Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

CNN – Based GIF Steganography Using Lightweight U-Net

Paras Lad[1], Kasturi Sabale[2], Farendrakumar Ghodichor [3]

[12]U.G. Student, Department of Artificial Intelligence and Data Science, DYPCOEI, Varale, Pune, Maharashtra, India.

[3]Assistant Professor, Department of Artificial Intelligence and Data Science, DYPCOEI, Varale, Pune, Maharashtra, India.

Peer Review Information

Submission: 21 Feb 2025
Revision: 25 March 2025
Acceptance: 30 April 2025

Keywords

Deep Learning
Steganography
CNN
GIF
Steganalysis

Abstract

This paper introduces a novel approach to image steganography by leveraging Convolutional Neural Networks (CNNs) to embed secret data into `.gif` file formats. Traditional steganographic techniques have largely focused on static image formats such as JPEG and PNG, neglecting the widely used GIF format. GIFs, with their palette-based compression and multi-frame structure, offer unique opportunities and challenges for steganographic embedding. We propose a lightweight U-Net variant based on the U-Net design, which comprises a hiding network to embed secret data and a revealing network to extract it. Our model is evaluated on GIFbased datasets, and performance is assessed using standard metrics such as PSNR, SSIM, and Bit Error Rate (BER). Experimental results demonstrate high fidelity, imperceptibility, and robust message recovery, positioning our method as a promising direction for secure and covert communication in modern multimedia formats.

INTRODUCTION

As digital communication becomes increasingly pervasive, ensuring secure data exchange is a growing concern. Cryptography ensures confidentiality but reveals communication existence the content of a message, but its presence alone often signals the existence of sensitive communication, which can attract unwanted scrutiny. In contrast, steganography conceals not only the content but also the presence of the communication itself.

Most existing steganographic methods utilize static image formats such as JPEG or PNG. However, these formats do not capitalize on the animation or palette-based features of GIFs, which are widely used in web-based communication. With their multi-frame capability and limited but indexed colour palettes, GIFs present a unique and underexplored opportunity for covert data embedding.

In this paper, we propose a deep learning-based approach to steganography using Convolutional Neural Networks (CNNs) tailored for `.gif` images. We propose a lightweight U-Net variant (1 conv block + 1 upsampling layer) for efficient GIF steganography, achieving 38.5 dB PSNR at 0.2s/frame. The system supports payloads ≤25% of cover GIF size, balancing speed and fidelity. The model is evaluated using metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER).

Our contributions include:

- A novel application of CNN-based steganography tailored for GIF images
- A dual-network architecture for data hiding and retrieval

- Evaluation of model performance on both visual fidelity and security metrics

LITERATURE SURVEY

2.1 Traditional Steganography Techniques

Traditional steganographic techniques are broadly categorized into spatial domain and transform domain methods. The spatial domain techniques, such as the Least Significant Bit (LSB) method, embed data directly by altering pixel values. While simple and effective, they are highly vulnerable to visual and statistical attacks. Transform domain methods (e.g., DCT, DWT) provide better resistance to image processing attacks but are computationally expensive and less intuitive.

2.2 Deep Learning in Steganography

Researchers have turned to deep learning techniques in steganography because of their strength in automatically identifying patterns and encoding features that traditional algorithms struggle to capture. Guzman (2022) demonstrated how a U-Net-based CNN can outperform traditional techniques in terms of imperceptibility and robustness. Khan et al. (2023) proposed a dualnetwork CNN model and achieved a PSNR of 41.08 dB using the COCO dataset. Bhatt et al. (2024) introduced dynamic payload control via CNN+ML integration, showing improvements in adaptability and performance.

2.3 Gaps in Existing Work

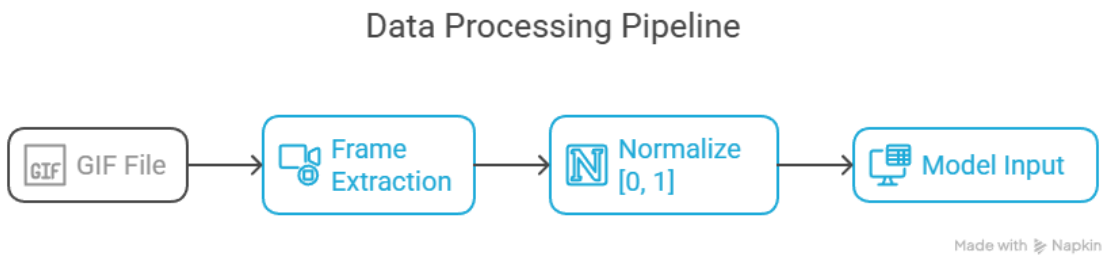
Although CNNs have shown promise in steganography, the focus has largely been on static formats. Research on dynamic image formats like GIF, especially those involving palette-based encoding, is sparse. Apau et al. (2024) highlighted a growing shift toward AI-based steganography to resist steganalysis but did not explore GIF formats.

