NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 2, December 2025
E – ISSN – 2583-7559

An Extensive Analysis of Statistical Steganalysis Methods for LSB Image Steganography and Their Developments and Uses

Sougata Saha
Student, School of Forensic Sciences
National Forensic Sciences University.
Gandhinagar, India.
E-mail –sougata.bsmsfs1212649@nfsu.ac.in

Dr. Kapil Shukla
Assistant Professor, School of Forensic Sciences
National Forensic Sciences University
Gandhinagar, India.
E-mail– kapil.shukla@nfsu.ac.in

Dr. Krishna Modi
Assistant Professor, School of Forensic Science
National Forensic Sciences University.
Gandhinagar, India.
E-mail– krishna.modi@nfsu.ac.in

***Abstract*— Steganalysis has developed into a digital branch of cybersecurity which protects digital forensics from the rising threat of digital steganography utilized for secret communications and data concealment. Forensic analysts face major difficulties in detecting concealed payloads because digital images serve as the primary method used by attackers who employ Least Significant Bit (LSB) substitution to hide their payloads. The study provides a systematic assessment of traditional statistical steganalysis methods which researchers developed to combat LSB-based embedding techniques through analysis of Chi-square testing RS testing Sample Pair Analysis (SPA) and the Least Square Method (LSM). The analysis evaluates each technique according to its theoretical basis detection approach existing advantages existing disadvantages and its application in actual forensic fieldwork. The study shows how digital forensic experts encounter real-world difficulties because they must deal with unreliable tools which create different results across various detection system and because the field increasingly adopts blind or universal steganalysis methods that use feature engineering and machine learning. The study investigates how common image pre-processing techniques including scaling and cropping and contrast enhancement affect detection performance. The discussion extends to cloud and IoT healthcare environments which show an increasing divide between steganographic technology and its corresponding steganalysis tools.**

Keywords*— *Chi-square, Least Significant Bit, Least Square Method, Local Binary Pattern, Steganography, Steganalysis.

1.INTRODUCTION

Steganography is the art and science of hiding information into a particular medium such that hidden communication can take place. Steganography hides data within a cover medium in a way that makes its presence almost undetectable and invisible, whereas cryptography scrambles a message to make it unintelligible. It has been practiced since ancient times and evolved from simple techniques involving invisible ink to more sophisticated digital methods using multimedia files. Digital multimedia, such as audio, video, and images, are easily accessible and widely used; therefore, they can serve ideally for secret communications.

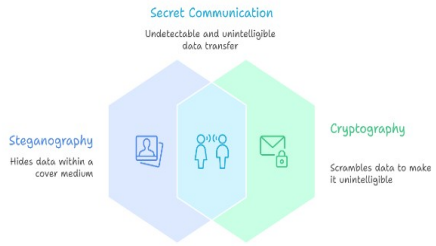


Figure 1. Steganography vs Cryptography: Hidden vs. Scrambled Communication.

According to Demircan and Ozekes [5], as it is inherently difficult to notice minute pixel changes, digital images have emerged as the most popular cover medium. Steganalysis is the opposite of steganography, and it deals with the study of detecting and extracting the secret data from a stego-file to identify questionable hidden signals and the reliability of current steganography methods. As mentioned by Shehab and Alhaddad [20], steganalysis is critical in homeland security, digital forensics, and law enforcement. Finding, retrieving, or extracting any potentially hidden information is a forensic analyst's primary responsibility in steganalysis.

Scope and Organisation

The specific focus of this review paper is digital image steganalysis, with a focus on methods that are used to counter Least Significant Bit (LSB) replacement steganography. We examine how steganalysis has changed technically over time, moving from traditional statistical techniques (targeted attacks) to more recent strategies that make use of feature engineering, machine learning, and deep learning (blind/universal attacks).

The arrangement of this paper is as follows: The fundamental LSB steganography methods and their prerequisites are described in Section 2. Classical statistical steganalysis

techniques (Chi-square, RS, SPA, and LSM) are covered in Section 3, their practical applications in digital forensics, cloud security, and Section 4 looks at tool evaluation, Section 5 discusses current problems and limitations, and Section 6 wraps up the review.

2.FOUNDATIONS OF IMAGE STEGANOGRAPHY

This section states about the core concept of LSB steganography i.e. about how this works, about its variations and enhancements and also the key requirements.

