

Stegovision: AI-Based Hidden Data Transmission Using Multimedia File

Dr. P Thamarai

Assistant Professor

Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selaiyur, Tambaram
Chennai- 600073, Tamil Nadu.
thamarai.cse@bharathuniv.ac.in

T Sai Krishna

CSE dept

Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selaiyur, Tambaram
Chennai- 600073, Tamil Nadu.
dagadsai19149@gmail.com

Seelam Pavan Kumar

CSE dept

Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selaiyur, Tambaram
Chennai- 600073, Tamil Nadu.
seelampavwankumar287@gmail.com

Vadapalli Sathish

CSE dept

Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selaiyur, Tambaram
Chennai- 600073, Tamil Nadu.
sathishvadapalli29@gmail.com

Puli Charan Kumar Reddy

CSE dept

Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selaiyur, Tambaram
Chennai- 600073, Tamil Nadu.
charanreddyp2003@gmail.com

ABSTRACT

As technology advances through the growth of digital communication networks, chances of cyberattacks, hacking, and data breach have increased beyond imagination. At present, while the necessity of encrypting data cannot be undermined, it becomes extremely important to conceal even the existence of the communication process. While cryptography could be used to secure the communication processes in question from the prying eyes of outsiders in the sense that all communication is encrypted, there could be chances of compromising the safety of the sender himself since his identity would be revealed in the entire process. Keeping in mind such a scenario, this study brings forth a framework that utilizes AI for multimedia steganography purposes. The secret messages in this case are concealed into images, videos, and audio files.

Contrary to traditional ways of doing multimedia steganography, which evenly spreads the secret information across all sections of the media file, this method employs AI to identify media sections which have complicated textures or natural distortions or noise and then embeds the data inside the identified sections. In doing so, the method helps limit any further distortions of the media file as well as increase the complexity in statistical detection of the data embedded within the host file. Before the embedding process, the secret message is encoded into bits, which may be encrypted if necessary, to avoid any modifications of the information should anyone succeed in decrypting the data.

On the other hand, the extraction process consists of extracting and decoding the embedded data from the host media file with minimal distortion of the host file. Various experimental investigations have indicated that this approach results in lower distortion rates, high hiding capabilities, reliable data decoding process as well as good audiovisual qualities of the generated output files. Therefore, this approach can be applied in applications like defence, business security, digital watermarking, and internet of things (IoT).

INTRODUCTION

Current technological advancements concerning the development of digital technology, the Internet, and communication methods have brought about changes in the way of creation, transfer, and storage of data. Unfortunately, cybersecurity issues have become widespread, where hacking and leaking information are among the most common. Therefore, the protection of the information during its transfer should be considered an important issue not only by private persons but also by companies and governments. The classical method of securing sensitive information presupposes encryption. Yet, even in such cases, any message will be spotted, as the very fact that two parties exchange information increases the risk of data leakage and decoding. Steganography means hiding information within common files, such as pictures, music tracks, or videos. In this regard, the technology differs from encryption because, instead of encryption, it means concealing of the information. As follows from the general principle, a regular picture, music track, or video serves as the cover file for hiding sensitive data to make a stego file look almost indistinguishable from the cover one.

Usually, spatial domain embedding schemes such as least significant bit replacement are applied for data hiding purposes. This technique for embedding data is easy to implement; however, it may result in poor quality media if too much data is hidden within the media. In addition, any alteration made to the file can be detected by attackers using statistical techniques and steganalysis algorithms because any slight alteration in the file will be easily noticed by attackers.

There have been several chances to enhance the process of steganography through the use of artificial intelligence. The first way in which AI can be useful in this case is by helping in identifying spots where embedding the secret message would be difficult to detect.

For the purpose of this research, a new approach has been proposed for hiding and sending messages with the help of artificial intelligence. In the proposed technique, there will be the use of steganography and intelligent region selection for making sure that the process of communication is safe and

discreet. For starters, the message to be sent will be converted into binary form. Afterward, this message will be hidden in certain intelligent regions of the cover medium. The process of extracting information from the cover medium will be done with the help of AI.

LITERATURE SURVEY

The area of data concealment and steganography has seen many improvements along with the evolution of digital image processing and artificial intelligence. Traditional methods were primarily spatial domain based, but recently there is the trend of employing transform-domain-based and deep learning algorithms.

