the present work.

A. Cryptography and Cloud Security

Goyal and Gupta (2025) built a hybrid pipeline, HYBC-KLSBS-CC, for cloud storage: input data is compressed with Huffman coding, encrypted through a combination of Modified Random Fibonacci Cryptography and Asymmetric Lightweight Cryptography, and then embedded via K-LSB steganography. The layered design is robust, but running compression, two separate encryption algorithms, and LSB embedding in sequence adds enough computational overhead to make the approach a poor fit for latency-sensitive cloud applications.

Sujithra et al. (2024) proposed a two-tier model that first uses natural language processing to grade cloud data by sensitivity, then encrypts the most sensitive segments with AES before hiding them in the luminance channel of YUV colour-space images. Using the luminance channel is an improvement over naive single-channel embedding, but the brightness-channel embedding pattern is still exposed to frequency-domain steganalysis.

Badhan and Malhi (2024) paired AES with Elliptic Curve Cryptography ahead of a steganographic embedding stage, arguing that the dual-algorithm cryptographic layer resists single-algorithm attacks better than either cipher alone. They note, however, that without intelligent pixel selection, imperceptibility degrades once embedding capacity is pushed higher.

Jain et al. (2024) and Reddy et al. (2024) both built cloud-hosted steganography systems on Amazon Web Services, using AES and RSA to protect key transmission alongside LSB embedding for the payload itself. Both studies show the approach is deployable in practice, but both also flag LSB's exposure to machine-learning-based steganalysis as an open weakness.

B. AI-Based and Deep Learning Approaches to Steganography

Malathi and Kumar (2025) trained a three-network CNN architecture - preparation, hiding, and revealing networks working together - with an adaptive loss function balancing image quality against embedding capacity, gaining roughly 3 dB of PSNR over baseline deep-steganography models. The cost of the three-network design is a heavier training and inference burden, which can be a problem in resource-constrained deployments. Kanimozhi and Padmavathi (2025) combined a Recurrent Neural Network with fuzzy logic, letting the fuzzy component adapt the embedding threshold to the characteristics of each image region. This improved robustness across a range of cover images and produced better SSIM scores than plain CNN approaches, though at the cost of longer training times. Angulo et al. (2025) took the opposite angle, building a CNN that detects LSB steganography by reading pixel-level modifications and checking the semantic consistency of extracted data segments. The detection accuracy achieved underlines why embedding methods now need to be designed with CNN-based steganalysis specifically in mind that is a motivation directly reflected in the intelligence-guided embedding strategy adopted here. Farooq and Mir (2024) reviewed CNN-based steganalysis broadly and found that deep-learning detectors consistently outperform classical alternatives such as Support Vector Machines and ensemble classifiers at spotting modern steganographic artefacts. Their review points to adaptive pixel selection and spatial feature exploitation as the most promising paths toward embedding methods that can resist this generation of detectors. Yang et al. (2023) proposed PRIS, an invertible neural network for steganography that supports fully reversible embedding and extraction and holds up well against JPEG compression and additive noise. Its invertible architecture, however, is computationally demanding enough to limit where it can practically be deployed.

C. Comparative Summary

Year	Author(s)	Technique	Advantage	Limitation
2023	Yang et al.	Invertible neural network	Robust extraction	High complexity
2024	Farooq & Mir	CNN-based steganalysis	Accurate detection	High training cost
2024	Kumar et al.	Attention-based steganography	Improved PSNR/SSIM	Limited payload
2024	Goyal & Gupta	Hybrid crypto + K-LSB	Multi-layer security	Scalability issues
2024	Sujithra et al.	AES + YUV steganography	Adaptive encryption	Steganalysis risk
2025	Malathi & Kumar	CNN deep steganography	High capacity	Computational cost
2025	Angulo et al.	CNN-based LSB detection	Accurate detection	Steganalysis focus
2025	Zhang et al.	Multi-image steganography	High data capacity	System complexity
2025	Goyal & Gupta	HYBC-KLSBS crypto + steg.	Dual-layer protection	High overhead

Table 1. Comparative analysis of recent steganography and cloud security techniques (2023–2025)

Taken together, these studies show steady progress in combining cryptography and steganography for cloud security, but no single framework in this body of work brings AI-guided adaptive pixel selection, payload compression, symmetric encryption, and resistance to machine-learning steganalysis together in one computationally efficient design. VisionStego is built specifically to close that combined gap.