2.1. The Method of Least Significant Bit (LSB)

LSB substitution is one of the most popular and straightforward method in the domain of image steganography. It consists of substituting secret bits with one or more of the cover image's least important pixels. The main reasons for its popularity are its simple, speedy nature, while it offers high imperceptibility provided that the changes remain minimal. For instance, a PSNR of 30 dB normally indicates no visible degradation in the quality of an image [5].
However, success of LSB steganography depend on several factors, including the selection of the cover item, the embedding rate, the vulnerability to steganography, and the computational complexity. Although LSB is fast and simple, it generally suffers from low capacity and is detectable by dedicated statistical methods.

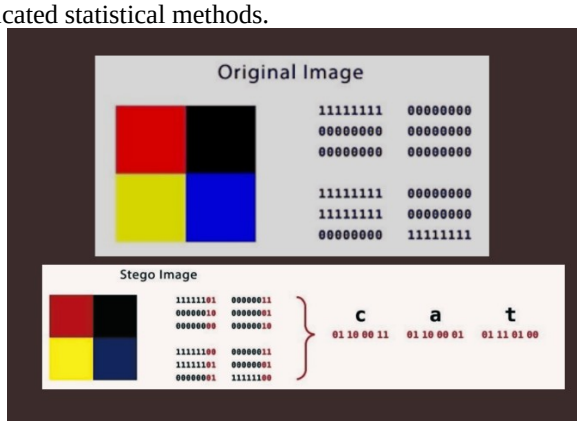


Figure 2. This Fig shows how data is being embedded in an image using LSB Steganography.

2.2. LSB Variations and Enhancements

Several changes have been suggested to address the recognised shortcomings of straightforward LSB substitution:
1. LSB-M (LSB Matching): This technique, which includes LSB Plus-Minus (LSBPM), only adjusts the LSB when the cover bit and secret bit do not match. If a modification is necessary, it randomly adds or subtracts one from the pixel value, producing zero-or-one changes. This
alteration complicates straightforward Chi-square attacks by making the resulting stego-image histogram appear more symmetrical. [11]

2**. LSB++ and RHTF**: As mentioned by Nag et al. [17], the LSB++ scheme generates less distortion on the output image but is also susceptible to steganalysis attacks. The RHTF method very frequently results in extremely high-level distortion of images; however, it exploits a modulo function technique that resists common steganalysis attacks such as chi-sqaure detection and RS analysis. Researchers have shown that the deficiencies of both LSB++ and RHTF can be surmounted by jointly applying these two schemes for generating enhanced security to successfully evade RS attacks and chi-square detection.
3. **Segmentation-Based LSB**: Advanced steg techniques make use of picture segmentation to decide the most appropriate high-entropy regions for concealing data with the minimum changes to retain the properties of a cover image. [5]
4. **Integration with Cryptography**: Gudivaka and Gudivaka [7], stated that steganography is often used together with encryption techniques such as AES, DES, and RSA for added security. This integration ensures, due to robust encryption, that even when the stego image is detected, the secret data will remain safe from hackers.

2.3. Key Steganographic Requirements

For a steganography method to be considered successful, it has to meet a number of basic criteria with respect to quality, capacity, robustness, and security. Imperceptibility is the ability of the stego-image to resemble the original cover image, such that distortions introduced during the embedding process are not noticeable, and this is usually measured using indices such as Structural Similarity Index (SSIM) and Peak Signal-to-Noise Ratio (PSNR), where higher PSNR values, usually above 30 dB, are an indication of good imperceptibility [5].

PSNR

PSNR calculates the ratio of the maximum possible power of the signal to the power of the noise corrupting the signal (in dB). The larger the PSNR value, the better the image quality.
Equation:
$PSNR = 10.\ Log_{10}\ (MAX_I^{\ 2} / MSE)$

- **MAX_I :** Maximum possible pixel value (e.g., 255 for 8-bit images).
- **MSE (Mean Squared Error)**: Average squared difference between the two images.

Equation:

Where I and k are the 2 images of size m * n.
Steps to Calculate:

- Calculate the MSE between the original and modified image.
- Square the maximum pixel value (usually $255^2 = 65025$).

- Divide MAX_I^2 by MSE.
- Take 10 * $\log_{10}$ of that result.

Structural Similarity Index Measure (SSIM)

SSIM assesses the perceived quality by comparing luminance, contrast, and structure between two images. It returns a value between -1 and 1, where 1 means the images are identical.
Equation:

Where,

- $\mu_{x,\ y}$: Mean intensity values of images.
- : Variances of images x and y.

