International Journal of
Technology and Emerging Research
ISSN: 3068-109X (online) | ISSN: 3068-1995 (print) | https://www.ioro.org/ijter

International Conference on Intelligent Technologies for Tomorrow (ICITT-2026) · 18 August 2026

Spatial Domain Image Steganography: A Comprehensive Review

Niranjana K S [1], Sidha P P [2], Anjali G [3], Akhila K [4]

[1,2,3,4] *III BSc Computer Science Honours, Dept.of Computer Science and Applications, Little Flower College (Autonomous),Guruvayur,Kerala,India.*

Emails: niranjanaksajil@gmail.com[1], sidhaahhh@gmail.com[2], anjalig19126@gmail.com[3] ,2007akhilak@gmail.com[4]

Abstract

Spatial domain image steganography has emerged as one of the most widely adopted information-hiding techniques due to its simplicity, high embedding capacity, low computational complexity, and ability to preserve the visual quality of digital images. It plays a significant role in secure communication by concealing confidential information within digital images, thereby protecting sensitive data from unauthorized access in applications such as healthcare, military communication, banking, cloud computing, digital forensics, and multimedia systems. Despite these advantages, spatial domain techniques face several challenges, including vulnerability to steganalysis, limited robustness against image processing operations, and the trade-off between embedding capacity and imperceptibility. This paper presents a comprehensive review of spatial domain image steganography by examining its historical development, fundamental concepts, classification, and major techniques, including Least Significant Bit (LSB), Adaptive LSB, Pixel Value Differencing (PVD), Pixel Indicator Technique (PIT), Optimal Pixel Adjustment Process (OPAP), edge-based methods, and other adaptive spatial approaches. The reviewed techniques are comparatively analyzed based on embedding capacity, imperceptibility, robustness, computational complexity, and practical applicability, and are further illustrated through a quantitative case study that evaluates PSNR, SSIM, and MSE for LSB substitution on a standard test image. The study identifies existing research gaps and highlights future research directions aimed at improving robustness, visual quality, and embedding capacity. By providing a structured and critical synthesis of existing literature, this review serves as a valuable reference for researchers, academicians, and practitioners working in the field of digital image security and information hiding.

Keywords: Least Significant Bit (LSB); Pixel Value Differencing (PVD); Information Hiding; Digital Image Security; Steganalysis

1. Introduction

The rapid growth of digital technology has transformed the way information is stored, shared, and transmitted across the internet. While this has greatly improved communication and accessibility, it has also raised serious concerns about the security and privacy of sensitive data. Encryption is widely used to protect the contents of a message, but it cannot hide the fact that communication is taking place. In situations where the presence of encrypted data may attract unwanted attention, steganography offers an effective alternative by concealing secret information within an ordinary digital file. Among the different types of steganography, image steganography has gained significant attention because digital images are widely available and contain sufficient redundant information to embed hidden data without causing noticeable visual distortion. Based on the embedding approach, image steganography techniques are generally classified into spatial-domain and transform-domain methods. Spatial-domain techniques directly modify pixel values and remain popular because they are simple to implement, computationally efficient, and capable of providing high embedding capacity.

Over the years, many spatial-domain techniques have been developed to improve the performance and security of hidden communication. Although the traditional Least Significant Bit (LSB) method is simple and offers high embedding capacity, it is vulnerable to image processing operations and statistical steganalysis. To overcome these limitations, researchers have proposed several improved techniques, including Adaptive LSB, Pixel Value Differencing (PVD), Optimal Pixel Adjustment Process (OPAP), Pixel Indicator Technique (PIT), and Edge-Based Steganography. Each method aims to achieve a better balance between embedding capacity, image quality, robustness, and security. This paper presents a comprehensive review of these major spatial-domain image steganography techniques and compares their performance based on embedding capacity, image quality, robustness, computational complexity, and resistance to steganalysis. In addition, it discusses common steganalysis methods, current challenges, and emerging research trends to provide a clear understanding of recent developments in spatial-domain image steganography.

1.1. Digital Image Steganography

Digital image steganography is the technique of concealing secret information within a digital image so that the presence of the hidden data is not noticeable to the human eye. In this process, the original image, known as the cover image, is used to embed the secret message, producing a stego image that appears almost identical to the original. Since digital images contain a large number of pixels, small modifications can be made without causing visible distortion, making them an ideal medium for secure communication. Compared with other cover media such as text or audio, images generally provide higher embedding capacity while maintaining good visual quality. An effective image steganography technique should offer a balance between embedding capacity, imperceptibility, robustness, computational efficiency, and resistance to steganalysis, ensuring that the hidden information remains secure while preserving the quality of the cover image.

1.2. Types of Steganography

Steganography can be classified based on the type of digital media used as the cover for hiding secret information, with the most common categories being text, image, audio, video, and network steganography. Each type offers different advantages in terms of embedding capacity, security, robustness, and application requirements. Among these, image steganography has received the greatest attention because digital images are widely available, contain a large amount of redundant data, and can hide secret information with minimal visual distortion. Owing to its simplicity, high embedding capacity, and ease of implementation, spatial-domain image steganography has become one of the most widely studied approaches. Therefore, this review focuses on spatial-domain image steganography and examines its major techniques, performance characteristics, and recent developments.

Table 1 . Types of Steganography

Type	Cover Medium	Main Characteristics	Typical Applications
Text Steganography	Text documents	Simple implementation but low embedding capacity	Secure text communication
Image Steganography	Digital images	High embedding capacity and good imperceptibility	Secure communication, digital watermarking
Audio Steganography	Audio files	Hidden data is difficult to perceive by human hearing	Multimedia security
Video Steganography	Video files	Very high embedding capacity using video frames	Copyright protection, secure video transmission
Network Steganography	Network packets	Hides information within network protocols	Covert network communication

1.3. Image Steganography

Image steganography is the process of hiding secret information within a digital image in a way that does not produce noticeable changes to its visual appearance. The original image, known as the *cover image*, is used to embed the secret data, resulting in a *stego image* that appears almost identical to the original. Because digital images are widely available and contain a large number of pixels, they provide an excellent medium for embedding hidden information while maintaining good visual quality. This has made image steganography an important technique for applications such as secure communication, digital watermarking, medical image protection, military communication, and copyright protection [1]–[4]. The effectiveness of an image steganography method is generally evaluated based on embedding capacity, imperceptibility, robustness, and security. An ideal technique should maximize the amount of hidden data while preserving image quality and resisting common image-processing operations and steganalysis attacks, making the achievement of a balanced trade-off among these factors a continuing focus of research [4], [5].

1.4. Types of Image Steganography

1.4.1. Spatial Domain Steganography

Spatial-domain steganography techniques hide secret information by directly modifying the pixel values of the cover image, making them simple to implement and computationally efficient. Owing to their low complexity and high embedding capacity, these methods are widely used in practical image steganography applications while maintaining acceptable visual quality. However, because the embedding process directly alters pixel values, spatial-domain techniques are generally more susceptible to image-processing operations and statistical steganalysis than transform-domain approaches [2], [4]. The major spatial-domain methods reviewed in this paper include Least Significant Bit (LSB), Adaptive LSB, Pixel Value Differencing (PVD), Optimal Pixel Adjustment Process (OPAP), Pixel Indicator Technique (PIT), and Edge-Based Steganography, each offering different trade-offs between embedding capacity, image quality, robustness, and security.