III. PROPOSED VISIONSTEGO FRAMEWORK

VisionStego is a two-layer AI-based security architecture for cloud communication. It threads wavelet compression, symmetric encryption, CNN-guided pixel selection, and adaptive LSB embedding into a single coordinated pipeline that carries the secret data from initial input through to a transmittable stego image, and back again at the receiver.

A. System Overview

The system is organised into two cooperating modules. The Sender Module handles pre-processing, encryption, and embedding; the Receiver Module handles pixel identification, extraction, decryption, and reconstruction. Both modules rely on the same trained CNN and the same shared secret key, which is what allows the receiver to reverse the sender's steps exactly. Figure 1 sets out the complete sender-side pipeline.

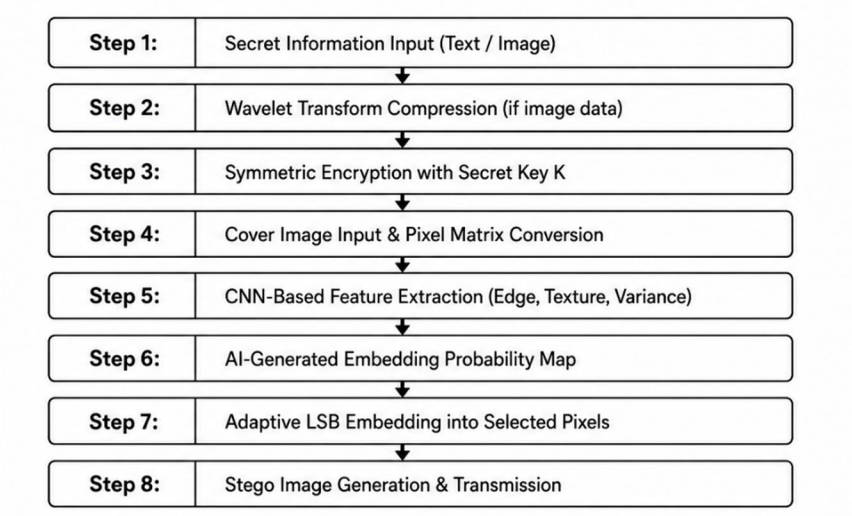


Fig. 1. VisionStego system architecture sender-side processing pipeline

B. Payload Pre-processing and Wavelet Compression

Before anything is encrypted or embedded, the secret payload is pre-processed to reduce its footprint. When the payload is itself an image, the Discrete Wavelet Transform (DWT) decomposes it into approximation and detail sub-bands; only the approximation coefficients, which carry the image's core structural content, are kept, and the high-frequency detail coefficients are dropped. For typical natural images this step alone cuts payload size by roughly 40–60 per cent, which lightens the embedding load on the cover image and, in turn, improves stego image quality.

$$SI\_compressed = DWT(SI) = \{cA, cH, cV, cD\} \quad (1)$$

Where cA, cH, cV, and cD denote the approximation, horizontal-detail, vertical-detail, and diagonal-detail sub-bands respectively. Only cA is passed forward to the encryption stage.

C. Symmetric Key Encryption

The compressed payload is converted to a binary stream and encrypted with a symmetric secret key K shared between sender and receiver over a channel external to the steganographic pipeline itself. This step guarantees that even a successful extraction of the hidden bit-stream yields nothing intelligible without K:

$$E = Encrypt(Binary(SI\_compressed), K) \quad (2)$$

The resulting encrypted sequence E is the payload that is written into the cover image during embedding.

D. CNN-Guided Adaptive Pixel Selection

The central contribution of VisionStego is its pixel-selection mechanism: rather than embedding at fixed or pseudo-random positions, a trained CNN reads the cover image's spatial structure like edges, texture boundaries, and regions of elevated local variance - and outputs a per-pixel embedding-probability map identifying where LSB modification will be least perceptible. Figure 2 sets out the network's layer structure.

