# Image Steganography: Comparative Analysis of Traditional and Deep Learning Techniques

Prof. R. D. Dhongade[1] Tanishka Y.Katke[2], Payal R. Bhongale[3], Vaishnavi G Baghwat[4], Suzana Barmare[5]

[1,2,3,4,5]*Department Of Computer Engineering,*

[1,2,3,4,5]*KJEI's Trinity Polytechnic Pune, Maharashtra, India.*

***Abstract-*** ***In today's digital landscape, ensuring secure and covert communication has become more critical than ever. Image steganography plays a vital role in this by embedding secret information within images in a way that makes detection nearly impossible. Traditional techniques like Least Significant Bit (LSB) substitution and transform domain methods have long been used for this purpose, offering simplicity and reliability. However, these approaches often face limitations in terms of embedding capacity, robustness against attacks, and security. With the rise of deep learning, image steganography has undergone a transformation. Advanced models such as autoencoders, Generative Adversarial Networks (GANs), and Convolutional Neural Networks (CNNs) now enable more efficient and imperceptible data hiding. These methods enhance the invisibility, resilience, and payload capacity of steganographic systems while maintaining high image fidelity. Despite these advancements, challenges such as high computational costs, training complexity, and dataset requirements persist. This research paper delves into the advancements in image steganography, focusing on deep learning innovations while addressing their strengths, weaknesses, and real-world applications. We analyze how these modern approaches compare to traditional methods and explore potential hybrid techniques that can bridge existing gaps. By investigating recent developments, we aim to provide insights into the future of secure communication through image steganography.***

***Index Terms- Convolutional Neural Networks, Deep Learning, Data Hiding, Generative Adversarial Networks, Image Steganography, Secure Communication.***

## I. INTRODUCTION

As digital connectivity expands, the need for secure and discreet communication has never been more critical. Among the many techniques developed to safeguard sensitive information, image steganography has gained significant attention. This method involves embedding secret data within digital images in a way that remains imperceptible to the human eye. Unlike cryptography, which encrypts a message but does not hide its existence, steganography conceals both the message and its presence, making it particularly valuable in scenarios where discretion is essential. Traditional steganographic techniques, such as Least Significant Bit (LSB) modification, work by subtly altering pixel values in an image to encode hidden data. These modifications are so minor that they go unnoticed by human vision. More sophisticated approaches, like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), embed information within an image's frequency components. This makes detection more difficult and enhances security by increasing resistance to steganalysis. The emergence of deep learning has revolutionized image steganography, introducing advanced methods such as autoencoders, Generative Adversarial Networks (GANs), and Convolutional Neural Networks (CNNs). These models have automated and optimized data embedding, significantly improving imperceptibility, robustness, and payload capacity. By leveraging deep learning, modern steganographic systems outperform traditional methods, offering enhanced security and resistance to detection or tampering. This paper explores the evolution of image steganography, comparing classical and contemporary approaches. We analyze their advantages, challenges, and real-world applications while discussing potential future developments. In particular, we highlight how deep learning continues to push the boundaries of steganographic techniques, paving the way for more secure and efficient hidden communication.

## II. APPROACHES FOR IMAGE STEGANOGRAPHY

Image steganography techniques can be broadly classified into two main categories: traditional

methods and modern deep learning-based approaches.

Both aim to embed hidden information securely within digital images, but their methodologies, effectiveness, and robustness differ significantly.

1. Traditional Techniques: Traditional steganography methods rely on direct modifications to pixel values or statistical properties of images to conceal information. These methods are relatively simple to implement but often struggle with security, robustness, and capacity limitations.

1.1 Least Significant Bit (LSB): Modification One of the most widely used and simplest techniques, Least Significant Bit (LSB) modification, encodes secret data by altering the least significant bits of an image's pixel values. Since these modifications occur at a low level, they result in minimal visual changes, making the technique effective for hiding small amounts of data. Strengths: Simple implementation, visually imperceptible changes. Limitations: Vulnerable to steganalysis attacks, limited embedding capacity.