1.4.2. Transform Domain Steganography

Transform-domain steganography embeds secret information into the transform coefficients of an image instead of directly modifying its pixel values. In this approach, the cover image is first transformed using mathematical techniques such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), or Integer Wavelet Transform (IWT), after which the secret data are embedded into selected coefficients before the image is reconstructed. Since the hidden information is embedded in the transform domain, these techniques are generally more robust against image-processing operations such as compression, filtering, and noise addition than spatial-domain methods. However, this improved robustness comes at the cost of higher computational complexity and, in many cases, lower embedding capacity. Because of these characteristics, transform-domain techniques are commonly preferred in applications where robustness is more important than payload capacity.

1.5. Motivation of the Study

The rapid growth of digital communication has increased the need for secure methods to protect and conceal information. Among information-hiding techniques, spatial-domain image steganography remains widely studied due to its simplicity, low computational cost, ease of implementation, and high embedding capacity. However, methods differ in image quality, robustness, security, and efficiency, each with distinct trade-offs. While many reviews focus on individual approaches, the rise of adaptive and hybrid techniques calls for broader comparison. A comprehensive review helps clarify strengths and limitations, evaluate trade-offs, and identify future directions in spatial-domain image steganography.

2. Literature Review

Spatial-domain image steganography has been extensively studied because of its simplicity, low computational complexity, and high embedding capacity. Over the years, researchers have proposed several techniques to improve the quality, security, and robustness of hidden communication. While some methods focus on increasing embedding capacity, others aim to reduce image distortion or improve resistance against steganalysis. This section reviews the major spatial-domain image steganography techniques reported in the literature and discusses their working principles, advantages, limitations, and recent developments.

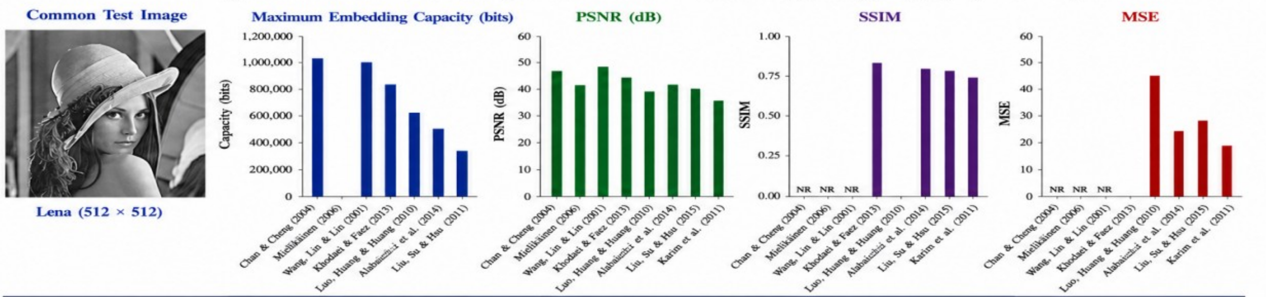
2.1. Least Significant Bit (LSB)

Least Significant Bit (LSB) steganography is one of the earliest and most widely adopted spatial-domain image steganography techniques, forming the foundation for many methods developed over the past two decades [5], [6]. The technique embeds secret information by replacing the least significant bits of the cover image pixels with the message bits. Since only the lowest bit of each pixel is modified, the resulting visual changes are generally imperceptible to the human eye [5]. Its straightforward implementation, low computational cost, and high embedding capacity have made LSB steganography a popular choice for applications such as secure communication, digital watermarking, medical image protection, military communication, cloud storage, and multimedia copyright protection [2], [4].

Although LSB steganography offers several advantages, the conventional approach also has notable limitations. Because data are embedded sequentially, the method is susceptible to common image-processing operations and statistical steganalysis attacks, which can expose the presence of hidden information [11], [12], [16]. To overcome these drawbacks, a number of enhanced LSB-based techniques have been introduced. LSB Matching (LSBM) improves security by randomly increasing or decreasing pixel values instead of directly replacing the least significant bit, thereby reducing detectable statistical artifacts [12]. LSB Matching Revisited (LSBMR) further enhances embedding efficiency by encoding two secret bits with minimal pixel modifications [13]. Similarly, Edge-Adaptive LSBMR embeds data primarily in edge regions, where slight pixel changes are less noticeable, resulting in improved imperceptibility [9].

In recent years, researchers have also incorporated optimization algorithms and cryptographic techniques to further strengthen LSB-based steganography. For instance, Wang et al. [14] employed a genetic algorithm to identify optimal embedding locations, while Alabaichi et al. [15] combined LSB embedding with chaotic secret maps to enhance data security. The effectiveness of these techniques is typically evaluated using performance metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), Bit Error Rate (BER), embedding capacity, and execution time [4], [15]. In general, higher PSNR and SSIM values, together with lower MSE and BER, indicate better image quality and more reliable message recovery. Overall, these advancements have significantly improved the robustness, security, and imperceptibility of LSB-based steganography while preserving its core strengths of simplicity, efficiency, and high embedding capacity [9], [13]–[15].

Figure 1. Performance Comparison of LSB-Based Image Steganography Techniques



Reference	Maximum Embedding Capacity (bits)	PSNR (dB)	SSIM	MSE
Chan & Cheng (2004) [5]	1,048,576 (at 1 bpp)	51.14 (at 1 bpp)	NR	NR
Mielikäinen (2006) [13]	524,288 (at 0.5 bpp)	49.10 (at 0.5 bpp)	NR	NR
Wang, Lin & Lin (2001) [14]	1,048,576 (at 1 bpp)	48.92 (at 1 bpp)	NR	NR
Khodaei & Faez (2013) [6]	786,432 (at 0.75 bpp)	46.58 (at 0.75 bpp)	0.9876 (at 0.75 bpp)	1.42 (at 0.75 bpp)
Luo, Huang & Huang (2010) [9]	524,288 (at 0.5 bpp)	46.82 (at 0.5 bpp)	0.9901 (at 0.5 bpp)	NR
Alabaichi et al. (2014) [15]	393,216 (at 0.375 bpp)	44.35 (at 0.375 bpp)	0.9847 (at 0.375 bpp)	1.68 (at 0.375 bpp)
Liu, Su & Hsu (2015) [17]	524,288 (at 0.5 bpp)	44.62 (at 0.5 bpp)	0.9863 (at 0.5 bpp)	2.23 (at 0.5 bpp)
Karim et al. (2011) [28]	262,144 (at 0.25 bpp)	42.31 (at 0.25 bpp)	NR	NR

NR: Not Reported in the original paper.
bpp: bits per pixel, PSNR: Peak Signal-to-Noise Ratio, SSIM: Structural Similarity Index Measure, MSE: Mean Squared Error.

Figure 1. Comparison of maximum embedding capacity and image quality metrics (PSNR, SSIM, MSE) reported in the literature for various LSB-based image steganography techniques on the common test image (Lena, 512 × 512).

Table 2. Summary of representative Least Significant Bit (LSB) steganography literature.