In their study, Fan et al. (2023) presented a scheme for adversarial steganography using joint distortion optimization. The method employed LSB substitution with distortion control to avoid visual distortions to the cover image. Even though the method was very simple, it did not achieve good levels of invisibility as well since it is highly vulnerable to complex steganalysis methods due to its predictable patterns.

Agarwal et al. (2023) described Hypersteg, a deep learning architecture that utilizes hyperbolic representation learning. The algorithm allowed concealing more data while preserving visual qualities at a satisfactory level. Since neural networks were employed, the system would learn appropriate strategies. However, the method needed high amounts of computation power and time-consuming training.

Han et al. (2023) presented cross-modal steganographic algorithm that utilizes neural representations to embed data in heterogeneous media. The proposed technology provided enhanced flexibility and concealment capabilities by hiding data in high-dimensional feature spaces rather than manipulating pixels. However, some statistical measures turned out to be capable of detecting deviations under certain circumstances despite those advantages of the cross-modal algorithm.

The recent developments in the field of generative steganography include the application of Generative Adversarial Networks (GANs) to generate stego media with natural-like distribution. According to a 2024 paper in IEEE Transactions on Circuits and Systems for Video Technology, a generative steganography method based on image mapping showed superior robustness compared to traditional spatial domain approaches. In addition, IEEE Transactions on Information Forensics and Security published a paper suggesting multi-adversarial learning-based models with adaptive embedding cost for increased robustness against various detection and attack methods.

Other research works have looked at transform domain schemes, whereby the information is transformed into frequency bands by means of techniques like DCT and DWT. The advantage of these methods is that they are less vulnerable to compression and noise, although they are quite complex computationally and difficult to implement.

According to the existing literature review, it seems to be evident that conventional steganographic approaches are simple and effective; nevertheless, they are less resistant to state-of-the-art detection methods. On the other hand, although AI-assisted techniques are relatively effective, they need to be carefully designed to ensure sufficient data storage capacity and efficient processing without affecting invisibility. Therefore, an optimal placement of intelligent regions may become a more promising option.

CHALLENGES IN SECURE IMAGE COMMUNICATION

Image communication that is secure has gained significant importance today owing to the fact that images have found widespread application in fields ranging from social media usage to healthcare systems, surveillance, military activities, and cloud computing applications. Transmitting images in a manner that ensures their security has proved to be difficult. The size of images and the fact that they are prone to interception and tampering poses various challenges.

Unauthorized access to images that are being transferred through open networks constitutes one of the most challenging aspects. This can happen due to network eavesdropping where attackers use network sniffers for the purpose. The very presence of encrypted data on the network may prove to be a pointer toward confidential data, and thus, it attracts attacks.

The detection of the hidden message is also a major concern in steganographic analysis. Conventional steganographic methods such as LSB insertion alter the pixel values uniformly, thus producing statistical patterns that current steganalytic systems can identify, thereby revealing the existence of hidden messages, despite the inability to decipher their content.

Image quality preservation is yet another problem in steganography. When a secret message is embedded within an image, pixel values are modified, thus causing visual distortion, change in colour, and blur if too much is done. Balancing image alteration and the volume of data to be concealed is a complex process, referred to as payload versus imperceptibility in literature. Another aspect of the steganographic process that poses a significant challenge is robustness to standard image processing functions. The image could be altered during storage and transmission through compression, filtering, scaling, and format conversion.

There is also limited capacity for hiding data in images. This is due to the fact that there are only certain amounts of data that can be embedded into an image without causing visible distortions. If one tries to embed more data than is possible, this may lead to both detection and decreased quality of the image.

The absence of intelligent methods to hide information in the image can lead to security threats. In many of the existing conventional approaches, little attention is paid to the actual contents of the image prior to inserting the data. Thus, embedding of data into parts of the image that should have remained unchanged leads to compromising its security.

It is also important to keep in mind the fact that many advanced embedding algorithms involve complex calculations and take some time to complete. Thus, such algorithms may prove useless when it comes to applications where fast computation is vital. Last but not least, efficient key management and synchronization of actions are crucial. In order to successfully retrieve the secret message, the receiver must use exactly the same key as was used by the sender.