σxy : Covariance of x and y.

c_1,c_2 : Stabilizing constants ().

Steps to Calculate**:**

- Convert images to grayscale if they are color, or compute per-channel.
- Apply a sliding window (e.g., 11×11 Gaussian) across the images to calculate local statistics ().
- Calculate the SSIM for each window.
- Average the SSIM values across all windows to get the final score.

Capacity is the maximum amount of secret data that can be embedded without impairing the cover medium, and this is usually measured in bits per pixel (bpp), which is a measure of the efficiency of the method [2], [3]. Robustness and security are the combined abilities of the embedded secret data to withstand steganalysis attacks and common image processing tasks such as compression, filtering, and scaling, and this is usually measured based on the secrecy of the embedded message and the undetectability of the stego-image [19].

3. Classical Statistical Steganalysis (Targeted Attacks)

The classical methods for performing steganalysis are "targeted"; that is, they attempt to break a specific embedding algorithm, most usually LSB substitution. They rely on the statistical changes induced by the hidden data in the cover image.

3.1. Chi-square Attack

The Chi-square attack, proposed by A. Westfeld and A. Pfitzmann in 1999, is one of the earliest statistical steganalysis attacks designed to identify LSB-based embedding. The attack takes advantage of the fact that LSB substitution changes the least significant bits of the cover image pixels, thus changing the histogram of the image and disrupting the statistical distribution of pixel values by creating pairs of adjacent pixel values (POVs) [15]. In other words, the attack calculates the statistical difference between the actual and expected frequencies of these pixel pairs in a suspected stego-image, and a large difference between the two distributions reveals the possible presence of hidden data [5], [11]. Performance analysis indicates that the Chi-square attack is very effective in identifying sequential LSB embedding attacks, reaching a detection accuracy of 99.8% when embedding is performed in all cover pixels, but its performance decreases dramatically for small payload sizes [11]. Moreover, some methods, such as Randomized Hiding Techniques with Frequency (RHTF), can successfully resist Chi-square attacks, although the attack is valid for both grayscale and color images [6].

3.2 RS (Regular-Singular) Analysis

RS analysis is a key statistical steganalysis technique introduced by Fridrich, Goljan, and Du in 2001, designed to detect and estimate hidden information embedded using LSB substitution. The method is based on analyzing the behavior of regular (R) and singular (S) pixel groups, as LSB embedding alters the proportion of these groups within an image [15]. It operates by dividing the image into pixel groups and measuring noise variations after selectively flipping the LSBs of fixed pixels; depending on whether the noise level increases or decreases, groups are classified as R or S, enabling estimation of the embedded payload length [11], [16]. In terms of performance, RS analysis has been shown to be more accurate than the Chi-square method for steganography detection, although it fails when the embedding rate is extremely low (below 0.005 bits per pixel). The technique performs best at embedding rates above approximately 3% and is applicable to both grayscale and color images; however, reported accuracy varies across studies, with combined RS and SPA approaches detecting large payloads with accuracies of around 54% and 55%, respectively [6], [16].

3.3. Sample Pair Analysis (SPA) and Least Square Method (LSM)

The main goal of the quantitative steganalysis methods Sample Pair Analysis (SPA) and the Least Square Method (LSM) is to estimate the size of the hidden messages embedded in digital media. Sample Pair Analysis, first introduced by Dumitrescu et al. in 2003, is based on a finite state machine where internal states produce trace multisets that represent sets of sample pairs. Analysis by Demircan and Ozekes [5] revealed that random LSB embedding affects the statistical dependencies and pair values of these multisets, allowing SPA to estimate the size
of the hidden messages with high precision using a quadratic function [11]. The Least Square Method, first introduced by Lu et al. in 2004 for fast detection of LSB substitution, is considered an extension of SPA, working on the same principles but using a least-squares estimation method; however, analysis suggests that the error distribution of LSM is slightly negatively skewed with heavy-tailed outliers instead of normal distribution [6]. In terms of performance, RS analysis is slightly less accurate than SPA, although SPA

becomes invalid if the trace multisets are unchanged after embedding, with the maximum estimation error of SPA being 8.6%, slightly better than RS analysis [6].

