AI & CYBER FORUM
AN INTERNATIONAL JOURNAL
OPEN ACCESS
ISSN 3117-6399
Review Article
Check for updates

Adaptive Pixel Selection-Based Image Steganography Using Modified Least Significant Bit Substitution for Improved Imperceptibility

Pankaj Nandan

Department of Computer Applications, Government Degree College, Ramkote, Jammu and Kashmir 184205, India

Corresponding author: **Pankaj Nandan** | E-mail: **prof.pankajnandan@gmail.com**

Citation: Pankaj Nandan (2023). Adaptive Pixel Selection-Based Image Steganography Using Modified Least Significant Bit Substitution for Improved Imperceptibility. *AI & Cyber Forum: An International Journal.* **DOI: https://doi.org/10.51470/AI.2023.2.2.01**

Received 04 August 2023 | Revised 03 September 2023 | Accepted 05 October 2023 | Available Online November 07, 2023

Abstract

The increasing demand for secure digital communication has stimulated extensive research into image steganography techniques capable of concealing confidential information while maintaining the perceptual quality of digital media. Among the various information-hiding approaches, Least Significant Bit (LSB) substitution remains widely investigated because of its simplicity, low computational complexity, and relatively high embedding capacity, conventional LSB-based steganography is often associated with sequential pixel modification, statistical irregularities, and susceptibility to steganalysis, particularly when large payloads are embedded. Adaptive pixel selection and modified LSB substitution have therefore emerged as promising strategies for improving image imperceptibility by considering the local characteristics of the cover image before information embedding. This review critically examines the principles, development, and recent advancements of adaptive pixel selection-based image steganography, with particular emphasis on modified LSB substitution techniques. The explores spatial-domain embedding mechanisms, image-complexity analysis, edge-based and texture-based pixel selection, pixel-value-difference strategies, adaptive embedding rates, randomized embedding patterns, and optimization-based approaches. The relationship between embedding capacity, visual distortion, statistical detectability, computational efficiency, and robustness is discussed through established evaluation metrics, including Mean Squared Error, Peak Signal-to-Noise Ratio, Structural Similarity Index Measure, and bits per pixel. The review further considers the limitations of adaptive embedding, including selection-map synchronization, payload constraints, computational overhead, and vulnerability to advanced statistical and machine-learning-based steganalysis.

Keywords: *Image steganography; adaptive pixel selection; least significant bit substitution; imperceptibility; information hiding.*

1. Introduction

The rapid development of digital communication, cloud computing, online transactions, multimedia sharing, and interconnected information systems has significantly increased the volume of confidential data exchanged through digital platforms. Personal communications, financial information, institutional records, authentication details, research data, and business documents are routinely transmitted across networks that may be exposed to unauthorized monitoring, interception, or manipulation. Consequently, protecting sensitive information during transmission has become an important requirement in modern information security [1]. Traditional cryptographic techniques provide an effective means of protecting the contents of digital messages by transforming readable information into ciphertext using mathematically defined encryption algorithms. Although encryption provides confidentiality, the presence of encrypted communication may remain visible and identifiable, potentially attracting attention from unauthorized individuals or monitoring systems.

This limitation has encouraged the development of information-hiding techniques that conceal the existence of confidential communication within ordinary digital media. Steganography represents an important branch of information security concerned with concealing secret information within an apparently harmless communication medium. Unlike cryptography, which primarily focuses on protecting the meaning of transmitted information, steganography aims to make the existence of the hidden message difficult to recognize [2]. Digital images are particularly suitable for steganographic applications because they contain large numbers of pixels, spatial redundancies, colour information, texture variations, and perceptual characteristics that can be exploited for information embedding. Image steganography generally involves a cover image, a secret message, an embedding mechanism, and a resulting stego-image that is transmitted to the intended recipient. The recipient subsequently applies an extraction procedure to recover the hidden information.