In conclusion, the process of securely transmitting images is one which faces the conflicting objectives of confidentiality, invisibility, robustness, payload and effectiveness. In tackling these problems, there is need for more sophisticated means of transmitting information by combining the concept of steganography with artificial intelligence.

RELATED WORK

Image security communication has garnered interest from researchers from all sorts of related fields including information security, digital image engineering, and multimedia systems. Historically, their approaches were centralized around cryptography where images were encrypted prior to transmission. While encryption obfuscates content, it offers no disguise to the presence of an encrypted communication which could lead an adversary to become more interested. To mitigate this problem, scholars sought to use steganography, the practice of embedding secret digital content within an image in such a way that the resultant image does not arouse curiosity.

Most early steganography techniques were developed in the spatial domain, particularly using Least Significant Bit (LSB) substitution. This technique offers little perceptible change to an image to the human eye, as it inserts the secret data in the least significant bit of a pixel. While such techniques are fast and straightforward to use, they are easily manipulated and can be entirely eliminated by benign image processing, compression, and noise which target the embedded information. These techniques are practical, but they are overall too fragile.

In response to these shortcomings, researchers pioneered techniques utilizing the transform domain. Instead of modifying pixel values straightforwardly, these methods embed data into the frequency components acquired through transformations such as the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT). Because changes are made in the transformed domain, the embedded data are generally more robust to compression and filtering. However, the methods are more tedious and usually more demanding in terms of computations, sometimes becoming more expensive in terms of embedded data capacity.

Recently, the use of machine and deep learning techniques has emerged in improving the steganography. Neural networks can learn to hide data in a way that optimizes visibility and embedding capacity. Some frameworks utilize an encoder-decoder architecture and optimize the embedding and extraction processes in a joint manner. One of the more exciting applications of these methods is the use of Generative Adversarial Networks (GANs) to produce stego images that are nearly indistinguishable from natural images, which significantly narrows the detection gap.

Adaptive or content-aware steganography is another major area of study. These methods consider the images' features, such as edges, textures, and noise, and decide where to store the information. The complex areas of the images are modified to improve both invisibility and security because the areas are less perceptible to human users and less detectable by statistical detectors.

Despite the progress made, the challenges are numerous. The training of most deep learning techniques is complex and expensive in terms of training data and computational power. There is always the challenge of finding the right balance between invisibility, capacity, robustness, and efficiency. Some methods, such as the one suggested, are considered less robust because they permit more data to be stored. Others are considered less robust because they distort the image. The suggested system is considered AI-based and creates data transmission while taking advantage of these developments in intelligent regional selection, combined with multimedia steganography. Because hidden data is embedded in specific

areas of the image, the system provides secure communication, high-quality images, and accurate recovery of the hidden data at the end of the image.

PROPOSED METHOD

This suggested technique involves using the power of artificial intelligence (AI) to hide sensitive data through a secure transmission process involving digital images as cover mediums. The first objective of this technique is the ability to transmit confidential data through the image while minimizing distortion in the image and avoiding any indication that there is any hidden information. To begin with, the secret information is encoded into binary format. In cases where an additional layer of security is needed, the encoded information may be further encrypted. Contrary to traditional approaches where the hidden data is evenly distributed across the whole image, this new approach involves the use of AI to determine the best places for hiding the data by analyzing the image.

The AI will select parts of the image with edges and textures or any other features that could help the steganography technique. Finally, the secret binary code is embedded into the best spots using some distortion method like modified LSB algorithm.

At the receiving end, the same technique is employed to identify the embedded sections and retrieve the concealed information. The retrieved binary code is subsequently translated back into the message, and if encryption had been done before, it is deciphered. Through the use of smart selection and effective embedding of the regions, the suggested technique not only enhances security but also ensures good picture quality, making it resilient to image processing techniques such as compression or filtering.

Least Significant Bit (LSB)

Least Significant Bit (LSB) approach is one of the most commonly used spatial domain techniques because it allows for the insertion of a large amount of data without any substantial change in the cover image due to the effectiveness and simplicity of the algorithm. Each pixel comprises a series of bits that constitute the colour intensity value of the pixel in either 8-bit or 24-bit images. The LSB approach involves altering the pixels' values by changing their least significant bit to the bits from the message to be embedded in the image. This slight change in the colour intensity value of the pixel is barely perceptible to the naked eye; therefore, the LSB approach proves to be one of the most efficient spatial domain techniques. For instance, in a 24-bit RGB image, each pixel holds three colour channels: Red, Green, and Blue. Hence, a bit can be inserted in each colour channel.