3.4. Comparative Performance and Limitations

Technique	*Targeted Application*	*Key Advantage*	*Key Disadvantage*	*Accuracy/Detection*
Chi-square	Sequential LSB	Detects 100% payload well.	Performs poorly for small payloads	99.8% for 100% embedding. [6]
RS Analysis	Sequential & Random LSB	Reliable estimation of message length	Fails if embedding rate <0.005	Better than chi-square in reliability. [6], [11]
SPA	Random LSB	More accurate than RS.	Fails if trace multisets don't changes.	Max error 8.6%. [5], [11]
LSM	Random LSB	Similar performance to SPA	Error distribution is not normal	Close accuracy to SPA. [6]

Table 1: The trade-offs between the traditional statistical methods are highlighted by a comparative analysis.

These methods retain their relevance even with the emergence of blind steganalysis techniques.

4. Steganalysis in Practical Applications and Digital Forensics

The findings of steganalysis are very important for DFIs and, in certain security contexts like cloud computing, the deployment of steganalysis tools is increasing.

4.1. Steganalysis for Digital Forensic Investigators (DFIs)

The difficult process of identifying and extracting concealed information from cover media is mainly the responsibility of digital forensic analysts, and the choice of an effective steganalysis method is greatly dependent on the type and availability of information. In cases where the embedding scheme is unknown, blind or universal steganalysis methods should be used, as recommended by Karampidis et al. [11]; wavelet coefficient correlation and Fisher Criterion-based methods have shown very high detection rates of 95% or more against popular tools such as F5 and OutGuess, although no universal method currently exists that can achieve both high precision and low computational complexity [16]. In cases where the steganographic method is known, statistical and signature-based methods are more appropriate, with statistical methods such as RS analysis being more effective than signature-based methods in the absence of the original cover image and when only the stego-object is available [3], [8], [10]. The early pioneering efforts of Johnson and Jajodia in the late 1990s formed the foundation for the development of current technologies and techniques used in steganalysis and related fields that aim to

4.2. Tool Evaluation and Benchmarking

In order to provide better assistance to digital forensic analysts, it is necessary to have a practical assessment of steganalysis methods, as shown in recent research that evaluated a number of popular free steganography and steganalysis software. The experimental outcome shows that Steghide is more trustworthy than OutGuess and F5 for steganographic embedding, while blind steganalysis methods based on AI were shown to be susceptible to stego-images created by F5 and OutGuess. In regard to steganalysis performance, although StegExpose had a higher average accuracy in the test environment, Aletheia was shown to be more trustworthy when comparing detection abilities in different settings. Moreover, feature analysis showed that simple image features such as file size, color distribution, Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE) cannot be considered conclusive for the presence of secret messages in JPEG images, although PSNR and MSE are significant parameters for assessing the quality and distortion of stego-images compared to their original cover images [16].

4.3. Steganography and Steganalysis in Forensics

Steganography has been widely investigated for implementation in security-sensitive domains where confidentiality and data integrity are of prime importance. In cloud computing setups, LSB steganography remains an area of active research as a standalone solution for countering data loss, modification, and theft, and its efficiency is further amplified when combined with cryptographic methods like AES and RSA, which greatly enhance data security and confidentiality in the form of JPEG images, although at the expense of increased file size. In IoT healthcare systems, steganography is discussed for secure authentication and protection of healthcare data, often using multi-layered security strategies to attain higher levels of imperceptibility and robustness. Moreover, the increasing adoption of online services like cloud storage services and IP telephony for steganographic communication creates grave challenges for digital forensic analysts, as standardized steganalysis solutions for network traffic are still not available, making it difficult to perform network steganalysis [7].

4.4. Image Preprocessing and Attack Resilience

Among the prominent risks to the efficiency of steganalysis is the unintentional alteration or processing of the cover image either before or during the transmission process. Digital images are usually preprocessed with various operations such as cropping, resizing, and contrast enhancement before secret message embedding, which can greatly affect the statistical pixel characteristics and, in turn, the security and detectability of steganographic methods. Experimental results show that pre-embedding processing tasks such as cropping, resizing, and contrast enhancement can greatly impair the detection accuracy of advanced LSB steganalysis algorithms like LSBPM and WOW. Cropping reduces the amount of information available for analysis, resizing increases the number of false alarms, and contrast enhancement introduces a large number of detection errors due to its reliance on the intensity level of the pixels, which are also used during embedding. However, some feature-based steganalysis techniques, such as SPAM and joint entropy features, have shown relatively better robustness by exploiting the residual impact of preprocessing on spatial domain steganography [3].

