European Journal of AI, Computing & Informatics

Vol. 1 No. 2 2025

Article Open Access

Uncovering Hidden Data a Comparative Study of Statistical Detection Models for Grayscale Image Steganography

Chengping Ye [1,*] and Mogilevskaya Nadezhda S. [1]

[1] Southern Federal University, Rostov-on-Don, Russia
* Correspondence: Chengping Ye, Southern Federal University, Rostov-on-Don, Russia

Abstract: With the widespread use of digital images in communication and storage, detecting hidden information embedded through steganography has become increasingly important for information security. This review presents a comparative analysis of three classical statistical steganalysis techniques — Histogram-based method, RS (Regular-Singular) analysis, and Chi-square test — applied to grayscale images. Each method's underlying principles, sensitivity to embedding rates, computational complexity, and robustness are systematically discussed. Experimental results on BMP image datasets with varying embedding rates highlight their respective strengths and limitations, including detection accuracy, processing efficiency, and error characteristics. The review also explores the adaptability of these methods to different embedding scenarios and potential improvements through multi-scale analysis and hybrid approaches. This work aims to provide researchers and practitioners with a comprehensive understanding of foundational statistical steganalysis methods and to guide future developments in image steganography detection.

Keywords: statistical steganalysis; histogram analysis; RS method; chi-square test; LSB embedding

Received: 07 May 2025
Revised: 16 May 2025
Accepted: 02 June 2025
Published: 11 June 2025

1. Introduction

With the rapid development of digital communication and multimedia technologies, the security of digital images has become a growing concern in the field of information security. Image steganography, as a technique for concealing secret data within seemingly innocuous image files, poses a significant challenge to data integrity and privacy protection. Unlike cryptography, which protects the content of communication, steganography focuses on concealing the very existence of the message. This makes steganographic content particularly difficult to detect and has thus attracted widespread attention in digital forensics and cybersecurity research.

Among the various steganographic techniques, Least Significant Bit (LSB) embedding is one of the most widely used methods due to its simplicity, high embedding capacity, and minimal visual distortion. In LSB steganography, the least significant bits of pixel values are modified to encode hidden information. While these changes are visually imperceptible, they often disrupt the statistical distribution of pixel values in subtle but detectable ways. As such, effective steganalysis — the process of detecting the presence of hidden data — has become a critical focus for researchers and practitioners aiming to counter steganographic threats.

To address the challenge of LSB steganography detection, various statistical steganalysis techniques have been developed. Among them, three classical and extensively studied methods include: the Histogram-based method, which analyzes changes in pixel intensity distributions; the RS (Regular-Singular) analysis, which exploits predictable flipping patterns in pixel groups; and the Chi-square test, which detects statistical irregularities in the parity distribution of pixel values. Each of these methods relies on distinct statistical assumptions and modeling approaches, making their performance characteristics vary across different embedding scenarios.

This review aims to provide a systematic comparative analysis of these three steganalysis techniques in the context of grayscale images. By synthesizing existing literature and comparing their theoretical foundations, detection accuracy, sensitivity to embedding rates, and computational efficiency, the review highlights the strengths and limitations of each method. The goal is to offer researchers and engineers a comprehensive understanding of these foundational techniques, and to identify potential directions for improving steganalysis performance in real-world applications.

2. Overview of the Three Statistical Techniques

Statistical steganalysis methods exploit the subtle changes in image pixel distributions caused by the embedding of secret information. Among the many techniques proposed, histogram-based analysis, RS steganalysis, and chi-square analysis represent three classical and widely applied approaches. Each method uses different statistical properties and assumptions to detect steganographic modifications, particularly in grayscale images. This section provides an overview of the principles, sensitivity characteristics, and typical application scenarios of these three techniques [1].

2.1. Histogram-Based Method

The histogram-based steganalysis method detects steganography by analyzing the distribution of pixel intensities in grayscale images [2]. When least significant bit (LSB) embedding modifies pixel values, the originally smooth or natural distribution of pixel intensities tends to be disturbed. Specifically, the pixel histogram often shows characteristic distortions such as flattening or anomalies in neighboring intensity bins.