© ***Authors:*** *Published in AI & Cyber Forum: An International Journal under the CC BY-NC-ND 4.0 license (http://creativecommons.org/licenses/by-nc-nd/4.0/). No commercial use or modifications permitted.*

The effectiveness of an image steganography technique depends on its ability to conceal information without introducing noticeable modifications to the cover image or creating statistical patterns that may reveal the presence of hidden data. Among the different image steganography approaches, spatial-domain methods remain attractive because they directly modify pixel values and generally require less computational processing than transform-domain techniques. The Least Significant Bit substitution method is one of the most widely explored spatial-domain techniques because it enables information embedding through the replacement of the least significant bit of selected pixel intensity values. In an 8-bit grayscale image, a pixel intensity can range from 0 to 255, and modification of the least significant bit generally changes the pixel intensity by only one unit. Such small modifications may remain imperceptible under relatively low embedding rates, making LSB substitution suitable for applications requiring efficient information concealment. In colour images, the red, green, and blue channels can provide additional embedding locations, thereby increasing the potential payload capacity [3]. Sequential embedding, in which secret bits are inserted into consecutive pixel locations, may generate detectable statistical patterns in the resulting stego-image. The indiscriminate modification of pixel values may also produce greater visual distortion in smooth or homogeneous regions than in textured or edge-rich areas. Increasing the amount of embedded information generally increases the number of modified pixel components, potentially affecting image quality and raising the probability of detection by statistical steganalysis. Furthermore, conventional LSB substitution does not inherently provide resistance against image processing operations, such as lossy compression, resizing, filtering, or colour transformation. These limitations have motivated the development of modified LSB techniques incorporating adaptive pixel selection, pixel-value-difference analysis, randomized embedding locations, variable embedding depths, and image-content-dependent embedding strategies. Adaptive pixel selection has emerged as an important direction in spatial-domain steganography because it allows embedding locations to be selected according to the characteristics of the cover image. Rather than distributing secret information uniformly across all available pixels, adaptive approaches identify locations that may better accommodate small modifications without substantially affecting perceptual image quality. Image complexity can be estimated using local intensity variation, neighbourhood differences, edge strength, entropy, texture characteristics, or other statistical properties. Regions containing substantial texture and structural variation may exhibit greater tolerance to small pixel modifications than smooth areas, although this perceptual advantage does not necessarily translate into resistance to statistical steganalysis. Adaptive embedding techniques therefore seek to establish a balance between the amount of hidden information, the perceptual quality of the resulting image, and the statistical characteristics of the modified pixel distribution [4]. Modified LSB substitution techniques extend the basic embedding principle through changes in pixel selection, embedding direction, bit allocation, neighbourhood analysis, or the number of modified pixel components. Some methods use edge detection to identify suitable embedding locations, whereas others employ local variance, pixel-value differences, or texture complexity to determine embedding priorities. Additional approaches integrate cryptographic encryption before embedding, thereby protecting the content of the hidden message even if the embedded data are successfully extracted. Optimization-based methods may employ genetic algorithms, particle swarm optimization, artificial intelligence, or other computational approaches to identify embedding configurations that reduce distortion while maintaining acceptable payload capacity. These developments indicate that the performance of image steganography is not determined exclusively by the embedding operation itself but also by the manner in which embedding locations are selected and modifications are distributed across the cover image.

2. Fundamentals of Digital Image Steganography

2.1 Concept and Architecture of Image Steganography

Image steganography involves concealing secret information within digital images through controlled modification of image data. The basic architecture consists of a cover image, secret information, an embedding algorithm, a stego-image, and a corresponding extraction mechanism. The cover image provides the carrier medium, while the embedding algorithm modifies selected image components according to the binary representation of the secret message. The resulting stego-image is transmitted through a communication channel, and the recipient uses the appropriate extraction mechanism to recover the embedded information. Depending on the design of the system, the embedding and extraction procedures may require a secret key, a shared embedding parameter, or an image-dependent selection rule [5]. The quality of an image steganography system is generally determined by several interrelated characteristics. Imperceptibility represents the extent to which modifications introduced during embedding remain visually undetectable. Embedding capacity indicates the amount of information that can be concealed within the cover image. Robustness refers to the ability of the embedded information to survive image processing operations or communication disturbances. Security considers the extent to which unauthorized individuals can detect, extract, or interpret the hidden message. Computational efficiency reflects the time and resources required for embedding and extraction. These characteristics are often interdependent, and improving one property may adversely affect another. For example, increasing embedding capacity may require additional pixel modifications, potentially reducing imperceptibility and increasing statistical detectability.