5. Result and Discussion

From the literature review, it is clear that classical statistical steganalysis methods such as Chi-square testing, RS analysis, Sample Pair Analysis (SPA), and Least Square Method (LSM) are successful in identifying statistical anomalies caused by Least Significant Bit (LSB) image steganography. The accuracy of detection is found to be high when the embedding policy is known and the message size is moderate to large. Specifically, Chi-square analysis is found to have detection rates close to 99% for full sequential LSB embedding, while RS analysis is found to be more robust as it allows both detection and estimation of approximate message size.

Further results reveal that SPA and LSM are more useful for estimating the size of the embedded message rather than making binary detection. SPA has been found to have a lower estimation error compared to RS analysis, while LSM has similar estimation accuracy but with non-uniform error distributions. For all methods, the detection accuracy is found to be low for low embedding rates, random embedding policies, and images with high texture complexity.

The results indicate that there is no universal detection capability offered by any classical statistical steganalysis technique against all types of LSB steganography. The detection capability is highly dependent on various factors such as the embedding rate, image content, and adaptive or random hiding processes. Therefore, a combination of statistical techniques offers more accurate forensic results compared to the use of individual techniques.

Moreover, the literature review points out the great effect of image preprocessing tasks such as cropping, resizing, and contrast enhancement on the accuracy of steganalysis. These tasks may conceal steganographic marks or produce false positives, making classical steganalysis techniques less applicable in practical forensic tasks. Although machine learning-based blind steganalysis techniques are gaining popularity, classical statistical techniques are still applicable due to their low computational complexity, interpretability, and efficiency in known embedding mechanisms. Future research should aim at developing hybrid techniques that combine statistical analysis with feature-based and learning-based steganalysis to improve robustness against sophisticated steganographic methods.

6. Challenges and Future Prospects

However, in spite of the essential development in this direction, there are still several crucial drawbacks in steganalysis that prevent the building of really universal and reliable tools within this scope.

According to Dalal and Juneja [3], there is a very noticeable imbalance in research, with steganography techniques and tools far outnumbering the methods of steganalysis. This is further reflected by the publication frequency in which research articles in the realm of steganography always outweigh that of steganalysis between the publishing giants Springer, IEEE, and Elsevier. Perhaps this is because steganalysis is an arduously difficult task to conduct and mostly requires highly dedicated and astute researchers and experts. The ultimate but yet unattainable objective is a steganalysis technique which identifies all embedding algorithms with excellent accuracy and minimal computing requirements. [11]

However, the recent methods of steganalysis, especially those using machine learning and deep learning, have some

challenges in terms of scalability and efficiency. Most of the current image steganalysis classification (ISC) methods use feature vectors of a very high dimension, which makes the computational complexity and processing time much higher, hence restricting their performance [8]. Furthermore, the design and training of sophisticated AI models, such as convolutional neural networks and VisionStego systems, are much more resource and budget-intensive compared to traditional statistical approaches [2]. Additionally, finding a balance between the three primary requirements of steganography—imperceptibility, high embedding rate, and robustness—and overall security is still a challenge, as any improvement in one area leads to degradation in the other areas.

However, despite the continuous progress, there are still a number of important challenges that need to be addressed in steganalysis research. Although image steganalysis datasets like BOSSBase, NRCS, and Corel are publicly available and have been widely used for comparison, there is a substantial lack of standardized publicly available datasets for video and audio steganalysis, which results in inconsistent evaluation and unfair comparison of performance among the proposed methods in these areas [20]. Moreover, the development of effective detection and extraction tools is still remarkably behind the progress made in embedding techniques, as most of the existing steganalysis tools are mainly designed to detect distortions or artifacts caused by embedding rather than extracting the embedded information itself; therefore, there is an urgent need for specialized research to develop more effective and reliable tools for both detection and extraction [3]. Moreover, universal steganalysis methods also have some natural limitations, especially the lack of a generalized convolutional neural network (CNN) model that can be used for the reliable detection of hidden messages in unseen data, as the performance of steganalysis significantly degrades when tested on images outside the training data distribution [20].