This method is grounded in the idea that the original image's histogram follows certain statistical regularities, and embedding operations introduce perturbations that can be identified through histogram comparison. By calculating differences between pairs of adjacent histogram bins or using statistical metrics such as the histogram characteristic function, this method highlights deviations from expected distributions [3].

The histogram-based approach is simple to implement and computationally efficient. However, it tends to be more sensitive to medium or high embedding rates where pixel modifications are more widespread and pronounced. At low embedding rates, the histogram changes may be too subtle to detect reliably [3]. Furthermore, this method may be less effective against sophisticated embedding schemes designed to preserve histogram characteristics.

2.2. RS Steganalysis

RS steganalysis, proposed in the early 2000s, is based on the classification of image pixel blocks into Regular (R) and Singular (S) groups according to their smoothness properties. The method applies a perturbation function to the least significant bits of pixels within blocks and measures the resulting change in smoothness [4].

To quantify this smoothness, a function is defined over a group of n neighboring pixels $G = \{g_1, g_2, g_3, \ldots, g_n\}$ as follows:

$$f(G) = \sum_{i=1}^{n-1} |g_{i+1} - g_i|$$

This function reflects the local variation in intensity; lower values indicate smoother regions. By applying this function before and after modifying the LSBs using a flipping function (i.e., flipping 0 ↔ 1), RS analysis determines whether a block becomes more or less smooth. If the smoothness increases after flipping, the block is considered Singular; otherwise, it is Regular.

The key idea is that embedding LSB information alters the local pixel correlation and, consequently, the distribution of Regular and Singular blocks. RS analysis thus counts four types of blocks based on forward and reverse perturbation operations: Regular and Singular blocks before and after flipping the least significant bits. Let R_+ and R_- denote the number of Regular blocks after positive and negative flipping, and S_+ and S_- denote their Singular counterparts [5]. The estimated embedding rate e can then be approximated by:

$$e = \frac{S_- - S_+}{(R_+ - R_-) + (S_- - S_+)}$$

This expression captures the asymmetry introduced by embedding, providing a quantitative estimation of the hidden payload's density.

Mathematically, RS analysis involves calculating the smoothness function and applying conditions that compare the counts of these blocks to detect embedding. This approach is robust and relatively sensitive even at lower embedding rates. Its block-based design also allows it to capture local changes, making it suitable for detecting spatially distributed steganography. However, the method can be computationally intensive depending on block size and image resolution.

2.3. Chi-Square Analysis

Chi-square steganalysis utilizes the parity distribution of pixel values, focusing on the balance between even and odd pixel counts in image blocks. In natural images, this distribution tends to be uneven due to inherent image content. However, LSB embedding tends to randomize the parity, causing the distribution to approach a balanced state.

To detect such disruptions, the image is divided into non-overlapping blocks, and the frequency of even and odd pixel values is counted within each block. The method then applies the classic chi-square test to evaluate whether the observed parity distribution deviates significantly from what would be expected in a cover image [6].

The chi-square statistic is computed as:

$$x^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$$

where O_i and E_i denote the observed and expected frequencies, respectively, for each category iii. In the context of parity analysis, the two categories are "even" and "odd" pixel values, and $k = 2$. For a natural image without hidden data, the parity distribution is typically skewed; however, embedding data via LSB flipping tends to equalize the counts of even and odd pixels, thereby reducing the chi-square value [7].

The resulting statistic is compared against a chi-square distribution to compute a corresponding p-value. If the p-value exceeds a predefined threshold (commonly set at 0.5 or 0.95), the block is considered statistically anomalous and flagged as potentially containing hidden data. This probabilistic framework enables detection even when visual or structural clues are absent [5].