2.2 Classification of Image Steganography Techniques

Image steganography techniques are commonly categorized according to the image representation or domain in which secret information is embedded. Spatial-domain techniques modify image pixels directly, whereas transform-domain methods manipulate coefficients generated through mathematical transformations. Other approaches incorporate adaptive embedding, statistical modelling, encryption, or intelligent optimization mechanisms to improve performance.

Table 1: Major categories of image steganography techniques

Technique	Embedding principle	Advantages	Limitations
Spatial-domain steganography	Direct modification of pixel values	Simple implementation and low computational cost	Statistical detectability and limited robustness
LSB substitution	Replacement of least significant bits	High capacity and low visual distortion at low payloads	Vulnerability to statistical analysis
Modified LSB	Improved pixel selection or embedding rules	Better control over distortion and embedding patterns	Increased algorithmic complexity
Adaptive steganography	Image-content-dependent embedding	Better allocation of modifications across image regions	Selection and synchronization challenges
Transform-domain steganography	Embedding in DCT, DWT, or other coefficients	Potentially improved robustness	Greater computational complexity
Edge-based steganography	Embedding in edge or high-gradient regions	Improved perceptual concealment	Edge detection errors and capacity variation
Statistical steganography	Embedding based on statistical properties	Potentially improved distribution control	Dependence on accurate statistical modelling
Optimization-based steganography	Selection of embedding parameters using optimization	Can improve objective quality measures	Computational overhead and parameter sensitivity
Deep-learning-based steganography	Neural-network-based embedding and extraction	Potentially adaptive and complex representations	Training requirements and model vulnerability

2.3 Spatial-Domain Information Hiding

Spatial-domain steganography operates directly on the pixel values of a digital image. The embedding process generally modifies one or more pixel components to represent the secret message. Spatial-domain methods are attractive because the mathematical operations are straightforward and can be implemented with relatively limited processing resources. The embedding operation may involve bit substitution, pixel-value adjustment, parity-based modification, neighbourhood-dependent encoding, or combinations of these techniques [6]. The principal limitation of spatial-domain embedding is that direct pixel modification may alter statistical characteristics of the image, particularly when the embedding rate is high or the modification pattern is predictable, the development of spatial-domain methods has increasingly focused on reducing distortion and distributing embedding changes in a manner that is less perceptually and statistically conspicuous.

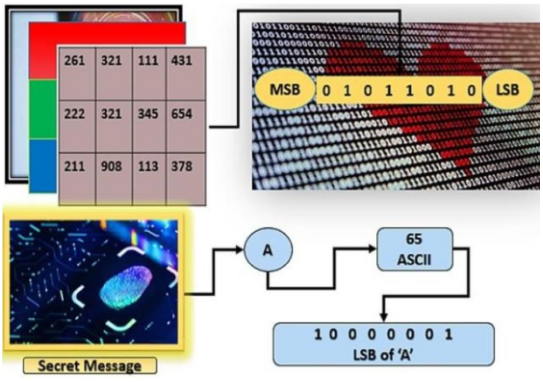

Figure 1. Basic architecture of image steganography

3. Least Significant Bit Substitution

Least Significant Bit (LSB) substitution is a widely used spatial-domain image steganography technique in which the lowest-order bit of a pixel intensity is replaced with a secret-message bit.

In an 8-bit grayscale image, each pixel is represented by eight binary bits, and modifying the least significant bit generally changes the pixel intensity by a maximum of one unit. The embedding process is mathematically expressed as (P'=(P\ &\ 254)\ |\ m), where (P) and (P') represent the original and modified pixel values, respectively, and (m) denotes the secret bit. Consequently, the pixel modification satisfies (|P'-P|\leq1), allowing secret information to be embedded with minimal visual distortion. For a grayscale image of dimensions (W\times H), the theoretical embedding capacity is (WH) bits, whereas an RGB image can accommodate up to (3WH) bits when one bit is embedded in each colour channel. The embedding rate is commonly expressed in bits per pixel (BPP), calculated as (BPP=B_e/(WH)), where (B_e) represents the number of embedded bits. Despite its simplicity, computational efficiency, and relatively high capacity, conventional LSB substitution is susceptible to statistical steganalysis, predictable embedding patterns, and image-processing operations. Furthermore, uniform pixel embedding may unnecessarily modify smooth regions, motivating modified LSB techniques incorporating adaptive pixel selection, edge and texture analysis, randomized embedding, and optimized bit allocation to improve imperceptibility and reduce detectability while maintaining embedding capacity.