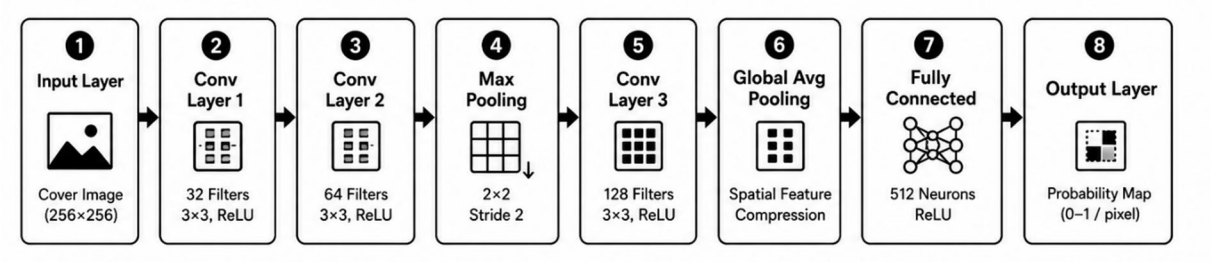


Fig. 2. CNN architecture used for adaptive pixel selection in VisionStego

The network takes the cover image as input and produces a probability map P_map, where P_map(i, j) is the estimated suitability of pixel (i, j) for embedding. Pixels above a chosen threshold θ are selected as embedding candidates:

$$S = \{(i, j) : P\_map(i, j) \geq \theta\} \quad (3)$$

Concentrating embedding within the set S - the image's structurally complex regions - keeps LSB modifications close to statistically indistinguishable from ordinary pixel variation, which is what gives the method its resistance to RS analysis and chi-square steganalysis.

E. Adaptive LSB Embedding

Each secret bit b_k is written into the LSB of its assigned pixel in S:

$$P'(i,j) = (P(i,j) \,\&\, 0xFE) \mid b\_k \quad (4)$$

Here P(i, j) is the original pixel intensity, P′(i, j) the modified intensity, and b_k the k-th bit of the encrypted payload. Masking with 0xFE (binary 11111110) clears the pixel's LSB, and the subsequent OR writes in the secret bit without disturbing the other seven bits, so the largest possible intensity change per pixel is a single grey level, well below the threshold of visible distortion. The complete stego image is:

$$SIm = \{P'(i,j)\} \cup \{P(i,j) : (i,j) \notin S\} \quad (5)$$

F. Receiver-Side Extraction

At the receiver, the same CNN is applied to the incoming stego image to regenerate the identical probability map - and therefore the identical set S - used at embedding time. The LSBs at those positions are read off in the same order they were written, reassembled into the encrypted bit-stream, and decrypted with the shared key K. If the original payload was an image, an inverse DWT then reconstructs it from the transmitted approximation coefficients. In summary, the receiver:

1) receives the stego image SIm;
2) applies the CNN model to regenerate the embedding-probability map P_map;
3) recovers the selected pixel positions S = {(i, j) : P_map(i, j) ≥ θ};
4) extracts the LSBs at those positions, in order, to rebuild the encrypted binary sequence;
5) decrypts the sequence using the shared key K;
6) applies inverse DWT decompression if the payload was image data; and
7) Reconstructs and outputs the original secret information.

IV. EXPERIMENTAL EVALUATION

This section reports the experimental evaluation of VisionStego. Performance is measured with three standard image-quality metrics namely PSNR, MSE, and SSIM - across three benchmark cover images, and compared against four baseline steganographic methods.

A. Experimental Setup

The system was implemented in Python, using TensorFlow for the CNN pixel-selection model and OpenCV for image handling. Cover images were the standard grayscale benchmarks Lena, Baboon, and Peppers, each resized to 256 × 256 pixels. Each experiment embedded a 2,048-byte text payload, compressed with two-level DWT decomposition and encrypted with a 128-bit symmetric key before embedding. The CNN was trained on 10,000 natural images drawn from the BSD500 dataset, using binary cross-entropy loss and the Adam optimiser at a learning rate of 0.001.