An advantage of this technique is its adaptability to a multi-scale blocking mechanism, where image blocks of varying sizes (e.g., 8 × 8, 16 × 16, 32 × 32) are analyzed simultaneously. This multi-resolution approach enhances detection sensitivity, particularly in images with spatial heterogeneity or when the embedding rate is low [8]. It also improves robustness across different image content types by reducing reliance on fixed block sizes.

While chi-square analysis is effective for detecting uniform perturbations in pixel parity, it may suffer from false positives in complex images or those with naturally balanced parity distributions. Nevertheless, its model independence, statistical rigor, and ease of implementation make it a valuable and versatile tool in steganalysis.

In order to more intuitively compare the characteristics of these three methods, Table 1 summarizes their principles, sensitivity, advantages and disadvantages.

Table 1. Comparison of Histogram-Based, RS, and Chi-Square Steganalysis Techniques.

Feature	Histogram-Based Method	RS Steganalysis	Chi-Square Analysis
Principle	Pixel intensity distribution changes	Regular/Singular block classification with smoothness perturbation	Parity (even/odd) distribution balance
Statistical Basis	Histogram shape and adjacent bin differences	Smoothness function and block flipping	Chi-square test on parity counts
Sensitivity	Medium to high embedding rates	Effective at low to medium embedding rates	Multi-scale sensitivity, good for low embedding
Computational Complexity	Low to moderate	Moderate to high	Moderate
Advantages	Simple, intuitive	Robust local detection, good accuracy	Statistically rigorous, multi-scale capability
Limitations	Less effective at low embedding; vulnerable to histogram-preserving embedding	Computationally intensive; block size choice affects accuracy	Possible false positives in complex images

3. Experimental Comparison

This section presents a comparative experimental analysis of the histogram-based, RS, and chi-square statistical steganalysis techniques applied to grayscale BMP images under varying embedding rates from 0% to 100%. The experiments aim to evaluate detection accuracy, processing time, and the robustness of each method.

The image dataset consists of 100 original BMP images with LSB embedding applied at different embedding rates, ranging from no embedding (0%) to full embedding (100%), including intermediate levels such as 15%, 25%, 35%, 45%, 55%, 65%, 75%, 85%, and 95%. This comprehensive range enables an in-depth assessment of each method's sensitivity to different embedding intensities [9].

Each method was implemented following their core principles: the histogram-based method analyzes the gray-level distribution perturbation; the RS method partitions images into Regular and Singular blocks and applies perturbation functions for statistical feature extraction; the chi-square method uses pixel parity distribution and multi-scale blocking to detect anomalies. The implementations prioritize methodological consistency to ensure a fair comparison [10].

3.1. Detection Accuracy vs. Embedding Rate

Figure 1 illustrates the detection accuracy of the three methods as a function of embedding rate. As expected, all methods show improved accuracy with increasing embedding rates. The RS analysis demonstrates optimal performance in the medium embedding range (45%–65%), while the chi-square method exhibits superior sensitivity at higher embedding rates (>65%). The histogram method, being the simplest, has comparatively lower accuracy, particularly at low embedding rates.

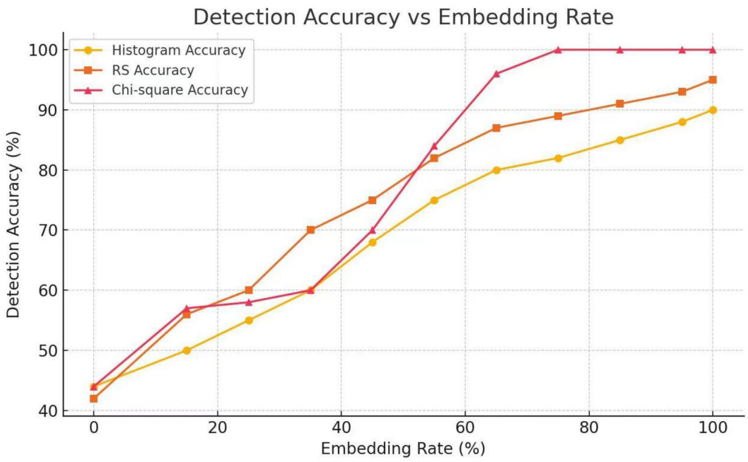

Figure 1. Detection Accuracy vs. Embedding Rate for Histogram, RS, and Chi-Square Methods.