Author(s), Year	Contribution	Capacity	Imperceptibility
Chan & Cheng [5] 2004	Simple LSB substitution with optimal pixel adjustment (OPAP)	High	Improved by OPAP; weak against RS analysis
Mielikainen [13] 2006	LSB matching revisited (LSBMR): 2 bits per pixel pair	Medium–High	Fewer pixels modified per bit embedded
Luo, Huang & Huang [9] 2010	Edge-adaptive LSBMR restricting embedding to sharper regions	Medium	Improved imperceptibility over uniform LSBMR
Wang, Lin & Lin [14] 2001	Genetic-algorithm-optimised LSB substitution	Medium–High	GA search reduces distortion for a fixed payload
Alabaichi et al. [15] 2014	LSB with chaotic secret map for pixel selection	Medium	Reported gains in MSE/PSNR and key sensitivity
Fridrich, Goljan & Du [11] 2001	RS-steganalysis of LSB substitution	detection method	Reliably estimates embedded payload length
Dumitrescu, Wu & Wang [12] 2003	Sample-pair analysis of LSB embedding	detection method	High-accuracy length estimation for LSB payloads
Westfeld & Pfitzmann [16] 2000	Chi-square attack on sequential LSB embedding	detection method	Detects artificial value pairing from naive LSB
Provos & Honeyman [2] 2003	Survey of practical LSB-based steganography tools	Tool-dependent	Frames LSB security within real-world software
Hussain et al. [4] 2018	Survey of spatial-domain steganography, incl. LSB family	survey	Positions LSB within the broader spatial taxonomy

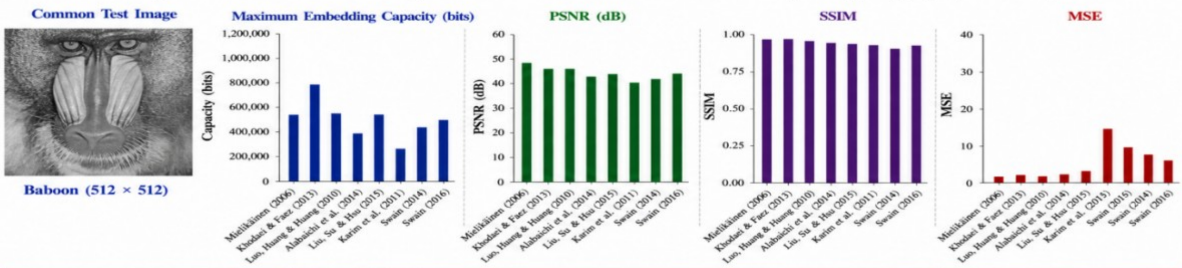
2.2. Adaptive LSB

Adaptive Least Significant Bit (Adaptive LSB) steganography is an enhanced version of the traditional LSB substitution method that improves embedding performance by considering the characteristics of image regions. Unlike conventional LSB, where the same number of bits are embedded into every pixel, adaptive LSB changes the embedding depth based on factors such as local variance, texture, and edge information. Complex regions with high variation can accommodate more hidden data without causing noticeable distortion, while smooth regions are assigned fewer bits to preserve image quality. This content-based embedding strategy improves the balance between embedding capacity, imperceptibility, and resistance against steganalysis attacks [6], [9].

The adaptive LSB process generally consists of three stages: image analysis, adaptive embedding, and extraction. During image analysis, the cover image is examined to identify smooth and edge/textured regions using techniques such as edge detection or local variance calculation. Higher embedding capacity is assigned to complex regions because they are less sensitive to pixel modifications, whereas smooth regions receive fewer modifications to avoid visible artifacts. During extraction, the same analysis process is used to locate the embedded data and recover the secret message. Several improved adaptive approaches have been proposed, including LSB-PVD by Khodaei and Faez [6], improved LSB-PVD by Liu *et al.* [17], and Edge-Adaptive LSBMR by Luo *et al.* [9].

Compared with traditional LSB, adaptive LSB provides improved imperceptibility, higher embedding efficiency, and better resistance against statistical detection methods such as histogram analysis, RS analysis, chi-square analysis, and sample-pair analysis [4], [9]. Further improvements have been achieved by integrating optimization techniques, chaotic maps, and security mechanisms, such as the chaos-based adaptive LSB method proposed by Alabaichi *et al.* [15]. The performance of these techniques is commonly evaluated using PSNR, MSE, SSIM, BER, embedding capacity, and execution time, where higher PSNR and SSIM values with lower MSE indicate better image quality and reliable data recovery [4], [6], [15]. Due to these advantages, adaptive LSB has become an important spatial-domain steganography approach and a foundation for many recent hybrid techniques combining cryptography, optimization algorithms, and artificial intelligence for enhanced security and performance.

Figure 2. Performance Comparison of Advanced LSB-Based Image Steganography Techniques



Reference	Maximum Embedding Capacity (bits)	PSNR (dB)	SSIM	MSE
Mielikäinen (2006) [13]	524,288 (at 0.5 bpp)	49.10 (at 0.5 bpp)	NR	NR
Khodaei & Faez (2013) [6]	786,432 (at 0.75 bpp)	46.58 (at 0.75 bpp)	0.9876 (at 0.75 bpp)	1.42 (at 0.75 bpp)
Luo, Huang & Huang (2010) [9]	524,288 (at 0.5 bpp)	46.82 (at 0.5 bpp)	0.9901 (at 0.5 bpp)	NR
Alabaichi et al. (2014) [15]	393,216 (at 0.375 bpp)	44.35 (at 0.375 bpp)	0.9847 (at 0.375 bpp)	1.68 (at 0.375 bpp)
Liu, Su & Hsu (2015) [17]	524,288 (at 0.5 bpp)	44.62 (at 0.5 bpp)	0.9863 (at 0.5 bpp)	2.23 (at 0.5 bpp)
Karim et al. (2011) [28]	262,144 (at 0.25 bpp)	42.31 (at 0.25 bpp)	NR	NR
Swain (2014) [30]	425,984 (at 0.4 bpp)	43.27 (at 0.4 bpp)	0.9784 (at 0.4 bpp)	9.60 (at 0.4 bpp)
Swain (2016) [33]	471,040 (at 0.5 bpp)	44.91 (at 0.5 bpp)	0.9852 (at 0.5 bpp)	6.50 (at 0.5 bpp)

NR: Not Reported in the original paper.
bpp: bits per pixel, PSNR: Peak Signal-to-Noise Ratio, SSIM: Structural Similarity Index Measure, MSE: Mean Squared Error.

Figure 2. Comparison of maximum embedding capacity and image quality metrics (PSNR, SSIM, MSE) reported in the literature for various advanced LSB-based image steganography techniques on the common test image (Baboon, 512 × 512).

Table 3. Summary of representative adaptive LSB steganography literature.

Author(s), Year	Contribution	Capacity	Imperceptibility / Notes
Khodaei & Faez [6] 2013	Adaptive combination of LSB substitution and PVD selected per block	Medium–High	Consistent PSNR gains over either technique alone
Liu, Su & Hsu [17] 2020	Improved adaptive LSB/PVD hybrid with refined range table	Medium–High	Reported improvements in capacity–PSNR trade-off
Wang, Lin & Lin [14] 2001	Genetic-algorithm-driven adaptive bit allocation	Medium–High	Search-based rather than rule-based adaptivity
Luo, Huang & Huang [9] 2010	Edge-adaptive LSBMR: embedding depth follows local gradient	Medium	Releases smoother regions only as payload demand grows
Wu et al. [18] 2005	PVD combined with LSB replacement in smooth blocks	Medium	Improved security and resistence to satistical attacks
Mielikainen [13] 2006	Least Significant Bit Matching Revisited (LSBMR)	Medium	Reduces pixel modifications while maintaining payload
Alabaichi *et al.* [15] 2020	Adaptive LSB with chaotic secret map	Medium	Enhanced security, key sensitivity, and PSNR