4.1 Adaptive Embedding

Adaptive embedding techniques modify the embedding process according to the characteristics of the cover image. Rather than assigning the same embedding rate to every pixel, the algorithm identifies regions with different perceptual or statistical properties and determines the embedding allocation accordingly. Smooth regions may receive fewer modifications, whereas more complex regions may be considered for greater embedding activity. This approach can reduce the perceptual impact of embedding, particularly when local image characteristics are used to guide modification

intensity [8]. Adaptive embedding strategies differ considerably in their selection criteria and implementation. Some methods use local intensity variation, whereas others rely on image-gradient magnitude, entropy, neighbourhood differences, or texture classification. The effectiveness of adaptive embedding depends on the accuracy of the selected complexity measure and its relationship with both human perception and statistical detectability.

4.2 Modified Bit Replacement and Embedding Direction

Modified LSB substitution may employ alternative pixel-modification rules to reduce the magnitude or frequency of changes. Instead of always replacing the least significant bit directly, the algorithm may select between different modification operations according to the original pixel value and the secret bit. Some approaches attempt to minimize the numerical difference between the original and modified pixel values, while others consider neighbouring pixels or the local distribution of intensity values. These mechanisms may reduce image distortion, particularly when embedding is performed at moderate or high payload rates [9]. The effectiveness of such methods depends on whether the modification strategy introduces additional statistical irregularities. A method that minimizes pixel-level error may not necessarily minimize the detectability of the stego-image. Therefore, modified LSB approaches should be evaluated using both image-quality metrics and security-oriented detection tests.

4.3 Pixel-Value-Difference-Based Embedding

Pixel-value-difference techniques use the difference between neighbouring pixel intensities to determine embedding capacity or modification allocation. Greater differences between neighbouring pixels may indicate more complex regions, whereas small differences may represent relatively smooth areas. The pixel-value-difference method can therefore be used to allocate more information to areas with higher local variation and reduce embedding in regions that are more perceptually sensitive [10]. However, the relationship between pixel-value differences, visual complexity, and steganographic security is not straightforward. Embedding based on predefined difference ranges may alter the distribution of pixel differences and potentially introduce detectable patterns. Consequently, the selection of difference thresholds and embedding rules must be examined through systematic evaluation.

4.4 Multi-Bit LSB Embedding

Multi-bit LSB embedding involves replacing more than one least significant bit of selected pixel values. The technique can increase embedding capacity substantially, particularly when two or three bits are modified per selected pixel. However, increasing the number of modified bits also increases the maximum possible change in pixel intensity and may produce greater visual distortion [11]. For example, embedding two bits within an 8-bit intensity value may produce a modification of up to three intensity levels, whereas embedding three bits may result in a change of up to seven levels. Although these changes may remain difficult to detect under certain image conditions, they can become more noticeable in smooth regions or at high embedding rates. Adaptive multi-bit techniques therefore seek to determine an appropriate embedding depth according to the local characteristics of the image.

5. Adaptive Pixel Selection Mechanisms

Adaptive pixel selection is an important advancement in modified LSB image steganography, as it determines suitable embedding locations based on the structural, statistical, and perceptual characteristics of the cover image. Edge-based selection identifies regions with significant intensity or colour variations using operators such as Sobel, Prewitt, and Laplacian, allowing secret information to be embedded in structurally complex areas where minor modifications may be less perceptible [12]. Similarly, texture-based selection utilizes local variations, neighbourhood differences, and texture descriptors to identify regions containing complex patterns, such as foliage, fabric, rocks, and natural landscapes, which may provide better perceptual masking than smooth regions [13]. Local variance is another commonly employed criterion for estimating image complexity by measuring intensity fluctuations within a defined neighbourhood, with higher variance generally indicating greater local variation and potentially improved tolerance to embedding modifications. Entropy-based selection further characterizes the information content and intensity distribution of image regions using enabling the identification of regions with diverse pixel distributions, although higher entropy does not necessarily guarantee resistance to steganalysis.