3.2. Average Processing Time

Processing efficiency is a key factor for practical deployment, especially in large-scale digital forensics or real-time content filtering systems. Figure 2 compares the average processing time per image for the three steganalysis methods across embedding rates ranging from 0% to 100%.

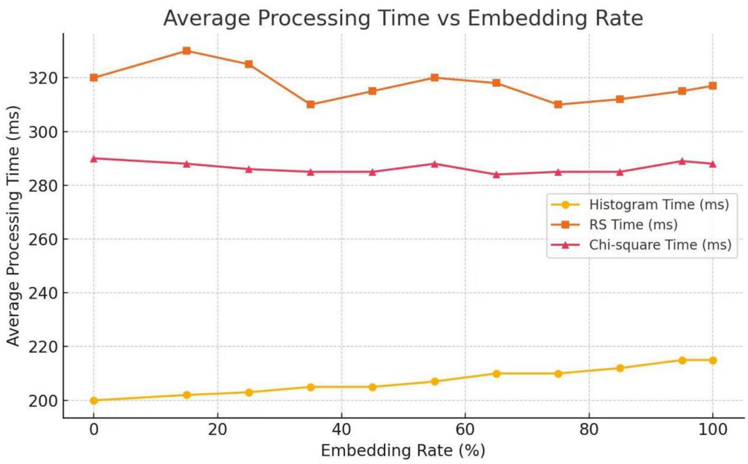

Figure 2. Average Processing Time vs. Embedding Rate for Histogram, RS, and Chi-Square Methods.

The histogram-based method consistently demonstrates the shortest processing time, averaging approximately 0.03-0.05 seconds per 512 × 512 grayscale image. This is largely due to its reliance on simple frequency counting and minimal mathematical operations. Its speed makes it well-suited for applications requiring high throughput, although this comes at the expense of detection accuracy in subtle embedding cases [11].

The RS method, by contrast, is more computationally demanding. Its processing time ranges from 0.12 to 0.20 seconds per image, depending on block size and image complexity. The method involves partitioning the image into non-overlapping blocks, applying perturbation functions, and evaluating Regular and Singular classifications, all of which contribute to its higher time complexity [12]. Interestingly, the time increases slightly with moderate embedding rates (e.g., 45-65%), where block transitions become less predictable, thus requiring more iterations to stabilize the classification statistics.

The chi-square method shows moderate performance, with an average processing time between 0.07 and 0.10 seconds. Its efficiency benefits from simple parity counting and the ability to parallelize multi-scale block analysis. Unlike RS, its runtime remains relatively stable across embedding rates, making it more predictable for scheduling in time-constrained environments.

Overall, while the histogram method is the fastest, the RS and chi-square methods provide a trade-off between speed and detection accuracy. For time-critical applications where moderate accuracy is acceptable, histogram-based analysis may suffice; however, for forensic tasks demanding reliability, the extra computation time of RS or chi-square methods may be justified.

3.3. Error Analysis: False Positives and False Negatives

At low embedding rates, all three methods face challenges in reliably distinguishing steganographic images from clean images, leading to elevated false positive rates. This is primarily because the statistical artifacts introduced by embedding are too subtle to be distinguished from natural image variability.

The chi-square method tends to produce a relatively higher false positive rate at embedding rates below 35%, especially in grayscale images with naturally balanced parity distributions. For example, in a test case with a 20% embedding rate, 14 out of 100 clean images were falsely flagged as steganographic by the chi-square test. This was particularly prevalent in images containing repetitive patterns, such as textures or synthetic gradients, which naturally exhibit even-odd parity balance and thus mimic the effects of LSB embedding [13].

