Substitution Techniques in Image Steganography: A Review

Bharti Chugh
Ph.D. Scholar,
Assistant Professor,
Department of Computer Science,
Vanita Vishram Women's University, Surat – 395007, Gujarat, India
Email - bhartichugh08@gmail.com

Dr. Nimisha Modi
Assistant Professor,
Department of Computer Science,
VNSGU, Surat – 395007, Gujarat, India
Email - nimishamodi@vnsgu.ac.in

Abstract:

One of the most renowned techniques for secure communication by concealing confidential information within digital images - Image Steganography is still widely used because of its efficacy, simplicity and also adaptability to different image formats. The technique is traditional still it is widely growing and emerging. This review paper aims to provide a comprehensive study of substitution techniques that are widely used in steganography and majorly focuses on Least Significant Bit (LSB) substitution techniques and their numerous enhancements. The paper aims to compare several techniques in terms of embedding capacity, imperceptibility, robustness etc. offering insights to their strengths and weaknesses. This paper aims to highlight emerging trends, research gaps and opportunities for developing more robust substitution-based steganography schemes by critically analysing existing literature. This study also aims to be a foundation for researchers seeking to advance data concealing techniques.

1. Introduction:

Steganography is a technique that is used to hide confidential data including text, images, audio and videos in an undetectable manner such that no one can detect it. A renowned technique known as Image-based steganography uses images as a media to hide and transmit confidential information over the web. The primary goal of steganography is to ensure secret communication between two users. An unknown person cannot be able to detect any information by having a look on the image. Image- based steganography is a very conventional technique which is still popular because of its simplicity, capacity to embed data without degrading image quality etc. so recently different image steganography methods have been proposed. However, image steganography is a challenging task at the same time because of security, payload, computational efficiency etc. [1]

Steganographic techniques may be broadly divided into two categories: spatial domain techniques, such as Least Significant Bit (LSB) replacement, and transform domain approaches, such as embedding based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). [Despite their simplicity and massive payload, spatial domain tactics are more vulnerable to steganalysis and image processing attacks than transform domain techniques, which provide more resilience at the cost of computing complexity. Performance evaluation metrics like Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are commonly employed to gauge image quality and imperceptibility. In this paper various substitution techniques for image steganography are critically reviewed to address their shortcomings and challenges so that further work can be done in this field.