$$H = -\sum_{i=0}^{L-1} p_i \log_2 p_i$$

The adaptive channel selection can distribute secret information across red, green, and blue components according to their perceptual characteristics and sensitivity to modification, potentially reducing visible distortion while maintaining embedding efficiency [15]. Additionally, randomized and key-dependent pixel selection employs pseudorandom sequences or secret keys to determine embedding locations, reducing predictable sequential patterns and restricting extraction to authorized receivers possessing the corresponding key or parameters [16]. Although these adaptive mechanisms can improve embedding flexibility, perceptual quality, and resistance to predictable embedding patterns, their effectiveness depends on image content, payload size, selection thresholds, computational requirements, and the statistical characteristics of the resulting stego-image; therefore, adaptive pixel selection should be integrated with appropriate embedding-rate control and evaluated using both perceptual quality metrics and steganalysis-based security assessments.

Table 2: Adaptive pixel-selection strategies and their characteristics

Selection strategy	Principal parameter	Potential advantage	Major limitation
Edge-based selection	Gradient magnitude	Embedding in structurally complex regions	Edge concentration may create detectable patterns
Texture-based selection	Texture complexity	Improved perceptual masking	Texture may not correspond to statistical security
Local variance	Neighbourhood intensity variance	Simple adaptive classification	Threshold sensitivity
Entropy-based selection	Local entropy	Identification of information-rich regions	Higher computational cost
Pixel-value difference	Difference between neighbouring pixels	Variable embedding allocation	Distribution changes may be detectable
Colour-channel selection	RGB channel characteristics	Additional capacity and perceptual flexibility	Channel-specific artifacts
Randomized selection	Pseudorandom sequence	Reduced predictability of embedding positions	Does not guarantee resistance to steganalysis
Key-dependent selection	Secret key and embedding seed	Controlled extraction and access	Key management and synchronization requirements

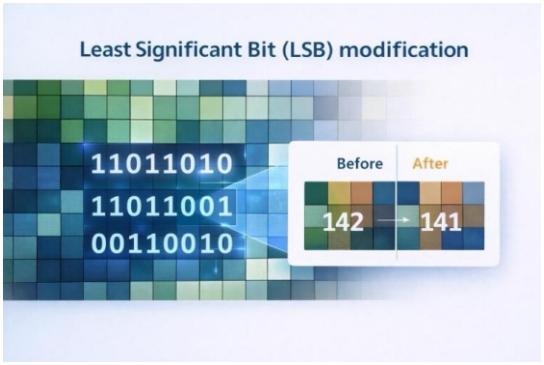

Figure 2. Conventional and modified LSB substitution

6. Modified LSB Strategies for Improved Imperceptibility

Modified LSB strategies aim to improve image quality and embedding efficiency by controlling how secret information is distributed and how pixel values are modified during the embedding process. Adaptive embedding-rate techniques allocate different quantities of secret information across image regions according to local characteristics, such as variance, edge magnitude, entropy, and texture complexity, allowing higher embedding capacity in complex regions and lower modification rates in smooth areas to minimize perceptual distortion [17]. Pixel modification minimization further improves embedding efficiency by selecting operations that produce the smallest possible difference between original and modified pixel values, potentially involving conventional bit replacement, controlled increment or decrement operations, and neighbourhood-dependent modification rules. The overall modification objective can be expressed as

$$D = \sum_{i=1}^{N} |P_i' - P_i|, \text{ where } P_i \text{ and } P_i'$$

where \(P_i\) and \(P_i'\) represent the original and modified pixel values, respectively, and \(N\) denotes the total number of modified pixels. Although minimizing this difference may improve visual quality, it does not necessarily ensure statistical security, which also depends on the distribution and spatial characteristics of embedding modifications. Neighbourhood-based embedding approaches consider relationships between selected pixels and their surrounding regions through pixel-pair encoding, local difference modification, neighbour-dependent bit allocation, and adaptive parity mechanisms, potentially reducing unnecessary modifications and improving local consistency [18].

However, such techniques may increase computational complexity and require synchronized embedding and extraction procedures. Furthermore, integrating cryptographic encryption with image steganography provides an additional layer of protection by encrypting the secret message before embedding it into the cover image using an LSB-based technique [19]. Symmetric encryption algorithms such as the Advanced Encryption Standard (AES), particularly when implemented through authenticated-encryption modes such as AES-GCM, can protect message confidentiality and integrity, whereas steganography conceals the presence of the communication itself. Nevertheless, encryption alone does not improve the statistical concealment of the stego-image; therefore, the embedding mechanism must independently maintain acceptable visual quality, controlled distortion, and resistance to steganalysis.