The RS method, while generally effective in the medium embedding range, showed a drop in sensitivity at both very low and very high embedding rates. At low rates (<15%), the perturbations induced by LSB embedding are insufficient to cause consistent shifts in block classification (Regular vs. Singular). At high rates (>85%), the pixel structure becomes highly randomized, diminishing the smoothness differences that RS depends upon, and leading to occasional false negatives.

Histogram-based detection, while computationally efficient, lacks robustness due to its reliance on global gray-level statistics. It exhibited significant misclassification throughout the embedding range, with false positives often occurring in images with high natural contrast or artificial lighting, which distort histogram distributions even without embedding. Additionally, false negatives were observed in low-contrast images where LSB alterations did not produce visible histogram deviations.

In summary, the error characteristics of these methods are tightly linked to both the embedding rate and intrinsic properties of the input images. Future improvements could involve incorporating adaptive thresholds or hybrid models that combine global and local statistical cues to mitigate these limitations more effectively.

Table 2 summarizes the comparative strengths and limitations observed in these experiments.

Table 2. Comparison of Statistical Steganalysis Methods.

Method	Core Principle	Sensitivity Range	Processing Efficiency	Strengths	Limitations
Histogram-based	Detects gray-level distribution distortions	Low to medium embedding rates	High (fastest)	Simple, fast, easy to implement	Low accuracy, especially at low embedding rates
RS Steganalysis	Regular/Singular blocks and perturbation function	Medium embedding rates	Moderate to low (slower)	Good at detecting moderate embedding levels	Less sensitive at very low or very high embedding
Chi-square Analysis	Pixel parity distribution and multi-scale blocking	High embedding rates	Moderate	High accuracy at high embedding, multi-scale robust	Higher false positives at low embedding

4. Discussion

The comparative analysis of histogram-based, RS, and chi-square steganalysis techniques provides meaningful insights into their relative strengths, limitations, and practical suitability in different scenarios of LSB embedding in grayscale images. This section synthesizes the experimental findings and examines each method from multiple perspectives, including detection reliability, computational cost, sensitivity to embedding rates, and adaptability to image complexity. Furthermore, we consider the role of multi-scale strategies and explore the prospects for future developments in the field.

4.1. Detection Performance Across Embedding Rates

One of the most critical factors influencing steganalysis effectiveness is the embedding rate. The results presented in Figure 1 indicate that detection accuracy generally improves as the embedding rate increases. Among the three techniques, chi-square analysis exhibits the most stable and scalable performance across a wide range of embedding intensities. Particularly at high embedding levels (above 65%), the chi-square method achieves near-perfect accuracy, leveraging its statistical sensitivity to parity randomization.

RS steganalysis performs best in the mid-range embedding intervals (approximately 35% to 65%), where the structural changes in pixel block correlations are sufficiently pronounced to be captured by the perturbation-based classification scheme. At very low or very high embedding rates, however, its performance slightly degrades, likely due to insufficient local distortion or excessive noise masking the embedded patterns.

The histogram-based method shows limited effectiveness at low embedding rates (<25%) due to the subtlety of pixel-level changes. It relies heavily on global distribution patterns, which are more likely to remain statistically stable under light embedding. Only when the embedded payload becomes large enough to distort the histogram does the method yield reliable detection results.

4.2. Computational Efficiency and Practicality

From a deployment perspective, computational efficiency is vital, especially in batch processing or real-time detection applications. As illustrated in Figure 2, the histogram method clearly excels in speed, owing to its reliance on a single-pass analysis of gray-level frequencies. Its lightweight design makes it ideal for rapid screening, albeit at the cost of reduced detection depth.

RS steganalysis, while more accurate in certain embedding scenarios, incurs higher computational overhead. Its block-wise perturbation and classification processes scale with image resolution and block size, making it less suitable for time-sensitive environments unless optimized.