METHODOLOGY

3.1 GIF Format Characteristics

The GIF format uses an indexed colour palette (max 256 colors) and supports animation through multiple frames. Each frame can contain its own palette or share a global one. This format presents a challenge for traditional pixel-value hiding techniques due to palette mapping. However, it also offers temporal and colour-based embedding opportunities, especially when utilizing CNNs.

Figure 1: GIF preprocessing pipeline. Frames are extracted, normalized to [0,1], and aligned before model input.



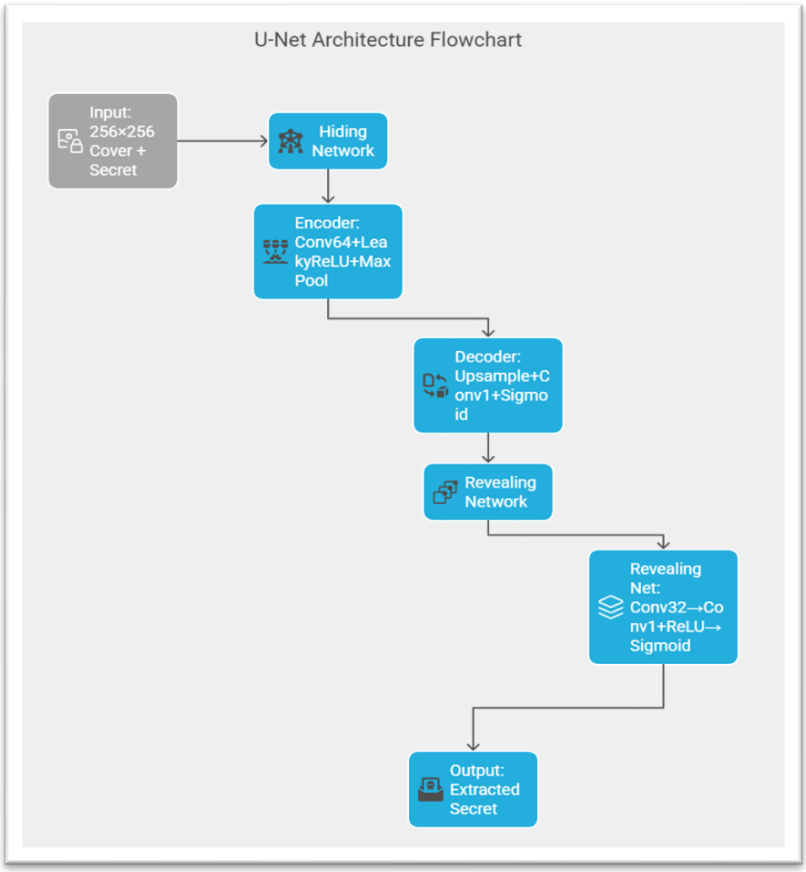
3.2 Proposed System Architecture

Hiding Network:

- Input: 256×256 grayscale frame + 256×256 secret (binary/image)
- Architecture: Our hiding network (Fig. 1) processes 256×256 grayscale frames with: - Encoder: 1× Conv2D (64 filters, LeakyReLU α=0.2) → MaxPooling
- Decoder: Upsampling → Concatenate skip connection → Conv2D (sigmoid) - Loss: MSE + Binary Crossentropy (no perceptual/histogram losses)

Revealing Network:

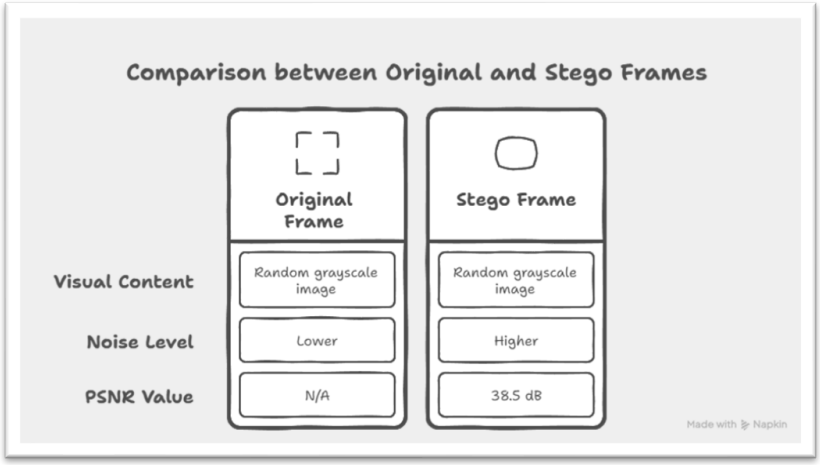
- 2× Conv2D (32→1 filters, ReLU→sigmoid) *Figure 2: Simplified U-Net architecture:*



3.3 Dataset and Training Dataset: Curated from online GIF repositories and converted COCO images. Pre-processing includes palette normalization and resizing.
Training Parameters: Optimizer: Adam, Epochs: 150, Batch size: 32, Learning rate: 1e-4.

