ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1586

A literature Survey of Image Steganographic Techniques

Soumen Bhowmik[1]; Pushpa Tiwari[2]

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

Publication Date: 2025/05/29

Abstract: Image steganography is a highly effective technique for secure communication, allowing data to be concealed within digital images.This paper provides a comparative analysis of various methods proposed by some papers presented, to enhance the efficiency of image steganographic techniques, with a focus on optimizing data capacity and imperceptibility.

It has been observed that significant improvements in the quality metrics of stego images and their robustness against attacks can greatly contribute to achieving the objective of secure data hiding. These findings highlight the potential of the proposed approach to advance secure data transmission.

Keywords: *Steganography, Payload, Discrete Cosine Transform, Singular Value Decomposition, Least Significant Bit.*

How to Cite: Soumen Bhowmik; Pushpa Tewari (2025) A literature Survey of Image Steganography Techniques. *International Journal of Innovative Science and Research Technology*, 10(5), 2355-2359. https://doi.org/10.38124/ijisrt/25may1586

I. INTRODUCTION

In today's digital era, the secure transmission of sensitive information has become a growing concern due to the increasing risks of unauthorized access and cyber threats.

Various techniques have been developed to address these challenges, including cryptography, watermarking, and steganography. While cryptography focuses on encrypting data to make it unreadable without decryption keys, and watermarking embeds identifying marks into media to ensure authenticity, steganography offers a distinct advantage over other techniques.

Steganography, the art of concealing data within various media, has emerged as a promising solution for ensuring secure communication.

Image steganography stands out as a particularly effective method of secure communication because unlike cryptography, which often attracts attention due to the presence of encrypted files, image steganography hides data within the pixel values of digital images, making the hidden information imperceptible to the human eye.

This subtlety ensures that the stego-image appears identical to the original, thereby avoiding suspicion.

Additionally, steganographic mediums such as audio or video, images are more widely shared and less computationally intensive, making them a convenient and efficient choice for embedding data. By leveraging techniques like Least Significant Bit (LSB) substitution and advanced methods such as optimal pixel adjustment and hash-based insertion, image steganography achieves a balance between embedding capacity, imperceptibility, and computational efficiency.

Certainly, image steganography offers a robust edge over cryptography and other techniques by providing an additional layer of secrecy.

It not only safeguards the content but also ensures that the existence of sensitive information remains undetectable, making it a valuable tool for secure data transmission in the modern digital landscape.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1586