The chi-square method, despite involving multi-scale analysis, maintains a balance between detection performance and processing speed. It benefits from efficient statistical computations and reduced dependence on image structure, offering both robustness and scalability.

4.3. False Positives and Misclassification Patterns

A closer look at misclassification patterns reveals important differences. The chi-square method, though powerful in detection, tends to produce higher false positive rates when dealing with images that naturally exhibit balanced parity distributions, especially at low embedding rates. This is consistent with the assumption that parity randomness introduced by LSB embedding is statistically similar to natural image noise in certain cases.

RS steganalysis demonstrates more balanced false positive and false negative rates in mid-range scenarios but shows inconsistent behavior outside its optimal range. Histogram-based analysis, on the other hand, suffers from significant underperformance at low embedding rates and may misclassify clean images if their natural histograms deviate from typical patterns (e.g., due to high contrast or synthetic content).

4.4. Robustness Enhancement via Multi-Scale Design

One of the standout features of the chi-square method is its ability to apply a multi-scale blocking strategy, significantly enhancing its robustness. By analyzing parity distributions across different block sizes (e.g., 8 × 8, 16 × 16, 32 × 32), the method captures both localized and global embedding artifacts. This hierarchical approach is particularly effective in detecting steganographic payloads that are spatially non-uniform or concentrated in specific regions.

Multi-scale design also helps mitigate the sensitivity of block-based methods to local image structure. Smaller blocks capture fine-grained distortions, while larger blocks provide contextual information and statistical stability. This feature distinguishes the chi-square method as a versatile and adaptable tool, especially in heterogeneous image datasets.

4.5. Future Directions and Emerging Trends

While the statistical methods reviewed in this paper are foundational and interpretable, they are increasingly challenged by modern steganography techniques designed to minimize statistical artifacts. To address this limitation, a promising direction involves hybridizing classical statistical models with modern machine learning techniques.

For instance, integrating handcrafted features (e.g., chi-square statistics, RS indicators) into machine learning pipelines — such as support vector machines or convolutional neural networks — can enhance detection performance, especially in complex or adversarial environments. Moreover, end-to-end deep learning approaches, when supplied with sufficient labeled data, have shown potential in automatically learning discriminative representations that may surpass handcrafted features.

Another area of exploration is adaptive or content-aware steganalysis, where methods dynamically adjust their detection thresholds or feature extraction strategies based on local image complexity or texture characteristics. Such techniques may reduce false positives and improve generalizability.

In conclusion, each of the three methods exhibits distinct advantages under specific conditions. Histogram analysis is efficient and easy to implement, RS steganalysis excels in mid-range detection with local sensitivity, and chi-square analysis offers the best overall accuracy and scalability through multi-scale enhancement. Future steganalysis systems may benefit from fusing these techniques with intelligent algorithms to achieve improved robustness and adaptability in real-world scenarios.

5. Conclusion

This study conducted a systematic comparison of three classical statistical steganalysis techniques — histogram-based analysis, RS (Regular-Singular) analysis, and chi-square analysis — within the context of grayscale LSB image steganography. By examining their theoretical underpinnings, detection accuracy under varying embedding rates, computational efficiency, and susceptibility to false classifications, the strengths and limitations of each method have been clarified.

The histogram-based method is simple, fast, and easy to implement. It performs best when the embedding rate is moderate to high, where visible distortions in pixel intensity distributions are more likely to occur. However, its reliability decreases significantly in low embedding scenarios, and it is vulnerable to advanced histogram-preserving embedding schemes.

RS steganalysis offers strong performance in medium embedding rate ranges due to its sensitivity to local changes in pixel smoothness. Its block-based design makes it more robust than the histogram method, though it requires more computational resources and may be sensitive to block size configurations.

The chi-square analysis, with its multi-scale blocking strategy, demonstrates the best overall detection performance, particularly at high embedding rates. Its statistical rigor and adaptability across block sizes enhance its robustness, although it can produce higher false positives in certain naturally balanced images.

