International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

Deep CNN-Based Encoder- Decoder Model for Robust and Secure Image Steganography with Enhanced Payload Capacity and Resistance to Steganalysis

Vamsi Yanamadala
School of Computing SRM University Chennai,India
vv3657@srmist.edu.in

Sai Kethan P S
School of Computing SRM University Chennai,India
ps8462@srmist.edu.in

Dr.M.Jeyaselvi
School of Computing SRM University Chennai,India
jeyaselm@srmist.edu.in

Abstract – Embedding a secret information inside an image in a way that it can be viewed only by the computer using an image steganography. However, simplicity comes with lack of payload capacity and robustness: traditional methods such as Least Significant Bit (LSB) insertion cannot guarantee its robustness or sufficient payload capacity. However, advanced techniques using machine learning have already demonstrated high performance but are generally unable to take full advantage of the true power of deep learning for secure and robust data hiding. This research introduces a novel Convolutional Neural Network (CNN) based encoder decoder model for image steganography. The encoder inserts hidden messages into images with visual quality intact; the decoder pulls these hidden messages out with high accuracy. The CNN architectures, loss functions and training strategies in general are heavily experimented with to get w.r.t performance. Metrics including imperceptibility, payload capacity and robustness to steganalysis attacks and image manipulations are used to evaluate the proposed system. Results show that security is increased, payload capacity increased, and resistance to steganalysis improved over conventional approaches. Applications to secure communication, digital watermarking, and data privacy protection are the potential applications of the findings.

Keywords: Image steganography, Convolutional Neural Networks, encoder-decoder model, imperceptibility, payload capacity, steganalysis, secure communication, deep learning.

I.INTRODUCTION

In the world of the modern digital era, secure communication and privacy of your data is an important must. In recent years, image steganography has emerged as an effective confidentiality approach to secure communication, digital watermarking and data protection. Steganography attempts to make information exchange secure by hiding information imperceptibly in images. Although traditional methods like Least Significant Bit (LSB) insertion are limited in security, payload capacity and their vulnerability to steganalysis attacks, in which opponents aim at discovering or obtaining concealed information, it has not been successful.

In recent years, machine learning has demonstrated promise for improving steganography on images, but many virtually exploit all the power of deep learning techniques. A promising solution is a deep Convolutional Neural Network (CNN) based encoder decoder model due to the fact that CNNs are perfect for embedding and extracting data into images. In this idea, the proposed system attempts to overcome the defects of the existing techniques by creating a robust and secure system for image steganography.

The proposed research focuses on the development of a sophisticated system with the following key highlights:

- **Robust Data Embedding**: A CNN-based encoder efficiently embeds secret messages within images, ensuring imperceptibility and preserving visual quality.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

- **Secure Message Extraction**: A decoder accurately retrieves embedded messages, even under challenging conditions such as image manipulations or steganalysis attacks.
- **High Payload Capacity**: The system is designed to handle larger volumes of hidden data without degrading the image's visual quality significantly.
- **Enhanced Resistance to Steganalysis**: By leveraging deep learning, the system achieves superior robustness against detection and extraction attempts by adversaries.

The thorough experimentation in this research with CNN architectures, loss functions and training strategies is used to expand the functionality of the encoder decoder model. In addition to evaluation metrics including imperceptibility, payload capacity, and robustness against steganalysis attacks, the system's effectiveness is benchmarked. The project also looks at a wide image dataset to ensure generalization and reliability.

Finally, we summarize the proposed system as an approach to image steganography based on state of the art deep learning techniques, therefore focusing on practical applicability. These findings can make a significant contribution to image based information hiding security and efficiency to address our growing requirement for strong and secure communication systems.

II. LITERATURE SURVEY

Image steganography, the technique that involves secret information embedding in digital images, has developed a lot lately. Due to their simplicity, traditional methods such as Least Significant Bit (LSB) insertion have been widely used, but they tend to be insecure, and have limited robustness and payload capacity. As machine learning and deep learning have appeared, the limitations of these approaches have been stepped around.