Some of the promising areas of research that could be explored in the future include transform domain steganalysis, in which the effect of preprocessing steps, which have been explored to a great extent in the spatial domain until now, needs to be explored in the transform domain, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [3]; the design of hybrid steganalysis methods that can combine methods in the spatial and transform domains, or methods that can combine classical statistical analysis with advanced feature extraction to improve embedding capacity, imperceptibility, and robustness [16]; the use of advanced deep learning models, especially Generative Adversarial Networks (GANs), to improve the anti-detection capabilities of steganographic systems [2]; and the design of robust detection methods that can detect hidden information in images that have been subjected to common cover modifications, such as cropping, scaling, or other forms of preprocessing that can severely affect steganalysis performance [3].

7. Conclusion

Digital picture steganalysis has evolved in a very complex manner-from basic statistical attacks to highly complex, AI-driven detection systems-particularly with respect to approaches based on LSB replacement. Modern adaptive steganography methods are increasingly bypassing classical techniques such as Chi-square, RS analysis, SPA, and LSM that nevertheless remain relevant in identifying known, sequential embedding. The most reliable route toward universal detection is provided by the paradigm change given to blind steganalysis, afforded by SPAM and SFTA feature engineering methods in conjunction with deep learning classifiers, such as CNNs and DRNs. The review performed herein confirms that Aletheia outperforms StegExpose as a more reliable steganalysis tool, while Steghide represents a robust steganography option. Most important is the fact that preprocessing (scaling, cropping) of images significantly undermines practical security in steganography and simultaneously enhances it by integrating cryptographic methods, AES/RSA. While good progress is being made, the prevailing asymmetry between the ease of steganography and the difficulty of steganalysis remains the core challenge for researchers and forensic professionals. Indeed, future efforts should be directed toward closing this gap by developing computationally efficient, feature-based AI tools specifically designed for countering data-hiding in modified cover media.

References

[1] Z. A. Alher, B. M. A. Imran, and I. A. Ali, “LSB as a Steganography Tool in Information Security,” *5th International Conference on Communication Engineering and Computer Science (CIC-COCOS’24)*, pp. 348–355, Jan. 2024, doi: 10.24086/cocos2024/paper.1157. Available: http://dx.doi.org/10.24086/cocos2024/paper.1157

[2] H. Alshamrani, S. H. Alajmani, R. Y. Alyami, and B. Soh, “Comprehensive Comparison of Image Steganography Techniques with Security Enhancement,” *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 14, no. 2, pp. 7–19, Jul. 2025, doi: 10.35940/ijrte.a8249.14020725. Available: https://doi.org/10.35940/ijrte.a8249.14020725

[3] S. Chhikara and R. Kumar, “Information theoretic steganalysis of processed image LSB steganography,” *Multimedia Tools and Applications*, vol. 82, no. 9, pp. 13595–13615, Sep. 2022, doi: 10.1007/s11042-022-13931-8. Available: https://doi.org/10.1007/s11042-022-13931-8

[4] M. Dalal and M. Juneja, "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5723–5771, Oct. 2020, doi: 10.1007/s11042-020-09929-9. Available: https://doi.org/10.1007/s11042-020-09929-9

[5] Y. Y. Demircan and S. Ozekes, "A novel LSB steganography technique using image segmentation," *JUCS - Journal of Universal Computer Science*, vol. 30, no. 3, pp. 308–332, Mar. 2024, doi: 10.3897/jucs.105702. Available: https://doi.org/10.3897/jucs.105702

[6] B. R. Ghosh, S. Banerjee, and J. K. Mandal, "A survey on LSB Replacement-Based Statistical Image Steganalysis Techniques," in *Lecture notes in electrical engineering*, 2023, pp. 313–320. doi: 10.1007/978-981-99-3656-4_32. Available: https://doi.org/10.1007/978-981-99-3656-4_32

[7] R. L. G. R. L. Gudivaka and R. K. G. R. K. Gudivaka, "A dynamic Four-Phase data security framework for cloud computing utilizing cryptography and LSB-Based steganography," *International Jounal of Information Technology and Computer Engineering.*, vol. 17, no. 3, pp. 29–41, Jul. 2021, doi: 10.62643/ijerst.2021.v17.i03.pp29-41. Available: https://doi.org/10.62643/ijerst.2021.v17.i03.pp29-41

[8] B. T. Hammad, I. T. Ahmed, and N. Jamil, "A Steganalysis classification algorithm based on distinctive texture features," *Symmetry*, vol. 14, no. 2, p. 236, Jan. 2022, doi: 10.3390/sym14020236. Available: https://doi.org/10.3390/sym14020236