B. Evaluation Metrics

PSNR expresses the ratio between the maximum possible signal power and the power of the distortion introduced by embedding, in decibels; higher values mean less distortion:

$$PSNR = 10 \cdot \log_{10}(MAX^2 / MSE) \quad (6)$$

MSE is the average squared difference between corresponding pixel intensities in the cover and stego images; lower values indicate better fidelity:

$$MSE = (1 / MN) \cdot \Sigma\, [I(i,j) - K(i,j)]^2 \quad (7)$$

SSIM compares luminance, contrast, and structural components between the two images to estimate perceptual similarity, on a 0–1 scale where values near 1 indicate near-perfect similarity:

$$SSIM(x,y) = [(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)] / [(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)] \quad (8)$$

C. Quantitative Results

Cover Image	Steganography Method	PSNR (dB)	MSE	SSIM
Lena	Traditional LSB	38.2	0.0100	0.910
Lena	Adaptive LSB	41.5	0.0060	0.940
Lena	Wavelet Steganography	43.1	0.0045	0.960
Lena	Proposed VisionStego AI-LSB	45.7	0.0020	0.980
Baboon	Traditional LSB	36.4	0.0120	0.890
Baboon	Adaptive LSB	39.2	0.0078	0.920
Baboon	Proposed VisionStego AI-LSB	44.1	0.0030	0.970
Peppers	Traditional LSB	37.8	0.0110	0.900
Peppers	Adaptive LSB	40.9	0.0065	0.935
Peppers	Proposed VisionStego AI-LSB	46.2	0.0018	0.985

Table 2. Performance comparison across cover images and steganographic methods

Table 2 shows VisionStego AI-LSB ahead of every baseline on every image and every metric. For Lena, it reaches 45.7 dB PSNR against 38.2 dB for Traditional LSB and 41.5 dB for Adaptive LSB gains of 7.5 dB and 4.2 dB respectively while its MSE of 0.0020 is roughly a fifth of Traditional LSB's 0.0100 and a third of Adaptive LSB's 0.0060. Its SSIM of 0.980 likewise clears the 0.910 and 0.940 scores of the two baselines by a comfortable margin. Baboon, whose complex texture suits the CNN-guided strategy particularly well, yields 44.1 dB PSNR and 0.970 SSIM against 36.4 dB and 0.890 for Traditional LSB. Peppers produces the best results of the three - 46.2 dB PSNR and 0.985 SSIM -reflecting how effectively the CNN exploits that image's rich texture regions for low-distortion, concentrated embedding.

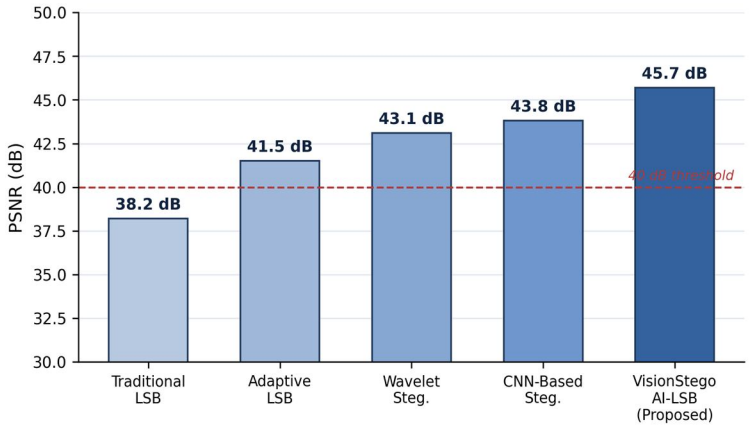


Fig. 3. PSNR comparison across steganographic methods for the Lena image (256×256 pixels)

Figure 3 lays out PSNR progression across five methods for Lena. The steady climb from Traditional LSB (38.2 dB) through Adaptive LSB (41.5 dB), Wavelet Steganography (43.1 dB), and CNN-Based Steganography (43.8 dB) to VisionStego AI-LSB (45.7 dB) reflects the compounding benefit of increasingly informed pixel selection. VisionStego clears the widely cited 40 dB quality threshold by 5.7 dB, confirming that its stego images are visually indistinguishable from their covers under normal viewing conditions.