7. Imperceptibility and Image-Quality Evaluation

Imperceptibility is a fundamental performance characteristic of image steganography, as the stego-image should retain visual similarity to the original cover image despite the embedding of confidential information. Its evaluation generally involves objective image-quality metrics and statistical analysis to assess the extent of embedding-induced distortion and potential detectability. Mean Squared Error (MSE) measures the average squared difference between the pixel intensities of the cover image and stego-image and is calculated as

$$MSE = \frac{1}{WH} \sum_{x=1}^{W} \sum_{y=1}^{H} [I(x,y) - I_s(x,y)]^2,$$

where $I(x,y)$ and $I_s(x,y)$

represent the original and modified pixel intensities, respectively, and \(W\) and \(H\) denote the image dimensions. Lower MSE values indicate smaller numerical differences between the images. Peak Signal-to-Noise Ratio (PSNR) is another widely used metric for evaluating image quality and is expressed as

$$PSNR=10\log_{10}\left(\frac{MAX_I^2}{MSE}\right),$$

where \(MAX_I\) represents the maximum possible pixel intensity, typically 255 for an 8-bit image; higher PSNR values generally indicate lower distortion and greater image similarity.

Structural Similarity Index Measure (SSIM) provides a perceptually oriented assessment by considering luminance, contrast, and structural information, with its mathematical expression given by

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)},$$

where μ_x and μ_y represent local mean intensities, σ_x^2 and σ_y^2 denote variances, σ_{xy} represents covariance, and C_1 and C_2 are stabilizing constants. SSIM values closer to 1 indicate greater structural similarity between the compared images. In addition to image-quality measurements, embedding capacity and payload rate must be considered when comparing conventional and adaptive LSB techniques, as lower distortion achieved through embedding a smaller quantity of information may not represent an equivalent performance improvement.

The embedding rate is commonly expressed as

$$BPP = \frac{B_e}{WH}, where (B_e)$$

denotes the total number of embedded bits and (WH) represents the number of image pixels. Therefore, comparative evaluations should maintain consistent payload sizes or clearly report embedding rates across different methods. Importantly, visual imperceptibility and statistical undetectability represent distinct aspects of steganographic performance, since an image may appear visually unchanged while exhibiting statistical irregularities detectable through the analysis of pixel distributions, neighbouring-pixel correlations, frequency characteristics, and residual features [17]. Accordingly, a comprehensive evaluation of adaptive LSB techniques should combine MSE, PSNR, SSIM, embedding capacity, and statistical steganalysis measures, with machine-learning-based detection experiments clearly specifying the dataset, payload rate, model architecture, and testing procedure.

Table 3: Common evaluation metrics for adaptive LSB image steganography

Metric	Purpose	Desired characteristic
MSE	Pixel-level distortion	Lower
PSNR	Image reconstruction quality	Higher
SSIM	Structural similarity	Closer to 1
BPP	Embedding rate	Report at equivalent payload conditions
Embedding capacity	Maximum concealed payload	Higher, subject to security and quality constraints
BER	Extraction errors	Lower, ideally zero under lossless transmission
Embedding time	Computational efficiency	Lower
Extraction time	Recovery efficiency	Lower
Detection accuracy	Steganalysis performance	Lower for the detector
AUC	Steganalysis discrimination ability	Closer to 0.5 under balanced testing

8. Statistical Steganalysis of LSB-Based Techniques

Steganalysis refers to the identification, detection, and analysis of concealed information within digital media by examining visual, statistical, structural, and computational characteristics that may indicate the presence of steganographic modifications. Conventional LSB substitution is particularly relevant to steganalysis because replacing pixel bits can influence intensity distributions, neighbouring-pixel correlations, and statistical relationships between image components [18]. Among the established detection approaches, chi-square analysis examines the frequency relationships between pixel-value pairs that may be altered through LSB replacement, identifying statistical irregularities that can help distinguish original cover images from stego-images. Regular-Singular (RS) analysis provides another statistical approach by examining changes in the distribution of regular, singular, and unusable pixel groups under defined pixel-flipping operations, thereby investigating patterns associated with LSB embedding. In addition to these conventional methods, machine-learning-based steganalysis has gained considerable importance through the application of handcrafted statistical features and automatically learned image representations to classify images as cover or stego. Convolutional neural networks and other deep-learning architectures have been investigated for detecting subtle embedding-related modifications that may not be readily identified through conventional statistical analysis [19].

