International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Review paper of Least Significant Bit (LSB) based steganography with encryption.

Sunit Jana , Rakhi Biswas ,Disha Das, Deepshikha Chatterjee , Nikita Pal , Debasmita Basak ,Koushik Pal

Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology , Kolkata

Abstract - In the age of pervasive digital communication, ensuring the confidentiality of sensitive information has become increasingly vital. Image steganography, particularly techniques based on Least Significant Bit (LSB) manipulation, offers a covert channel for data hiding. However, classical LSB methods lack robustness and are vulnerable to various attacks. This research presents a comparative and consolidated study of advanced LSB-based image steganography techniques enhanced with cryptographic mechanisms such as Huffman Coding, Triple DES (3DES), Multi-Level Encryption (MLE), and MD5 hashing. A novel approach—Huffman Code LSB-based Image Steganography using Multi-Level Encryption and the achromatic component (HC-LSBIS-MLE-AC)—is reviewed for its use of the HSI color model, Magic Matrix scrambling, and Huffman encoding, significantly improving security, payload capacity, and visual imperceptibility. Additionally, a hybrid technique employing 3DES with LSB embedding and MD5 key hashing is evaluated for its simplicity and effectiveness in secure communication.

Key Words: Image Steganography, Data Hiding ,Encryption ,Huffman Coding, Multi-Level Encryption (MLE) ,3DES (Triple DES) ,MD5 Hashing ,Achromatic Component (Intensity Channel) ,HSI Color Model , Steganalysis Resistance, Imperceptibility ,Hybrid Security Systems , Robustness ,CovertCommunication,Digital Forensics

1.INTRODUCTION

In a world where digital connectivity and information exchange are everywhere, protecting sensitive data is more important than ever. From government agencies and defense sectors to corporate enterprises and individuals, an enormous amount of confidential data moves across public and private networks. Sadly, many of these channels are insecure or poorly protected, making sensitive information easy to intercept, tamper with, or access without permission.

In contrast, steganography provides a different approach by focusing not on encrypting the message, but on hiding its existence entirely. The term comes from the Greek word steganos, meaning "covered" or "concealed." Steganography embeds secret information within seemingly harmless media, such as images, audio files, videos, or even text documents. Since digital images are common and have built-in redundancy, image-based steganography is the most popular method used.

The Least Significant Bit (LSB) technique is among the most basic and widely used steganographic methods. This technique works by replacing pieces of the secret message with the least important pixel values. Because changes in LSBs usually result in minimal differences in color or brightness, they are often not noticeable to the human eye, making LSB steganography a straightforward yet effective tool for covert communication.
Despite its benefits, conventional LSB steganography has several significant limitations:

- It is highly vulnerable to standard image processing tasks such as cropping, resizing, rotation, and format conversion.
- It can be detected using statistical steganalysis techniques like histogram analysis and chi-square attacks.
- It provides minimal defense against brute-force extraction if the embedding method is discovered.

Beyond cryptographic pre-processing, more robustness can be achieved through color space transformations, such as changing images from RGB to HSI or YCbCr, and applying matrix-based operations, like block-level scrambling using magic squares. These improvements not only enhance invisibility but also lessen the effects of geometric attacks and lossy image processes.

2. Importance of lsb in stenography

The importance of this research comes from its response to the changing landscape of cybersecurity threats and the rising need for covert, high-capacity, and strong data protection mechanisms. As digital information becomes essential for government, defense, healthcare, finance, and other critical sectors, traditional security models, which mainly focus on cryptography, are not enough on their own.

This research is important for several reasons:

1. Improving Security Through Hybrid Systems

By combining cryptographic techniques with LSB-based image steganography, this work suggests a **multi-layered security model that provides both data concealment and data protection. The outcome is a strong system that not only hides the message within an image but also ensures that even if the content is extracted, it remains unintelligible without the correct decryption keys.

2. Boosting Resistance to Steganalysis and Image Attacks

Traditional LSB methods face many attacks, including histogram analysis, **rotation, **resizing, and **noise insertion. The techniques covered in this research, such as **embedding in the HSI color model, **Huffman coding, and **matrix-based scrambling, enhance **resilience against image processing actions and statistical detection.

3. Working Principle

The proposed steganographic framework is based on the *Least Significant Bit (LSB) substitution method. This method changes the lowest-order bits of digital image pixels to hide encrypted information. It is preferred for its simplicity, efficiency, and invisibility, making it ideal for real-time applications. This work improves the method by adding *Huffman compression, multi-level encryption, and color model transformation, resulting in a secure and strong stego-system.