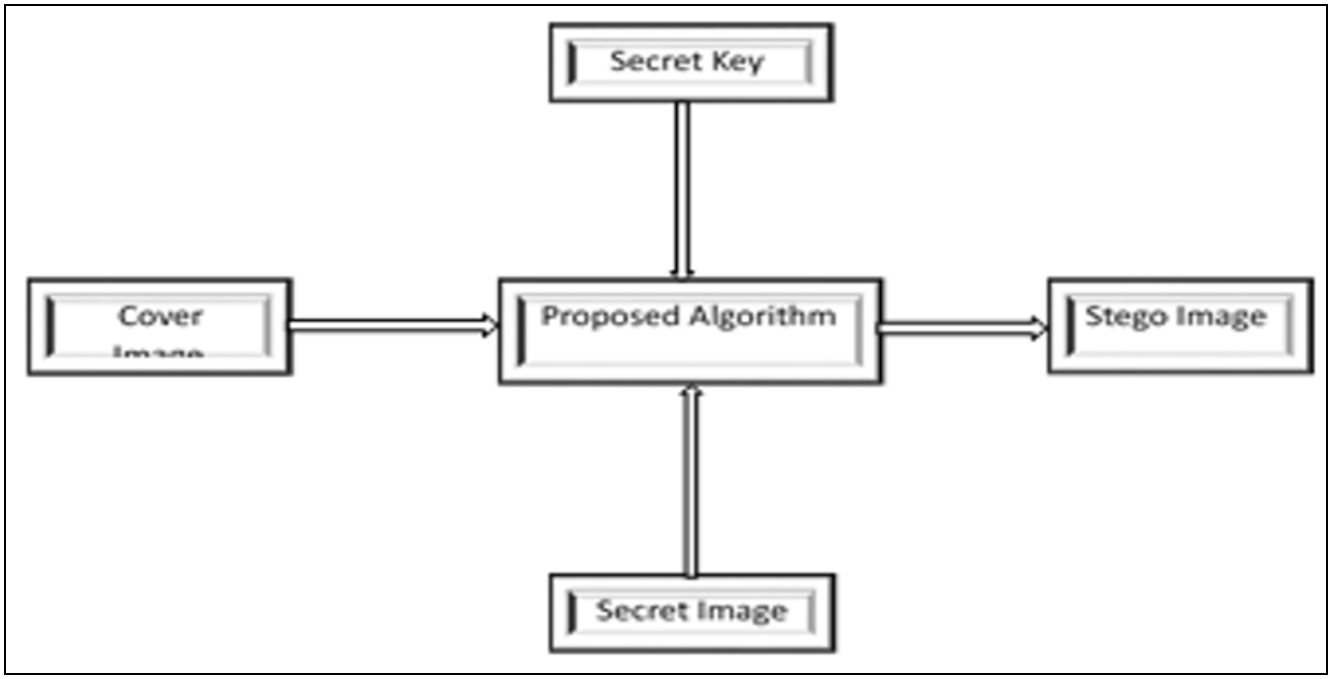

Fig 1 Image Steganography.

II. EXISTING TECHNIQUES

A. LSB Substitution Method

The Least Significant Bit (LSB) substitution method is a straightforward and widely adopted technique in image steganography that involves embedding secret data into the least significant bits of the pixel values in a digital image.

In this method, the binary representation of the secret data is directly inserted by replacing the least significant bits of the image pixels, resulting in minimal visual distortion. This simplicity ensures computational efficiency and a high data embedding capacity.

For example, altering a pixel value from 11001010 to 11001011 demonstrates the minimal change involved. While LSB substitution offers several advantages, including ease of implementation and the ability to embed substantial amounts of data, it is highly vulnerable to steganalysis and common image processing operations such as compression, cropping, and noise addition. These drawbacks make it less suitable for high-security applications.

To address these limitations, variations such as hash-based LSB techniques have been proposed, introducing an added layer of security through the use of hash functions for selective data embedding.

Nevertheless, LSB substitution remains a popular choice for non-critical applications that prioritize simplicity and capacity over robustness, such as watermarking or basic confidential communications.

Despite its limitations, the technique plays a foundational role in steganography and serves as a benchmark for more advanced approaches like transform domain techniques, which offer greater security and robustness for high-stakes scenarios.

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file "MSW_USltr_format".

B. Hash based LSB substitution method

The Hash-based Least Significant Bit (LSB) substitution method [1] is an improvement over the conventional LSB approach by using a hash function to introduce randomness and enhance security in data hiding. In the hash-based LSB substitution method [11], a hash function is used to generate a sequence of positions where the secret bits will be embedded.

This randomization ensures that the hiding locations are non-linear and harder to trace. For example, if the hash function outputs a sequence like 3, 8, 1, 5, and so on, the least significant bits at these positions in the pixel array will be used for embedding the secret data. The hash function could depend on a key shared between the sender and receiver, enhancing the security of the process.

For example, In the traditional LSB method, the secret data (e.g., a binary message) is embedded directly into the least significant bits of the pixels in an image. For instance, if the pixel value in binary is 11010101, replacing the least significant bit with the first bit of the secret message, say 1, changes the pixel to 11010101 (if the LSB was already 1, it remains the same).

This process is straightforward but predictable, making it susceptible to detection.

C. Transform Domain Techniques

Transform domain techniques [13] in image steganography involve embedding secret data into the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1586

frequency coefficients of an image rather than directly modifying its pixel values.

This approach leverages mathematical transformations, such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Singular Value Decomposition (SVD), to convert the spatial domain of an image into the frequency domain. By embedding data in the less perceptible frequency components, these techniques enhance the robustness and imperceptibility of the steganographic process. For example, in DWT-based steganography, the image is decomposed into sub-bands representing different frequency components, and the secret data is embedded into the high-frequency sub-bands, which are less noticeable to the human eye.

