ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1051

A Study of Recent Advancement of Image Steganography

Sudipa Ghosh[1]; Soumen Bhowmik[2]

[1] Research Scholar M. Tech, CSE, Bengal Institute of Technology and Management
[2] Head of the Department, Dept. of CSE, Bengal Institute of Technology and Management
Santiniketan, Birbhum, India

Publication Date: 2026/05/27

Abstract: Due to today's availability of internet technology, there is much need for data security methods. With the growing usage of communication through the internet, it has become necessary to maintain the confidentiality of the data being used and transmitted. One such technique is steganography, whereby data or information is hidden in the form of an image. Image steganography refers to the method of hiding the existence of the communicated data in such a manner that the confidentiality of the message can be maintained in a digital image. Information can be concealed using this method in the form of text, image, or video inside the cover image in an invisible form. In this paper, a review and comparison of recent advancements in image steganography are discussed. Different methods, such as spatial domain, transform domain, encryption-based, and deep learning-based methods, have been studied. Performance parameters, including PSNR, MSE, embedding capacity, and robustness, have been compared. It has been found that the use of modern methods, especially those based on encryption and deep learning, offer better security and concealment of data.

Keywords: *Image Steganography, LSB, DWT, AES, CNN, GAN, Data Hiding, Steganalysis*.

How to Cite: Sudipa Ghosh; Soumen Bhowmik (2026) A Study of Recent Advancement of Image Steganography. *International Journal of Innovative Science and Research Technology*, 11(5), 1889-1892. https://doi.org/10.38124/ijisrt/26may1051

I. INTRODUCTION

Secure communication has become very necessary in today's world of the internet because there is a very rapid growth of the internet, and data transmission takes place through the internet. Multimedia data, including images, sound clips, video clips, etc., are exchanged using the internet network. Cryptography, a conventional technique of securing data, converts data into some unreadable form. This form might attract hackers. Steganography offers another form of security by concealing the presence of the secret message in a cover medium [1].

Steganography is a term coined from Greek, where stegeanos means "covered" while grapheia means "writing." Image steganography refers to the process of concealing secret data within an image file so that one cannot observe the secret message. Image files are chosen because of the huge amount of redundancy present in them [3].

Various scholars have looked at other strategies for enhancing the effectiveness and security of image steganography. For instance, traditional LSB algorithms have proved popular owing to their simple application and fast processing speed, yet they are prone to attacks and lack robustness [4]. Other techniques that attempt to solve the problems associated with conventional techniques include transformations such as DCT and DWT, which resist image attacks and compression [5].

Furthermore, techniques involving encryption are integrated with image steganography algorithms to increase the security of the transmitted information. In this strategy, the message is first encrypted before being embedded in the cover image, hence increasing its security from any illegal extraction [5].

Lastly, other recent improvements in image steganography involve the introduction of machine learning and deep learning concepts. This technique involves the use of CNN and GAN models that enhance imperceptibility and embedding capability [4].

Additionally, many studies have highlighted the need to measure the performance of steganographic schemes through performance measures like PSNR, MSE, robustness, and embedding capacity. Such measures are critical in analyzing the quality and efficacy of the steganographic system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1051

In summary, current research has shown that combining old methods with new techniques like encryption, compression, and artificial intelligence algorithms could enhance the effectiveness of image steganography systems.

Hence, this paper focuses on studying and comparing new developments in image steganography systems with respect to their performance, security, and efficiency.

II. LITERATURE REVIEW

The field of steganography has been thoroughly investigated by scientists, and there exist numerous methodologies that can be adopted to increase security and efficiency of the embedding process.

In their paper, Parmar et al. [2] explained the basic principles of image steganography and outlined the significance of this methodology for secure communication. According to the authors, the main objective of steganography is to ensure that information remains hidden and undetected.

Powar et al. [1] explored various categories of steganographic approaches, such as spatial domain steganography, frequency domain steganography, and distortion-based methods. Each approach has specific advantages and disadvantages regarding embedding capacity and robustness.

Subramanian et al. explored recent advancements in deep learning-based steganography, including CNN and GAN models. These techniques significantly improve the imperceptibility and resistance against steganalysis attacks [4].

Hameed et al. discussed evaluation metrics such as PSNR, MSE, and robustness for comparing different steganography techniques. These metrics are essential for assessing the quality and security of stego-images [6].

Evaluation matrices such as MSE, PSNR and robustness play an important role in steganography techniques. These techniques are used to measure the performance of steganography. MSE or Mean Square Root indicates the measure of distortion occurred, means calculates the average difference between cover image and stego image. Peak Signal-to-Noise Ratio (PSNR) is executed from MSE and represents the visual similarity between the two images in decibels; higher PSNR indicates that the hidden data is imperceptible to human vision. Robustness evaluates the ability of the embedded secret data or information to survive common attacks such as compression, noise, cropping, and filtering, often measured using Bit Error Rate (BER). An effective steganography method aims for low MSE, high PSNR, and strong robustness to ensure secure and reliable data hiding.