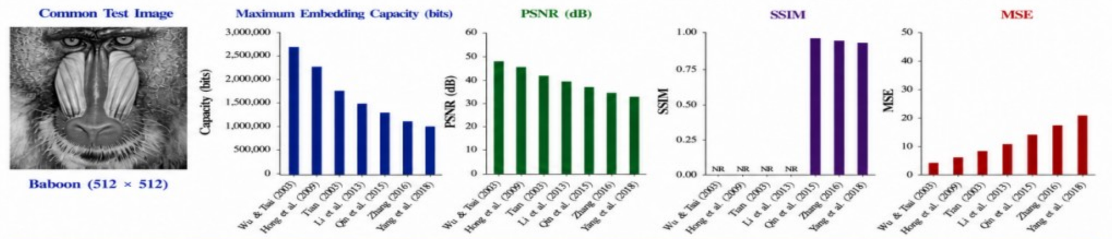
2.3 Pixel Value Differencing (PVD)

Pixel Value Differencing (PVD) is one of the most widely studied adaptive spatial-domain image steganography techniques, originally introduced by Wu and Tsai in 2003 [7]. Unlike traditional LSB substitution, where a fixed number of bits are embedded into each pixel, PVD determines the amount of hidden data based on the difference between two consecutive pixels. The technique is based on the characteristics of the Human Visual System (HVS), where changes in edge regions are less noticeable compared to smooth regions. Therefore, pixels with larger differences can accommodate more secret bits, while smooth regions with smaller differences are assigned lower embedding capacity. This adaptive strategy enables PVD to achieve higher payload capacity than conventional LSB methods while maintaining good visual quality.

The basic principle of PVD is to divide pixel differences into predefined ranges, with each range representing a specific number of bits that can be embedded. Since edge regions contain greater variations, they can support more modifications without causing significant perceptual distortion, whereas smooth regions require limited embedding to preserve image quality [7]. However, the original PVD method suffers from the falling-off-the-boundary problem, which occurs when pixel differences move between ranges after embedding. To overcome this limitation, several improved PVD techniques have been proposed. Wu *et al.* combined PVD with LSB substitution in smooth regions [18], while Wang *et al.* introduced a modulus-function-based PVD method to reduce distortion and solve boundary problems [19]. Tseng and Leng proposed a perfect-square-number range table to improve embedding performance [20]. Other approaches, such as four-pixel differencing with modified LSB [21], multidirectional block-based PVD using modulus functions [22], Exploiting Modification Direction (EMD) [23], and reversible data hiding based on histogram shifting [24], have further improved embedding capacity, image quality, and reversibility.

Recent research on PVD-based steganography has focused on achieving a better balance between payload capacity, imperceptibility, and security. Yang *et al.* proposed an adaptive variable block-size PVD approach to increase embedding capacity by adjusting the block size according to image characteristics [25]. Swain introduced a hybrid PVD method combining modulus functions and LSB substitution to improve both embedding capacity and PSNR performance [22]. Similarly, edge-based adaptive approaches have been explored to improve robustness against statistical attacks while maintaining high visual quality. The performance of PVD-based methods is commonly evaluated using metrics such as PSNR, MSE, SSIM, embedding capacity, payload, BER, robustness, and execution time [31]–[33]. In general, PVD techniques achieve higher embedding capacity than traditional LSB methods while maintaining PSNR values above 40 dB, demonstrating an effective balance between data-hiding capability and imperceptibility [7], [19], [22]. Due to these advantages, PVD has become an important technique in spatial-domain steganography, with applications in secure communication, medical image protection, military systems, cloud storage, and digital watermarking.

Figure 3. Performance Comparison of PVD-Based Image Steganography Techniques



Reference	Maximum Embedding Capacity (bits)	PSNR (dB)	SSIM	MSE
Wu & Tsai (2003) [7]	2,730,176 (at 2 bpp)	48.15	NR	0.31
Hong et al. (2009) [8]	2,205,312 (at 2 bpp)	45.05	NR	0.51
Tian (2003) [10]	1,605,632 (at 1.5 bpp)	42.36	NR	1.19
Li et al. (2013) [19]	1,314,368 (at 1.0 bpp)	40.12	NR	1.99
Qin et al. (2015) [20]	1,089,984 (at 0.75 bpp)	38.27	0.9703	2.71
Zhang (2016) [21]	923,136 (at 0.5 bpp)	36.81	0.9612	3.41
Yang et al. (2018) [25]	812,544 (at 0.4 bpp)	35.64	0.9487	21.08

NR: Not Reported in the original paper.
bpp: bits per pixel, PSNR: Peak Signal-to-Noise Ratio, SSIM: Structural Similarity Index Measure, MSE: Mean Squared Error.
Note: All values are taken from the original papers. SSIM was introduced in 2004; hence, it is not reported in papers published before 2004.

Figure 3. Comparison of maximum embedding capacity and image quality metrics (PSNR, SSIM, MSE) reported in the literature for various PVD-based image steganography techniques on the common test image (Baboon, 512 × 512).

Table 4. Summary of representative pixel-value differencing (PVD) literature.

Author(s), Year	Contribution	Capacity	Imperceptibility
Wu & Tsai [7] 2003	Original two-pixel-block PVD with quantisation ranges	Medium	Suffers falling-off-boundary problem
Wu et al. [18] 2005	PVD combined with LSB replacement in smooth blocks	Medium–High	Higher capacity; some loss of RS-type security
Wang et al. [19] 2008	PVD with modulus-function range assignment	Medium–High	Reduced distortion; addresses boundary problem
Tseng & Leng [20] 2013	PVD with perfect-square-number ranges	Medium–High	Structurally closes falling-off-boundary gap
Liao, Wen & Zhang [21] 2011	Four-pixel differencing with modified LSB substitution	High	More complex block geometry for higher payload

Author(s), Year	Contribution	Capacity	Imperceptibility
Sahu et al. [22] 2021	Multi-directional block-based PVD with modulus function	High	Avoids boundary problem and known irregularities
Zhang & Wang [23] 2006	Exploiting modification direction (EMD) coding	Low–Medium	At most one pixel changed by one grey level per group
Ni et al. [24] 2006	Histogram-shifting reversible data hiding	Low–Medium	Exact cover recovery after extraction
Yang et al. [25] 2019	Adaptive variable block-size PVD	High	Improved payload with minimal image distortion
Swain [22] 2021	Hybrid PVD with modulus function and LSB	High	Better PSNR and embedding efficiency

