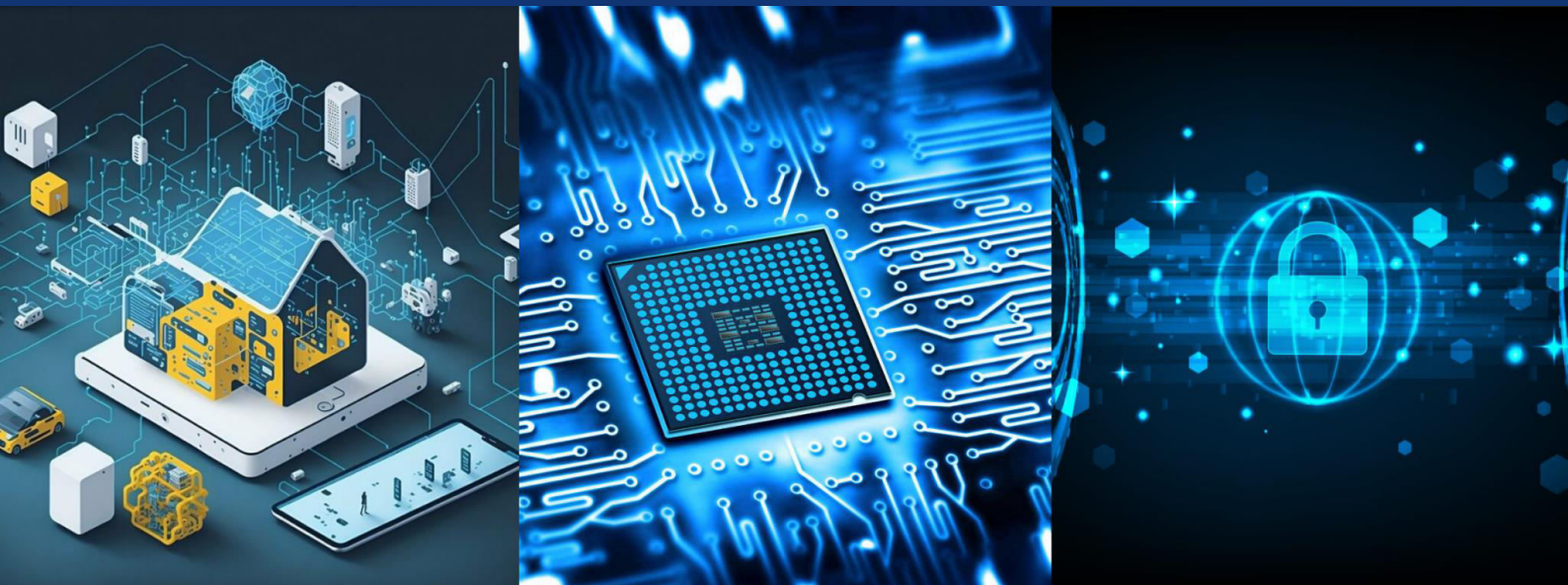
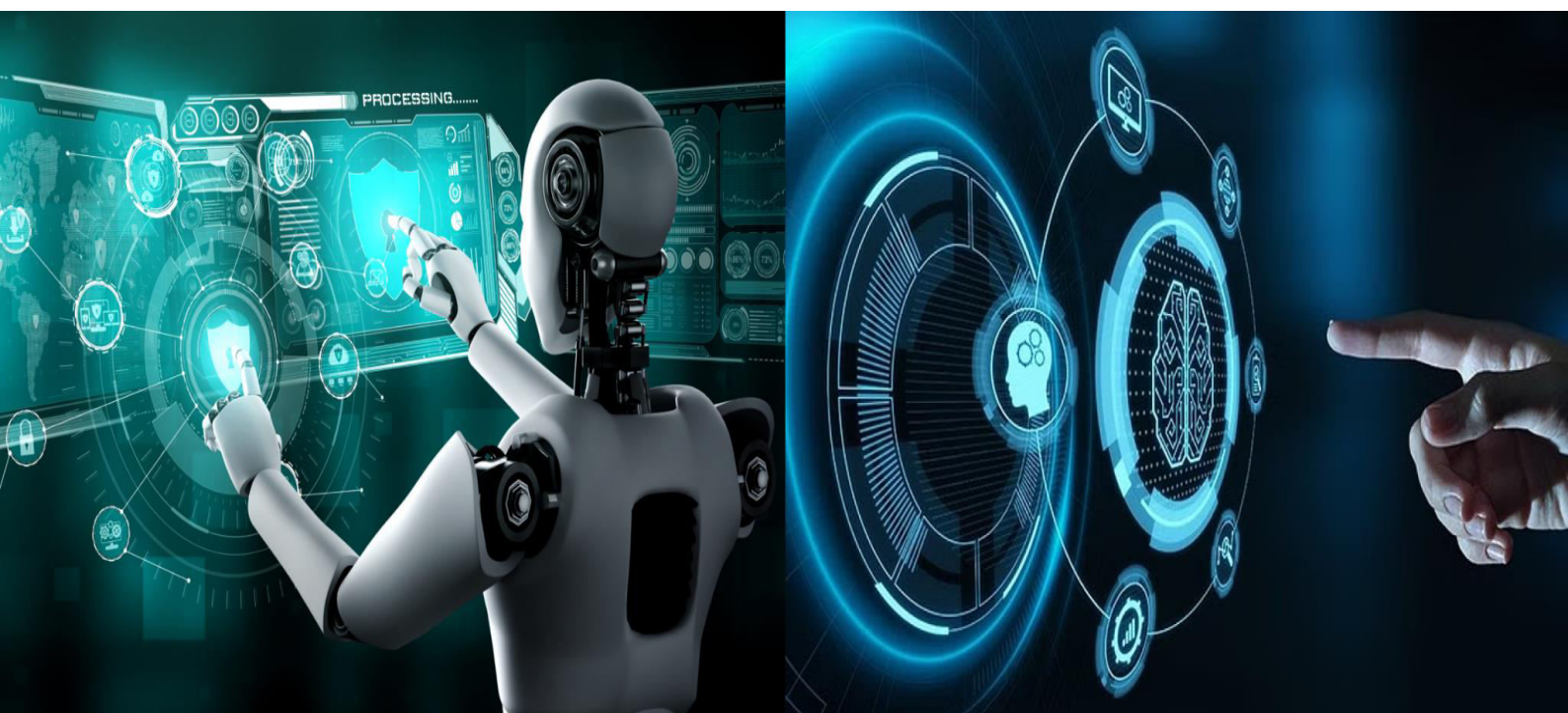




