LIGHTWEIGHT CNN AND LSB STEGANOGRAPHY FOR SECURE METADATA EMBEDDING IN UAV COMMUNICATION

Prateeksha Gaur, Amit Verma, Manish Kumar Sharma

Dr. K. N. Modi University, Newai, Rajasthan

ABSTRACT

This paper presents a lightweight framework for secure metadata embedding in unmanned aerial vehicle (UAV) communication. An on-board convolutional neural network (CNN) classifier generates image predictions, which are directly embedded into the corresponding image using Least Significant Bit (LSB) steganography. This approach eliminates the need for separate metadata channels, thereby enhancing confidentiality and improving bandwidth efficiency. The proposed framework is validated on a subset of the CIFAR-10 benchmark dataset as well as the UAV-specific VisDrone2019-DET dataset. The predicted class labels and confidence scores are embedded within the images and can be extracted without error. The methodology includes CNN model design, LSB embedding and extraction, and evaluation across classification accuracy and image quality metrics. The evaluation employs accuracy, Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM). Experiments show classification accuracies of 33.0% on CIFAR- 10 and 48.36% on VisDrone. Visual quality is preserved, with PSNR values above 63.0 dB and SSIM scores near 1.0.The results confirm that the proposed method achieves secure metadata embedding with negligible visual distortion, offering an efficient and lightweight solution for UAV communication

KEYWORDS

UAV Communication, Steganography, Lightweight CNN, LSB Embedding, Secure Metadata Transmission

1. INTRODUCTION

This The Unmanned Aerial Vehicles are integral to modern applications. As an example, surveillance, disaster response, reconnaissance, precision agriculture, and environmental monitoring use them. The systems often operate in dynamic, resource constrained environments; they require secure, good mechanisms for communication. One important challenge is embedding contextual metadata into transmitted imagery. This metadata includes classification labels and confidence scores - it is important to avoid an increase in bandwidth use. It is also important to avoid significant distortions.

Traditional approaches to metadata transmission rely on separate communication channels. This probably introduces overhead, increases transmission delay, and increases the risk of interception or packet loss. Steganography offers a good solution - it invisibly embeds metadata into the captured images. There is integration of information within a single data stream. Among the various approaches, Least Significant Bit (LSB) steganography is computationally simple and easy to implement - this approach is suitable for UAV platforms because those platforms have limited power plus hardware resources [1].

DOI:10.5121/ijci.2026.150121

The study of steganography occurs across spatial and trans- form domains. Johnson but also Jajodia [2] explored basic principles of LSB methods; they showed their use for simple data hiding. Cheddad et al. [3] gave a complete survey of image steganography techniques. That survey showed trade offs among imperceptibility, capacity along with robustness. Spatial-domain methods are fast to compute, but they are more open to compression and statistical steganalysis. Deep learning helps make steganography more robust. Hayes besides Danezis [4] presented adversarial training methods. The methods create steganographic images that resist detection. Small convolu- tional neural networks (CNNs), like MobileNets [5], allow fast computation on embedded platforms. This is important for UAV deployments.

The CIFAR-10 dataset [6] acts as a benchmark for image classification tasks - it is widely used in studies that evaluate lightweight CNN performance. Wang et al. [5] introduced the Structural Similarity Index (SSIM) for image quality evaluation. SSIM, with Peak Signal-to-Noise Ratio (PSNR), remains a standard metric for evaluation of perceptual simi- larity between cover and stego images. The present methods meet problems with use in UAV situations. Transform-domain methods are firm, but they have a high computation cost. Such methods are not practical for real time work on embedded UAV hardware.

By contrast, traditional LSB methods are good for use, but they are open to noise, compression along with dis- covery by advanced steganalysis tools. Little study shows on board CNN-based classification with real time steganographic placing. This would make UAV talk simpler.

Contributions: This paper makes the following contributions:

- The process integrates convolutional neural networks (CNNs) with Least Significant Bit (LSB) steganography in a unified pipeline. A lightweight CNN performs on- board image classification, and the classification results, including the label and confidence score, are embedded into the image using LSB steganography.

- A compact CNN architecture is trained on the CIFAR- 10 and VsDrone-19 dataset for demonstration, showing the feasibility of the method even on resource-constrained hardware platforms [7].

- The proposed method is validated using standard metrics, achieving high imperceptibility with successful message recovery. The Peak Signal-to-Noise Ratio (PSNR) measures approximately 63 dB, and the Structural Similarity Index (SSIM) is about 1.0.