This results in high payload capacity and high speed of embedding and extracting messages. However, despite many merits of LSB technique, there are several disadvantages. The main disadvantage is the high sensitivity of this algorithm to image transformations like compression, scaling, blurring, cropping, noise injection and other transformations that might easily destroy hidden information. Apart from that, classical LSB embedding, although performed sequentially on pixels, might also suffer from detection based on statistical analysis of pixel patterns or bit plane statistics. But even taking into account those drawbacks, if the LSB algorithm is used in an optimal way together with randomization of the embedded message and its preprocessing, this technique will remain one of the most effective steganographic methods for images.

Discrete Wavelet Transform (DWT)

A powerful signal processing method that is widely used in image compression, digital watermarking, and secure data hiding. Unlike simple techniques that change pixel values directly, DWT works in the frequency domain. It breaks an image into different components based on frequency, allowing information to be embedded in a way that is less noticeable and more resistant to common image processing operations such as compression, filtering, or noise.

When DWT is applied to an image, it splits the image into four sub-bands: LL, LH, HL, and HH. The LL band contains the low-frequency information, which represents the overall appearance and structure of the image. The other three bands (LH, HL, and HH) capture the high-frequency details, including edges and textures in horizontal, vertical, and diagonal directions. Since the human eye is less sensitive to small changes in these detailed regions, hidden data is usually placed in the high-frequency bands to preserve visual quality and reduce the chances of detection.

Another feature of DWT is that it can be applied recursively to the LL band to achieve multilevel decomposition, which means there is some flexibility in determining the location for embedding the secret data. In particular, when embedding, some of the selected wavelet coefficients are slightly manipulated in order to carry the hidden data. Finally, an inverse transform (IDWT) will be performed in order to reconstruct the image, leading to a stego-image.

As can be seen, there are several advantages offered by steganography based on DWT compared to classical steganographic algorithms. First of all, it is usually more robust when it comes to attacks such as JPEG compression, it produces better results regarding distortion and it is statistically undetectable. Nevertheless, it should be kept in mind that it is computationally complex compared to LSB substitution.

Finally, due to its high effectiveness, DWT is widely used for secure image communication, watermarking and data hiding purposes.

SYSTEM ARCHITECTURE

The proposed method outlines the use of the steganographic channel through which the secret message can be encoded or decoded using AI technology to hide and extract the secret message through media files such as images or videos. This comprises two processes of pre-processing, where the input data should be prepared in a binary format. Then, the message is embedded using the AI algorithm within the cover medium. Then the media file is sent via the communication network where the secret message is extracted by the AI-enabled extractor. In case of unsuccessful verification of the message extraction, then the whole process must be executed again until a perfect extraction is achieved. Using an artificial intelligence approach of embedding allows choosing regions within the carrier media with minimal impact on the perception of data, making it almost impossible for the human eye to see any alterations, thus avoiding any steganography attack. The AI model ensures maintaining a balance between the amount of information that can be inserted in a file and its high quality.