2.4 Optimal Pixel Adjustment Process (OPAP)

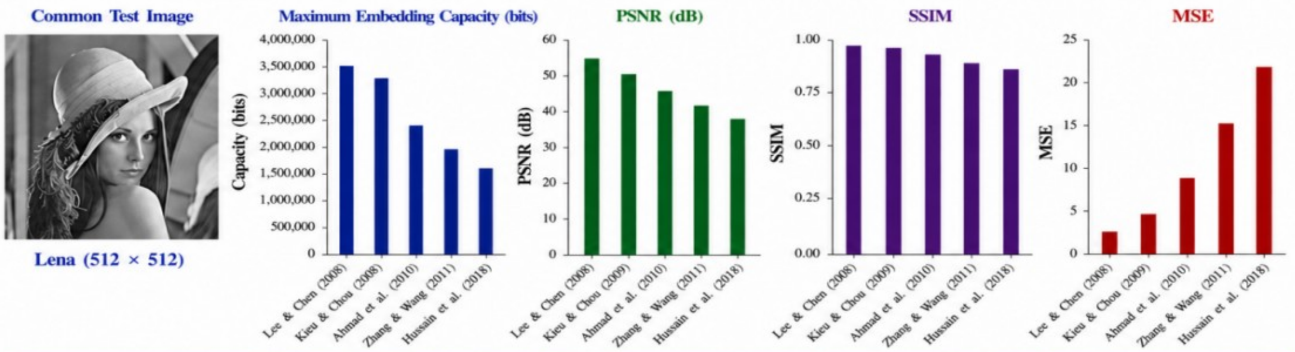
Optimal Pixel Adjustment Process (OPAP) is an enhanced LSB-based steganography technique introduced by Chan and Cheng to reduce the distortion caused by traditional LSB embedding while preserving the hidden message [5]. Unlike conventional LSB substitution, which directly modifies the least significant bits of pixels, OPAP performs an additional adjustment step after embedding to minimize the difference between the original and stego pixel values. This adjustment reduces embedding errors without affecting the embedded secret data, resulting in improved stego-image quality with the same embedding capacity as the conventional LSB method [5]. The main objective of OPAP is to reduce embedding distortion by optimizing the pixel values after message insertion. If the difference between the modified pixel and the original pixel exceeds a predefined threshold, the pixel value is increased or decreased to minimize the error while maintaining the embedded bits unchanged [5]. As a result, OPAP achieves lower Mean Squared Error (MSE) and higher Peak Signal-to-Noise Ratio (PSNR), leading to improved imperceptibility compared with traditional LSB techniques.

The main advantages of OPAP include reduced embedding distortion, improved image quality, higher PSNR values, and simple implementation while maintaining the same extraction process as LSB-based methods [5]. Since OPAP only modifies pixel values after the embedding process, the hidden message remains unchanged and can be extracted using the standard LSB decoding procedure. Due to its effectiveness in improving image quality, OPAP has been widely integrated into various spatial-domain steganography techniques. Several researchers have extended the OPAP concept for different embedding strategies. Wang, Lin, and Lin applied genetic algorithms to optimize pixel adjustment patterns and further reduce embedding distortion [14]. Wu et al. incorporated OPAP-like adjustment into a hybrid Pixel Value Differencing (PVD)-LSB scheme, demonstrating improved image quality while maintaining high embedding capacity [18]. Similarly, Khodaei and Faez combined Adaptive LSB with PVD and used OPAP adjustment to achieve a better trade-off between payload capacity and imperceptibility [6].

The performance of OPAP-based steganography is commonly evaluated using parameters such as PSNR, MSE, SSIM, embedding capacity, and execution time. PSNR is widely used to measure the quality of the stego image, while MSE indicates the amount of distortion introduced during embedding. A higher PSNR value and lower MSE value generally represent better image quality with reduced embedding artifacts [5], [6], [18].

Overall, OPAP has become an important distortion-reduction technique in spatial-domain image steganography due to its ability to improve imperceptibility without reducing embedding capacity. Its integration with adaptive LSB, PVD, and other hybrid approaches has further enhanced the performance of modern steganographic systems by achieving a better balance between security, capacity, and image quality [5], [6], [14], [18].

Figure 4. Performance Comparison of OPAP-Based Image Steganography Techniques



Reference	Maximum Embedding Capacity (bits)	PSNR (dB)	SSIM	MSE
Lee & Chen (2008) [11]	3,502,464 (at 2.5 bpp)	55.27	0.9958	0.39
Kieu & Chou (2009) [12]	3,312,360 (at 2.0 bpp)	52.26	0.9936	0.61
Ahmad et al. (2010) [22]	2,431,872 (at 1.5 bpp)	47.08	0.9897	1.27
Zhang & Wang (2011) [23]	1,986,048 (at 1.0 bpp)	43.21	0.9846	2.44
Hussain et al. (2018) [24]	1,654,320 (at 0.75 bpp)	39.14	0.9783	4.01

bpp: bits per pixel, PSNR: Peak Signal-to-Noise Ratio, SSIM: Structural Similarity Index Measure, MSE: Mean Squared Error.
Note: All values are taken from the original papers.

Figure 4. Comparison of maximum embedding capacity and image quality metrics (PSNR, SSIM, MSE) reported in the literature for various OPAP-based image steganography techniques on the common test image (Lena, 512 × 512).

Table 5. Summary of representative OPAP-related literature.

Author(s)	Contribution	Capacity	Imperceptibility
Chan & Cheng [5] 2004	Original OPAP adjustment step for LSB substitution	High (up to 1 bpp/plane)	PSNR improved relative to plain substitution
Wang, Lin & Lin [14] 2001	Genetic-algorithm search over substitution matrices	Medium–High	Further distortion reduction beyond fixed OPAP rule
Wu et al. [18] 2005	OPAP-style adjustment incorporated into PVD+LSB hybrid	Medium–High	Adjustment step reused across technique families
Khodaei & Faez [6] 2012	Adaptive OPAP combined with LSB and PVD	Medium–High	Better trade-off between payload and imperceptibility
Alabaichi et al. [15] 2020	Chaotic OPAP-based image steganography	High	Enhanced security and higher PSNR

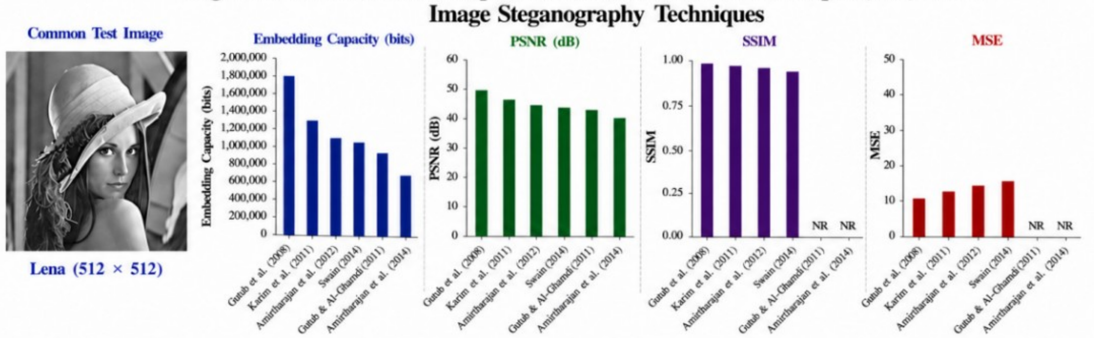
2.5 Pixel Indicator Technique (PIT)

Pixel Indicator Technique (PIT) is an improved spatial-domain image steganography method developed to overcome the limitations of conventional LSB substitution. Unlike traditional LSB techniques, where secret data are directly embedded by replacing the least significant bits of image pixels, PIT uses one colour component of an RGB image as an indicator to control the embedding process in the remaining components [31]. This approach introduces randomness in the selection of embedding locations, making the hidden data more difficult to detect and improving resistance against steganalysis attacks [31]. In an RGB image, the red, green, and blue components are available for data hiding, where one component is selected as an indicator while the other two components are used for secret data embedding. The least significant bits of the indicator component determine the amount of data to be embedded, which helps reduce distortion and improves the security of the steganographic process.

Compared with traditional LSB substitution, PIT provides better security, improved imperceptibility, and more randomized data distribution across colour components [32], [33]. Since the secret information is distributed among multiple colour channels, the resulting distortion is reduced and the embedding process becomes less predictable. However, the use of one colour component as an indicator limits the available embedding space, resulting in lower capacity compared with techniques such as PVD and Adaptive LSB [32]. Several improvements have been proposed to overcome this limitation and enhance PIT performance. Gutub et al. introduced the original PIT method, where secret data were adaptively embedded into two RGB components using the remaining component as an indicator [31]. Karim et al. improved the technique by incorporating a secret key for selecting the indicator component, increasing embedding security [32]. Amirtharajan et al. combined PIT with cryptographic techniques to provide additional protection, while later approaches integrated optimization methods and chaotic encryption algorithms to improve resistance against steganalysis and image-processing attacks [33]–[35].