- A practical framework for UAV communication is established, where low-cost and secure transmission is critically important.

- Future work will enhance robustness by incorporating error-correcting codes and adopting transform-domain embedding techniques.

Reference	Contribution	Limitation	Our Proposed Approach
Johnson & Jajodia [1]	Introduced principles of LSB steganography	Vulnerable to compression and detection	Builds on LSB for simplicity and low computational cost in UAVs
Cheddad et al. [2]	Comprehensive survey of steganography methods	Highlighted trade-offs between imperceptibility and robustness	Prioritizes imperceptibility and low overhead for UAV communication
Hayes & Danezis [3]	Proposed adversarial training for robust steganography	Computationally expensive	Focuses on lightweight LSB embedding without adversarial overhead
Howard et al. [4]	Developed MobileNets for lightweight CNN inference	Accuracy trade-offs compared to deeper models	Demonstrates feasibility using a small CNN, extendable to MobileNet
Krizhevsky [5]	Released CIFAR-10 dataset for benchmarking classification	Limited image resolution (32×32)	Uses CIFAR-10 subset for proof-of-concept evaluation
Wang et al. [6]	Introduced SSIM metric for image quality assessment	Sensitive to structural distortions	Employs SSIM and PSNR for quantitative evaluation of cover vs. stego images
Valikhanli & Abdullayeva [7]	Secured UAV flight data using lightweight crypto + steganography	Moderate robustness, extra crypto overhead	Integrates CNN-based metadata embedding with minimal cost for UAV imagery
Kanimozhi & Padmavathi [8]	RNN + fuzzy logic for robust image steganography	Medium computational cost, not UAV-specific	Provides UAV-specific lightweight solution with simpler LSB-based embedding
Devi et al. [9]	Hybrid DWT-SVD watermarking for UAV image transmission	High computational cost	opts for LSB embedding for efficiency on UAV platforms
Kareem et al. [10]	Drone video steganography demonstration	Focused on video, limited to specific scenarios	Extends to still images with CNN metadata for lightweight UAV deployment

TABLE 1. Summary of Literature Review with Recent Advances

2. FORMAT RELATED

Research about steganography and secure image communication has developed significantly over the past two decades, producing several methods with different imperceptibility, robustness, and computational complexity properties. Early studies centered on spatial domain methods, such as Least Significant Bit (LSB) substitution [4]. This method provided simplicity and high embedding capacity, but it had limited resilience against compression and detection. Nevertheless, such approaches remain widely used in scenarios where minimizing computational cost is essential. To improve robustness, researchers explored transform domain techniques, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) embedding

[2]. The methods show good resistance to compression and filtering operations. They suit applications that need higher resilience. They cause higher computational overhead. This is not always practical for UAVs or edge devices with limited energy and precession. The incorporation of deep learning is recent for both steganography and steganalysis. Hayes but also Danezis [3] showed that adversarial training can produce stegano- graphic images that resist detection by conventional statistical models. Subsequent research built on this by using convolu- tional neural networks plus generative adversarial networks (GANs) to get more imperceptibility and robustness. But such models require much computation but also are not practical for real time UAV applications. In parallel, there is much progress in designing lightweight CNN architectures. The are good for mobile and embedded environments. Howard et al. [4] proposed MobileNets, which use depthwise separable convolutions to reduce parameter count as well as computational cost. Other compact architectures, such as SqueezeNet besides ShuffleNet, show high efficiency with some accuracy trade-offs. The developments are relevant for UAVs, because they require models that operate on board without reliance on cloud processing. The CIFAR-10 dataset [5] is a standard benchmark for image classification. Many researchers use the datasets to check lightweight CNNs for edge applications, so models achieve good accuracy with limited resources. At the same time, image quality assessment metrics, such as PSNR but also SSIM [6], are important for judging how embedding processes affect image clarity. Despite this progress, a research gap is visible where UAV- based image processing, lightweight CNN classification, and real-time steganographic embedding meet. Most studies either improve steganography for protection against steganalysis or improve CNNs for classification accuracy in edge situations. Few works really combine the two to allow secure, low over- head metadata transfer in UAV systems. This paper addresses this gap by showing a single framework which combines lightweight CNN inference with LSB embedding, checked by PSNR, SSIM along with successful message retrieval.