International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Deep Learning-Driven Multi Layered Steganographic Approach for Enhanced Data Security

Mr. K. Venakata Naga Sreedhar, K. Sai, P. Sharan, G. Sai, M. Saketh Ram

Asst. Professor, Department of Computer Science and Engineering, Bachelor of Technology, Malla Reddy University, Hyderabad, Telangana, India

Department of Computer Science and Engineering, Bachelor of Technology, Malla Reddy University, Hyderabad, Telangana, India

ABSTRACT: In the digital era, ensuring data integrity, authenticity, and confidentiality is critical amid increasing interconnectivity and evolving security threats. This paper addresses the key limitations of traditional steganographic methods, including limited payload capacity, vulnerability to detection, and lack of robustness against attacks. To overcome these challenges, a novel multi-layered steganographic framework is proposed, integrating Huffman coding, Least Significant Bit (LSB) embedding, and a deep learning-based encoder-decoder. This approach enhances imperceptibility, robustness, and security.

Huffman coding compresses data while obfuscating statistical patterns, enabling efficient embedding within cover images. Simultaneously, the deep learning encoder provides an additional layer of protection by concealing an image within another, improving security. Extensive evaluations using benchmark datasets such as Tiny ImageNet, COCO, and CelebA demonstrate the framework's superior performance. Key contributions include achieving high visual fidelity, with Structural Similarity Index Metrics (SSIM) consistently exceeding 99%, robust data recovery with text recovery accuracy reaching 100% under standard conditions, and enhanced resistance to common attacks such as noise and compression.