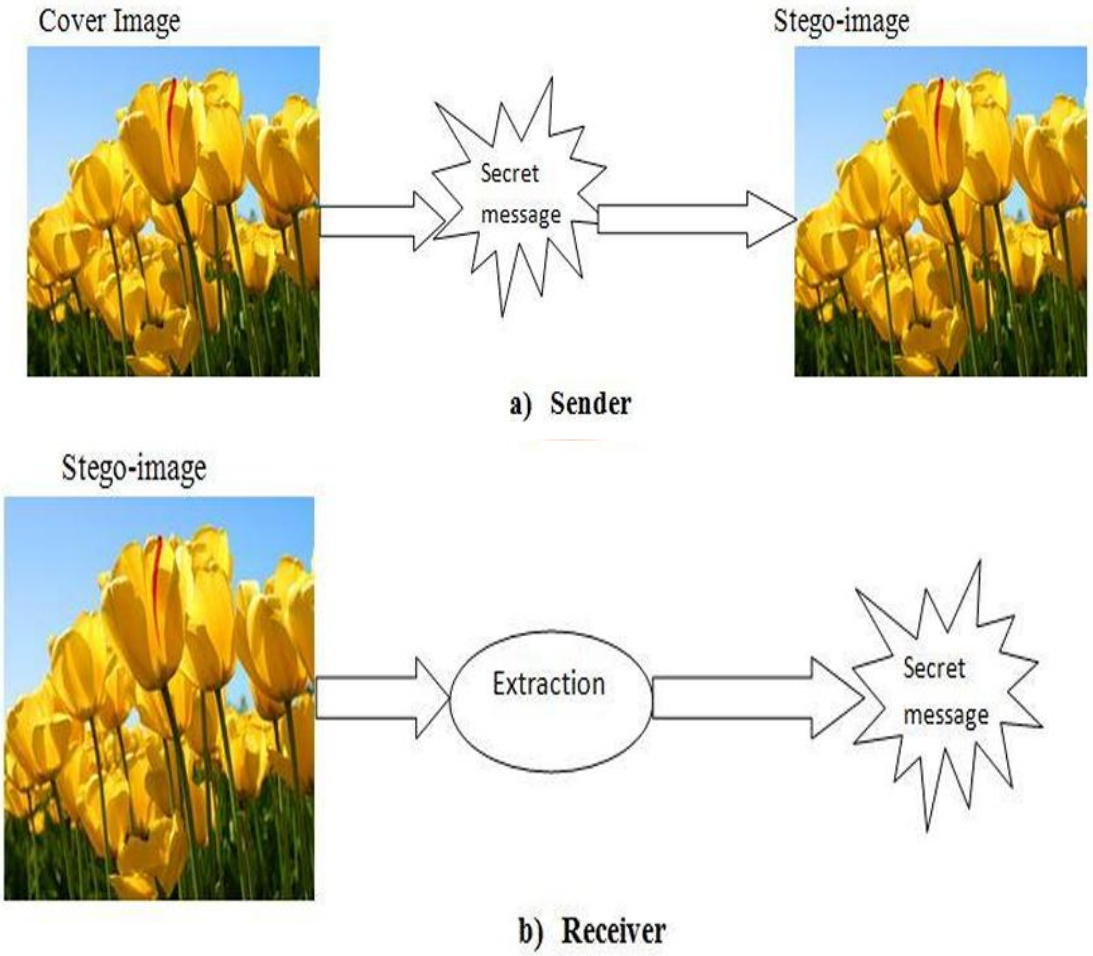

Fig 1: Steganography Process [3]

2. Substitution techniques

Substitution in steganography is the method of concealing secret information by substituting bits of the concealed data with certain cover medium components, often the least important picture pixel segments.[10] By making just minor changes to the cover image, this method makes sure that the changes are invisible to the naked eye. Various substitution-based steganography techniques are discussed and further compared:

A steganography technique called LSB (Least Significant Bit) replaces the lowest-order bits of picture pixels with message bits to conceal secret data with little to no visible alteration.[11] It is the most widely used substitution technique because of its simplicity.

(MGMx) with LSB adds randomization and enhances the security of concealed data by first dividing the cover picture into blocks and shuffling them using a magic matrix before applying LSB replacement. Only a key holder can decipher the concealed message thanks to Secret Key Steganography with Insertion Scheme (SKSIS), which uses LSB substitution to implant secret data into picture pixels.

LSB substitution with chaotic position selection (Logistic map) and payload XOR using Tent map is a steganography technique that improves security and imperceptibility by first XOR-encrypting secret data with a Tent map sequence before embedding it into pixel LSBs at locations chosen by a Logistic map.

Before embedding a message in steganography, Huffman Coding (lossless substitution compression) reduces the total message size without sacrificing information by substituting shorter binary codes for often appearing data symbols and larger codes for less frequently occurring ones.

In steganography, the performance of a method is generally evaluated using the main characteristics:

1. Embedding capacity, which is measured in bits per pixel, is the amount of data that can be concealed inside an image; the more bits, the better.
2. Robustness: the degree of picture modification that a hidden message can withstand; the greater this value, the more effective the concealing technique.
3. Security: a steganographic image's resistance to steganalysis procedures is measured using an attack resistance ability metric; the greater the resistance, the stronger the security.
4. Imperceptibility: the degree to which the presence of a concealed message can be quickly ascertained by looking only at the steganographic image's quality, the higher the better. SSIM and/or PSNR scores are frequently used to test these criteria.

3. Literature Review

Substitution is one of the most widely used techniques for hiding data because of its simplicity. Although the Least Significant Bit (LSB) technique remains prone to compression and statistical threats, it has been commonly adopted as a key strategy because it allows for a substantial embedding capacity while causing little perceptual distortion. To increase efficiency and optimize the payload that can be carried within the images, approaches like PVD (Pixel Value Differencing) and Optimal Pixel Adjustment Process (OPAP) have been unveiled. Even though their capacity is limited, transform domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) have been studied to improve robustness against changes in images.[4]

Recent studies have focused on hybrid substitution methods that optimize the balance between robustness, imperceptibility, and capacity by integrating spatial and transform domain strategies. [12] Despite these advancements, substitution-based approaches continue to

struggle against advanced steganalysis, highlighting the necessity for improved algorithms that achieve a balance between security and efficiency.