- *Spatial Domain:*

The spatial-domain embedding techniques are more common in comparison with the transform domain because of ease of implementation and extraction processes, but not as strong [8]. The spatial domain steganography involves secret information being directly embedded through manipulation of pixel values. In other words, these approaches work on image pixels directly. Commonly used spatial techniques include least significant bits (LSB), pixel value differencing (PVD). For example, LSB technique involves hiding the information in least significant bit of cover image pixel [1].

- *Frequency domain:*

The frequency domain describes a signal or a function by its frequency in terms of its frequency components rather than time, displaying how signal energy is distributed over a range of frequencies. In frequency domain technique instead of hiding data directly into pixel, first image is transforms into frequency domain. This technique provides less capacity. Most commonly used transformations are DCT, DWT, DFT [1].

- *Distortion-Based Methods:*

Distortion-based methods are techniques which are used to distort signals, images. Secret data extraction occurs based on the difference between the cover image and stego image [1]. Ansari et al. developed AES-based image steganography technique whereby secret data are encrypted and hidden in images using LSB & DWT technique. AES-Based Image Steganography improves security and compression efficiency.[5] Ansari et al. carried out the comparative study of different steganography methods used in BMP, JPEG and PNG image files. They emphasize the need for choosing an appropriate image file for data concealment.[3].

- *JPEG:*

JPEG stands for Joint Photographic Experts Groups and most commonly used image files formats. In 1987, ISO formed Joint Photographic Expert Group to research on how to transmit video and images into small files through data compression. JPEG is a type of digital image compression. In JPEG, image data are compressed into smaller file size with low probability of attacks. JPEG uses lossy compression technique that reduces the size of the images. JPEG is ideal for frequency-domain steganography techniques as it compresses full color and grey scale images. Compression is achieved in JPEG through removal of some visual details to reduce image size. The JPEG coefficient values vary a range from –1024 to +1023. JPEG image data embedding methods store secret data between these two phases. DCT transformed cosine values cannot be back- calculated exactly and repeated calculation using limited precision number produces a rounding error hence, it is called lossy compression [3].

- *BMP:*

BMP file format or Bitmap is an image format used to save the raster graphics of digital images. The BMP file format is considered to be one of the simplest and oldest image formats which are mostly used to store uncompressed high-resolution images. It can store 2D digital images at different color depths. An 8-bit Bitmap will have 256 colors per pixel. RGB comes in 16 bits, 24 bits, 36 bits, and 48 bits. Out of all of them, 48 bit images will contain high color depth because each channel contains 16 bits. When it comes to 24 bits format, each channel uses 8 bits and ranges from 0 to 256 brightness. Each pixel will consist of two bytes and the amount of bits each channel uses in the 16-bit format is [3].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1051

➢ *PNG:*

PNG stands for Portable Network Graphics. It is considered as a raster graphics image format, which supports lossless compression of data. PNG is generally used in order to store the smallest possible file size with no loss in quality. It was created specifically to transfer digital images over the Internet. It provides support for various colors and also allows degrees of transparency [3].

➢ *CNN*

CNN and GAN-based methods have significantly improved modern image steganography by using deep learning to automatically learn optimal data-hiding strategies. Convolutional Neural Networks (CNNs) are used to identify complex image features and determine the best locations to embed secret data with minimal visual distortion. Generative Adversarial Networks (GANs) further enhance performance by using a generator–discriminator framework, where the generator creates realistic stego images and the discriminator tries to detect hidden data, forcing the system to produce highly secure and imperceptible results. These deep learning approaches offer improved capacity, better image quality, and stronger resistance to steganalysis compared to traditional techniques.

Overall, existing research indicates that modern steganography techniques combining encryption, compression, and deep learning provide better performance compared to traditional methods.

III. ANALYSIS OF EXISTING METHODOLOGIES

Different image steganography techniques have been developed over time to improve data security, imperceptibility, and robustness. These techniques can broadly be categorized into spatial domain methods, transform domain methods, encryption-based approaches, and deep learning-based techniques. Each method has its own advantages and limitations depending on the application requirements.

Table 1: Comparison table

Technique	Method Type	Advantages	Limitations
LSB (Least Significant Bit)	Spatial Domain	Simple, fast, high capacity	Low security, vulnerable to attacks
DCT / DWT	Transform Domain	Better robustness, compression resistant	Complex implementation
AES + Steganography	Encryption-based	High security, data confidentiality	Increased computational cost
Hybrid (LSB + DWT + AES)	Combined Approach	Balanced performance and security	More complex system
CNN-based Steganography	Deep Learning	High imperceptibility, adaptive embedding	Requires training data
GAN-based Steganography	Deep Learning	Very high security, realistic output	High complexity and training cost

The LSB (Least Significant Bit) technique is one of the most widely used spatial domain methods due to its simplicity and low computational cost. It works by replacing the least significant bits of image pixels with secret data. Although this method provides high embedding capacity, it is highly vulnerable to statistical and visual attacks, making it less secure for sensitive applications [4].