Although adaptive pixel selection, nonuniform embedding, and modified LSB strategies may influence the statistical characteristics examined by these detection methods, they do not necessarily eliminate the possibility of detection. The effectiveness of steganalysis depends on several factors, including image-dataset diversity, embedding algorithm, payload rate, image characteristics, feature extraction procedures, and the similarity between training and testing distributions. Therefore, comprehensive security evaluation of modified LSB techniques should incorporate appropriate statistical and machine-learning-based detection approaches rather than relying exclusively on visual quality metrics such as PSNR, MSE, and SSIM.

9. Comparative Analysis of Adaptive and Conventional LSB Techniques

Conventional LSB substitution offers a straightforward embedding mechanism with low computational overhead and relatively high theoretical capacity. However, its fixed or sequential embedding strategy may result in predictable modification patterns. Adaptive LSB techniques attempt to improve the distribution of embedding modifications by selecting pixels according to image characteristics. Modified embedding approaches may further incorporate variable bit allocation, pixel-value differences, local statistical analysis, or optimization-based mechanisms.

The advantages of adaptive techniques are generally associated with improved control over embedding locations and modification intensity. Nevertheless, adaptive approaches may require additional computational processing and may introduce extraction synchronization requirements. The performance of such methods depends on the selection criteria, thresholds, embedding rate, image content, and statistical characteristics of the resulting modifications.

Table 4: Comparative characteristics of conventional and adaptive LSB approaches

Characteristic	Conventional LSB	Modified LSB	Adaptive pixel-selection LSB
Embedding principle	Direct bit replacement	Modified embedding rules	Content-dependent embedding
Pixel selection	Fixed or sequential	Variable	Image characteristics
Computational complexity	Low	Low to moderate	Moderate
Embedding capacity	Relatively high	Variable	Dependent on selection policy
Visual distortion	Payload-dependent	Potentially reduced	Potentially reduced
Smooth-region protection	Limited	Method-dependent	Can be prioritized
Texture/edge utilization	Not inherent	Optional	Commonly incorporated
Statistical detectability	Potentially high	Method-dependent	Requires testing
Extraction complexity	Low	Variable	Moderate to high
Robustness	Generally limited	Method-dependent	Generally limited for spatial LSB
Key-based embedding	Optional	Optional	Often incorporated
Optimization potential	Limited	Moderate	High

10. Applications of Adaptive Image Steganography

Adaptive image steganography offers potential applications in confidential digital communication, secure document exchange, digital authentication, and multimedia security, particularly in situations where sensitive information must be transmitted while concealing the presence of communication. In confidential communication, adaptive LSB embedding can conceal textual messages within ordinary digital images while selecting embedding locations according to image characteristics to minimize perceptual distortion; however, practical implementation requires appropriate encryption and secure key management. Similarly, digital images may serve as carriers for small quantities of confidential document-related information, including identifiers, metadata, and verification details, particularly when transmitted through lossless communication channels, although steganography should complement rather than replace established cryptographic file-protection mechanisms. Another potential application involves digital authentication and information verification, where authentication data, identifiers, or verification codes are embedded within images and combined with cryptographic authentication mechanisms or digital signatures to support the identification of unauthorized modifications. Furthermore, adaptive image steganography may contribute to multimedia security systems involving image sharing, digital content protection, and controlled information exchange by selecting embedding locations according to local image characteristics to maintain visual quality under defined conditions. Nevertheless, the practical reliability of these applications depends on the embedding algorithm, payload capacity, communication channel, extraction mechanism, and resistance to image processing and steganalysis.