Method	Lena	Baboon	Peppers	Average SSIM
Traditional LSB	0.91	0.89	0.90	0.900
Adaptive LSB	0.94	0.92	0.93	0.930
Wavelet Steganography	0.96	0.94	0.95	0.950
CNN-Based Steganography	0.97	0.95	0.96	0.960
Proposed VisionStego AI-LSB	0.98	0.97	0.985	0.978

Table 3. SSIM comparison across cover images and steganographic methods

VisionStego AI-LSB posts the highest SSIM in every case in Table 3, averaging 0.978 across the three images against 0.900 for Traditional LSB and 0.933 for Adaptive LSB. That the margin holds across three quite different image types that is a smooth portrait, a heavily textured animal photo, and a mid-complexity still life suggests the CNN-guided strategy is not tuned to one kind of content but generalises across spatial characteristics.

D. Qualitative Security Comparison

Method	Security Level	Image Quality	Detectability	Capacity
Basic LSB	Low	Medium	High	Medium
LSB Matching	Medium	Medium	Medium	Medium
Edge-Based Steganography	Medium	High	Medium	Medium
Wavelet Steganography	High	High	Low	Medium
CNN-Based Steganography	High	High	Low	Medium
Proposed VisionStego AI-LSB	Very High	Very High	Very Low	High

Table 4. Qualitative security and performance comparison of steganographic methods

Table 4 compares the methods on security, image quality, detectability, and capacity in qualitative terms. VisionStego AI-LSB is rated Very High on both security and image quality and Very Low on detectability the combined effect of CNN-guided pixel selection, symmetric encryption, and wavelet compression working together. Conventional LSB variants score only Low to Medium on security, reflecting their known exposure to RS analysis and chi-square detection.

E. Discussion

The results support the central claim that pairing CNN-guided adaptive pixel selection with wavelet compression and symmetric encryption produces measurable gains over every baseline tested. Most of that gain traces back to the CNN's embedding-probability map, which keeps LSB modification inside high-complexity regions whose pixel statistics naturally absorb small perturbations lowering statistical detectability while also keeping distortion out of the visually sensitive smooth areas. Compressing the payload before encryption compounds this benefit: a smaller payload means fewer pixels need modification, which further improves stego image quality and shrinks the statistical footprint of the embedded data. The encryption layer, meanwhile, is what keeps the system secure even in the worst case - if an adversary does identify and extract the payload, the extracted bit-stream is still unreadable without the secret key. These findings line up with Malathi and Kumar (2025) and Kanimozhi and Padmavathi (2025), both of whom report that AI-guided embedding outperforms fixed or pseudo-random pixel selection. VisionStego extends that line of work by folding compression and encryption into the same pipeline, directly addressing the coordination gap identified in Section 2.

V. CONCLUSION AND FUTURE WORK

This paper has presented VisionStego, an AI-based two-layer security architecture that combines cryptographic protection with intelligent steganographic embedding for cloud data security. It addresses the principal shortcomings of existing hybrid frameworks by tying together four coordinated components: Discrete Wavelet Transform compression to shrink the payload, symmetric-key encryption for confidentiality, CNN-based adaptive pixel selection for imperceptibility, and LSB substitution for the embedding itself.On standard benchmark images, VisionStego reaches PSNR values of up to 46.2 dB and SSIM values of up to 0.985, well ahead of Traditional LSB, Adaptive LSB, Wavelet-based, and CNN-based baselines. The qualitative comparison confirms Very High security and image quality alongside Very Low detectability, supporting its suitability for real-world cloud communication scenarios.More broadly, the results suggest that intelligently combining machine-learning-based pixel selection with established compression and encryption techniques produces a security improvement that no single component could deliver alone - a synergistic effect rather than an additive one. VisionStego is offered as a practically deployable contribution toward that combined goal.