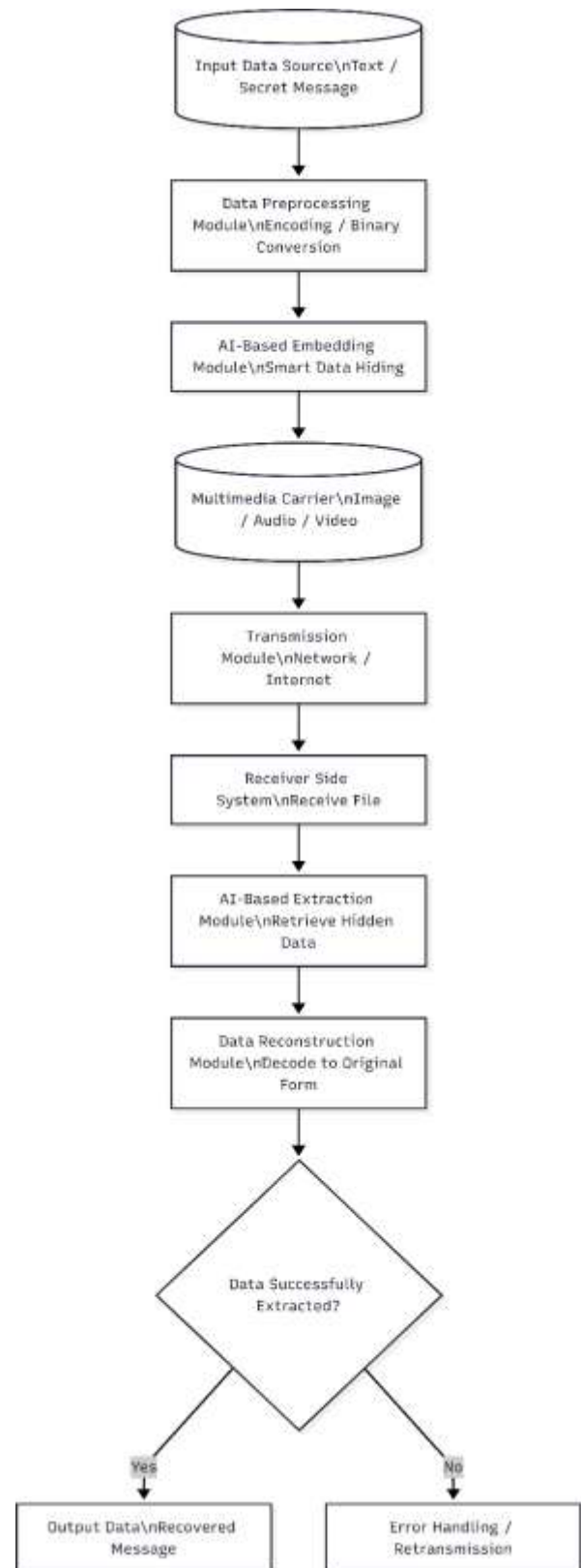


Fig 1: Architecture diagram

Input Data Source

The first step involves picking up the secret message, which can come in any format, whether it's plain text or sensitive information. Such data will serve as the payload, which must be securely stashed into a multimedia carrier.

Data Preprocessing Module

In this phase, the message to be embedded is converted to binary form for encoding. The encoded messages can then be used to represent the text using various encoding methods.

The pre-processing stage may also include steps such as data compression and normalization.

AI-Based Embedding Module

This module is the most important part of the entire system. Here, the techniques of artificial intelligence are used to examine the multimedia medium and determine the best places to hide the data. Usually, complicated places like the edges and textures are chosen because changes made here are not easily detected by the human eye. The secret data is then hidden in the medium using appropriate methods of steganography.

Multimedia Carrier

The system is capable of using more than one carrier format, such as images, sound, and video files. Carriers are employed as cover media that carry the confidential information hidden inside. This capability increases the versatility of the system.

Transmission Module

The stego file created after embedding the information is then transmitted via communication networks, such as computer networks and the internet. It guarantees that the transmission of the stego file does not interfere with the information that has been concealed.

Receiver Side System

The receiving end receives the stego file and prepares it for extraction. The system synchronizes itself with the configuration at the sender end to extract the hidden information accurately.

AI-Based Extraction Module

Similarly, AI is employed to detect areas in which the data has been concealed. Thereafter, the hidden data bits are retrieved from the detected areas using a decoding technique that corresponds to them.

Data Reconstruction Module

The binary data thus extracted is then decoded. Decoding procedures are used to convert the extracted binary data into their original state or format.

Decision and Output Module

A validation procedure will then be carried out to ensure that data extraction has taken place. If so, then the original message will be output. Otherwise, error correction techniques like retransmission will come into play.

MODULES

1. Input Module

This module represents the first stage of the system input interface, in which the carrier and the hidden message are entered. The carrier may come in the form of a picture, audio or video file, all of which are supported in standard formats like JPG, PNG, MP3, and MP4. Validation procedures are carried out at this stage to confirm that the carrier meets the requirements for being embedded with information.