Conclusion

Adaptive pixel selection-based image steganography using modified Least Significant Bit substitution represents an important development in spatial-domain information hiding. Conventional LSB techniques offer computational simplicity, low implementation requirements, and relatively high embedding capacity, but their fixed or sequential modification patterns may result in perceptual distortion and statistical detectability. Modified LSB techniques seek to address these limitations by introducing alternative embedding rules, pixel-value adjustment strategies, variable embedding rates, and neighbourhood-dependent operations. Adaptive pixel selection further enhances embedding control by incorporating local image characteristics, including edge intensity, texture variation, entropy, and pixel-value differences, into the selection of suitable embedding locations. The review highlights the potential advantages of adaptive embedding in improving perceptual quality while emphasizing that visual imperceptibility, embedding capacity, robustness, and statistical security are distinct characteristics. Although complex or textured regions may provide greater perceptual tolerance to small modifications, their selection does not automatically guarantee resistance to steganalysis. The performance of adaptive techniques therefore requires systematic evaluation using objective image-quality metrics, embedding-rate measurements, computational analysis, and statistical detection experiments. The sensitivity of spatial-domain LSB methods to lossy compression and image-processing operations also remains a significant limitation and adaptive modified LSB steganography remains a promising research direction for image-based information hiding, particularly when its design and evaluation consider the competing requirements of imperceptibility, capacity, security, and practical reliability.

References

1. Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. *IEEE Journal on Selected Areas in Communications, 16*(4), 474–481. https://doi.org/10.1109/49.668971
2. Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*(3), 469–474. https://doi.org/10.1016/j.patcog.2003.08.007

3. Chefranov, A. G., & Öz, G. (2022). Adaptive to pixel value and pixel value difference irreversible spatial data hiding method using modified LSB for grayscale images. *Journal of Information Security and Applications, 70*, Article 103314. https://doi.org/10.1016/j.jisa.2022.103314
4. Dumitrescu, S., Wu, X., & Wang, Z. (2003). Detection of LSB steganography via sample pair analysis. *IEEE Transactions on Signal Processing, 51*(7), 1995–2007. https://doi.org/10.1109/TSP.2003.812753
5. Fillatre, L. (2012). Adaptive steganalysis of least significant bit replacement in grayscale natural images. *IEEE Transactions on Signal Processing, 60*(2), 556–569. https://doi.org/10.1109/TSP.2011.2174231
6. Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color and gray-scale images. *IEEE Multimedia, 8*(4), 22–28. https://doi.org/10.1109/93.959097
7. Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color and grayscale images. In *Proceedings of the 2001 ACM Workshop on Multimedia and Security* (pp. 27–30). Association for Computing Machinery. https://doi.org/10.1145/1232454.1232466
8. Hameed, M. A., Hassaballah, M., Aly, A., & Awad, A. I. (2019). An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques. *IEEE Access, 7*, 185189–185204. https://doi.org/10.1109/ACCESS.2019.2960254
9. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T. S., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication, 65*, 46–66. https://doi.org/10.1016/j.image.2018.03.012
10. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26–34. https://doi.org/10.1109/2.657957
11. Kalita, M., Tuithung, T., & Majumder, S. (2019). An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. *Cryptologia, 43*(5), 414–437. https://doi.org/10.1080/01611194.2019.1579122
12. Lerch-Hostalot, D., & Megías, D. (2013). LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers & Security, 32*, 192–206. https://doi.org/10.1016/j.cose.2012.11.005
13. Liao, X., Wen, Q., & Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. *Journal of Visual Communication and Image Representation, 22*(1), 1–8. https://doi.org/10.1016/j.jvcir.2010.08.007
14. Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security, 5*(2), 201–214. https://doi.org/10.1109/TIFS.2010.2041812
15. Mielikainen, J. (2006). LSB matching revisited. *IEEE Signal Processing Letters, 13*(5), 285–287. https://doi.org/10.1109/LSP.2006.870357
16. Westfeld, A., & Pfitzmann, A. (2000). Attacks on steganographic systems. In A. Pfitzmann (Ed.), *Information hiding* (Lecture Notes in Computer Science, Vol. 1768, pp. 61–75). Springer. https://doi.org/10.1007/10719724_5
17. Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24*(9–10), 1613–1626. https://doi.org/10.1016/S0167-8655(02)00402-6
18. Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security, 3*(3), 488–497. https://doi.org/10.1109/TIFS.2008.926097
19. Zhang, X., & Wang, S. (2004). Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. *Pattern Recognition Letters, 25*(3), 331–339. https://doi.org/10.1016/j.patrec.2003.10.014111111111