3. System Overview

The proposed framework is designed to operate entirely on- board a UAV platform. The workflow can be divided into three stages:

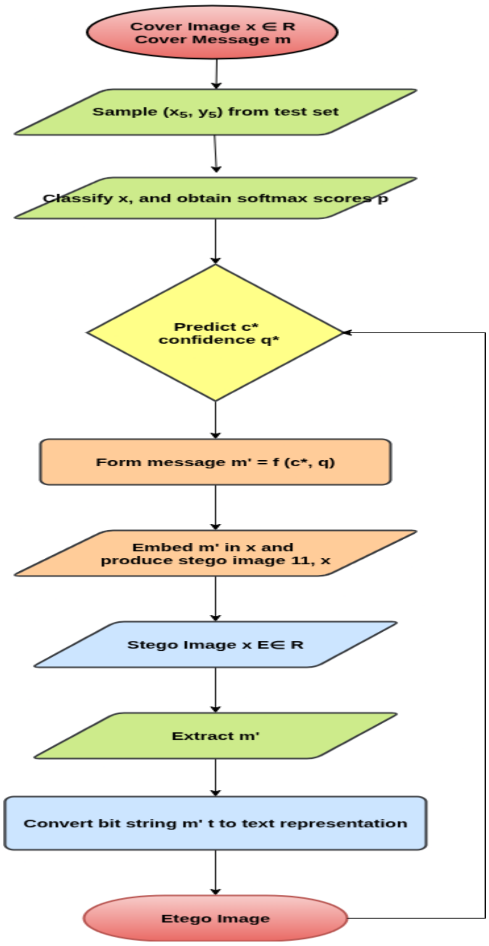
1. **Image Capture and Classification:** UAVs capture im- ages via their sensors. A lightweight CNN performs local inference to classify the scene (e.g., vehicle, pedes- trian, or vegetation).
2. **Metadata Embedding:** The classification result (label and confidence score) is converted into binary format and embedded into the captured image using LSB steganography.
3. **Transmission and Recovery:** The modified image is transmitted over the UAV communication channel. At the receiver side, the metadata is extracted by reversing the LSB embedding process while ensuring the percep- tual quality of the image remains intact.

This unified design eliminates the need for transmitting metadata separately,
There by reducing bandwidth requirements and mitigating risks of interception.

4. Methodology

The proposed framework combines lightweight convolu- tional neural network (CNN) classification with Least Signif- icant Bit (LSB) steganography to achieve secure and efficient metadata transmission in UAVs. The overall process is divided into four main stages: dataset preparation, CNN-based classi- fication, message embedding, and evaluation.

4.1. Flowchart of the Proposed Framework


Cover Image x ∈ R
Cover Message m
Sample (x_5, y_5) from test set
Classify x, and obtain softmax scores p
Predict c*
confidence q*
Form message m' = f (c*, q)
Embed m' in x and
produce stego image 11, x
Stego Image x E∈ R
Extract m'
Convert bit string m' t to text representation
Etego Image

4.2. Dataset and Pre-processing

The proposed framework is validated using two datasets: CIFAR-10 and VisDrone2019-DET. CIFAR-10 Dataset: The CIFAR-10 dataset contains 60,000 color images, cat- egorized into 10 classes. Each image has a resolution of 32 × 32 pixels. For this study, a reduced subset of 2,000 training images and 200 testing images is used. This reduction lowers computational requirements and enables deployment on UAV-like platforms with limited resources. The images are preserved at their original resolution and converted into tensor format for CNN training. Pixel values are normalized to the [0, 1] range, which facilitates faster convergence during training. VisDrone2019-DET Dataset: The VisDrone2019-DET dataset [6] includes over 10,000 aerial images. The pictures come from UAVs in urban and suburban areas - it has 12 object categories, such as pedestrian, car, bus, truck along with tricycle. The original images are large, up to 2000 × 1500 pixels. For consistency with the CNN input dimension and reduced computer needs, researchers resize them to 32 × 32 pixels. Annotation files in .txt format provide object bounding boxes plus class IDs. From the files, the primary object class becomes the image label.

3.3. CNN-Based Image Classification

A compact CNN architecture is employed to classify cap- tured UAV images into ten predefined categories. The model consists of two convolutional layers, pooling layers, and fully connected layers. The softmax output provides both class label and confidence score, which are later embedded into the image.