For practical steganalysis, a combination of methods may be ideal, especially in environments with unknown or variable embedding rates. Histogram analysis can be used for fast initial screening, followed by RS or chi-square methods for deeper inspection. Looking ahead, hybrid approaches that integrate statistical features with machine learning or deep learning models hold strong promise for improving detection accuracy and generalization across diverse image types and embedding strategies.

References

1. R. Apau, M. Asante, F. Twum, J. Ben Hayfron-Acquah, and K. O. Peasah, "Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review," *PLoS One*, vol. 19, no. 9, p. e0308807, 2024, doi: 10.1371/journal.pone.0308807.
2. Y. Y. Demircan and S. Ozekes, "A Novel LSB Steganography Technique Using Image Segmentation," *J. Univers. Comput. Sci.*, vol. 30, no. 3, 2024, doi: 10.3897/jucs.105702.
3. K. F. Rafat and S. M. Sajjad, "Advancing reversible LSB steganography: Addressing imperfections and embracing pioneering techniques for enhanced security," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3468988.
4. M. Njoum, R. Sulaiman, Z. Shukur, and F. Qamar, "High-Secured Image LSB Steganography Using AVL-Tree with Random RGB Channel Substitution," *Comput. Mater. Continua*, vol. 81, no. 1, 2024, doi: 10.32604/cmc.2024.050090.
5. R. Deval, N. Gupte, J. K. Pinto, A. R. Modak, A. Verma, A. Sharma, et al., "Exploring advanced steganography techniques for secure digital image communication: A comparative analysis and performance evaluation," *Int. J. Electron. Secur. Digit. Forensics*, vol. 17, no. 1–2, pp. 233–266, 2025, doi: 10.1504/IJESDF.2025.143471.
6. A. F. M. Abadin, R. Sulaiman, and M. K. Hasan, "Randomization Strategies in Image Steganography Techniques: A Review," *Comput. Mater. Continua*, vol. 80, no. 2, 2024, doi: 10.32604/cmc.2024.050834.
7. K. D. Michaylov and D. K. Sarmah, "Steganography and steganalysis for digital image enhanced forensic analysis and recommendations," *J. Cyber Secur. Technol.*, vol. 9, no. 1, pp. 1–27, 2025, doi: 10.1080/23742917.2024.2304441.
8. K. F. Rafat and S. M. Sajjad, "Reversing the Irreversible LSB Steganography: Transformative Advances in Reversible Data Hiding," in *Proc. 6th Int. Conf. Adv. Comput. Sci. (ICACS)*, Feb. 2025, pp. 1–8, doi: 10.1109/ICACS64902.2025.10937874.
9. W. Alexan, E. Mamdouh, A. Aboshousha, Y. S. Alsahafi, M. Gabr, and K. M. Hosny, "Stegocrypt: A robust tri-stage spatial steganography algorithm using TLM encryption and DNA coding for securing digital images," *IET Image Process.*, vol. 18, no. 13, pp. 4189–4206, 2024, doi: 10.1049/ipr2.13242.
10. L. C. Chin, Y. C. Li, H. M. Hsieh, and C. M. Wang, "TIRDH: A Novel Three-Shadow-Image Reversible Data Hiding Algorithm Using Weight and Modulo," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3552661.
11. C. F. Lee and K. C. Chan, "A novel dual image reversible data hiding scheme based on vector coordinate with triangular order coding," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3421545.
12. K. F. Rafat and S. M. Sajjad, "Mastering Concealment: Dual-Veil and the Evolution of Secure Data Transmission," in *Proc. 6th Int. Conf. Adv. Comput. Sci. (ICACS)*, Feb. 2025, pp. 1–8, doi: 10.1109/ICACS64902.2025.10937884.
13. S. H. O. Hashemi, M. H. Majidi, and S. Khorashadizadeh, "A new architecture based ResNet for steganography in color images," *Multimed. Tools Appl.*, pp. 1–20, 2024, doi: 10.1007/s11042-024-19675-x.