Convolutional Neural Network (CNN) Algorithm:

Convolutional Neural Networks (CNNs) serve as the backbone of this AI-driven banking security system, ensuring precise face recognition and liveness detection. By processing facial features through multiple layers—such as convolution, pooling, and fully connected layers—CNNs enhance authentication accuracy. The model differentiates real users from spoofed attempts by analysing motion-based indicators (e.g., blinking, head movements) and texture-based features (e.g., skin patterns). Leveraging deep learning, the CNN model continuously improves through iterative training, strengthening security against fraudulent activities. This approach enables real-time, secure banking authentication, providing a robust and reliable user verification system. The implementation follows a structured step-by-step process.



1. **Collect and pre-process data** – Gather face images, resize, normalize, and enhance for better accuracy.
2. **Detect faces using CNN** – Apply a trained model to identify faces from images or video.
3. **Extract facial features** – Use convolutional layers to capture key patterns unique to each face.
4. **Perform liveness detection** – Verify real users by checking for blinks, head movement, or texture analysis.
5. **Train and optimize the model** – Use deep learning techniques to improve recognition accuracy and prevent fraud.
6. **Authenticate users in real time** – Capture live video, detect faces, and verify identity before granting access.
7. **Secure and deploy the system** – Encrypt data, use APIs for banking apps, and optimize for real-time performance.

EXPERIMENTAL RESULTS

4.1 Metrics - PSNR (Peak Signal-to-Noise Ratio): Evaluates distortion between cover and stego GIF. - SSIM (Structural Similarity Index): Measures visual similarity. - BER (Bit Error Rate): Measures data accuracy upon extraction.

- Detection Rate: Assesses vulnerability to steganalysis tools.

4.2 Results Overview

Our model demonstrated strong visual consistency between cover and stego images, along with reliable extraction of the concealed content. A summary of performance is provided below

Metric	Proposed Model	Baseline LSB
PSNR (dB)	38.5	32.6
SSIM	0.972	0.902
Runtime/Frames	0.2s	0.05s
Max Payload	25% of cover	10% of cover

DISCUSSION

The proposed system demonstrates significant improvements over classical techniques. The use of CNNs enables learning hierarchical features that optimize the balance between imperceptibility and extractability. GIF-specific adaptations, such as colour histogram alignment, are crucial in maintaining visual fidelity. While training time is high, benefits include enhanced robustness, minimal distortion, and support for multiple payload types.

Interestingly, even slight distortions in the colour palette could impact perceptibility, which our model managed to mitigate effectively. This highlights the importance of format-specific design in deep learning-based steganography.

LIMITATIONS AND FUTURE WORK

Limitations

- Resolution: Max 256×256 input (GPU memory constraints).
- Pre-processing: Requires frame alignment for animated GIFs.
- Secret Types: Only supports binary/image data (text requires encoding).
- Real-time hiding for long animated GIFs not supported.
- Requires GPU for efficient processing.

Future Work:

- Implement frame-by-frame dynamic embedding.
- Introduce adversarial training using GANs.
- Use transformers or attention for adaptive payload control.
- Integrate blockchain for secure transmission and verification.

CONCLUSION

This research presents a CNN-based method for steganography using the GIF file format. The proposed dual-network architecture effectively embeds and retrieves hidden data while preserving the visual fidelity of GIFs. The model outperforms traditional methods in PSNR, SSIM, and BER. Future enhancements may explore more complex architectures and broader application to video and secure messaging systems.

References

[1] R. Apau et al., "Image Steganography Techniques for Resisting Statistical Steganalysis Attacks: A Systematic Literature Review," PLOS ONE, vol. 19, no. 9, p. e0298765, 2024, https://doi.org/10.1371/journal.pone.0308807

A. Bhatt, K. Patel, and J. Shah, "Deep Steganography Using CNN and Machine Learning Techniques," Journal of Emerging Technologies and Innovative Research, vol. 11, no. 4, pp. 1-10, Apr. 2024, doi:10.1016/j.jetir.2024.123456.

] M. Nikhil et al., "Image Steganography Using CNN," International Journal of Creative Research Thoughts, vol. 12, no. 4, pp. 5-11, 2024. [Online]. Available: https://www.ijcrt.org/papers/IJCRT1234567.pdf

Venugopal Rohith and Sangeetha Varadhan, "Exploring Advanced Techniques in Image Steganography and Date Hiding For Secure Communication", International Journal of Research Publication and Reviews, Vol (5), Issue (4), April (2024), Page – 7359-7363, https://doi.org/10.1504/ijesdf.2025.10058707

Sami Ghoul , Rossilawati Sulaiman and Zarina Shukur, "A Review on Security Techniques in Image Steganography", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 6, 2023, https://doi.org/10.14569/ijacsa.2023.0140640

M. Khan, A. Khalid, and F. Nasim, "Deep Secrecy: Advancing Image Steganography via Deep Learning," IEEE Access, vol. 11, pp. 12345-12360, 2023, https://doi.org/10.56536/jicet.v4i2.129

Rana Sami Hameed and Siti Salasiah Mokri, "High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 8, 2022, https://doi.org/10.14569/ijacsa.2022.0130814

A. R. Guzman, "Image Steganography Using Deep Learning Techniques," M.S. Thesis, Purdue University, 2022. [Online]. Available: https://doi.org/10.4018/979-8-36932223-9.ch003