5. Algorithms And Mathematical Analysis

This section provides pseudocode for the unified pipeline and mathematical analysis of embedding capacity, distortion, and message recovery.

Symbol	Description
$I \in \{0, . . . , 255\}^{H\times W \times 3}$	Cover image of size $H\times W$ with 3 color channels
$N = 3HW$	Total number of bytes in flattened RGB image
m	ASCII message to be embedded
$\|m\|$	Length of the message in characters
$L = 8\|m\| + 8$	Total bit-length after adding null terminator
$b_0, b_1, . . . , b_{L-1}$	Sequence of message bits
$I[i]$	i-th byte of flattened image, $0 \leq i < N$
$\mathrm{LSB}(x) = x \bmod 2$	Least Significant Bit operator

5.1. Algorithm 1: Unified Pipeline

Algorithm 1 On-board Classification and LSB Embedding Pipeline

```
Require: Cover image $I$, classification model $M$
Ensure: Stego image $S$
$pred\_probs \leftarrow softmax(M(I))$
$label \leftarrow \arg\max(pred\_probs)$
$conf \leftarrow 100 \times \max(pred\_probs)$
$m\_str \leftarrow$ format("Class:{label};Conf:{conf}")
$bits \leftarrow TEXT\_TO\_BITS(m\_str)$ + null terminator
if $len(bits) > N$ then
        error: message too long
end if
$S \leftarrow EMBED\_LSB(I, bits)$
. return$S$
```

5.2. Algorithm 2: EMBED_LSB

Algorithm 2 LSB Embedding Procedure

```
Require: Cover image $I$, message bits $bits$
Ensure: Stego image $S$
$flat \leftarrow flatten(I)$
for $k = 0$ to $len(bits) - 1$ do
    $flat[k] \leftarrow (flat[k]$ & $0xFE) \mid bits[k]$
end for
$S \leftarrow reshape(flat, I.shape)$
return $S$
```

Time complexity: $O(L)$, Space complexity: $O(N)$.

5.3. Algorithm 3: EXTRACT_LSB

Algorithm 3 LSB Extraction Procedure

```
Require: Stego image $S$
Ensure: Extracted message string
$flat \leftarrow flatten(S)$
$bits \leftarrow [\,]$
for $i = 0$ to $N - 1$ do
    append $(flat[i]$ & $1)$ to $bits$
    if $i \bmod 8 = 7$ and last 8 bits = null terminator then
        break
    end if
end for
return $BITS\_TO\_TEXT(bits)$
```

Worst-case complexity: $O(N)$.

5.4. Embedding Capacity

Total embeddable bits:

$$C_{\text{bits}} = N. \qquad (1)$$

Maximum message bytes:

$$C_{\text{bytes}} = \frac{N}{8} - 1. \qquad (2)$$

5.5. Distortion: MSE and PSNR

Let S be the stego image and $d_i = S[i] - I[i] \in \{-1, 0, 1\}$.
If C is the number of modified bytes:

$$\text{MSE} = C / N \qquad (3)$$

$$\text{PSNR} = 10 \log_{10} \; 255^2 / \text{MSE} \qquad (4)$$

5.6. Message Recovery Probability

Assume each embedded bit is flipped with probability p.
The probability that all L bits are received correctly:

$$P_{\text{all}} = (1 - p)^L. \tag{5}$$

5.7. Reliability with Error-Correcting Codes (ECC)

For block length n and correction capability t:

$$P_{\{block\}} = \sum_{i=0}^{m} \binom{n}{i} p^{i} (1-p)^{n-i} \tag{6}$$

For B blocks;