[9] L. Hu, L. Jiang, and C. He, "A novel steganalysis of LSB matching based on kernel FDA in grayscale images," *IEEE Int. Conference Neural Networks & Signal Processing. 2008*, vol. 1768, pp. 556–559, Jun. 2008, doi: 10.1109/icnnsp.2008.4590412. Available: https://doi.org/10.1109/icnnsp.2008.4590412

[10] A.Ibrahim, "Steganalysis in computer forensics," *Research Online (Edith Cowan University)*, Jan. 2007, doi: 10.4225/75/57ad58327ff2e. Available: https://ro.ecu.edu.au/adf/10

[11] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *Journal of Information Security and Applications*, vol. 40, pp. 217–235, Apr. 2018, doi: 10.1016/j.jisa.2018.04.005. Available: https://doi.org/10.1016/j.jisa.2018.04.005

[12] T. I. U. Khairun, S. Lutfi, R. Rosihan, and T. I. U. Khairun, "PERBANDINGAN METODE STEGANOGRAFI LSB (LEAST SIGNIFICANT BIT) DAN MSB (MOST SIGNIFICANT BIT) UNTUK MENYEMBUNYIKAN INFORMASI RAHASIA KEDALAM CITRA DIGITAL," *JIKO (Jurnal Informatika Dan Komputer)*, vol. 1, no. 1, pp. 34–42, Apr. 2018, doi: 10.33387/jiko.v1i1.1169. Available: https://doi.org/10.33387/jiko.v1i1.1169

[13] Lynn ND, Emmanuel G, Kawuwa H. A Novel Steganography and steganalysis model for Information Security: A case study of National Information Technology Authority-Uganda (NITA-U). Journal of Linguistics and Technology. 2025 May 1;92–114. Available: https://greatwordlinkedcenter.id/index.php/jlingtech/J-LINGTECH

[14] H. K. M, M. A. J. H, M. Y. S, and N. K, "LSB Based Steganography For Secure Digital Image Embedding," *TechRxiv*, Apr. 2025, doi: 10.36227/techrxiv.174362807.70650230/v1. Available: https://doi.org/10.36227/techrxiv.174362807.70650230/v1

[15] M. Mahdavi, Sh. Samavi, N. Zaker, and M. Modarres-Hashemi, "Steganalysis method for LSB replacement based on local gradient of image histogram," Oct. 01, 2008. Available: https://doaj.org/article/920732dd179d43d08f48b8e3537bfee3

[16] K. D. Michaylov and D. K. Sarmah, "Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations," *Journal of Cyber Security Technology*, vol. 9, no. 1, pp. 1–27, Jan. 2024, doi: 10.1080/23742917.2024.2304441. Available: https://doi.org/10.1080/23742917.2024.2304441

[17] A.Nag, S. Choudhary, S. Basu, and S. Dawn, "An Image Steganography Scheme based on LSB++ and RHTF for Resisting Statistical Steganalysis," *IEIE Transactions on Smart Processing and Computing*, vol. 5, no. 4, pp. 250–255, Aug. 2016, doi: 10.5573/ieiespc.2016.5.4.250. Available: https://doi.org/10.5573/ieiespc.2016.5.4.250

[18] R. Panigrahi and N. Padhy, "An effective steganographic technique for hiding the image data using the LSB technique," *Cyber Security and Applications*, vol. 3, p. 100069, Aug. 2024, doi: 10.1016/j.csa.2024.100069. Available: https://doi.org/10.1016/j.csa.2024.100069

[19] Srinivasan, Divyasree & Manojkumar, Khushi & Syed, Afreen & Nutakki, Harichandana. (2024). A Comprehensive Review on Advancements and Applications of Steganography. 10.13140/RG.2.2.13568.44807.

[20] D. A. Shehab and M. J. Alhaddad, "Comprehensive Survey of Multimedia Steganalysis: Techniques,

Evaluations, and Trends in Future research," *Symmetry*, vol. 14, no. 1, p. 117, Jan. 2022, doi: 10.3390/sym14010117. Available: https://doi.org/10.3390/sym14010117

[21] A.K. Singh, Amity University, J. Singh, Manipal University Jaipur, H. V. Singh, and Kamla Nehru Institute of Technology, Sultanpur, "Steganography in images using LSB technique," journal-article, 2023.