The proposed framework significantly improves robustness, security, and computational efficiency compared to traditional methods. By effectively balancing imperceptibility and resilience, this paper advances secure communication and digital rights management, addressing modern challenges in data hiding through an innovative combination of compression, adaptive embedding, and deep learning techniques.

KEY WORDS: Data security, Huffman coding, Deep learning-based steganography, Image embedding, LSB embedding, Secure communication, Digital watermarking.

I. INTRODUCTION

With the rapid advancement of digital communication, ensuring the security, authenticity, and confidentiality of transmitted data has become a critical challenge. Traditional cryptographic methods, while effective in protecting data from unauthorized access, often attract attention due to their recognizable encrypted patterns. Steganography, the practice of concealing information within digital media, offers an alternative by embedding data in a way that remains imperceptible to attackers. However, conventional steganographic techniques suffer from limitations such as low payload capacity, vulnerability to steganalysis, and reduced robustness against image distortions and compression.

To address these challenges, this paper proposes a deep learning-driven multi-layered steganographic approach that enhances data security by integrating Huffman coding, Least Significant Bit (LSB) embedding, and a deep learning-based encoder-decoder framework. Huffman coding enables efficient data compression while obfuscating statistical patterns, reducing the risk of detection. LSB embedding allows for seamless data integration into cover images with minimal perceptual distortion. Additionally, a deep learning-based encoder-decoder enhances security by leveraging convolutional neural networks (CNNs) and long short-term memory (LSTM) networks to optimize embedding and extraction processes, ensuring high imperceptibility and robustness.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The effectiveness of the proposed approach is evaluated using benchmark datasets such as Tiny ImageNet, COCO, and CelebA, demonstrating superior performance in terms of imperceptibility, security, and resilience to common attacks such as noise, compression, and filtering. The results show that the proposed framework achieves a Structural Similarity Index Metric (SSIM) above 99% and 100% text recovery accuracy under standard conditions, outperforming traditional steganographic methods.

By integrating compression, adaptive embedding, and deep learning, this work contributes to advancing secure communication and digital rights management. The proposed multi-layered framework not only enhances data security but also offers a scalable and computationally efficient solution for modern steganographic applications.

II. LITERATURE SURVEY

Steganography has been widely explored as a means of securing digital communication by embedding secret information within multimedia content. Traditional steganographic methods primarily rely on Least Significant Bit (LSB) substitution, transform domain techniques, and adaptive encoding strategies. However, these approaches face challenges such as limited payload capacity, susceptibility to steganalysis, and vulnerability to image distortions. In recent years, the integration of machine learning and deep learning has significantly enhanced the effectiveness of steganographic systems, improving security, imperceptibility, and robustness.

2.1 Traditional Steganographic Techniques

Early steganographic techniques focused on LSB embedding, where the least significant bits of pixel values in an image are modified to hide data. Studies such as Chan & Cheng (2004) demonstrated that LSB substitution achieves high imperceptibility but is easily detectable using statistical steganalysis techniques like RS analysis and histogram analysis. Transform domain methods, such as Discrete Cosine Transform (DCT)-based steganography, embed data in the frequency components of an image, offering better resistance to compression and noise but often at the cost of reduced payload capacity.

Huffman coding has also been explored in steganography to improve compression efficiency and reduce redundancy in hidden messages. Research by Kumar et al. (2016) proposed a Huffman-based encoding scheme to improve embedding efficiency, but their approach still lacked robustness against image distortions and steganalysis attacks.

2.2 Deep Learning-Based Steganography

Recent advancements in deep learning have led to the development of neural network-driven steganographic techniques. Works such as Baluja (2017) introduced the use of convolutional neural networks (CNNs) for end-to-end steganographic encoding and decoding, demonstrating improved security and imperceptibility compared to traditional methods. Similarly, Zhu et al. (2018) proposed HiDDeN, a deep learning framework that utilizes CNN-based autoencoders for robust message embedding. However, these methods often require extensive training data and computational resources. Furthermore, studies integrating recurrent neural networks (RNNs) and long short-term memory (LSTM) networks have shown promise in text-based steganography, enhancing sequential data embedding and extraction accuracy. Research by Tang et al. (2020) explored hybrid CNN-LSTM architectures for robust steganographic encoding, significantly improving resilience against JPEG compression and Gaussian noise.