To overcome these limitations, researchers introduced transform domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). These methods embed data in frequency components rather than pixel values, making them more robust against compression and image processing operations. Studies show that transform domain techniques provide better resistance to steganalysis compared to spatial domain methods [5].

Another important advancement is the integration of encryption techniques such as AES with steganography. In this approach, the secret data is first encrypted and then embedded into the image. This ensures that even if the data is extracted, it remains unreadable without the decryption key. This combination significantly improves security and confidentiality [5].

Hybrid approaches that combine multiple techniques, such as LSB with DWT and AES, provide a balanced solution by improving both security and embedding efficiency. These methods utilize the strengths of different techniques to overcome individual limitations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1051

Recent developments in the field include deep learning-based steganography techniques such as Convolutional Neural Networks (CNN) and Generative Adversarial Networks (GAN). CNN-based methods automatically learn optimal embedding patterns, improving imperceptibility and reducing detection probability. GAN-based techniques go a step further by generating highly realistic stego-images that are difficult to distinguish from original images, even using advanced steganalysis tools [4].

Furthermore, the performance of these techniques is evaluated using metrics such as PSNR, MSE, robustness, and embedding capacity. Higher PSNR values indicate better image quality, while lower MSE values indicate minimal distortion. Modern techniques aim to optimize these metrics while maintaining strong security [6].

The comparative analysis indicates that while traditional methods like LSB are efficient and easy to implement, they lack security. Transform domain and encryption-based methods offer better protection, while deep learning-based techniques represent the most advanced and secure solutions in recent image steganography research.

IV. CONCLUTION

Image steganography is one of the widely used techniques for the security of information exchange through digital images. The technique involves embedding secret data into a digital image in such a manner that does not allow one to identify the presence of hidden data. The following report examines and compares different image steganography approaches including traditional ones, transform domain ones, encryption-based approaches, and deep learning based approaches.

The traditional steganographic approach such as the LSB approach is efficient and easy to implement, but it lacks security and robustness. However, the techniques using transform domains such as DCT and DWT provide a high level of robustness and resistance. Encryption can be used to improve the security of embedded data and protect it from any manipulations and hacking attempts. Deep learning-based techniques like CNN and GAN provide enhanced protection and resistance. It can be concluded that, modern approaches using a combination of different approaches perform much better in comparison to traditional approaches in regard to all mentioned criteria.

REFERENCES

[1]. S. K. Powar, H. T. Dinde, and R. M. Patil, “A Study and Literature Review on Various Image Steganography Techniques,” International Research Journal of Engineering and Technology (IRJET), Vol:07, pp: 3258-3261, e-ISSN: 2395-0056, p-ISSN: 2395-0072, 08 Aug .2020.

[2]. A. K. M. Parmar and K. Chouhan, “A Study and Literature Review on Image Steganography,” International Journal of Computer Computer Science and Information Technology (IJCSIT) , Vol: 6 (1), pp: 685-688, ISSN: 0975-9646, 2015 .

[3]. A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, “A Comparative Study of Recent Steganography Techniques for Multiple Image Formats,” International Journal of Computer Network and Information Security (IJCNIS), Vol-1, pp: 11-25, 08 Jan. 2019.

[4]. N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “Image Steganography: A Review of the Recent Advances,” IEEE Access, vol: 9, pp: 23409–23423, 25 Jan. 2021.

[5]. V. D., S. H. K., and M. Tajuddin, “A Literature Review on Image Steganography Using AES,” International Research Journal of Engineering and Technology (IRJET), Vol:09, pp: 1092-1096, e-ISSN: 2395-0056, p-ISSN: 2395-0072, 01 Jan .2022

[6]. R. S. Hameed, A. R. H. Ahmad, M. M. Taher, and S. S. Mokri, “A Literature Review of Various Steganography Methods,” Journal of Theoretical and Applied Information Technology (JATIT), Vol. 100. No 5, pp: 1412-1427, ISSN: 1992-8645, E-ISSN: 1817-3195, 15th March,2022.

[7]. A. M. Alhomoud, “Image Steganography in Spatial Domain: Current Status, Techniques, and Trends”, Intelligent Automation & Soft Computing DOI:10.32604/iasc.2021.014773, 01 Nov. 2020 https://www.techscience.com/iasc/v27n1/41146/html

[8]. PNG File Format, https://en.wikipedia.org/wiki/PNG