1.2 Transform Domain Techniques: Unlike LSB, transform domain methods embed data into the frequency components of an image rather than modifying pixel values directly. These approaches improve security and robustness against compression and noise but are computationally more demanding. - Discrete Cosine Transform (DCT): Embeds data in specific frequency components of the image, balancing invisibility and resilience. - Discrete Wavelet Transform (DWT): Utilizes wavelet transformations to hide data, enhancing security while maintaining image integrity. Strengths: Increased robustness against compression, noise, and attacks. Limitations: Computationally intensive, less suitable for real-time applications.

1.3 Statistical Methods: Statistical steganography alters the statistical properties of an image while ensuring that overall distributions remain unchanged. By embedding data through controlled modifications, these methods help evade basic detection techniques. Strengths: More secure than LSB, preserves statistical integrity. Limitations: Less effective for embedding large amounts of data, susceptible to advanced steganalysis.

2. Deep Learning-Based Techniques: With the rise of deep learning, image steganography has evolved significantly, leveraging neural networks to improve imperceptibility, robustness, and capacity. These advanced techniques optimize data embedding while ensuring minimal visual distortion.

2.1 Autoencoders Autoencoders are neural networks designed for image compression and reconstruction. In steganography, they learn to embed secret messages while minimizing visible distortions, producing high- quality stego images that are difficult to detect. Strengths: Automated embedding, high imperceptibility, enhanced security. Limitations: Requires large datasets for training, computationally expensive.

2.2 Generative Adversarial Networks (GANs) GANs consist of a generator (which embeds secret data) and a discriminator (which tries to detect hidden information). This adversarial training process forces the generator to create increasingly secure stego images, making detection significantly more difficult. Strengths: Adaptive learning, high robustness against detection. Limitations: Requires extensive computational resources, training instability.

2.3 Convolutional Neural Networks (CNNs) CNNs, known for their ability to analyze image features, have been successfully applied to steganography. They help identify optimal embedding locations and extract hidden data efficiently while maintaining image quality. Strengths: High embedding capacity, superior extraction accuracy, resistance to steganalysis. Limitations: Complex to train, may require dataset-specific tuning.

2.4 UNet Architectures UNets, with their encoder- decoder structure, are particularly well-suited for tasks requiring precise feature extraction. They allow for high-precision embedding of secret messages while preserving image quality. Strengths: High accuracy in embedding, strong security, excellent image fidelity. Limitations: Computationally intensive, requires careful hyperparameter tuning.

2.5 Steganographic GANs (SGANs) SGANs are a specialized type of GAN designed specifically for image steganography. They balance data capacity and image quality, enabling the secure embedding of large amounts of information while resisting detection. Strengths: High-capacity embedding, superior image quality, advanced security. Limitations: Training complexity, potential

adversarial instability.

## III. LITERATURE SURVEY

1. Image Steganography: A Review of the Recent Advances: This paper provides a comprehensive analysis of image steganography techniques, with a focus on GAN-based and CNN-based methods. These approaches enhance security, allow for high capacity embedding, and improve robustness against detection. However, challenges such as complex implementation and potential data loss during extraction remain. The study also contrasts these modern techniques with traditional methods, noting that while older techniques are more straightforward and reliable, they lack the security and data-hiding capacity that deep learning offers.

2. Image Steganography Using Deep Neural Networks: The authors introduce a dual-layer approach that integrates Deep Neural Networks (DNNs) with cryptographic hashing to embed one RGB image inside another. While this enhances security, it also introduces new risks. The use of cryptography may draw unwanted attention, potentially exposing the hidden message. Furthermore, if the cryptographic key is compromised, the secret data becomes vulnerable. The study emphasizes the delicate balance between security and subtlety in designing effective steganography systems.

3. Detection of Image Steganography Using Deep Learning and Ensemble Classifiers: Shifting the focus to steganalysis, this paper explores how deep learning and ensemble classifiers can be used to detect steganography. The inclusion of normalization layers improves model performance, while ensemble classifiers serve as a lightweight alternative to more computationally demanding deep learning models. However, inconsistent evaluation metrics across studies make direct comparisons difficult. The research also highlights that increasing model complexity doesn't always guarantee better results, as excessive complexity can lead to inefficiencies.