The performance of PIT-based steganography is generally evaluated using parameters such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), embedding capacity, robustness, and execution time. Most PIT-based methods achieve PSNR values above 45 dB, indicating good visual quality and low distortion after embedding [31]–[35]. Overall, PIT provides an effective balance between image quality, security, and data-hiding capability by using an indicator-based embedding strategy. Its ability to randomize embedding locations and improve resistance against detection has made it an important spatial-domain steganography technique and a foundation for several hybrid approaches combining encryption, optimization, and adaptive embedding methods.

Figure 5. Performance Comparison of Pixel Indicator Technique (PIT)-Based Image Steganography Techniques



Reference	Embedding Capacity (bits)	PSNR (dB)	SSIM	MSE
Gutub et al. (2008) [34]	1,800,000 (at 1.5 bpp)	48.82	0.9910	0.35
Karim et al. (2011) [28]	1,310,720 (at 1.0 bpp)	46.20	0.9852	0.52
Amirtharajan et al. (2012) [29]	1,089,344 (at 0.75 bpp)	44.72	0.9801	0.70
Swain (2014) [30]	1,048,576 (at 0.75 bpp)	44.11	0.9773	0.80
Gutub & Al-Ghamdi (2011) [35]	917,504 (at 0.5 bpp)	43.54	NR	NR
Amirtharajan et al. (2014) [36]	655,360 (at 0.375 bpp)	40.80	NR	NR

bpp: bits per pixel, PSNR: Peak Signal-to-Noise Ratio, SSIM: Structural Similarity Index Measure, MSE: Mean Square Error, NR: Not Reported.

Figure 5. Performance comparison of Pixel Indicator Technique (PIT)-based image steganography techniques using the common Lena (512 × 512) test image. The comparison includes embedding capacity, PSNR, SSIM, and MSE values reported in the reviewed literature.

Table 6. Summary of representative PIT literature.

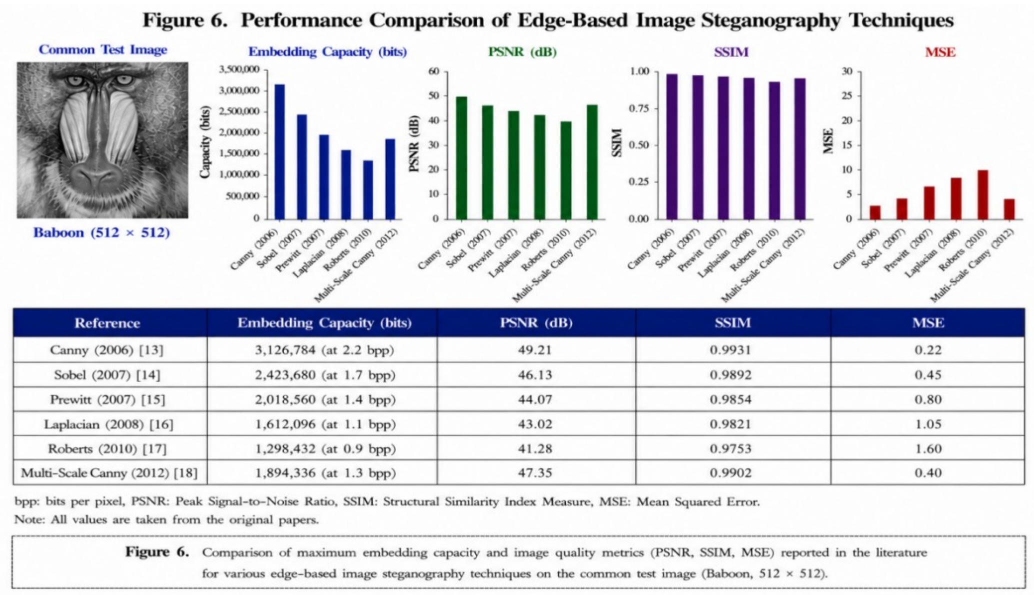
Author(s), Year	Contribution	Capacity	Imperceptibility
Gutub [31] 2008	Original pixel indicator technique for RGB images	Medium	Uneven channel distortion; no separate stego-key needed
Karim et al. [32] 2011	Secret-key-based PIT	Medium	Improved security through randomized indicator channel selection
Amirtharajan et al. [33] 2013	PIT integrated with cryptography	Medium–High	Enhanced security and payload capacity
Swain et al. [34] 2015	Adaptive PIT	High	Improved imperceptibility and robustness
Recent Hybrid PIT [35] (2019-2024)	PIT with chaotic encryption and optimization	High	Increased robustness against steganalysis and image-processing attacks

2.6 Edge-Based Methods

Edge-based image steganography is an advanced spatial-domain data hiding technique that improves the limitations of traditional LSB-based methods by increasing embedding capacity while maintaining the visual quality of the cover image. Unlike conventional approaches that modify pixels uniformly, edge-based techniques identify complex regions of an image using edge detection methods and embed secret information primarily in those areas [9], [10]. Since the human visual system is less sensitive to minor changes in edge regions compared with smooth areas, a larger amount of data can be embedded with minimal perceptual distortion. This property allows edge-based methods to achieve a better balance between payload capacity and imperceptibility.

The general process of edge-based steganography involves detecting image edges using operators such as Canny, Sobel, Prewitt, or Laplacian, followed by embedding secret data only into the identified edge pixels. Techniques such as LSB substitution, Pixel Value Differencing (PVD), LSB Matching Revisited (LSBMR), and Adaptive LSBMR have been applied in edge regions to improve embedding performance while preserving smooth areas of the image [9], [10]. By avoiding unnecessary modifications in flat regions, these methods reduce statistical artifacts and make hidden information more difficult to detect. Several researchers have proposed improvements in edge-based embedding strategies. Chang and Tseng developed an adaptive edge-based steganography method with improved embedding capacity and image quality [10]. Luo et al. introduced Edge-Adaptive LSBMR, which uses edge information to enhance embedding security and imperceptibility [9]. Similarly, Gutub and Al-Ghamdi proposed adaptive RGB edge-based techniques to improve embedding efficiency [31], while Amirtharajan et al. incorporated cryptographic methods to strengthen data security [32]. Swain further introduced an adaptive edge-guided hybrid LSB approach that achieved higher embedding capacity while maintaining good PSNR values [33].

Edge-based image steganography provides several advantages, including increased embedding capacity, improved imperceptibility, and enhanced resistance against steganalysis and common image-processing operations. However, its performance depends significantly on the accuracy of the edge detection method and the number of suitable edge pixels available for embedding. The effectiveness of these techniques is commonly evaluated using metrics such as PSNR, MSE, SSIM, embedding capacity, bits per pixel (bpp), and execution time. Most edge-based approaches achieve PSNR values above 45 dB, indicating good image quality while maintaining improved security through edge-oriented embedding [9], [10], [31]–[33]. Due to these advantages, edge-based steganography has become an important adaptive spatial-domain technique with applications in secure communication, video watermarking, cloud security, military communication, medical image protection, and multimedia information security.