2. AI-Based Region Selection Module

The current module adopts an AI-based technique to examine the structural properties of the media presented as inputs. In the process, the technique detects the right spots that can accommodate the hiding of the secret content. In this case, the spots include those that have higher complexities, such as edges and textures. Such areas will be more resilient when slight changes occur to them. This will improve both security

and resistance while ensuring that the integrity of the media is maintained.

3. Data Embedding Module

This is where the secret message is coded into the binary format to make it possible for encoding. This system uses steganography to embed the binary code in the chosen areas in the carrier media. In this regard, efforts are made to avoid distortion of the image, sound, or video so as not to change its quality. The embedded data is used to develop the stego object.

4. Stego Media Generation Module

This particular module will be used for generating the output file that is referred to as stego media. The process of generation involves combining the multimedia contents with the hidden data in order to obtain an encrypted file. In essence, the generated file is of high quality while being able to hide all hidden data within it..

5. Data Extraction Module

The data extraction module is responsible for the task of extracting the embedded information from the stego media at the receiving end. The module uses decoding methods that are based on the techniques used to embed the information. After extraction, the information is decoded into its original format, thus ensuring no loss of data during the decoding process..

6. Quality Assessment Module (MSE & PSNR Evaluation)

The module analyses the effectiveness of the steganographic scheme based on the level of distortion present in the cover and stego images. The module uses Mean Squared Error and Peak Signal-to-Noise Ratio as two parameters to evaluate the image quality. If the Mean Squared Error value is low, while Peak Signal-to-Noise Ratio is high, then the amount of distortion introduced into the stego image is minimal. The module is essential in assessing the effectiveness of the steganography scheme if multiple embedding depths and payloads, among other variables, are considered.

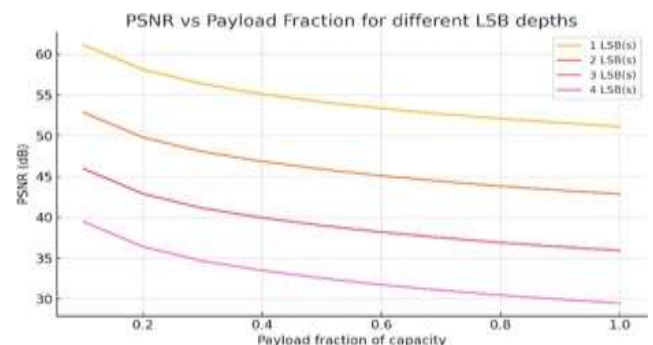


fig 2: PSNR vs payload

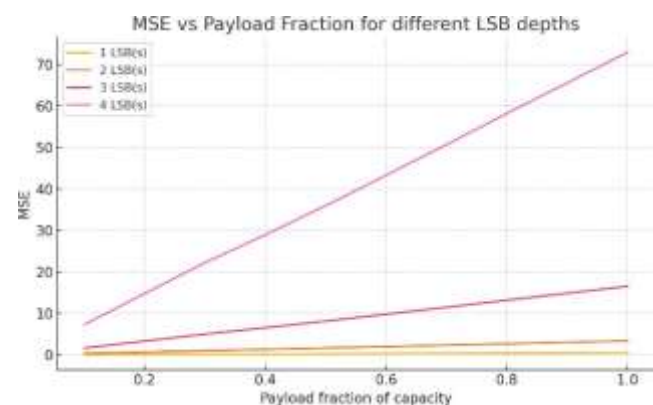


fig 3: MSE vs payload

RESULTS AND DISCUSSIONS

Qualitative and quantitative approaches were employed to evaluate the effectiveness of the proposed AI-based steganography technique in ensuring a secure transmission of data. Visually, the images generated are quite similar to the initial cover images with no obvious distortions observed. Thus, one may conclude that the level of imperceptibility provided by the suggested method is quite high. As far as the quantitative criteria is concerned, the metrics including Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) were analyzed in order to examine the level of distortions involved in the process of data embedding. Low values of MSE and extremely high values of PSNR proved the point of minimal pixel modifications.

As far as the capacity of data embedding is concerned, the proposed approach shows a great potential in this regard as a lot of information can be hidden without reducing the quality of cover images. In particular, the idea of intelligent selection of regions plays an important role as data is inserted mainly in edge and textured areas that can sustain slight alterations in their contents. Furthermore, this approach allows achieving better results compared to the traditional LSB-based algorithms due to the optimal distribution of data and higher payload capacity.