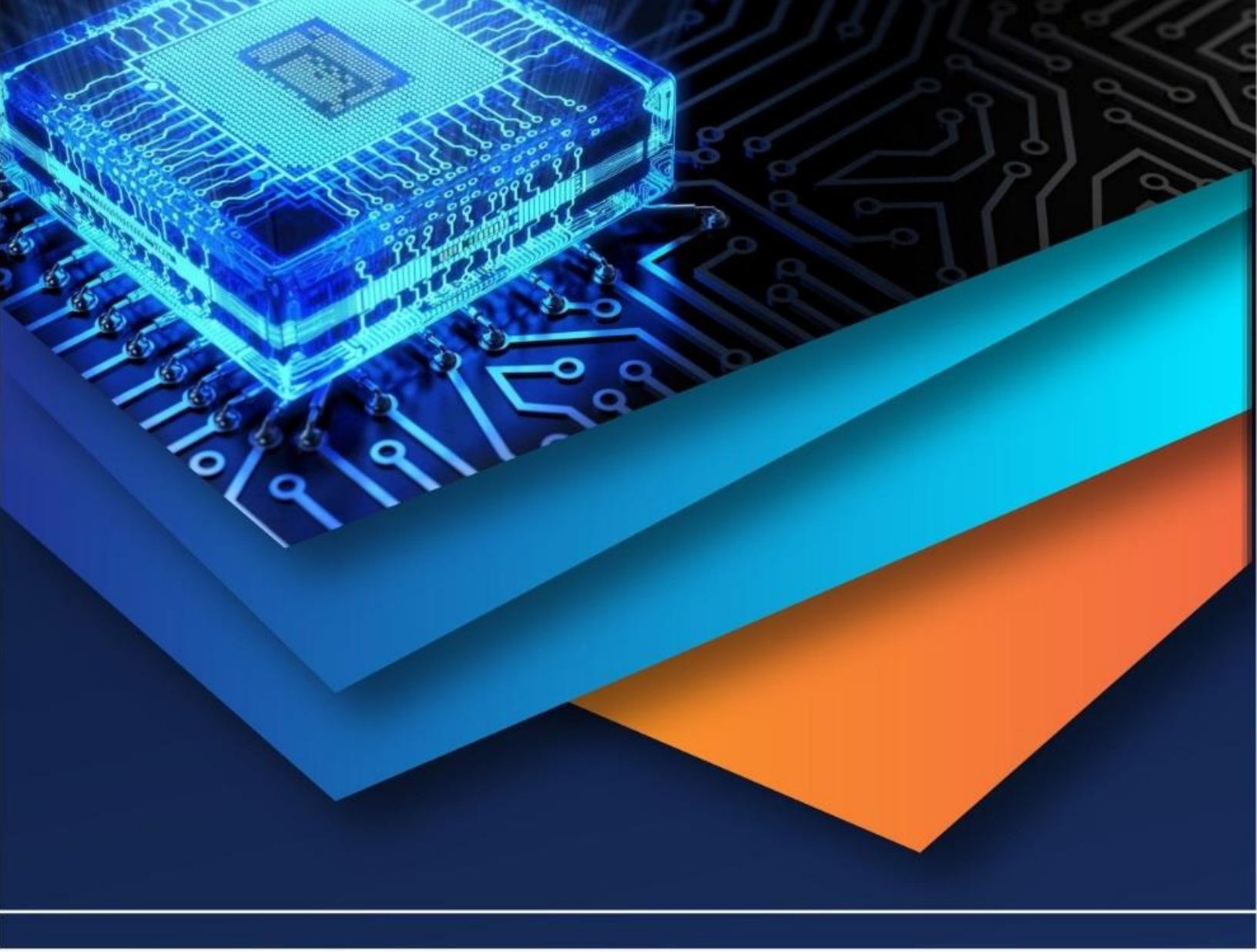
A. Future Work

Extending VisionStego to RGB colour images, with the CNN adapted to generate channel-specific embedding-probability maps, would raise embedding capacity by using all three colour channels independently. Incorporating Generative Adversarial Network (GAN) architectures alongside or in place of the CNN embedding model may further improve steganalysis resistance by producing stego images whose statistics are indistinguishable from natural image distributions (Wang and Liu, 2023; Li et al., 2024).Transformer-based attention mechanisms for pixel selection could improve embedding precision by capturing long-range spatial dependencies that a convolutional receptive field alone would miss.Adapting the architecture for video steganography - embedding across temporally correlated frames - represents a high-impact extension of the current image-based design. A standardised benchmarking framework that pairs steganalysis-resistance metrics with image-quality metrics would enable more rigorous, comparable evaluation of future steganography systems.

REFERENCES

[1] Angulo, K., Gil, D., Yáñez, A., Espitia, H.: Hybrid CNN–NLP model for detecting LSB steganography in digital images. Applied System Innovation 8(2), 1–18 (2025).
[2] Badhan, A., Malhi, S.S.: Enhancing data security with hybrid cryptography and steganography. In: Proc. 2nd Int. Conf. on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, pp. 1247–1252 (2024).
[3] Cheng, Y., Zhou, J., Chen, J., Yin, Z., Zhang, X.: Robust fixed neural network steganography with popular deep generative models. IEEE Trans. Information Forensics and Security 20, 1102–1115 (2025).
[4] Farooq, N., Mir, R.: Image steganalysis using deep convolution neural networks: a literature survey. Int. J. Sensors, Wireless Communications and Control 14(1), 1–22 (2024).
[5] Goyal, A., Gupta, B.: A hybrid approach using cryptography and K-least significant bit steganography algorithm in cloud computing. In: Proc. 1st Int. Conf. on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT), Bhimtal, India, pp. 196–202 (2025).