$$P_{\text{all}} = (\,P_{\text{block}}\,)^B \tag{7}$$

5.8. Security and Mitigations

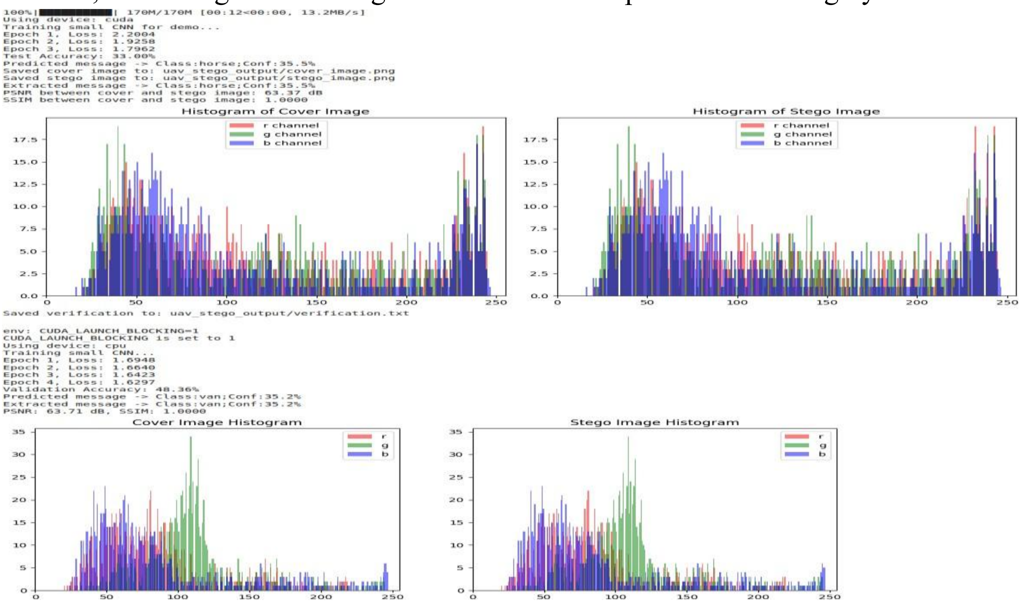
1. Adaptive embedding in high-texture regions to mask statistical artifacts.
2. Minimal payload embedding (only class label and confi- dence).
3. ECC with interleaving to increase robustness.
4. For compression-prone channels, extension to transform- domain methods.

6. Experimental Results

This section presents the results of the proposed frame- work, focusing on classification accuracy, message embedding, image quality metrics, and message extraction success. The experiments were conducted on both the CIFAR-10 subset and the VisDrone2019-DET dataset. A particular emphasis was placed on evaluating feasibility not only on a standard benchmark dataset, but also on UAV-specific aerial imagery.

6.1. Classification Results

1. The lightweight CNN was trained for three epochs on the CIFAR-10 subset. For training, 2, 000 images were used, and the model was evaluated on 200 test images. An overall test accuracy of 33.0% was achieved. This modest performance is due to the limited dataset size and short training time, but it demonstrates the feasibility of running CNN inference on small UAV platforms. With full-dataset training and improved architectures, accuracy can be significantly increased.
2. On the VisDrone2019-DET dataset, the same architecture achieved a validation accuracy of 48.36%, indicating a better alignment with UAV-captured aerial imagery.



```
100%|██████████| 170M/170M [00:12<00:00, 13.2MB/s]
Using device: cuda
Training small CNN for demo...
Epoch 1, Loss: 2.2004
Epoch 2, Loss: 1.9258
Epoch 3, Loss: 1.7962
Test Accuracy: 33.00%
Predicted message -> Class:horse;Conf:35.5%
Saved cover image to: uav_stego_output/cover_image.png
Saved stego image to: uav_stego_output/stego_image.png
Extracted message -> Class:horse;Conf:35.5%
PSNR between cover and stego image: 63.37 dB
SSIM between cover and stego image: 1.0000
```

```
Saved verification to: uav_stego_output/verification.txt

env: CUDA_LAUNCH_BLOCKING=1
CUDA_LAUNCH_BLOCKING is set to 1
Using device: cpu
Training small CNN...
Epoch 1, Loss: 1.6948
Epoch 2, Loss: 1.6640
Epoch 3, Loss: 1.6423
Epoch 4, Loss: 1.6297
Validation Accuracy: 48.36%
Predicted message -> Class:van;Conf:35.2%
Extracted message -> Class:van;Conf:35.2%
PSNR: 63.71 dB, SSIM: 1.0000
```

Fig. 2: Stego images fromtwo datasets: (Top) CIFAR-10, (Bot- tom) VisDrone. Both preserve visual quality after embedding

TABLE III: Sample predictions on a test image

Dataset	Predicted Class	Confidence
CIFAR-10 VisDrone	Horse Van	35.5% 35.2%

6.2. Steganographic Embedding Results

The messages were put into the cover images with the LSB method. The stego images looked the same as the original cover images. The embedding of metadata did not reduce visual quality, as the images looked identical.

6.3. Message Extraction Results

The hidden messages were successfully extracted from the stego images without any errors:

TABLE IV: Extracted messages from stage images

Dataset	Predicted Class	Confidence
CIFAR-10	Horse	35.5%
VisDrone	Van	35.2%

This demonstrates that the proposed approach ensures reli- able metadata recovery under normal operating conditions.