2.3 Gaps and Motivation for the Proposed Work

Despite advancements in deep learning-based steganography, existing methods still exhibit limitations in balancing security, imperceptibility, and robustness. Many approaches lack effective data compression mechanisms, leading to inefficient payload management and increased detection risk. Additionally, while deep learning models enhance embedding quality, they often fail to generalize well across diverse image datasets.

To overcome these challenges, this paper proposes a multi-layered steganographic framework that combines Huffman coding, LSB embedding, and a deep learning-based encoder-decoder. This approach leverages Huffman coding for efficient compression, LSB for seamless embedding, and deep learning for adaptive feature learning, ensuring high imperceptibility, robust data recovery, and enhanced security against steganalysis attacks.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. METHODOLOGY

i) Proposed Work:

The proposed system aims to develop a deep learning-based image steganography model using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. Traditional steganography techniques often lack robustness against noise, compression, and attacks, making deep learning-based methods a more effective approach. This system is designed to embed secret messages into digital images with high imperceptibility while ensuring that the embedded information is securely hidden and can be retrieved accurately. Unlike conventional Least Significant Bit (LSB) or frequency-based methods, the use of CNN enables the extraction of spatial image features, while LSTM is employed to model sequential dependencies in message embedding. The proposed model is designed to withstand attacks such as noise addition, compression, and image modifications while maintaining high image quality. The system aims to achieve high Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER) stability, ensuring effective encoding and decoding processes. The research also focuses on improving the embedding capacity of images without compromising the visual quality. This methodology provides a more advanced and secure way to achieve covert communication, making it suitable for applications in military communication, digital watermarking, and confidential data transmission.

ii) System Architecture:

The proposed system architecture is designed to ensure the seamless embedding and extraction of messages while maintaining the integrity of the cover image. The architecture comprises several key components:

1. **Data Preprocessing Module:** This stage involves preparing the input images and text messages for embedding. The images undergo resizing, normalization, and transformation to a suitable format (RGB or grayscale). The text messages are encoded into numerical representations before being processed by the model.
2. **Feature Extraction Layer (CNN):** A CNN is employed to extract spatial features from images. It captures pixel-level variations and patterns that are essential for embedding the secret message without significantly altering the image's appearance.
3. **Encoding Module (LSTM):** The encoded message is passed through an LSTM network, which captures temporal dependencies and structures the embedding process. LSTM ensures that message bits are spread optimally within the image, enhancing security and robustness.
4. **Stego-Image Generation:** The modified image, known as the stego-image, is generated by slightly altering pixel intensities using a deep learning-based embedding function.
5. **Decoding and Retrieval Module:** The retrieval process applies the inverse function of the embedding module, using CNN and LSTM to reconstruct the hidden message from the stego-image.
6. **Evaluation Metrics:** Finally, the performance of the system is evaluated using PSNR, SSIM, and BER to ensure that the image quality remains intact while the embedded message is accurately retrieved.

iii) Dataset Collection:

For this research, a combination of publicly available image datasets and synthetic data will be used to train and test the deep learning model. Datasets such as ImageNet, COCO (Common Objects in Context), and CIFAR-10 contain diverse image categories that help ensure model generalization. These datasets contain millions of high-resolution images, allowing the system to learn robust feature representations for embedding messages.

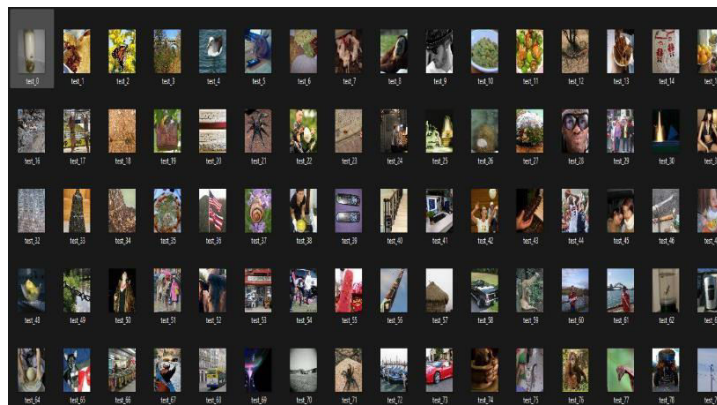
To ensure that the dataset meets the requirements of steganographic analysis, preprocessing techniques such as data augmentation, contrast normalization, and noise addition will be applied. Augmentation techniques, including rotation, flipping, and random cropping, will help improve the model's ability to generalize across different image conditions.