So, this paper majorly focuses on comparing a few substitution techniques which can serve as a basis for scholars to analyse various parameters regarding these techniques:

Sr No	Ref	Technique Used	Description	Evaluation Metrices
1	[1]	Least Significant Bit (LSB) Substitution (up to 4 bits)	Embeds secret data into the least significant bits of the cover image pixels (mainly blue channel).	PSNR: Avg. 71.81 dB (128×128), 77.31 dB (256×256), 79.63 dB (512×512) MSE: Very low (close to 0, exact values not always given). - SSIM, NCC, IF, QI: ≈ 1 (near-identical quality).
		Magic Matrix (MGMx) with LSB	Blue Channel is categorized into 4 chunks and shuffled with magic matrix which is followed by LSB embedding to increase randomness and enhance security.	PSNR > 50 dB across all cases, indicating imperceptibility.
		Multi-Level Encryption Algorithm (MLEA) + LSB	Secret bits are encrypted before LSB embedding using XOR, bit-flipping, and circular shifts making data extraction even harder.	Same quality metrics (PSNR > 70 dB, SSIM ≈ 1, NCC ≈ 1). Security tested against RS and PDH analysis: Resistant to RS, but weak to PDH.
2	[2]	LSB with XOR	Robustness and higher payload are provided as compared to 1-LSB. IMStego tool is used.	PSNR measured; improves imperceptibility compared to 1-LSB. No explicit MSE values provided.
3	[5]	Secret Key Steganography with Insertion Scheme (SKSIS)	Secret Key Steganography with Insertion Scheme (SKSIS)	Capacity: 786,432 bits; PSNR: 51.14 dB; Q: 0.9967; Processing time: 3.414 sec.
		Novel Insertion Method Algorithm (NIMA)	Extends LSB substitution by embedding 5–6 bits per pixel using a novel insertion scheme. Uses secret key + SHA-256 hashing for robustness and error detection.	Capacity: 1,399,591 bits; PSNR: 47.19 dB; Q: 0.9981; Processing time: 3.163 sec; MSE very low (close to LSB).
4	[6]	LSB substitution with chaotic position selection (Logistic map) and payload XOR using Tent map	Secret message bits are XORed with a Tent-map sequence, then embedded into pixel LSBs at positions determined by a Logistic-map sequence in a grayscale image.	PSNR: 68.33dB; MSE: 0.0096; SSIM: 0.9992

5	[7]	Character-sequence substitution	Secret code is examined word-by-word. When a match is found, the sequence is substituted by single-byte code.	PSNR :65.22 → 66.16(LSB-e-LSB); MSE: 0.01956 → 0.01575
6	[8]	Huffman Coding (Lossless substitution compression)	Secret message is compressed before embedding. A variable-length method that replaces frequent symbols with shorter codes and rare symbols with larger codes.	MSE ≈ 0.0028 – 0.0042 PSNR ≈ 42 – 48 dB SSIM ≈ 0.96 – 0.99
		DWT-based substitution (Lossy compression + LSB embedding)	Discrete Wavelet Transform substitutes pixel representation with frequency sub bands (LL, LH, HL, HH). Secret data is embedded in less perceptually sensitive sub bands using LSB, reducing visibility of changes.	MSE ≈ 0.0031 – 0.0065 PSNR ≈ 40 – 45 dB SSIM ≈ 0.95 – 0.98
7	[9]	XOR + Circular Bit-Shift + LSB	Secret text is carefully encrypted via XOR with Circular bit-shift key which is embedded in LSBs of RGB channels.	Avg PSNR = 64.85
		Hyper-Chaotic Shuffling + DCT	Cover image encrypted using hyper-chaotic map; secret message Huffman-coded and embedded in MSB of DCT coefficients.	PSNR = 77.16 – 53.68
		Symmetric Cipher + XOR Encoding	Secret message encrypted, XORed with cover bits, and embedded using block-wise inversion to minimize changes.	PSNR = 57.475 – 51.629

Table 1

4. Research Finding

Various steganography techniques especially substitution-based steganography techniques vary drastically in terms of payload, robustness, security and imperceptibility. Traditional substitution techniques i.e. Classical LSB substitution aims to achieve high imperceptibility but it is vulnerable to steganalysis attacks. Magic Matrix with LSB and LSB + MLEA enhance security by increasing randomness, yet face vulnerability issues from steganalysis. Methods especially focussing on payload such as NIMA (Novel Insertion Method Algorithm), can embed 5 to 6 bits per pixel but degrades image quality (PSNR ~ 47dB). Techniques such as Huffman coding reduce payload before embedding which minimizes distortion, while techniques like DWT (Discrete Wavelet Transform) enhances robustness against steganalysis but at a higher computational cost. Hybrid approaches including circular bit-shift, XOR or hyper chaotic DCT embedding, balance both security and imperceptibility, with PSNR

between 53 and 77 dB. In conclusion, basic LSB techniques focus on image quality but comprise on image quality while advanced hybrid techniques offer robustness and security but with added complexity.