6.4. Image Quality Metrics

To quantitatively assess image quality:

1. **PSNR:** 63.37 dB (CIFAR-10) and 63.71 dB (VisDrone), both values far exceeding the 40 dB threshold, indicating extremely high fidelity.
2. **SSIM:** 1.0000 for both datasets, confirming that struc- tural similarity was perfectly preserved between cover and stego images.

TABLE V: Summary of experimental results on CIFAR-10 and VisDrone2019-DET datasets

Metric	CIFAR-10	VisDrone
Test Accuracy	33.00%	48.36%
Example Predicted Message	Horse (35.5%)	Van (35.2%)
PSNR	63.37 dB	63.71 dB

SSIM	1.0000	1.0000
Message Extraction	Successful	Successful

6.5. Suggested Extended Experiments

The following experiments are proposed to evaluate the scalability and robustness of the system:

1. **Larger Dataset Training:** The system will be trained and evaluated on the full CIFAR-10 and full VisDrone datasets to achieve improved classification accuracy.
2. **Robustness Against Compression:** Message recovery will be tested under various JPEG compression levels, simulating realistic UAV transmission conditions.
3. **Transform Domain Steganography Comparison:** The current LSB approach will be compared with transform- domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), high- lighting the trade-offs between robustness and efficiency.
4. **Noise and Channel Impairments:** The system will be evaluated under Gaussian noise, packet loss, and other real-world transmission impairments to analyze reliability in practical scenarios.

7. Performance Evaluation

The framework is evaluated across four key aspects: *clas- sification accuracy*, *steganographic imperceptibility*, *message extraction reliability*, and *computational overhead*. The results are reported on the CIFAR-10 benchmark dataset as well as the VisDrone2019-DET UAV dataset.

7.1. Classification Performance

1. The lightweight CNN had an accuracy of 33% on the CIFAR-10 subset after three epochs. Although the ac- curacy was modest, it showed the possibility of use on platforms like UAVs with limited computation. Deeper networks, such as MobileNet or EfficientNet, significantly improve accuracy.
2. On the VisDrone2019-DET dataset, the same CNN achieved a validation accuracy of 48.36%, because it better aligned with aerial imagery situations.

7.2. Steganographic Imperceptibility

1. The Peak Signal-to-Noise Ratio (PSNR) on CIFAR-10 was 63.37 dB. On the VisDrone dataset, a value of 63.71 dB was observed. Both values are well above the 40 dB threshold, indicating that the LSB embedding process is imperceptible to the human eye.
2. The Structural Similarity Index Measure (SSIM) was close to 1.0000, confirming that the cover and stage images are structurally identical.

SSIM: An SSIM score of 1.0000 highlights that structural similarity between cover and stego images is perfectly preserved. This demonstrates that LSB embedding, when applied to short metadata messages, ensures high fidelity and negligible perceptual degradation.

7.3. Extraction Reliability

The message extraction was successful across both datasets. Theoretical analysis shows that the probability of error-free recovery is high. For short messages (under 128 bits) with low error probability, the recovery success rate is above 95%. Reliability can be further enhanced in future deployments by incorporating error-correcting codes (ECC).

7.4. Computational Efficiency

The embedding and extraction operations are linear in the number of embedded bits:

$$O(L), \quad (8)$$

and require negligible overhead compared to CNN inference. Thus, the bottleneck lies in CNN inference, which is feasible on embedded UAV hardware when using lightweight models. The overall system therefore remains suitable for real-time UAV operations.

7.5. Comparative Analysis

A comparative study of representative steganography meth- ods is summarized in Table VI.

TABLE VI: Updated Comparison of Recent Steganography Methods for UAV Communication

Method	Key Metrics (PSNR/SSIM)	UAV Suitability
Proposed LSB + CNN (2025)	Very High (63 dB / 1.0)	Excellent
Lightweight Crypto + LSB [8]	High (>50 dB)	High
RNN + Fuzzy Steganography [9]	High (>45 dB)	Moderate
DWT-SVD Hybrid (UAV Image Tx) [1]	Mod–High (40–45 dB)	Limited
Drone Video Steganography [10]	High (>40 dB, SSIM ~0.95)	Limited
GAN-based (General)	High (>40 dB, SSIM)	Limited

This comparison highlights that the proposed LSB-based approach achieves an excellent balance of imperceptibility and computational efficiency, making it especially well-suited for UAV platforms.