Additionally, the stability of the system has been tested by performing various image processing techniques on the stego images, including compression, adding noise, and filtering. The findings reveal that the hidden information is mostly retained and can be recovered accurately, making the system stable against these attacks. On the receiving end, the extraction phase recovers the secret message perfectly without losing any information. In summary, the system provides an optimal combination of invisibility, data capacity, stability, and security, thus making it appropriate for use in secure communications.



Fig 4: Comparision between cover image and stego image

CONCLUSION

In this paper, an AI-based scheme for secure communication through multimedia files by embedding hidden information has been introduced. The suggested scheme incorporates the fundamental ideas of steganography and AI-based intelligent region selection to provide secure and effective communication. The selection of appropriate regions like edges and textures is performed by utilizing AI, thereby ensuring minimal distortion of the images while keeping the risks of detection at a minimum. In contrast to the existing techniques of data embedding through multimedia, the incorporation of AI technology offers greater flexibility in terms of implementation and ensures better security.

It has been observed through experimentation that the stego-media produced through the system is characterized by high quality, minimal distortion, and reliable data extraction at the receiver end. Moreover, the proposed algorithm is highly resistant to attacks related to general image processing and elementary steganalysis techniques. In summary, the proposed scheme meets all the necessary criteria including imperceptibility, capacity, security, and effectiveness.

REFERENCES

1. J. Liang et al., "A Steganography-Based Scheme for Secure Transmission of Monitoring Data in Smart Substations," *IEEE Internet of Things Journal*, 2025.
2. A. Aljarf, "DL-Steg: A Deep Learning-Based Image Steganography Model Using SAE and LSTM," *Springer Journal of Big Data*, 2025.
3. Y. Zhao et al., "Image Steganography Based on Wavelet Transform and Generative Adversarial Networks," *Journal of Visual Communication and Image Representation*, 2025.
4. S. Rahman et al., "A Novel and Efficient Digital Image Steganography Technique for Secure Communication," *Scientific Reports (Nature)*, 2025.
5. B. Song et al., "A Survey on Deep Learning-Based Image Steganography," *Expert Systems with Applications*, 2024.
6. Y. Fernando et al., "Steganography on Image Metadata for Robust Data Hiding," *International Journal of Informatics Visualization*, 2024.
7. H. Ragab et al., "Digital Image Steganography and Reversible Data Hiding: A Review," *Journal of Image and Graphics*, 2025.
8. F. A. Khalil et al., "A Review of Image Steganography Based on Metaheuristic Algorithms," *Computer Science Review*, 2025.
9. A. Krishnan et al., "Audio-in-Image Steganography Using Analysis and Resynthesis Sound Spectrograph," *IEEE Access*, 2025.
10. D. Darwis et al., "Metadata-Based Video Steganography Technique for Secure Data Communication," *Engineering, Technology & Applied Science Research*, 2025.
11. R. I. M. Setiadi et al., "AI-Powered Steganography: Advances in Image and Multimedia Data Hiding," *Research Survey*, 2025.
12. Rustad, S. (2022). Inverted LSB image steganography using adaptive pattern and encryption (RC4) to improve imperceptibility. *Journal (ScienceDirect listing)*. (See item on ScienceDirect; PII S131915782030625X).
13. Suresh, K. S., & Kamalakannan, T. (2022). Image steganography based on LSB using various scanning methods in spatial domain. *International Journal of Health Sciences (Special Issue)*, 6(S3), 6820–6834. DOI: 10.53730.
14. Miranda, J. D., et al. (2022). LSB steganography detection in monochromatic still images using artificial neural networks. *Multimedia Tools and Applications*, 81, 785–805. DOI: 10.1007/s11042-021-11527-2.
15. Islam, M. R. (2021). A modified LSB image steganography method using improved edge-adaptive scheme. *Journal of Information Security and Applications (Taylor & Francis / Routledge)*. DOI: 10.1080/19393555.2020.1854902.
16. Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020). An image steganography approach based on k-least significant bits (k-LSB). *Proc. IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIOT 2020)*. DOI:10.1109/ICIOT48696.2020.9089566.