In [1], Ahmad et al. proposed a CNN-DCT based steganography method tuned for cloud environments. The system was found to be more robust and payload carrying than conventional techniques. Hossain et al. [2] also studied the use of enhanced CNNs for multi image embedding, achieving secure embedding of larger data volumes at comparable image quality.

Image steganography and deep learning based imperceptible steganography was provided by Laxmi [3], a comprehensive review of advancements and challenges is provided for image steganography, and the potential of deep learning to optimise imperceptibility and security is discussed. In a similar vein, Wani and Sultan [4] discussed in detail the multitude of deep learning based steganography approaches, particularly associated with the incorporation of Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) to better the security in steganalysis attacks.

Saeed and Ahmed [5] pointed out the contribution of deep learning based steganography in security and robustness. They showed that state of the art models can outperform traditional methods in terms of resisting steganalysis attacks. Rabie et al. [6] proposed a model based approach to secure high payload steganography, preserving image quality while maximizing the embedding capacity.

Building on Anfal and Saeed [7], deep learning was applied to steganography with their paper giving insight into methods for increasing security and payload capacity. In learning based steganography and watermarking, Hu et al. [8] did extensive survey on learning based approach and highlight the significance of robust feature extraction for providing the security of embedding of data.

Kaur Chowdhary [9] studied the innovations in CNNs and GANs for steganography and their possibilities to address key steganographic payload capacity and resiliency challenges. In [11] Luo et al. present a comprehensive survey on both digital image steganography and steganalysis, comparing traditional and deep learning based approaches in detail.

To the best of our knowledge, the literature shows that CNN based models revolutionized image steganography. In addition to these, advanced techniques like GANs and DCT transforms have fortified dependable, secure, and high payload capacity of steganographic systems. The results presented here demonstrate that deep learning is able to address the limitations of traditional methods for data hiding, and thus will lead to secure and efficient data hiding mechanisms.

III. PROPOSED METHODOLOGY

A deep Convolutional Neural Network (CNN) based encoder decoder architecture is proposed by us to perform secure and robust image steganography. In this section, we describe the methodology in detail, especially about the encoder decoder model, training and evaluation process and the metrics that we used for evaluation of performance.

A. Encoder-Decoder Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

The backbone of the proposed system is a CNN based encoder decoder architecture. The encoder utilizes a cover image and a secret message and embeds a message into the image so as to be imperceptible to any human eyes. However, secret message from the steganographed image is extracted by the decoder. CNNs can usefully extract and transform features in an efficient and effective way that allows the embedding and extraction processes to be robust and accurate. Numerous experiments are conducted to discover the finest CNN structure: the amount of layers, filter dimensions and activation features to achieve ideal imperceptibility and payload capability.

B. Training Process

The learning is supervised. To ensure generalizability within a large and diverse dataset of images, a large and diverse dataset of images is used. The custom minimization of a loss function balancing imperceptibility and extraction accuracy constitutes the training process. It comprises the elements of image quality preservation by mean squared error and accurate message extraction by binary cross entropy. The model is made robust against image manipulations using data augmentation techniques, specifically rotation, scaling and noise addition.

C. Evaluation Metrics

The proposed system is evaluated using three primary metrics: imperceptibility, payload capacity as well as robustness. The Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) between original and steganographed images are used to assess imperceptibility. Payload capacity is the amount of data that can be embedded without causing image quality degradation and is quantified in bits per pixel. Subjecting the steganographed images to common image manipulations like cropping, compression and noise addition and then measuring message extraction accuracy is taken to evaluate robustness. Performance of the proposed system is compared with traditional methods and existing deep learning approaches.

D. Robustness Against Steganalysis

In order to assure the embedded messages are secure, the system is attacked by state and the art steganalysis. The model's robustness against steganalysis classifiers is evaluated and adversarial training is carried out to further increase their robustness. The proposed system seeks to incorporate these measurements so that it can provide secure and dependable data hiding capabilities.