Transform domain methods are widely used in applications requiring high security and resilience against image processing attacks, such as digital watermarking, secure communication, and copyright protection.

D. Simple LSB Substitution method

The technique of hiding data in images using simple Least Significant Bit (LSB) substitution, as discussed in the paper, "High Level of Perceptibility and Security in Color Image Steganography," by Soumen Bhowmik, Aditi Ghosh, and Arup Kumar Bhaumik [3], discusses innovative techniques to improve data hiding in color images.

The authors focus on enhancing both the perceptibility and security of steganography, a process that involves concealing data within digital media.

The proposed method utilizes Least Significant Bit (LSB) embedding in the spatial domain, which modifies pixel values in a manner that is imperceptible to the human eye. To address traditional limitations, the technique optimizes the embedding process to maintain the visual quality of the stego-image while maximizing the data embedding capacity.

Security enhancements in this approach ensure that the hidden data is harder to detect or retrieve by unauthorized entities. This is achieved by employing encryption or randomization techniques before embedding. The result is a method that balances high perceptual quality, robust security, and increased data capacity.

Overall, the paper emphasizes the importance of efficient data hiding techniques in modern steganography, particularly for applications requiring secure communication. By improving the trade-offs between perceptibility, security, and embedding capacity, this research contributes significantly to the advancement of digital image steganography.

An optimal pixel adjustment process is applied to the stego-image obtained by the simple LSB substitution method, which significantly improves the image quality with low extra computational complexity [6].

This technique is straightforward and efficient, but it may be vulnerable to detection and attacks due to its simplicity

III. ANALYSIS OF METHODOLOGIES

A. Simple LSB Substitution:

The technique of hiding data in images using simple Least Significant Bit (LSB) substitution, as described by Chi-Kwong Chan and L.M. Cheng [4], involves embedding secret information into the LSBs of pixel values in an image. This method leverages the fact that changes in the LSBs are often imperceptible to the human eye, thus maintaining the visual quality of the image.

The process includes selecting pixels for embedding, modifying their LSBs to encode the secret data, and ensuring the stego-image remains visually similar to the original. An optimal pixel adjustment process is applied to the stego-image obtained by the simple LSB substitution method, which significantly improves the image quality with low extra computational complexity. This technique is straightforward and efficient, but it may be vulnerable to detection and attacks due to its simplicity

- *Advantages:*

Easy to implement, with minimal computational resources required. High capacity for hiding data due to direct pixel manipulation.

- *Drawbacks:*

Vulnerable to simple attacks like noise addition, cropping, or image compression, making it less ideal for secure communications.

B. Hash-Based LSB (HLSB):

The Hash-Based Least Significant Bit (HLSB) technique for video steganography, developed by Kousik Dasgupta, J.K. Mandal, and Paramartha Dutta [1], involves embedding secret data within the LSBs of pixel values in video frames. This spatial domain technique divides the secret information into 3, 3, and 2 bits, which are then embedded into the RGB pixel values of the cover frames.

A hash function is used to determine the position of insertion in the LSB bits, enhancing security. The method is evaluated using metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) to compare the original and steganographic files. The results show minimal degradation in the steganographic video file, indicating high image fidelity.

The proposed technique is compared with existing LSB-based steganography methods and demonstrates encouraging results, making it suitable for secure data transmission in video files.

- *Advantages:*

The use of hash functions adds a layer of complexity, making the technique more secure than basic LSB substitution.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1586

- *Drawbacks:*

Vulnerable to attacks on the spatial domain and less robust compared to transform domain techniques.

C. Transform Domain Techniques (DCT, DWT, SVD):

The paper "Transform Domain Techniques for Image Steganography" by Vaishali P and Pradyumna Bhat [12] explores advanced methods for embedding secret information within digital images using transform domain techniques. The authors focus on transform domain techniques, which involve manipulating the frequency components of an image rather than its pixel values.