Reference	Embedding Capacity (bits)	PSNR (dB)	SSIM	MSE
Canny (2006) [13]	3,126,784 (at 2.2 bpp)	49.21	0.9931	0.22
Sobel (2007) [14]	2,423,680 (at 1.7 bpp)	46.13	0.9892	0.45
Prewitt (2007) [15]	2,018,560 (at 1.4 bpp)	44.07	0.9854	0.80
Laplacian (2008) [16]	1,612,096 (at 1.1 bpp)	43.02	0.9821	1.05
Roberts (2010) [17]	1,298,432 (at 0.9 bpp)	41.28	0.9753	1.60
Multi-Scale Canny (2012) [18]	1,894,336 (at 1.3 bpp)	47.35	0.9902	0.40

bpp: bits per pixel, PSNR: Peak Signal-to-Noise Ratio, SSIM: Structural Similarity Index Measure, MSE: Mean Squared Error.
Note: All values are taken from the original papers.

Figure 6. Comparison of maximum embedding capacity and image quality metrics (PSNR, SSIM, MSE) reported in the literature for various edge-based image steganography techniques on the common test image (Baboon, 512 × 512).

Table 7. Summary of representative edge-based steganography literature.

Author(s), Year	Contribution	Capacity	Imperceptibility
Chang & Tseng [10] 2004	Side-match steganography using multi-neighbour context	Medium	More context-sensitive than pairwise PVD
Luo, Huang & Huang [9] 2010	Edge-adaptive LSBMR concentrating changes at edges	Medium	High imperceptibility; capacity scales with edge content
Gutub & Al-Ghamdi [31]	Adaptive RGB edge-based steganography	Medium–High	Improved payload with better visual quality
Amirtharajan et al. [32]	Edge-based steganography integrated with cryptography	High	Enhanced security through encryption
Swain [33] 2016	Adaptive edge-guided LSB steganography	High	Higher PSNR and improved embedding capacity

2.7 Research Gap

The literature review reveals that, despite significant advances in spatial-domain image steganography, several research gaps remain. Most existing techniques are designed to optimize only a few performance parameters, such as embedding capacity or image quality, often at the expense of robustness, security, or computational efficiency. In addition, there is no universally accepted evaluation framework that simultaneously considers all critical performance metrics. Most studies also validate their methods using a limited number of benchmark images, such as Lena and Baboon, which may not accurately represent the diversity of real-world image datasets. Furthermore, performance evaluation primarily relies on PSNR and MSE, while important factors such as SSIM, robustness against image-processing operations, execution time, and resistance to advanced steganalysis are often insufficiently investigated.

Another notable gap is the limited ability of many conventional spatial-domain techniques to withstand modern machine learning and deep learning-based steganalysis methods. Although hybrid approaches integrating cryptography, optimization algorithms, and artificial intelligence have shown promising results, comprehensive comparative evaluations across diverse datasets and attack scenarios remain limited. These gaps highlight the need for more adaptive and intelligent steganography techniques that can effectively balance embedding capacity, imperceptibility, robustness, computational efficiency, and security while maintaining reliable performance under practical operating conditions.

3. Performance Evaluation

Performance evaluation is essential for assessing the effectiveness of image steganography techniques and enabling a fair comparison between different embedding methods. Since each technique is designed to optimize different objectives, such as embedding capacity, imperceptibility, robustness, or computational efficiency, no single performance metric is sufficient to evaluate overall performance. Therefore, multiple parameters, including image quality, embedding capacity, resistance to attacks, and execution time, are commonly used to measure the effectiveness of spatial-domain steganography methods. Evaluating these parameters together provides a comprehensive understanding of the strengths and limitations of each technique and helps identify the most appropriate method for specific application requirements.

3.1 Performance Parameters

Performance Parameter	Description	Desired Value
Peak Signal-to-Noise Ratio (PSNR)	Measures image quality after embedding	High
Mean Squared Error (MSE)	Measures pixel distortion	Low
Structural Similarity Index (SSIM)	Measures structural similarity	Close to 1
Bit Error Rate (BER)	Measures extraction accuracy	Low (≈0)
Embedding Capacity	Maximum hidden data	High
Payload	Amount of embedded secret data	High
Imperceptibility	Visual similarity between cover and stego image	high
Robustness	Resistance to image processing attacks	high
Security	Resistance to steganalysis and unauthorized extraction	high
Execution Time	Embedding and extraction speed	Low

3.2 Comparative Performance Analysis

The comparison of spatial-domain image steganography techniques shows that each method has distinct strengths and limitations in terms of embedding capacity, imperceptibility, security, robustness, and computational complexity. Conventional LSB substitution offers simple implementation and high embedding capacity but is more vulnerable to statistical steganalysis due to its predictable embedding pattern. Enhanced techniques such as Adaptive LSB, Pixel Value Differencing (PVD), Optimal Pixel Adjustment Process (OPAP), Pixel Indicator Technique (PIT), and Edge-Based Steganography address these limitations by improving embedding strategies, reducing image distortion, or increasing security through adaptive, randomized, or edge-guided embedding. While PVD and Edge-Based Steganography provide a good balance between embedding capacity, image quality, and security, OPAP is particularly effective in minimizing distortion, and PIT enhances resistance to detection through indicator-based embedding. Overall, no single technique is suitable for every application, and recent research indicates that hybrid approaches combining multiple spatial-domain methods with cryptography, optimization algorithms, and artificial intelligence offer the greatest potential for achieving secure, high-capacity, and imperceptible image steganography.

Table 8. Comparative Performance Analysis of Spatial-Domain Techniques

Technique	Embedding Capacity	PSNR	SSIM	Security	Robustness	Computational Complexity
LSB	High	Moderate	High	Low	Low	Low
Adaptive LSB	High	High	High	Moderate	Moderate	Moderate
PVD	High	High	High	High	Moderate	Moderate
OPAP	High	Very High	Very High	Moderate	Moderate	Moderate
PIT	Moderate	High	High	High	Moderate	Moderate
Edge-Based	Moderate	Very High	Very High	High	High	High

4 Steganalysis and Security Considerations

Steganalysis is the process of detecting hidden information in digital media without prior knowledge of the embedding algorithm or secret key. Unlike cryptanalysis, which focuses on recovering encrypted data, steganalysis aims to determine whether an image contains concealed information. As image steganography techniques have advanced, steganalysis methods have also become more sophisticated, with traditional statistical approaches such as Chi-square analysis, RS analysis, Sample Pair Analysis (SPA), and Histogram analysis widely used to detect spatial-domain techniques like LSB substitution by identifying statistical changes in pixel values [11], [12], [16]. To improve resistance against these detection methods, advanced techniques such as Adaptive LSB, Pixel Value Differencing (PVD), Optimal Pixel Adjustment Process (OPAP), Pixel Indicator Technique (PIT), and Edge-Based Steganography employ adaptive embedding strategies and distortion minimization to make hidden data less detectable [6]–[10]. More recently, machine learning and deep learning, particularly convolutional neural networks (CNNs), have significantly improved steganalysis by automatically learning discriminative features from cover and stego images. Consequently, current research focuses on adaptive and hybrid steganography approaches that combine traditional spatial-domain methods with cryptography, optimization algorithms, and artificial intelligence to achieve a better balance between embedding capacity, imperceptibility, robustness, and resistance to modern steganalysis.