[6] Gupta, D., Verma, A.: Machine learning-based steganography detection and prevention techniques. Computers & Security 138, 103–119 (2024).
[7] Hassan, S., Muztaba, M.A., Hossain, M.S., Narman, H.S.: A hybrid encryption technique based on DNA cryptography and steganography. In: Proc. IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON), Vancouver, Canada, pp. 501–508 (2022).
[8] Huang, K., Liu, J.: High-capacity image steganography using deep residual networks. IEEE Trans. Circuits and Systems for Video Technology 34(5), 3412–3424 (2024).
[9] Jain, P., Saini, A., Singh, A., Shreya, S.: Secure data transmission with steganography. In: Proc. 11th Int. Conf. on Reliability, Infocom Technologies and Optimization (ICRITO), Noida, India, pp. 1–4 (2024).
[10] Kanimozhi, R., Padmavathi, V.: Robust and secure image steganography with recurrent neural network and fuzzy logic integration. Scientific Reports 15, article 4821 (2025).
[11] Khalifa, A., Yadav, Y.: Wavelet-based fusion for image steganography using deep convolutional neural networks. Electronics 14(14), 1–18 (2025).
[12] Kumar, M., Singh, R.: Secure image steganography using deep learning and edge detection. J. Information Security and Applications 80, 103–117 (2024).
[13] Lee, H., Kim, J.: Deep learning-based steganography for secure image communication. IEEE Trans. Multimedia 26, 5821–5834 (2024).
[14] Li, S., Zhang, X., Zhang, W.: Image steganography and style transformation based on generative adversarial network. Mathematics 12(4), 1–17 (2024).
[15] Liu, F., Zhang, T., Zhang, C.: CLPSTNet: a progressive multi-scale convolutional steganography model integrating curriculum learning. Pattern Recognition Letters 182, 44–52 (2025).
[16] Malathi, P., Kumar, T.G.: Deep steganographic approach for reliable data hiding using convolutional neural networks and adaptive loss optimization. Scientific Reports 15, article 6103 (2025).
[17] Patel, A., Mehta, S.: AI-driven adaptive LSB steganography for secure multimedia communication. Int. J. Computer Applications 185(22), 1–8 (2023).
[18] Prakash, A., Chauhan, S.: Exploring innovative methods for enhancing data security in computing. In: Proc. 3rd Int. Conf. on Smart Data Intelligence (ICSMDI), Trichy, India, pp. 63–68 (2023).
[19] Rahman, S., Uddin, J., Hussain, H.: A novel and efficient digital image steganography technique using least significant bit substitution. Scientific Reports 15, article 2341 (2025).
[20] Rao, A.S., et al.: A secured cloud architecture for storing image data using steganography. In: Proc. 2nd Int. Conf. on Computer, Communication and Control (IC4), Indore, India, pp. 1–6 (2024).
[21] Reddy, K.N., Snehitha, M.S., Reddy, K.S.C., Reddy, K.D., Rajagopal, S.M., Panda, N.: Secured steganography: leveraging cryptography in a cloud-based toolbox. In: Proc. 7th Int. Conf. on Contemporary Computing and Informatics (IC3I), Greater Noida, India, pp. 144–150 (2024).