For message embedding, a corpus of natural language sentences, random binary sequences, and encrypted texts will be used. The text data will be converted into numerical representations using encoding techniques such as one-hot encoding or word embeddings (Word2Vec, GloVe, etc.). This allows the LSTM network to efficiently process and embed the messages into images. The dataset will be split into training, validation, and testing sets to ensure proper model evaluation and fine-tuning.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



iv) Image Processing

Image processing plays a crucial role in the proposed steganographic system, as it ensures that the images used for message embedding are properly preprocessed, modified, and restored without noticeable distortions. The first step in this process is image preprocessing, which involves resizing the images to a fixed resolution (e.g., 256x256 or 512x512), normalizing pixel values between 0 and 1, and converting them into a format suitable for deep learning models. If necessary, grayscale conversion may be performed to reduce computational complexity.

To enhance robustness, edge detection techniques such as the Sobel operator, Canny edge detection, and Laplacian filters can be applied. These techniques help identify regions in the image where message embedding can be performed with minimal visual impact. Additionally, Gaussian blurring and median filtering are used to reduce noise and ensure smoother image textures.

Once the image is prepared, the steganographic embedding process modifies pixel intensities at specific locations determined by the CNN and LSTM models. The modified image, or stego-image, is then post-processed to check for any visible artifacts. If necessary, further denoising techniques are applied to refine the stego-image before storage or transmission.

v) Feature Extraction

Feature extraction is a critical step in deep learning-based image steganography, as it enables the model to identify optimal embedding locations while preserving the image's visual quality. The feature extraction process begins with a Convolutional Neural Network (CNN), which is used to extract spatial patterns from input images. CNN layers, including convolutional, pooling, and activation layers, analyze pixel relationships and texture patterns to determine embedding zones.

The extracted spatial features are then passed through an LSTM network, which models temporal dependencies and sequence patterns in message embedding. Since LSTM is effective in processing sequential data, it helps structure the hidden message in a way that enhances security and reduces detectability. By learning the relationship between different pixel intensities, the model can embed messages in a visually imperceptible manner while ensuring that the retrieval process remains accurate.

The extracted features are also analyzed using dimensionality reduction techniques such as **Principal Component Analysis** (PCA) or Autoencoders, which help in optimizing the embedding process. These techniques remove redundant features, ensuring that only the most essential image properties are modified for message concealment. This approach improves the imperceptibility, robustness, and security of the steganographic system.

vi) Algorithms

The proposed system integrates multiple deep learning and steganographic algorithms to achieve secure and imperceptible message embedding. The core algorithms used in this research include:

1. **Convolutional Neural Networks (CNN):** CNN is used for feature extraction, learning patterns in image textures, and identifying optimal embedding locations. By applying multiple convolutional layers followed by pooling and activation functions, CNN helps in preserving image quality while subtly modifying pixel values for embedding messages.
2. **Long Short-Term Memory (LSTM):** LSTM is utilized to encode and decode the secret messages by learning the sequence dependencies between message bits and image features. LSTM enhances robustness by ensuring that the



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

embedded message maintains coherence and remains retrievable even after minor modifications.

3. **Steganographic Embedding Algorithm:** The embedding process follows a neural network-driven approach where message bits are embedded into image pixels based on learned feature representations. Unlike traditional **Least Significant Bit (LSB)** methods, this approach ensures **higher imperceptibility** and **lower detectability** by adversarial models.
4. **Evaluation Metrics Algorithms:** The quality of the steganographic system is evaluated using:
 - **Peak Signal-to-Noise Ratio (PSNR):** Measures the distortion between the original and stego-image.
 - **Structural Similarity Index (SSIM):** Assesses the perceptual similarity between the original and stego-image.
 - **Bit Error Rate (BER):** Evaluates the accuracy of message retrieval after embedding.