8. CONCLUSION

The paper describes a light framework for secure metadata insertion into UAV imagery - it unites convolutional neural network classification with Least Significant Bit steganogra- phy. This system allows UAVs to produce semantic labels with confidence scores and insert them into images. A separate metadata transmission is not necessary. Validation was on both CIFAR-10, a benchmark along with VisDrone2019-DET, which is UAV-specific, datasets. The results show that the framework keeps good visual quality. PSNR values stay above 63 dB, and SSIM scores are near 1.0. This shows impercepti- bility. Metadata removal was always right. The computational cost was small when compared to CNN inference - this con- firms that deployment on UAV platforms with few resources is possible. Classification accuracy was low, 33% on CIFAR- 10 and 48.36% on VisDrone. One can fix this problem with better light architectures, such as MobileNet or EfficientNet. Future work will also examine toughness under compression, noise in addition to steganalysis. That will prove practical use in UAV communication settings.

REFERENCES

[1] K. J. Devi *et al.*, “Enabling secure image transmission in unmanned aerial systems using hybrid dwt-svd watermarking,” *Expert Systems with Applications*, 2024.

[2] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “A survey of digital image steganography,”

[4] *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[5] J. Hayes and G. Danezis, “Generating steganographic images via adver- sarial training,” in *Advances in Neural Information Processing Systems (NeurIPS)*, 2017, pp. 1954–1963.

[6] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600– 612, 2004.

[7] A. Krizhevsky and G. Hinton, “Learning multiple layers of features from tiny images,” University of Toronto, Tech. Rep., 2009, cIFAR-10 Dataset.

[8] P. Zhu, L. Wen, D. Du, X. Bian, H. Ling, and Q. Hu, “Vision meets drones: A challenge,” in *Proceedings of the European Conference on Computer Vision (ECCV) Workshops*, 2018, pp. 0–0, visDrone2019-DET Dataset.

[9] O. Valikhanli and F. Abdullayeva, “Securing uav flight data using lightweight cryptography and image steganography,” *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 5, 2025. [Online]. Available: https://www.researchgate.net/publication/392377148

[10] R. Kanimozhi and V. Padmavathi, “Robust and secure image steganography with recurrent neural network and fuzzy logic integration,” *Scientific Reports*, 2025. [Online].

[11] Available: https://www.nature.com/articles/s41598-025-97795-6

[12] H. R. Kareem *et al.*, “Steganography in videos captured by a drone,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 2, 2025. [Online]. Available: https://www.jisem-journal.com/index.php/journal/article/view/2752

AUTHORS

Prateeksha Gaur, a dedicated tech professional, holds a BCA (2011) from Mewar Girls College, Chittorgarh (Mohanlal Sukhadia University) and an MCA (2014) from Government Women Engineering College, Ajmer (Rajasthan Technical University). Currently pursuing MTECH in Computer Science Engineering from Dr. KN Modi University.

Amit Verma was born in Kanpur, Uttar Pradesh, India. He holds a B.Tech in Computer Science & Engineering from CSA University, Kanpur, an M.Tech in Computer Science from BBA Central University, Lucknow, and a PG Diploma in Software Development from C-DAC Hyderabad. He has served as Teaching Associate at CSAUAT (Nov 2020–Apr 2022) and as Assistant Professor at KIT Kanpur (May 2022–Feb 2023), KL University, Vijayawada (Mar 2023–Aug 2023), and is currently an Assistant Professor at Dr. K. N. Modi University,

Rajasthan. He has published two UGC CARE Group research papers, three conference papers (two national and one international), and holds one national and one international patent. He is a member of SDIWC and IAENG, and is currently pursuing a Ph.D. in CSE at NIT Arunachal Pradesh (since Jan 2024).

Manish Kumar Sharma was born in Sawai Madhopur, Rajasthan, India. He completed his B.Tech in Electronics and Communication Engineering from Rajasthan Technical University, Kota, in 2012, and his M.Tech in Power Electronics from Dr. K. N. Modi University in 2023. He has four years of professional experience working on the Rajasthan State Wide Area Network (RAJSWAN) government project. Currently, he is working as an Assistant Professor in the Department of Electrical and Electronics Engineering at Dr. K. N. Modi University.