5. Research Gap

- Security and Robustness: The real-world application of classical and modified LSB algorithms is limited because to their susceptibility to steganalysis and their fragility against noise, compression, and scaling.
- Imperceptibility versus Capacity The trade-off While very undetectable approaches only enable modest capacity, techniques that achieve large payload frequently result in reduced picture quality (e.g., PSNR ~47 dB in NIMA).
- Practicality and Complexity: While advanced hybrid and chaos-based methods boost resilience, they also increase computing overhead and are frequently limited to particular picture formats.

6. Scope for future work

- Create Sturdy Substitution Techniques: Create algorithms that maintain data integrity even in the face of noise, compression, and typical picture alterations.
- Maximize Imperceptibility and Capacity Trade-off: Develop flexible techniques that optimize payload while preventing appreciable picture quality loss (PSNR, SSIM).
- Enhance Practical Usability: Expand substitution techniques to minimize computational cost for real-time applications and function well across a variety of picture formats.

7. Conclusion

Despite of the simplicity and high imperceptibility, substitution-based steganography still battles with robustness, capacity trade-offs and security which strongly highlights the need for more secure, robust and techniques that can embed larger payload in future research.

References

1. Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., ... & Espinosa, J. C. M. (2025). A novel and efficient digital image steganography technique using least significant bit substitution. *Scientific Reports*, *15*(1), 107.
2. BhanuRajeshNaidu, K., Manikanta, J., Vaseem, S. M. D., Adnan, S. M. D., & Kumar, C. N. (2025). Secure file sharing system using image steganography and cryptography techniques. In Challenges in Information, Communication and Computing Technology (pp. 120-124). CRC Press.

3. Kaur, A., Kaur, R., & Kumar, N. (2015). A review on image steganography techniques. *International Journal of Computer Applications*, *123*(4).
4. Panigrahi, R., &Padhy, N. (2025). An effective steganographic technique for hiding the image data using the LSB technique. *Cyber Security and Applications*, *3*, 100069.
5. Al-Jarah, A. I. H., & Ortega-Arjona, J. L. (2024). Enhancing the capacity and robustness of an LSB algorithm using a novel insertion method, hashing function, and secret key. *IEEE Access*.
6. Yakut, S. (2024). An Efficient Steganography Method Based on Chaotic Functions and XOR Operation for Data Hiding. *BilgisayarBilimleriveTeknolojileriDergisi*, *5*(2), 58-65.
7. Jayapandiyan, J. R., Kavitha, C., & Sakthivel, K. (2020). Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization. *Ieee Access*, *8*, 136537-136545.
8. Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE access*, *9*, 31805-31815.
9. Ghoul, S., Sulaiman, R., & Shukur, Z. (2023). A review on security techniques in image steganography. *International Journal of Advanced Computer Science and Applications*, *14*(6).
10. Kombrink, M. H., Geradts, Z. J. M. H., & Worring, M. (2024). Image steganography approaches and their detection strategies: A survey. ACM Computing Surveys, 57(2), 1-40.
11. Goel, S., Rana, A., & Kaur, M. (2013). A review of comparison techniques of image steganography. *Global Journal of Computer Science and Technology*, *13*(4), 9-14.
12. Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. IEEE Access, 8, 166589-166611.
13. Rehman, W. (2024). A novel approach to image steganography using generative adversarial networks. arXiv preprint arXiv:2412.00094.
14. Subramanian, N., Elharrouss, O., Al-Maadeed, S., &Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423.
15. Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. Information sciences, 609, 1451-1488.

16. Sahu, A. K., & Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. Indonesian Journal of Electrical Engineering and Computer Science, 2(3), 712-719.
17. Goel, S., Rana, A., & Kaur, M. (2013). A review of comparison techniques of image steganography. Global Journal of Computer Science and Technology, 13(4), 9-14.