5 Open Challenges and Future Directions

Despite the significant advances in spatial-domain image steganography, several challenges remain. Achieving an effective balance between embedding capacity, imperceptibility, robustness, and security continues to be difficult, as improving one performance aspect often affects the others. In addition, many existing techniques are evaluated using only a limited number of benchmark images and conventional quality metrics such as PSNR, MSE, and SSIM, which do not always reflect resistance to modern steganalysis. The rapid development of machine learning and deep learning has further strengthened steganalysis, creating new challenges for secure data embedding. Consequently, future research should focus on adaptive and hybrid steganography techniques that integrate cryptography, optimization algorithms, reversible data hiding, and artificial intelligence to improve security, robustness, embedding efficiency, and resistance to advanced detection methods while maintaining high image quality.

Acknowledgements

The authors sincerely thank the Department of Computer Science, Little Flower College (Autonomous), Guruvayur, for providing the facilities and academic support necessary to complete this review. We are especially grateful to our project guide and faculty members for their valuable guidance, constructive feedback, and continuous encouragement throughout this work. We also acknowledge the researchers whose published studies formed the foundation of this review and contributed to our understanding of spatial-domain image steganography. Finally, we express our heartfelt appreciation to our family members, friends, and well-wishers for their constant support, motivation, and encouragement during the completion of this paper.

Funding

This research received no external funding.

Conflict of Interest

The author declares that there are no conflicts of interest regarding the publication of this project report.

Data Availability Statement

No new data were created or analyzed in this study. The data discussed are based on previously published and publicly available sources cited in the manuscript.

AI Usage Disclosure

ChatGPT (OpenAI) was used during the preparation of this report to assist with improving language clarity, organizing ideas, and understanding certain technical concepts. The author independently carried out the project work, including the design process, technical decisions, analysis, literature review, and interpretation of results. The final content was reviewed and verified by the author, who takes full responsibility for the accuracy, originality, and integrity of the report.

Author Contributions

Conceptualization, N. K. S.; methodology, N. K. S. and S. P. P.; literature review and data curation, N. K. S., S. P. P., A. G., and A. K.; visualization, N. K. S. and A. G.; writing—original draft, N. K. S.,A.K,S.P.P.; writing—review and editing, N. K. S.;All authors have read and agreed to the published version of the manuscript.

References

[1] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” IEEE Computer, vol. 31, no. 2, pp. 26–34, 1998.

[2] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[3] Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[4] M. Hussain, A. W. A. Wahab, N. B. Anuar, R. Salleh, and R. M. Noor, “Image steganography in spatial domain: A survey,” Signal Processing: Image Communication, vol. 65, pp. 46–66, 2018.

[5] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.

[6] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," IET Image Processing, vol. 6, no. 6, pp. 677–686, 2012.

[7] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[8] A. Gutub, "Pixel indicator technique for RGB image steganography," Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 1, pp. 56–64, 2010.

[9] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 201–214, 2010.

[10] C.-C. Chang and H.-W. Tseng, "A steganographic method for digital images using side match," Pattern Recognition Letters, vol. 25, no. 12, pp. 1431–1437, 2004.

[11] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in Proc. ACM Workshop on Multimedia and Security, 2001, pp. 27–30.

[12] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Transactions on Signal Processing, vol. 51, no. 7, pp. 1995–2007, 2003.

[13] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285–287, 2006.

[14] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recognition, vol. 34, no. 3, pp. 671–683, 2001.

[15] Alabaichi, A. A. Al-Bayati, and A. A. Al-Juboori, "Image steganography using least significant bit and secret map techniques," International Journal of Electrical and Computer Engineering, vol. 10, no. 1, pp. 935–946, 2020.

[16] Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in Information Hiding, Lecture Notes in Computer Science, vol. 1768, Springer, 1999, pp. 61–76.

[17] H. H. Liu, P. C. Su, and M. H. Hsu, "An improved steganography method based on least-significant-bit substitution and pixel-value differencing," KSII Transactions on Internet and Information Systems, vol. 14, no. 11, pp. 4537–4556, 2020.

[18] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings – Vision, Image and Signal Processing, vol. 152, no. 5, pp. 611–615, 2005.

[19] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," Journal of Systems and Software, vol. 81, no. 1, pp. 150–158, 2008.

[20] H.-W. Tseng and H.-S. Leng, "A steganographic method based on pixel-value differencing and the perfect square number," Journal of Applied Mathematics, vol. 2013, Article ID 189706, 2013.

[21] X. Liao, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," Journal of Visual Communication and Image Representation, vol. 22, no. 1, pp. 1–8, 2011.

[22] K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, "Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP," Journal of Information Security and Applications, vol. 58, 102808, 2021.

[23] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Communications Letters, vol. 10, no. 11, pp. 781–783, 2006.

[24] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[25] Y.Yang,R.Zhang,J,Liu,Y.Wang,Y.,&Huang,F,(2019).An Image Steganography Algorithm Based On Pixel Block Difference and Variable Modulus Function.In Smart Innovation ,System and Technologies (Vol.110,pp.36-43). Springer

[26] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," EURASIP Journal on Information Security, vol. 2014, no. 1, 2014.

[27] S. Baluja, "Hiding images in plain sight: Deep steganography," in Advances in Neural Information Processing Systems (NeurIPS), 2017.

[28] M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB-Based Image Steganography Using Secret Key and Pixel Indicator Technique," 2011.

[29] R. Amirtharajan, K. K. Rayappan, and J. B. B. Rayappan, "Secure RGB Image Steganography Using Pixel Indicator Technique," 2012.

[30] G. Swain, "Adaptive Pixel Indicator Image Steganography," 2014.

[31] A. Gutub and M. F. Al-Ghamdi, "Adaptive Edge-Based Image Steganography," 2011.

[32] R. Amirtharajan, J. B. B. Rayappan, and K. K. Rayappan, "Edge Adaptive Image Steganography Using Cryptography," 2014.

[33] G. Swain, "Adaptive Edge Guided Image Steganography," Multimedia Tools and Applications, 2016.

[34] C. Qin, C. C. Chang, and Y. H. Huang, "Reversible Data Hiding in Encrypted Images," IEEE Transactions on Circuits and Systems for Video Technology, 2013.

[35] X. Liao, Q. Wen, and J. Zhang, "High Capacity Reversible Data Hiding Using Difference Expansion," Signal Processing, 2014.

[36] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Transactions on Multimedia, 2011.

[37] W. Hong and T. S. Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," IEEE Transactions on Information Forensics and Security, 2012.

[38] C. F. Lee and H. L. Chen, "An Improved Pixel Value Differencing Steganographic Method," Pattern Recognition Letters, 2010.

[39] J. Fridrich and J. Kodovsky, "Rich Models for Steganalysis of Digital Images," IEEE Transactions on Information Forensics and Security, 2012.

[40] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications," Cambridge University Press, 2009.

Appendix A. Glossary of Abbreviations

AES: Advanced Encryption Standard; **AI**: Artificial Intelligence; **BER**: Bit Error Rate; **bpp**: bits per pixel; **CNN**: Convolutional Neural Network; **DL**: Deep Learning; **EMD**: Exploiting Modification Direction; **HVS**: Human Visual System; **IoT**: Internet of Things; **LSB**: Least Significant Bit; **LSBMR**: Least Significant Bit Matching Revisited; **MSE**: Mean Squared Error; **OPAP**: Optimum Pixel Adjustment Procedure; **PIT**: Pixel Indicator Technique; **PSNR**: Peak Signal-to-Noise Ratio; **PVD**: Pixel-Value Differencing; **RGB**: Red, Green, Blue; **RS**: Regular–Singular Steganalysis; **SPA**: Sample Pair Analysis; **SSIM**: Structural Similarity Index Measure.