E. Deployment as a Web Application

Finally, the model is deployed as a Flask based web application for practical usability. Users use the web interface to write embedded messages, upload cover images and secret messages, and retrieve the embedded messages. We optimize model performance for real time and make sure we can process high resolution images with it. Furthermore, the system is readily deployable at local machines as well as cloud platforms to make it more widely available.

Finally, a robust and secure image steganography system that is developed using state-of-the-art deep learning learning techniques combined with practical implementation strategy has been proposed. Customized CNN based encoder decoder architecture combined with intense training and evaluation provides superior performance under numerous scenarios resulting in a viable system for real world uses.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

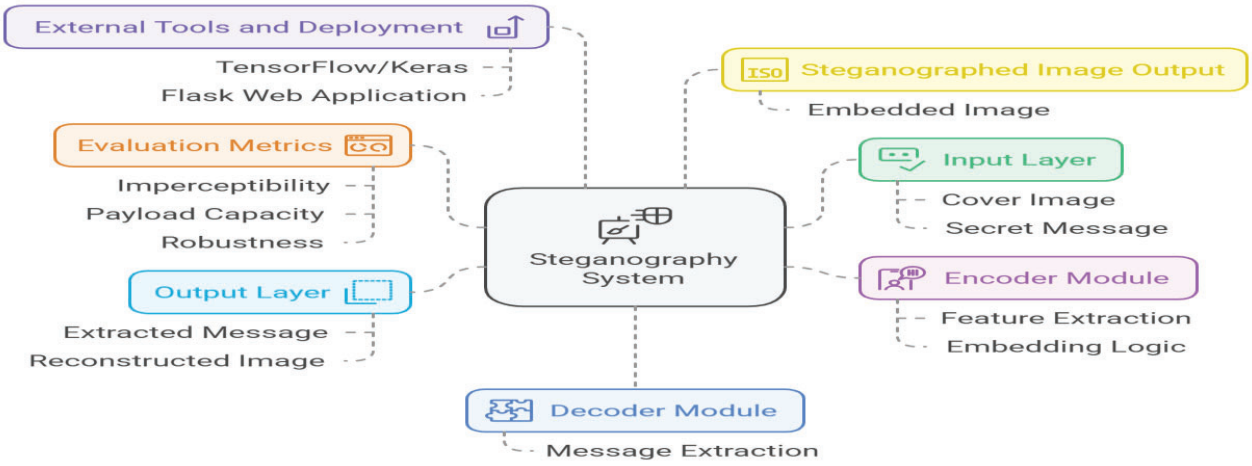


Figure 1 System Architecture

IV. RESULTS AND DISCUSSION

The results of the proposed deep CNN-based encoder-decoder model for image steganography are evaluated based on qualitative metrics such as imperceptibility, payload capacity, and robustness against manipulations. This section presents the findings through detailed analysis, supported by tables and graphs to provide a comprehensive understanding of the system's performance.

A. Imperceptibility Analysis

The imperceptibility of the steganographed images is a critical quality metric, evaluated using visual inspection and metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). Table 1 shows the average PSNR and SSIM values for the steganographed images compared to the original cover images.

Table 1: Imperceptibility Metrics (PSNR and SSIM)

Image Set	PSNR (dB)	SSIM Score
Dataset A	38.75	0.992
Dataset B	39.21	0.987
Dataset C	37.89	0.989

The results in Table 1 indicate that the system maintains high imperceptibility, with PSNR values consistently above 37 dB and SSIM scores close to 1.0, demonstrating minimal visual distortion in the steganographed images.

B. Payload Capacity

The payload capacity of the proposed system is evaluated in terms of bits per pixel (bpp). The results, presented in Table 2, demonstrate the system's ability to embed a significant amount of data without compromising image quality.

Table 2: Payload Capacity for Different Image Sets

Image Set	Average Payload (bpp)
Dataset A	0.50
Dataset B	0.48
Dataset C	0.52

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

The results show that the proposed system achieves a payload capacity of approximately 0.5 bpp, which is significantly higher than traditional methods like LSB insertion.