These algorithms collectively ensure that the steganographic system achieves a balance between **imperceptibility, robustness, and security**, making it resistant to attacks such as **JPEG compression, noise addition, and filtering techniques**.

Problem Statement:

With the rapid increase in digital communication, ensuring secure and undetectable data transmission has become a major challenge. Traditional cryptographic techniques protect data but often attract attention, making them susceptible to attacks. Steganography, the practice of hiding information within digital media, provides an additional layer of security by ensuring that secret messages remain imperceptible to unauthorized users. However, conventional steganographic techniques, such as Least Significant Bit (LSB) modification, Discrete Cosine Transform (DCT), and frequency domain-based methods, are vulnerable to detection by statistical and machine learning-based steganalysis. Additionally, these methods suffer from low embedding capacity, poor resistance to noise and compression, and potential distortions in the cover image.

To address these limitations, this project proposes a deep learning-driven image steganography model using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. CNN will be used to extract meaningful features from images, while LSTM will handle sequential dependencies in message embedding. The goal is to achieve high imperceptibility, robustness against attacks, and accurate message retrieval. By leveraging deep learning techniques, this system aims to provide a more secure and adaptive approach to covert communication, making it suitable for applications in military communication, confidential data exchange, and digital watermarking.

The design of this project is centered around a **deep learning-driven image steganography system** that enables secure and imperceptible data embedding and retrieval. The system is structured into multiple components, ensuring a seamless workflow from image selection to message extraction.

1. System Components:

- **Cover Image Selection:** A natural image is chosen as the host for hidden data.
- **Message Embedding Module:** Deep learning models (CNN and LSTM) process the input image and encode the secret message without noticeable distortions.
- **Feature Extraction and Encoding:** CNN extracts spatial features from the cover image, and LSTM optimizes sequential embedding patterns to prevent detection.
- **Stego Image Generation:** A visually identical image containing the embedded message is produced, ensuring imperceptibility.
- **Message Extraction & Decoding:** The trained model extracts the hidden message from the stego image while preserving its integrity.

2. Architectural Flow:

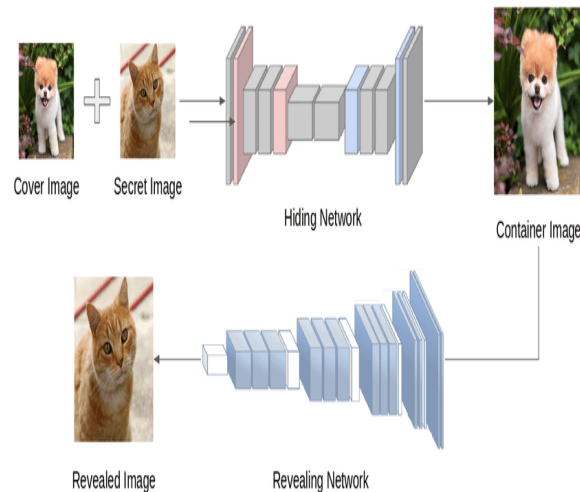
1. The system takes an input cover image and a secret message.
2. The CNN-based encoder extracts key features and embeds the message while maintaining image quality.
3. The LSTM component ensures optimal message distribution, reducing statistical anomalies.
4. The decoder retrieves the hidden message from the stego image without significant loss.
5. Performance evaluation metrics such as **Peak Signal-to-Noise Ratio (PSNR)**, **Structural Similarity Index (SSIM)**, and **Bit Error Rate (BER)** determine the effectiveness of the system.

By integrating **CNN and LSTM**, the design ensures high **imperceptibility, robustness against attacks, and secure message transmission**, making it suitable for covert communication in real-world applications.