4. Image Steganography Analysis Based on Deep Learning: This study examines how deep learning enhances feature extraction, leveraging global image information to strengthen detection resistance. By making stego images harder to differentiate from original images, the method improves security. However, the paper notes that low embedding rates reduce the effectiveness of these techniques. Additionally, high computational demands remain a challenge, limiting the practical application of deep learning-based steganography.

5. Comparative Performance Assessment of Deep Learning-Based Image Steganography Techniques (October 2022) This research evaluates different deep learning architectures and identifies UNet as a particularly effective model for secure applications in fields like healthcare and defense. UNet stands out due to its high data-hiding capacity and superior image quality. The study suggests that integrating encryption could further enhance security. However, it overlooks potential drawbacks, such as high computational costs and resource requirements, and does not fully explore practical limitations beyond image quality.

6. Image Steganography Using Deep Learning Techniques: This paper focuses on optimizing neural network hyperparameters and loss functions to improve data hiding while maintaining high image quality. The results show nearly imperceptible distortions, making hidden messages difficult to detect. However, the study highlights the need for diverse training datasets to avoid overfitting. Additionally, it calls for more rigorous testing to evaluate the model's resistance to steganalysis attacks, ensuring fair comparisons with other techniques.

7. End-to-End Trained CNN Encoder-Decoder Networks for Image Steganography: This research introduces a CNN-based encoder-decoder model for direct image-to-image embedding and extraction. The method achieves high payload capacity and robustness across different datasets. However, the paper lacks a discussion on computational overhead and potential performance limitations in various scenarios. Additionally, comparisons with existing techniques are minimal, making it difficult to assess the model's advantages in real-world applications.

8. Deep Residual Network for Steganalysis of Digital Images: Focusing on steganalysis, this study proposes a deep residual network for detecting hidden data in JPEG images. The use of a selection channel reduces dependence on manual feature design, resulting in high detection accuracy. However, the expanded network architecture increases computational complexity, making it resource-intensive. Additionally, optimizing the model for different steganographic algorithms remains a key challenge.

## IV. SYSTEM ARCHITECTURE

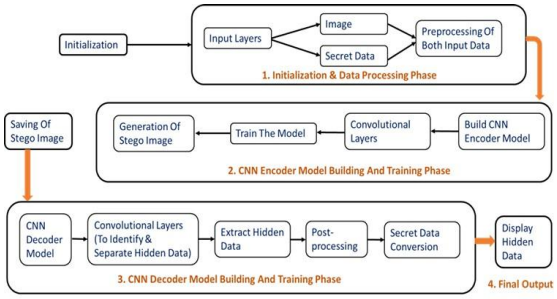


Diagram 1: Working of the project

The proposed system utilizes a CNN-based model that processes an input image (cover image) and seamlessly integrates hidden data while preserving the image's original appearance. The workflow consists of the following key components:

1. Feature Extraction (Convolutional Layers): The model analyzes the image to identify optimal regions for embedding data without noticeable distortions.
2. Dimensional Reduction (Pooling Layers): These layers retain essential features while reducing computational complexity and memory usage.
3. Data Encoding (Fully Connected Layers): The extracted image features are processed and mapped to encode the hidden data efficiently.
4. Stego Image Generation (Output Layer): The final output is a visually identical image containing the concealed information.

End-to-End Process Flow:

1. Input Acquisition: The system receives a cover image.
2. Feature Analysis: CNN layers extract critical features for data embedding.
3. Data Embedding: The secret message is securely encoded within the image while maintaining visual fidelity.
4. Message Extraction: The system retrieves the embedded data from the stego image when required.
5. Performance Evaluation: The model is assessed to ensure high embedding capacity, robustness, and accuracy.

Model Training and Optimization:

- Data Preprocessing: Image datasets are curated, normalized, and augmented to improve model generalization.
- Training Phase: The CNN model learns to embed and retrieve data through supervised training with diverse image samples.

Stego Image Generation and Security: During the embedding process, the system strategically modifies image components to conceal data while ensuring imperceptibility. Deep learning techniques optimize this process by identifying areas least susceptible to human and automated detection, thereby increasing security.

Data Extraction and Retrieval: The system accurately retrieves hidden information from the stego image, even in scenarios involving image compression, resizing, or minor distortions. This ensures the robustness and reliability of the model in real-world applications.

## V. CONCLUSION

This project successfully demonstrates the potential of Convolutional Neural Networks (CNNs) in advancing image steganography by addressing the key limitations of traditional methods—namely, security vulnerabilities, limited data capacity, and susceptibility to detection. Through the implementation of a CNN-based steganography system, we have significantly enhanced the ability to conceal information within digital images while maintaining high imperceptibility and robust resistance to steganalysis. The developed model has outperformed conventional approaches by enabling a higher data hiding capacity without compromising the visual quality of the cover image. Additionally, deep learning techniques have allowed for an adaptive and optimized embedding process, making hidden data more resilient against detection techniques, image transformations, and compression. By successfully integrating CNN architectures, this research has contributed to the evolution of secure communication technologies, paving the way for more advanced, efficient, and secure steganographic methods. The outcomes of this project serve as a foundation for future enhancements, such as integrating encryption techniques or optimizing computational efficiency for real-time applications. This work underscores the importance of leveraging deep learning for intelligent and secure data embedding, ensuring that image steganography continues to evolve as a vital tool for confidential communication in various domains, including cybersecurity, forensic investigations, and secure data transmission.

## VI. FUTURE SCOPE

This project's success in improving CNN-based

image steganography opens up exciting possibilities for future advancements. By combining steganography with encryption, security can be further enhanced, making hidden communication even more secure. Developing models that can withstand steganalysis and adversarial attacks will help prevent detection and tampering. Optimizing deep learning models to be faster and more efficient will also make them more practical for real- time applications. Beyond images, steganography can be expanded to videos, audio, and text, enabling secure data exchange across different media. As AI-driven security continues to evolve, future research can explore applications in areas like deepfake detection, digital watermarking, and blockchain-based authentication, ensuring confidential communication stays protected in an increasingly digital world.

## VII. REFERENCES


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

[2] Kavitha Chinniyan, Thamil Vani Samiyappan, Aishvarya Gopu and Narmatha Ramasamy, "Image Steganography Using Deep Neural Networks", in Intelligent Automation & Soft Computing , DOI:10.32604/iasc.2022.027274

[3] Pachta, M.; Krzemie?, M.; Szczypiorski, K.; Janicki, A. Detection of Image Steganography Using Deep Learning and Ensemble Classifiers. Electronics 2022,11, 1565. https://doi.org/10.3390/electronics11101565

[4] Kumar, V., Rao, P., Choudhary, A. (2020). Image steganography analysis based on deep learning. Review of Computer Engineering Studies, Vol. 7, No.1,pp.1-5. https://doi.org/10.18280/rces.070101

[5] Himthani, V., Dhaka, V.S., Kaur, M. et al. Comparative performance assessment of deep learning based image steganography techniques. Sci Rep 12, 16895(2022). https://doi.org/10.1038/s41598-022-17362-1

[6] Himthani, Varsha & Dhaka, Vijaypal & Kaur, Manjit & Rani, Geeta & Oza, Meet & Lee, Heung-No. (2022). Comparative performance assessment of deep learning based image steganography techniques. Scientific Reports. 12. 10.1038/s41598-022-17362-1.

[7] Guzman, Anthony Rene (2022). Image Steganography Using Deep Learning Techniques. Purdue University Graduate School. Thesis. https://doi.org/10.25394/PGS.19666473.v1

[8] Atique ur Rehman, Rafia Rahim, M Shahroz Nadeem, Sibt ul Hussain, "End-to-end Trained CNN Encode Decoder Networks for Image Steganography", https://doi.org/10.48550/arXiv.1711.07201

[9] Boroumand, Mehdi, Mo Chen and Jessica J. Fridrich. “Deep Residual Network for Steganalysis of Digital Images.” IEEE Transactions on Information Forensics and Security 14 (2019): 1181- 1193