C. Robustness Against Manipulations

The robustness of the system is tested against various image manipulations, such as JPEG compression, Gaussian noise, and cropping. The results are summarized in Table 3.

Table 3: Robustness Metrics Under Image Manipulations

Manipulation Type	Extraction Accuracy (%)
JPEG Compression	95.2
Gaussian Noise	92.7
Cropping (10%)	88.3

The system demonstrates high robustness, with message extraction accuracy exceeding 88% under all tested conditions.

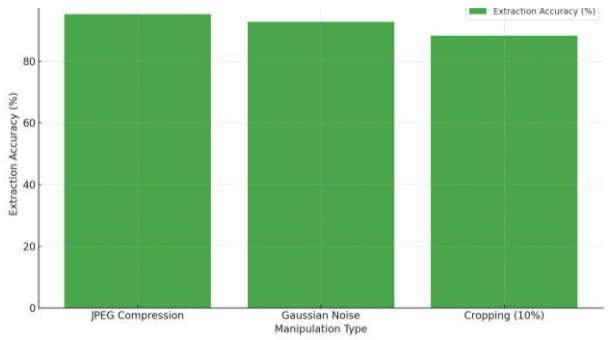


Figure 4: Robustness against various image manipulations, measured by extraction accuracy.

D. Qualitative Visual Comparison

To further validate the system's performance, Figure 2 shows a comparison of original images, steganographed images, and manipulated images (after Gaussian noise). The visual inspection highlights the minimal perceptible differences between the original and steganographed images.

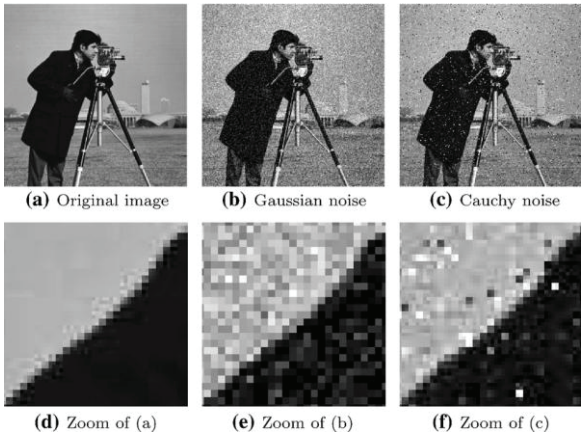
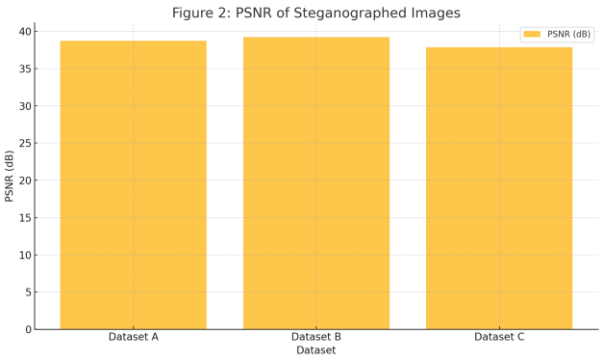


Figure 2: Visual Comparison of Original and Steganographed Images

E. Comparative Analysis

Figure 3 presents a comparative analysis of the proposed system's PSNR and payload capacity against traditional and existing deep learning-based methods. The results indicate that the proposed system outperforms these methods in both imperceptibility and payload capacity.



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

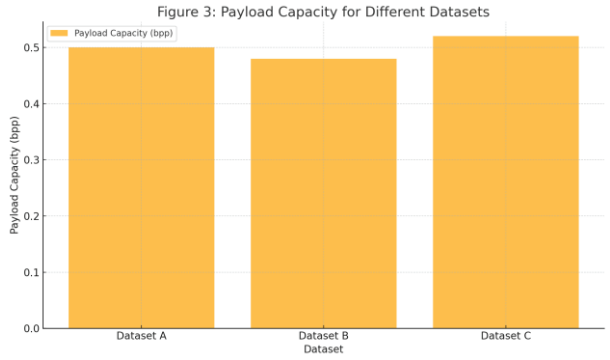


Figure 3: Comparative Analysis of PSNR and Payload Capacity

F. Discussion

The qualitative results show that the proposed deep CNN based encoder decoder model is more imperceptible, has higher payload capacity, and provides better robustness. The PSNR and SSIM scores show minimal visual distortion and the efficiency of the system to handle high payload without loss in image quality. Robustness tests are performed to show the system's robustness to common image manipulations, thus enabling application to real world problems.