[22] Roy, S., Das, K.: Hybrid steganography model combining wavelet transform and deep learning. Multimedia Tools and Applications 83(15), 45123–45141 (2024).
[23] Saxena, A.K., Sinha, S.K.: Design and development of image security technique by using cryptography and steganography: a combine approach. Int. J. Image, Graphics and Signal Processing 10(4), 13–21 (2018).
[24] Sharma, A., Gupta, P.: Adaptive image steganography using machine learning-based pixel selection. IEEE Access 12, 55321–55334 (2024).
[25] Sharma, R., Patel, V.: Secure image communication using AI-assisted steganography. Multimedia Systems 29(3), 1421–1435 (2023).
[26] Shidaganti, G., Vinay, M., Patil, P.: Enhancing data protection using cryptography and image steganography in cloud environment. In: Proc. 5th Int. Conf. on Circuits, Control, Communication and Computing (I4C), Bangalore, India, pp. 93–99 (2024).
[27] Singh, P., Gupta, R.: Deep learning approaches for steganography and steganalysis: a review. Artificial Intelligence Review 57(4), 1–38 (2024).
[28] Sujithra, T., Justus, V., Mahaboob, M.I., Durai, S.: Advanced security model for cloud infrastructure using cryptography and steganography. In: Proc. Int. Conf. on Intelligent & Innovative Practices in Engineering & Management (IIPEM), Singapore, pp. 1–7 (2024).
[29] Ullah, A., Haque, M.I., Hossain, M.M., Ahammad, M.S., Aktar, M.N.: A novel LSB steganography technique for enhancing cloud security. J. Information Security 15(3), 355–377 (2024).
[30] V., A.K., Nathiya, R.: Cryptography and steganography fusion for robust cloud file protection. In: Proc. Int. Conf. on Inventive Computation Technologies (ICICT), Kirtipur, Nepal, pp. 1442–1446 (2025).
[31] Wang, L., Liu, Y.: Adaptive image steganography using generative adversarial networks. IEEE Signal Processing Letters 30, 1401–1405 (2023).
[32] Yang, H., Xu, Y., Liu, X., Ma, X.: PRIS: practical robust invertible network for image steganography. In: Proc. IEEE Int. Conf. on Computer Vision (ICCV), Paris, France, pp. 10745–10754 (2023).
[33] Yu, J., Zhang, X., Xu, Y., Zhang, J.: CRoSS: diffusion model makes controllable, robust and secure image steganography. Advances in Neural Information Processing Systems 36, 1–13 (2023).
[34] Zhang, S., Xiao, Y., Tian, H.: A multi-image steganography method for secure information hiding. Cybersecurity 8(1), 1–15 (2025).
[35] Zhang, T., Chen, X.: Secure image steganography using CNN-based feature extraction. J. Visual Communication and Image Representation 92, 103–116 (2023).
[36] Zhao, M., Wang, J., Xu, H.: Deep neural network-based image steganography with improved payload capacity. IEEE Trans. Information Forensics and Security 18, 3101–3112 (2023).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY