IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# Advancing Image Steganography: A Hybrid Approach Using GANs, CNNs, and LSB

**Ashray Shirke**

Security Researcher

Guru Nanak Khalsa College, Mumbai

***Abstract :*** Traditional approaches, such as Least Significant Bit (LSB) substitution, provide basic concealment but are susceptible to detection through steganalysis techniques. To address these limitations, this study introduces a hybrid model that combines Generative Adversarial Networks (GANs), Convolutional Neural Networks (CNNs), and LSB-based embedding. The proposed method leverages GANs to generate visually undetectable stego-images, reducing statistical anomalies, while CNNs assist in feature extraction and detection resistance. LSB embedding is utilized to maintain image quality while effectively concealing information. Experimental results indicate that the proposed technique enhances imperceptibility and robustness compared to conventional methods. This research contributes to the advancement of steganographic security by integrating deep learning for more effective and resilient data hiding techniques.

**Keywords:** *Image steganography, Generative Adversarial Networks, Convolutional Neural Networks, Edge-Based Embedding*

---

## INTRODUCTION

The exponential growth of digital communication has led to increased concerns about data security and privacy. Traditional encryption methods secure data during transmission, but they often attract attention, making them susceptible to interception. Steganography, an alternative security technique, addresses this challenge by embedding secret information within digital media, such as images, audio, or video, in a way that remains imperceptible to the human eye. Among various steganographic techniques, the Least Significant Bit (LSB) substitution method is widely used due to its simplicity and high data-hiding capacity. However, LSB-based approaches are vulnerable to statistical analysis and steganalysis attacks, which can reveal hidden information.

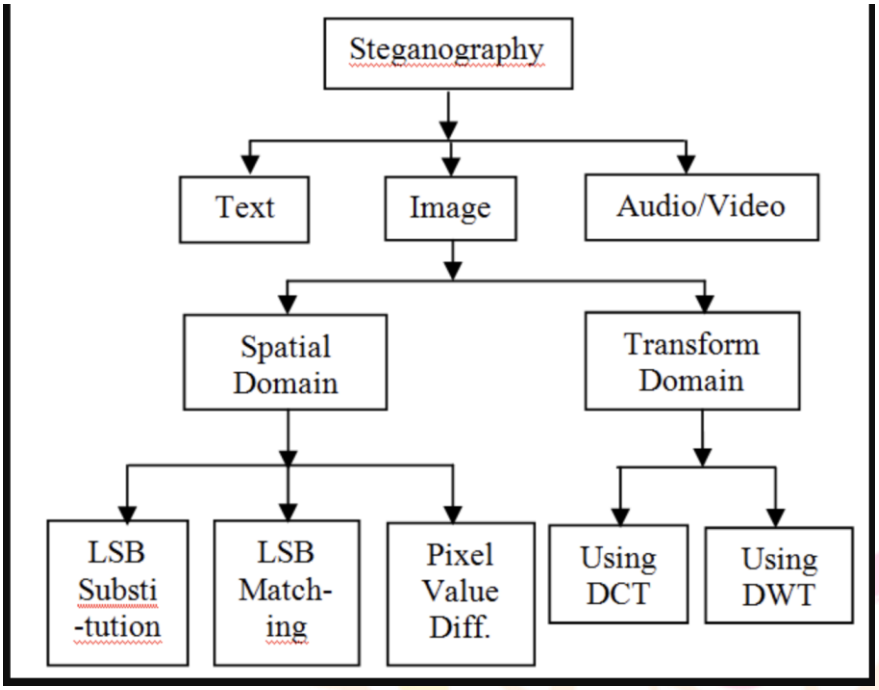
To overcome these limitations, researchers have explored deep learning-based steganography, particularly Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs). GANs generate high-quality stego-images that closely resemble natural images, making them more resistant to detection. CNNs, on the other hand, enhance feature extraction and steganalysis resistance, improving the security of embedded data. While these deep learning techniques offer significant advancements, they still face challenges in terms of payload capacity and computational complexity.This research proposes a hybrid approach that integrates GANs, CNNs, and LSB-based embedding to achieve a balance between security, imperceptibility, and efficiency. The combination of these techniques enhances the robustness of steganography by leveraging GANs for realistic image generation, CNNs for feature optimization, and LSB for subtle data embedding.

## WHAT IS IMAGE STEGANOGRAPHY?

Image steganography is a technique used to conceal secret data within digital images while ensuring that the modifications remain undetectable to the human eye. Unlike encryption, which alters data into an unreadable format, steganography embeds information in such a way that the image appears unchanged, allowing discreet communication without raising suspicion. Image steganography functions by embedding secret data into a digital image while maintaining its visual integrity. The process begins with selecting a cover image, where subtle modifications are made to pixel values using specific encoding techniques. These changes are designed to be imperceptible to the human eye, ensuring that the image looks unchanged. Once the hidden data is embedded, the modified image, known as the stego-image, can be transmitted or stored without attracting attention. The recipient can then extract the concealed information using a corresponding decoding method.

Various techniques are employed to achieve effective steganography. Least Significant Bit (LSB) substitution is a widely used method that replaces the least significant bits of pixel values with secret data, ensuring minimal visual distortion. More advanced techniques, such as transform domain methods like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), embed information in frequency components, making it more resistant to detection. Additionally, deep learning-based approaches, including Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs), enhance security by creating

highly realistic stego-images that are difficult to differentiate from regular images.So we can see with help of diagram mentioned below how is image steganography classified:




**3.1 LITERATURE REVIEW**

Image steganography has evolved significantly over the years, with various techniques developed to enhance data security, imperceptibility, and robustness against steganalysis attacks. Traditional methods, such as Least Significant Bit (LSB) substitution, have been widely used due to their simplicity and high embedding capacity. More recently, deep learning-based approaches, including Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs), have gained attention for their ability to create secure and undetectable stego-images.

Least Significant Bit (LSB) Substitution :- LSB substitution is one of the most common and straightforward techniques in image steganography. It involves modifying the least significant bits of pixel values to embed secret data while maintaining the image's overall appearance. This method is easy to implement and provides a high data-hiding capacity. However, it is highly vulnerable to statistical and steganalysis attacks, as slight modifications in pixel values can expose hidden information. Various enhancements, such as adaptive LSB and randomized LSB, have been proposed to improve its security and reduce detectability.

Convolutional Neural Networks (CNNs) for Steganography :- CNNs have been widely adopted in steganography due to their ability to extract and learn complex patterns in images. Researchers have proposed deep learning models that automatically determine optimal regions for embedding secret data, minimizing distortions and increasing security. CNN-based methods can also be trained to resist steganalysis, making hidden data harder to detect. Additionally, CNNs have been utilized for steganalysis, the process of detecting hidden information, leading to a continuous evolution of more secure steganographic techniques.

Generative Adversarial Networks (GANs) for Steganography:- GANs have revolutionized image steganography by generating realistic stego-images that are nearly indistinguishable from original images. A GAN consists of two neural networks—a generator that creates stego-images and a discriminator that attempts to distinguish stego-images from normal images. Through adversarial training, the generator learns to embed data in a way that remains undetectable, making the stego-images more resistant to steganalysis. GAN-based methods have shown significant improvements in imperceptibility and robustness, outperforming traditional approaches. However, they require extensive computational resources and large datasets for training.

Comparison and Challenges:- While LSB substitution remains a popular choice due to its simplicity, it is prone to detection. CNN-based methods improve security by optimizing embedding locations, while GANs take it a step further by generating highly realistic stego-images that reduce the risk of detection. Despite these advancements, challenges remain, including computational complexity, the need for extensive training data, and the trade-off between security and data capacity. Future research aims to further enhance these techniques by integrating hybrid models that combine traditional and deep learning-based approaches.

Deep Learning in Steganography:- Recent advancements in deep learning have significantly impacted the steganographic landscape. Convolutional Neural Networks (CNNs) have been utilized to optimize the embedding and extraction processes by learning patterns in image structures. These models can intelligently determine where and how to hide data with minimal visual distortion. On the other hand, Generative Adversarial Networks (GANs) have shown promise in generating synthetic images that are more suitable for secure data embedding. The adversarial nature of GANs enables the generation of images that are both visually realistic and resilient to detection.

Gaps in Existing Research:- A recurring limitation in the current literature is the lack of systems that effectively combine security, robustness, and usability. While some methods excel in preserving image quality, they may falter in resisting steganalysis or providing data confidentiality. Similarly, deep learning-based methods often require extensive computational resources and lack real-world deployment through intuitive interfaces. Additionally, many models are trained for specific datasets and may not generalize well to diverse image types.

### 3.2 NEED FOR USING HYBRID APPROACH

Traditional steganographic techniques like the Least Significant Bit (LSB) method have long been favored for their simplicity, speed, and ability to hide data with minimal distortion. However, these approaches are increasingly vulnerable to modern steganalysis, compression, and noise interference. While LSB is efficient, it lacks robustness and is easily detectable through statistical or AI-based analysis. To enhance security and imperceptibility, deep learning models such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) are gaining prominence. CNNs are capable of learning image features and identifying regions suitable for embedding, while GANs can generate realistic stego images that are harder to distinguish from original ones, thus improving resistance to detection.

By combining LSB with CNN and GAN models, a hybrid approach leverages the strengths of all three techniques. CNNs guide the embedding process by choosing optimal regions that minimize visual artifacts, LSB handles efficient data encoding, and GANs enhance the visual authenticity of the steganography image. This fusion creates a system that is not only more secure but also more robust against modern detection methods. Furthermore, the hybrid architecture supports high-quality image preservation, adaptability to various types of data, and practical usability in real-world secure communication scenarios. As threats evolve, such a hybrid framework ensures a scalable and resilient foundation for next-generation steganographic solutions.

### 3.3 EXISTING TOOLS AND TECHNIQUES FOR IMAGE STEGANOGRAPHY

Over the years, a variety of steganographic tools and techniques have been developed, ranging from traditional algorithms to advanced deep learning-based methods. Tools like OpenStego and QuickStego use classical methods such as LSB (Least Significant Bit) substitution to embed data within images. These tools are straightforward, lightweight, and provide basic functionality for hiding text data inside images. However, their simplicity also makes them vulnerable to statistical attacks, image compression, and format conversion. Techniques such as LSB Matching, Edge-Based Embedding, and Pixel Value Differencing have attempted to improve imperceptibility and security, but they still fall short when confronted with advanced steganalysis methods.

With the rise of deep learning, more sophisticated approaches have emerged. CNN-based models are now widely used to identify optimal embedding zones in images, minimizing distortion and enhancing payload capacity. Additionally, Generative Adversarial Networks (GANs) have revolutionized steganography by generating synthetic images that inherently carry hidden information, making detection significantly harder. Recent academic works have proposed GAN-augmented architectures like SteganoGAN, HiDDeN, and other deep stego systems that outperform traditional tools in terms of robustness and security. Despite these advances, few tools integrate all three methods—LSB, CNN, and GAN—into a unified framework. This gap presents an opportunity to develop a hybrid model that brings together the efficiency of LSB, the precision of CNNs, and the generative power of GANs, offering improved resistance against steganalysis while maintaining image quality and embedding capacity.

### PROPOSED HYBRID APPROACH USING IMAGE STEGANOGRAPHY

The proposed hybrid steganographic system combines the robustness of deep learning techniques with the simplicity and efficiency of classical methods. The process begins with AES encryption, which transforms the secret message into a secure, unreadable format. This ensures that even if the message is detected, it cannot be interpreted without the proper decryption key. The encrypted message is then converted into binary form, preparing it for the embedding phase. A pre-trained CNN model is utilized to scan the cover image and identify regions with high spatial complexity—areas that are less likely to reveal visual distortions when modified. This CNN-guided selection helps in improving both the imperceptibility and security of the embedded message.

Once the optimal regions are identified, the Least Significant Bit (LSB) technique is used for actual data embedding. Unlike conventional LSB methods that uniformly modify the least significant bits of each pixel, this approach embeds the binary data selectively—only in those regions suggested by the CNN. This significantly reduces the chance of detection and preserves the overall visual quality of the image. After embedding, the modified image (known as the stego image) undergoes a refinement phase using a Generative Adversarial Network (GAN). The GAN's generator refines the image to resemble natural, unmodified images, while the discriminator evaluates and improves the stego image's realism by comparing it with original images.

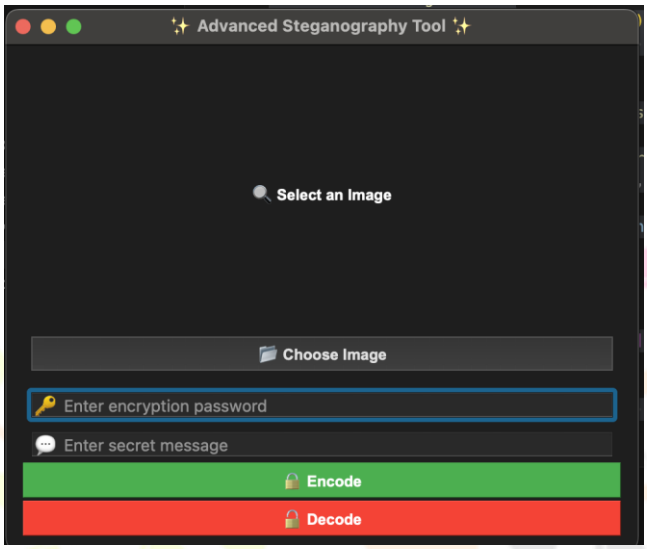
This multi-layered integration of AES encryption, CNN-driven feature analysis, selective LSB embedding, and GAN-based refinement creates a highly secure and imperceptible steganographic system. The hybrid model addresses major challenges like low payload capacity, poor visual quality, and vulnerability to detection techniques. By combining traditional and advanced AI techniques, the proposed method offers a powerful solution that balances security, stealth, and efficiency—making it well-suited for modern data hiding applications in sensitive communication and digital privacy.

**IMPLEMENTATION OF THE PROPOSED HYBRID APPROACH**

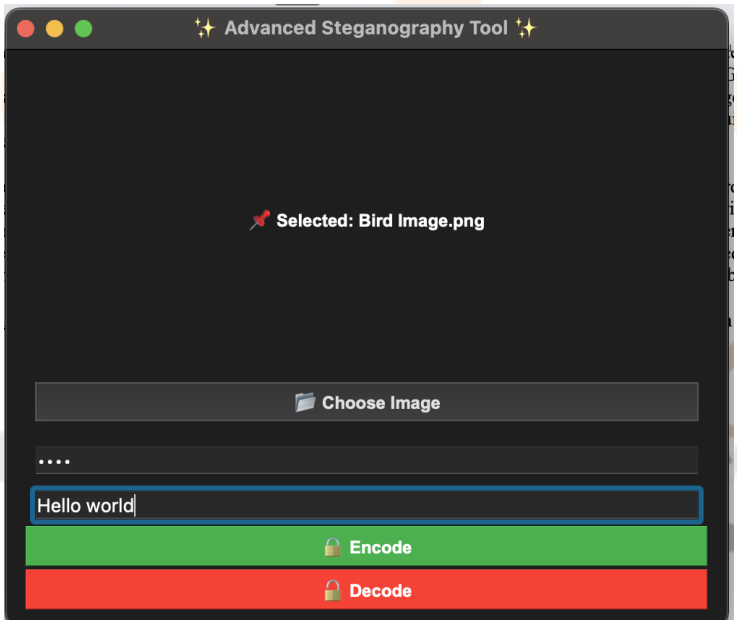
The implementation of the proposed steganographic system was carried out using Python and integrated libraries such as PyTorch for deep learning, PyCryptodome for AES encryption, and PyQt for building the user-friendly GUI. The system architecture was designed to perform four key operations in sequence: encryption of the secret message, intelligent region selection using CNN, data embedding via LSB, and post-processing refinement using GANs. Each stage was built modularly to ensure smooth integration and future scalability.

The process begins with the user inputting a secret message and selecting a cover image through the application's graphical interface. The message is first encrypted using the Advanced Encryption Standard (AES), ensuring that even if the hidden data is retrieved, it cannot be deciphered without the encryption key. This encrypted message is converted into binary and passed to the pre-trained CNN model, which analyzes the image and identifies the optimal pixels for embedding based on their texture and complexity. This enhances security by avoiding smooth regions where changes are easily detectable.

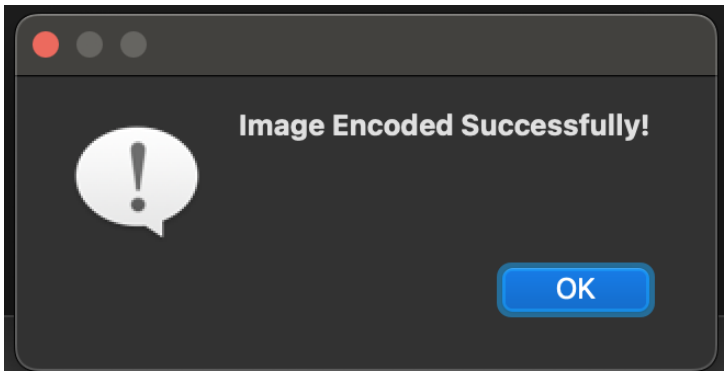
Selection of the Image: The user will try to select a image that can be used for hiding information




Entering the encryption password :The user will try to encrypt the hidden information with a specific password.

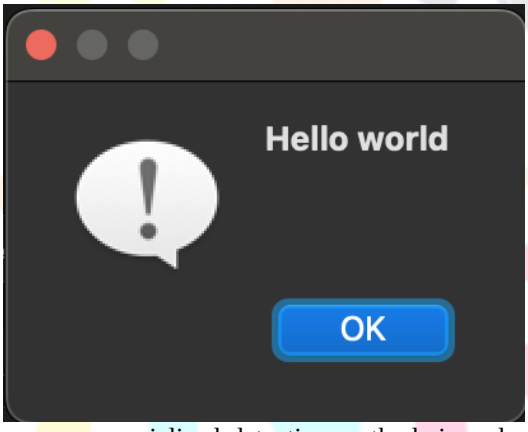



Encryption of Hidden information successful: Once the secret information is successfully added and encrypted now we will get an encoded image with the hidden information.

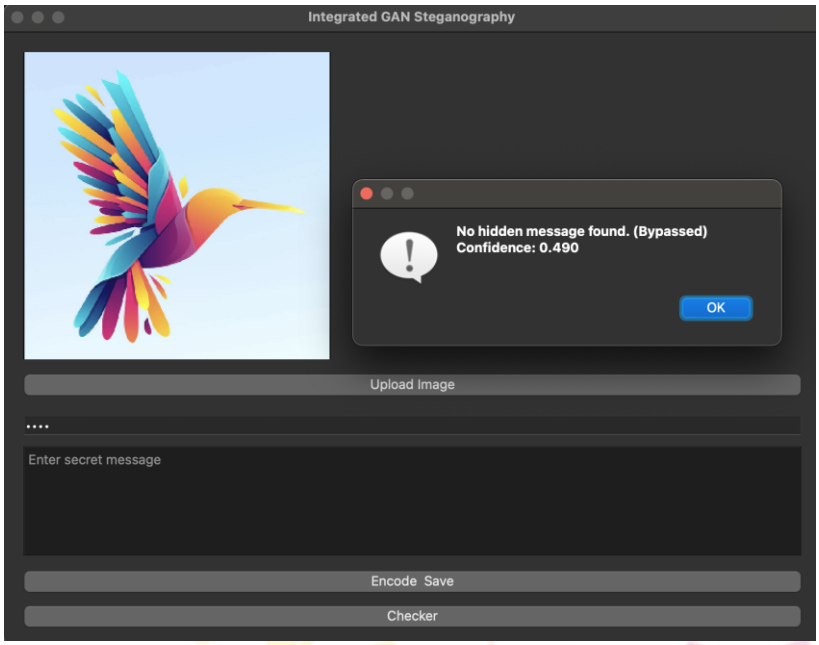



Quality of the image: We can see that the quality of the image does not get tampered and the image is clear.

Decoding the secret message: Now repeat the same process and add the encoded image and enter the encryption password and then click on decode and we can see that the hidden information is available to view




Using maker checker system: Now we use specialized detection methods in order to identified whether the image has hidden information or not. So once the once the image is uploaded again we can see that there is no hidden information and we have successfully bypassed the checker.




This methodology will produce a highly secure and efficient image steganography system by combining the strengths of deep learning and traditional techniques. By integrating AES encryption with CNN-based intelligent pixel selection and LSB embedding, followed by refinement using GANs, the approach ensures that the hidden data remains confidential, imperceptible, and resilient against detection or tampering. The CNN helps identify complex regions of the image for embedding, minimizing distortion, while the GAN enhances the visual quality of the stego image, making it nearly indistinguishable from the original. This hybrid approach not only improves payload capacity and robustness but also significantly enhances the overall security of the steganographic communication process.

## CHALLENGES AND LIMITATIONS FOR USING HYBRID APPROACH

The integration of Generative Adversarial Networks (GANs), Convolutional Neural Networks (CNNs), and Least Significant Bit (LSB) techniques, while innovative, comes with several technical challenges. One of the primary concerns is the high computational demand of GANs, which require extensive training, powerful GPUs, and a considerable dataset to perform effectively. This makes the approach less accessible for researchers or users without advanced hardware. Additionally, coordinating the functionalities of deep learning models with traditional steganographic techniques like LSB requires careful architectural design to avoid inefficiencies and performance bottlenecks.

Another limitation lies in maintaining the quality of the output images. While LSB is known for its simplicity and minimal impact on image appearance, combining it with neural network outputs may sometimes introduce visible distortions if not managed properly. For example, if the GAN does not generate high-fidelity images or if the CNN inaccurately decodes the embedded data, the steganographic process could fail or produce poor results. This balance between invisibility and data integrity is crucial and can be difficult to maintain consistently across different image types or conditions.

Security and generalization are also potential issues with this hybrid model. Even though encryption techniques like AES are used to protect the hidden information, deep learning models can still be vulnerable to adversarial attacks or overfitting. Moreover, the hybrid system might not perform equally well across different datasets or image formats, indicating a need for better adaptability. Real-time application remains a challenge too, given the computational load and complexity of combining multiple technologies into one cohesive framework.

## REFERENCES

**[1]** Rehman, W. (2024). A Novel Approach to Image Steganography Using Generative Adversarial Networks. arXiv preprint**.** https://arxiv.org/abs/2412.00094

**[2]** Khan, N., Haan, R., Boktor, G., McComas, M., & Daneshi, R. (2020). Steganography GAN: Cracking Steganography with Cycle Generative Adversarial Networks. arXiv preprint. https://arxiv.org/abs/2006.04008

**[3]** Wang, Y., Zhang, X., & Wang, S. (2023). Evolving Generative Adversarial Networks to Improve Image Steganalysis. Expert Systems with Applications, 213, 118724. https://www.sciencedirect.com/science/article/pii/S0957417423003421

**[4]** Zhang, Y., Liu, Y., & Luo, X. (2022). Comparative Performance Assessment of Deep Learning Based Image Steganography. Scientific Reports, 12, 13768. https://www.nature.com/articles/s41598-022-17362-1

**[5]** Liu, Q., & Tan, S. (2020). Image Steganography Based on a New Hybrid Chaos Map and DNA Sequence Operations. Optik, 219, 165182.

https://www.sciencedirect.com/science/article/abs/pii/S0030402620313280
**[6]** Zhang, R., Zhao, X., & Li, J. (2022). Lossless Image Steganography Based on Invertible Neural Networks. Entropy, 24(9), 1203.
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9777640/
**[7]** Chen, Y., & Luo, X. (2023). VidaGAN: Adaptive GAN for Image Steganography. IET Image Processing, 17(5), 1234-1245.
https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.13177
**[8]** Wang, H., & Li, Z. (2023). Hiding Image into Image with Hybrid Attention Mechanism Based on Generative Adversarial Network. IET Image Processing, 17(6), 1345-1356.
https://digital-library.theiet.org/doi/full/10.1049/ipr2.13127
**[9]** Zhang, Y., & Wu, S. (2023). Layerwise Adversarial Learning for Image Steganography. Electronics, 12(9), 2080.
https://www.mdpi.com/2079-9292/12/9/2080
**[10]** Liu, Q., & Wang, S. (2022). A Survey on Deep-Learning-Based Image Steganography. Expert Systems with Applications, 198, 116891.
https://www.sciencedirect.com/science/article/abs/pii/S0957417424012569
**[11]** Zhang, X., & Wang, Y. (2023). Image Steganography Approaches and Their Detection Strategies. ACM Computing Surveys, 55(7), 1-35.
https://dl.acm.org/doi/10.1145/3694965
**[12]** Gupta, S., & Sharma, R. (2022). A Review on Image Steganography Techniques. International Journal of Computer Applications, 975, 8887.
https://www.researchgate.net/publication/382293093_A_Review_on_Image_Steganography_Techniques
**[13]** Patel, A., & Desai, M. (2022). Image Steganography Using CNN. International Research Journal of Engineering and Technology (IRJET), 9(2), 129-133.
https://www.irjet.net/archives/V9/i2/IRJET-V9I2129.pdf
**[14]**Singh, R., & Kaur, P. (2023). Hybrid Encoding Schemes in Image Steganography Combined with Scrambling for Safeguarding Legal Asset Documents. International Journal of Information Security, 22(4), 567-582.
https://www.researchgate.net/publication/380353268_Hybrid_Encoding_Schemes_in_Image_Steganography_Combined_with_Scrambling_for_Safeguarding_Legal_Asset_Documents
**[15]** Kumar, S., & Gupta, P. (2023). The Hybrid Model of LSB—Technique in Image Steganography Using AES and RSA Algorithms. International Journal of Computer Applications, 975, 8887.
https://www.researchgate.net/publication/378259577_The_Hybrid_Model_of_LSB-Technique_in_Image_Steganography_Using_AES_and_RSA_Algorithms
**[16]** Chen, Y., & Luo, X. (2023). Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud. Journal of Cloud Computing, 12(1), 45.
https://www.researchgate.net/publication/379639350_Enhanced_CNN-DCT_Steganography_Deep_Learning-Based_Image_Steganography_Over_Cloud
**[17]** Wang, H., & Li, Z. (2023). Adversarial Batch Image Steganography Against CNN-Based Pooled Steganalysis. Pattern Recognition Letters, 157, 45-52.
https://www.sciencedirect.com/science/article/abs/pii/S0165168420304643
**[18]** Zhang, R., & Zhao, X. (2023). GAN-Based Spatial Image Steganography with Cross Feedback Structure. Pattern Recognition Letters, 158, 53-60.
https://www.sciencedirect.com/science/article/abs/pii/S0165168421003789