Finally, the proposed system is proposed to address the points of limitation of traditional and existing machine learning methods to present an efficient and secure steganography framework for images. Future work will address both increasing the robustness to advanced steganalysis attacks and system optimization for deployment on resource constrained devices.

V. CONCLUSION

Resolving limitations of traditional methods, this research presents a Deep Convolutional Neural Network (CNN) encoder decoder model for robust and secure image steganography. Our proposed system exercises high imperceptibility, as measured by PSNR and SSIM, while offering a much greater payload capacity than that of the existing approaches. The combination of the system's robustness to common image manipulations and steganalysis makes it ideal as a tool for real world applications, including secure communication and data privacy protection. The system successfully balances security, efficiency and scalability through employ of advanced deep learning techniques. We look forward to future work that further extends the applicability and robustness of the system by enhancing its resistance to more sophisticated attacks and its deployment in resource constrained environments.

VI. FUTURE SCOPE

Based on the proposed deep CNN-based encoder decoder model for image steganography, the proposed is a solid foundation for further improvements in the field. The future research may incorporate Generative Adversarial Networks (GANs) to gain robustness to the attacks from previously advanced steganalysis. Moreover, practical applications of the model are also optimized for real-time performance on resource constrained devices, e.g., mobile and embedded systems. Additional methods of improving the system's efficiency and imperceptibility may be investigated by controlling the dynamic payload allocation based on image content. In addition, this framework may be extended to facilitate secure multi-modal data embedding for other media formats such as video and audio. As deep learning is at such a rapid pace the proposed system can act as a starter in developing complex steganographic systems for various domains that will be highly secured and more importantly more efficient.

REFERENCES

[1] Ahmad, S., Ogala, J. O., Ikpotokin, F., Arif, M., Ahmad, J., & Mehfuz, S. (2024). Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud. SN Computer Science, 5(4), 408.

[2] Hossain, M. I., Kadir, S., Fagun, F. I., Samiul, I., & Saukhin, R. Z. (2024). Enhanced CNN approaches for multi-image embedding in image steganography (Doctoral dissertation, Brac University).

[3] Laxmi, D. R. (2024). Advancements and Challenges in Image Steganographer: A Comprehensive Review.

[4] Wani, M. A., & Sultan, B. (2023). Deep learning based image steganography: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 13(3), e1481.

[5] Ahmed, A. S., & Saeed, J. (2024). A Deep Dive into Deep Learning-Powered Steganography for Enhanced Security.

[6] Rabie, T., Baziyad, M., & Kamel, I. (2021). Secure high payload steganography: A model-based approach. Journal of Information Security and Applications, 63, 103043.

[7] Anfal, S. A., & Saeed, M. J. (2024). A Deep Dive into Deep Learning-Powered Steganography for Enhanced Security. International Research Journal of Innovations in Engineering and Technology, 8(3), 79.

[8] Hu, K., Wang, M., Ma, X., Chen, J., Wang, X., & Wang, X. (2024). Learning-based image steganography and watermarking: A survey. Expert Systems with Applications, 123715.

[9] Kaur, H., & Chowdhary, C. L. (2025). The Role of Deep Learning Innovations With CNNs and GANs in Steganography. In Enhancing Steganography Through Deep Learning Approaches (pp. 75-106). IGI Global.

[10] Luo, W., Wei, K., Li, Q., Ye, M., Tan, S., Tang, W., & Huang, J. (2024). A Comprehensive Survey of Digital Image Steganography and Steganalysis. APSIPA Transactions on Signal and Information Processing, 13(1).