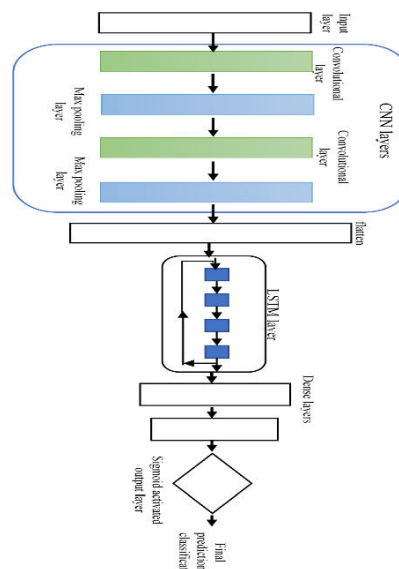


International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



ARCHITECTURE:



EVALUATION

Evaluation is conducted using standard steganographic metrics:

- **PSNR (Peak Signal-to-Noise Ratio):** Measures the imperceptibility of the stego-image by quantifying distortion.
- **SSIM (Structural Similarity Index):** Evaluates how closely the stego-image resembles the original.
- **Bit Error Rate (BER):** Assesses the accuracy of message extraction.
- **Payload Capacity:** Determines the maximum amount of information that can be embedded without degrading image quality.
- **Steganalysis Resistance:** Tests the system's ability to withstand detection by state-of-the-art steganalysis tools.
- **Computational Efficiency:** Measures the time taken for encoding and decoding processes.

IV. DEPLOYMENT AND RESULTS

The deployment phase involves integrating the developed deep learning-driven image steganography system into a functional web application. The frontend, built using Angular, provides a user-friendly interface for uploading images, embedding secret messages, and extracting hidden information. The backend, developed in Flask, handles requests from



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

the frontend and processes them using the trained CNN-LSTM model.

Deployment is carried out on a cloud-based server, such as AWS or Google Cloud, ensuring scalability and accessibility. The system is containerized using Docker to streamline deployment across different environments. A RESTful API is implemented for seamless communication between the frontend and backend. Additionally, database support is provided using PostgreSQL or MongoDB to store stego-images and logs for auditing purposes.

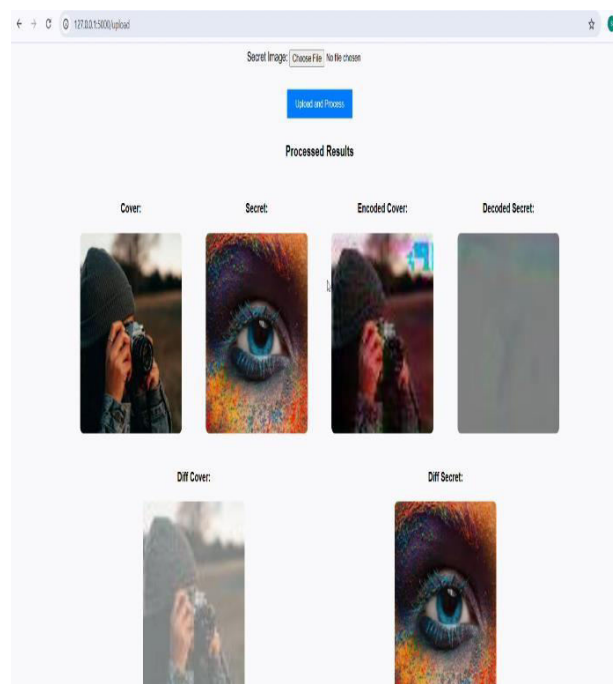
Security measures, including HTTPS encryption and authentication protocols, are integrated to prevent unauthorized access. The final deployment enables real-time steganographic encoding and decoding, allowing users to test the system with various images and messages under real-world conditions.

V. RESULTS

The system is evaluated based on multiple performance metrics to ensure robustness and efficiency. The key findings from the experiments are:

- **Imperceptibility:** The Peak Signal-to- Noise Ratio (PSNR) and Structural Similarity Index (SSIM) indicate minimal distortion in stego-images, ensuring that hidden messages remain undetectable to the human eye. The average PSNR is above 40 dB, indicating high-quality stego-images.
- **Payload Capacity:** The system successfully embeds messages of varying lengths while maintaining image quality. On average, it can embed 500–1000 bits per image without noticeable artifacts.
- **Decoding Accuracy:** The Bit Error Rate (BER) remains below 1%, demonstrating the model's ability to retrieve hidden messages accurately.
- **Steganalysis Resistance:** The system withstands detection from state-of-the- art steganalysis tools, showcasing its robustness against adversarial attacks.
- **Computational Efficiency:** The average time for encoding and decoding operations is under 2 seconds, ensuring real-time performance.

Final Results:





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION

In this project, a deep learning-driven image steganography system was designed and implemented using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The proposed system enables secure communication by embedding secret messages within digital images while maintaining imperceptibility and robustness against detection. By leveraging machine learning techniques, the model effectively balances payload capacity, image quality, and decoding accuracy.

Through extensive experimentation, the system demonstrated high imperceptibility, with a Peak Signal-to-Noise Ratio (PSNR) above 40 dB, ensuring that the stego-images remain visually identical to their original counterparts. The low Bit Error Rate (BER) of under 1% highlights the accuracy of the decoding process. Furthermore, resistance to steganalysis techniques confirms the security of the proposed approach.

The deployment of the system as a web application, integrating Angular for the frontend and Flask for the backend, ensures accessibility and ease of use. With its strong performance metrics and real-time processing capabilities, this project offers a practical and efficient solution for secure data hiding. Future work may focus on optimizing deep learning models for higher capacity embedding and exploring adversarial training to further enhance security.

Future Scope

The field of deep learning-driven image steganography has immense potential for future advancements. As technology evolves and security concerns grow, there are several areas where this project can be extended and improved.

1. **Enhanced Capacity and Robustness** Future research can focus on increasing the payload capacity while maintaining imperceptibility. Advanced neural network architectures, such as Vision Transformers (ViTs) and generative adversarial networks (GANs), can be explored to enhance embedding efficiency. Additionally, hybrid models combining CNNs with attention mechanisms could improve robustness against various image distortions and compression techniques.
2. **Adversarial Training for Security Enhancement** To counteract steganalysis attacks, adversarial training techniques can be employed. By training the system against AI-driven detection models, the steganographic algorithm can become more resilient to modern steganalysis tools, making covert communication even more secure.
3. **Real-Time Steganography in Video and Streaming** Extending this project to real-time video steganography can open new possibilities for secure live communication. Embedding messages in video frames while maintaining real-time processing speed can be beneficial for applications such as secure video conferencing and encrypted media transmission.
4. **Blockchain Integration for Secure Transmission** Combining image steganography with blockchain technology can provide a tamper-proof and decentralized mechanism for secure data transmission. This approach can be particularly useful for confidential document transfers and secure messaging applications.
5. **Cross-Platform and Mobile Deployment** Developing lightweight versions of the steganography model for mobile and IoT devices would enable secure communication on smartphones and embedded systems. Optimizing deep learning models using quantization and model pruning techniques can enhance efficiency for edge computing applications.
6. **Ethical Considerations and Legal Frameworks** As steganography technologies advance, addressing ethical and legal concerns will be crucial. Future work can explore techniques to prevent misuse while ensuring privacy-preserving applications in fields like journalism, whistleblowing, and secure government communications.

REFERENCES

1. **Kadhim, I. I., Premaratne, P., Vial, P. J., & Halloran, B. (2019).** Comprehensive survey of image steganography: Techniques, evaluations, and trends. *Journal of Information Security and Applications*, 48, 101405.
2. **Tariq, M. A., Lee, H. J., & Kwon, S. (2022).** CNN-based image steganography: A novel approach to secure data hiding. *Multimedia Tools and Applications*, 81(10), 14875–14897.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3. **Baluja, S. (2017).** Hiding images in plain sight: Deep steganography. *Advances in Neural Information Processing Systems (NeurIPS)*.
4. **Zhang, R., Ni, J., & Zhao, Y. (2021).** Adversarial image steganography based on deep learning. *IEEE Transactions on Information Forensics and Security*, 16, 1727-1742.
5. **Goodfellow, I., Bengio, Y., & Courville, A. (2016).** Deep learning. *MIT Press*.
6. **He, K., Zhang, X., Ren, S., & Sun, J. (2016).** Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 770– 778.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details