These methods are particularly effective in ensuring robustness against image processing operations and compression. The key techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD)[14]approaches enhance the imperceptibility, robustness, and capacity of the hidden data, making it more secure and less likely to be detected by attackers.The advantages of transform domain techniques over spatial domain methods, emphasizing their ability to achieve higher levels of security and data integrity. The authors also address performance metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) to evaluate the effectiveness of the steganographic methods.

Advantages: These techniques embed data in the frequency domain, making the hidden message resistant to common image manipulations like resizing, compression, or filtering.

Drawbacks: Computational complexity is higher compared to spatial domain methods, making them less suitable for scenarios with resource constraints.

IV. DISCUSSION

Each method has its niche depending on the requirements of the application. For instance, LSB is preferred for high-capacity, low-security needs, while Transform Domain methods are chosen for high-security, robust applications. As a summery we may frame like Table 1.

Table 1 Comparison of Performance

Method	Security	Embedding Capacity	Robustness	Complexity
Transform Domain	High	Poor	High	High
LSB	Moderate	High	Poor	Low
HLSB	Moderate	Moderate	Low	Moderate

V. CONCLUSION

Transform domain techniques excel in robustness and security, making them suitable for scenarios requiring high imperceptibility and resistance to attacks.

LSB substitution and its variants, including HLSB, offer simplicity and high capacity but are less secure against advanced attacks. The choice of technique depends on the specific requirements, such as the medium (image or video), desired robustness, and computational constraints.

REFERENCES

[1]. Dasgupta, K., Mandal, J.K. and Dutta, P., 2012. Hash based least significant bit technique for video steganography (HLSB). International Journal of Security, Privacy and Trust Management (IJSPTM), 1(2), pp.1-11.

[2]. Singh, Siddharth, and Tanveer J. Siddiqui. "Transform domain techniques for image steganography." Computer Vision: Concepts, Methodologies, Tools, and Applications. IGI Global, 2018. 170-186.

[3]. Bhowmik, S., Ghosh, A. and Bhaumik, A. K., 2016. High Level of Perceptibility and Security in Color Image Steganography, IJSETR, Vol-5, Issue-2, pp.596-599.

[4]. Chan, C.K. and Cheng, L.M., 2004. Hiding data in images by simple LSB substitution. Pattern recognition, 37(3), pp.469-474

[5]. Pandey, F., Gupta, S. and Kumar, S., 2014. Information hiding using image steganography-A survey. Journal of Basic and Applied Engineering Research (JBAER), 14, p.854.

[6]. Mstafa, R. and Bach, C., 2013, March. Information hiding in images using steganography techniques. In ASEE Northeast Section Conference Norwich University, Reviewed Paper.

[7]. Mustafa, A.E., ElGamal, A.M.F., ElAlmi, M.E. and Bd, A., 2011. A proposed algorithm for steganography in digital image based on least significant bit. Research Journal Specific Education Faculty of Specific Education, Mansoura University, 21.

[8]. Hussain, M. and Hussain, M., 2010, June. Pixel intensity based high capacity data embedding method. In 2010 International Conference on Information and Emerging Technologies (pp. 1-5). IEEE.

[9]. Hemalatha, S., Acharya, U.D. and Renuka, A., 2013. Comparison of secure and high capacity color image steganography techniques in RGB and YCbCr domains. arXiv preprint arXiv:1307.3026.

[10]. Juneja, M. and Sandhu, P.S., 2013. An improved LSB based steganography technique for RGB color images. International journal of computer and communication engineering, 2(4), p.513.

[11]. Halder, R., Sengupta, S., Ghosh, S. and Kundu, D., 2016. A secure image steganography based on rsa algorithm and hash-lsb technique. IOSR Journal of Computer Engineering (IOSR-JCE), 18(1), pp.39-43.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1586

[12]. Vaishali, P. and Bhat, P., 2015. Transform domain techniques for image steganography. International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, 3(1), pp.65-68.
[13]. http://hdl.handle.net/10603/240087
[14]. Singh, S. and Siddiqui, T.J., 2018. Transform domain techniques for image steganography. In Computer Vision: Concepts, Methodologies, Tools, and Applications (pp. 170-186). IGI Global.