3.1 Basic Principle of LSB Substitution

In a color or grayscale digital image, each pixel value is stored in binary format. For instance, each pixel in an 8-bit grayscale image represents an 8-bit binary value between 0 and 255. Changing a pixel's *least significant bit (rightmost bit) causes minimal visual distortion:

* Original pixel: 182
* After embedding: 183

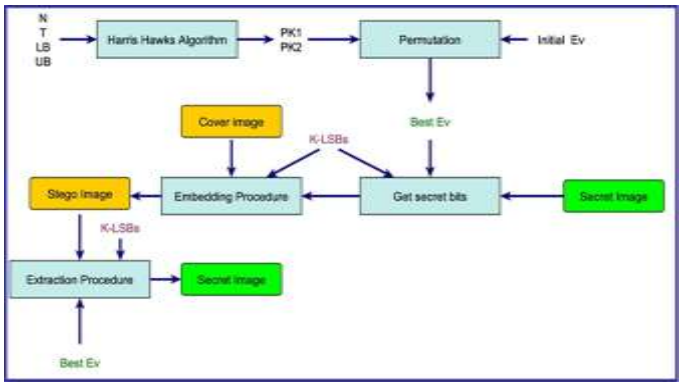
The visual difference between these two numbers is not noticeable to the human eye.

Each pixel in a 24-bit RGB image consists of three 8-bit values that represent the *Red, Green, and Blue components. This allows for up to 3 bits per pixel capacity for message embedding.

3.2 Enhanced LSB Embedding Process (Proposed Model)

The proposed model goes beyond LSB embedding. It includes pre-processing, encryption, and transformation steps to secure the message before embedding. Figure 1 illustrates the entire process.

Figure 1: Workflow of the Proposed LSB-Based Steganographic Framework



3.3 Key Operational Stages

1. Message Preprocessing
* The input message is first compressed using Huffman coding, reducing the overall size and adding an initial layer of complexity.

2. Multi-Level Encryption

* The compressed message undergoes multiple encryption layers, which may include substitution ciphers, XOR encryption, and key-based bit manipulations. This makes it tough to crack or extract, even if the stego image is captured.

3. Magic Matrix Scrambling

* The encrypted data is rearranged using a magic matrix or key-dependent block scrambling to disrupt linear patterns and improve resistance to spatial analysis.

4. HSI Color Model Conversion

* The RGB cover image transforms into the HSI (Hue, Saturation, Intensity) color space. This separates intensity from color information, allowing data to be embedded into the intensity (I) component, which reduces visual distortion and inter-channel dependencies.

5. LSB Embedding

* The scrambled, encrypted message bits are embedded into the least significant bits of the intensity component of the image. High invisibility is guaranteed by changing just one bit per pixel (or intensity value).

6. Image Reconstruction

* The modified HSI image is converted back to the *RGB color model, resulting in the final stego image. This image looks visually identical to the original but contains a secure hidden message.

7.4 Extraction Process

The extraction process reverses the embedding steps:

1. Convert the stego image to the HSI color space.
2. Extract LSBs from the intensity (I) channel.
3. Descramble the message using the shared matrix key.
4. Decrypt using the correct multi-level key sequence.
5. Apply Huffman decoding to retrieve the original message.

Having the correct keys and parameters at each stage is crucial for successful recovery. This adds an extra layer of access control and authentication.

4. Reviewed and Proposed Techniques

This section evaluates two LSB-based steganographic techniques that include cryptographic upgrades to enhance data confidentiality, image invisibility, and resistance to attacks. Both methods combine data hiding and data protection by using cryptographic algorithms, color space changes, and matrix operations to improve the strength and stealth of the stego system.

4.1 Huffman Coding + LSB with Multi-Level Encryption and Achromatic Component Embedding (HC-LSBIS-MLE-AC)

Proposed by: Shahid Rahman et al.

4.1.1 Technique Overview

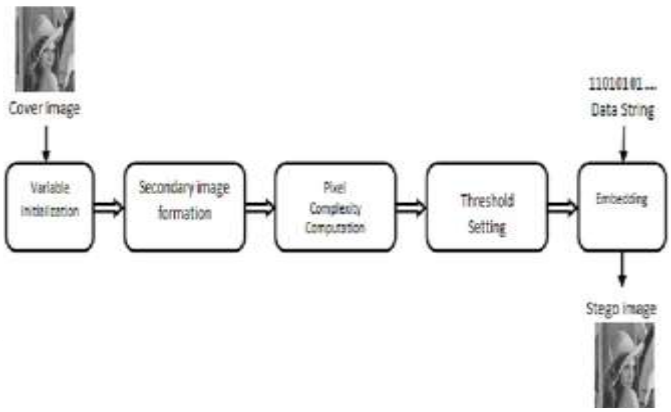
The HC-LSBIS-MLE-AC technique provides a new steganographic model that integrates:

* Huffman coding for compression and partial encryption,
* Multi-Level Encryption (MLE) for better cryptographic security,
* Least Significant Bit (LSB) embedding, and
* HSI color space transformation, focusing on data embedding in the Intensity (I) channel.

This method ensures the embedded data is not noticeable to the human eye and is resistant to statistical analysis.

4.1.2 Process Flow

Figure 1 (Below) illustrates the embedding process.



4.1.4 Strengths and Applications

* Highly secure and discreet; ideal for military, intelligence, and confidential medical communication.
* Strong resistance to statistical attacks and image analysis tools.
* By compressing images before embedding, larger messages can be hidden without losing image quality.

4.2 LSB with 3DES Encryption and MD5 Hashing (LSB-3DES-MD5)

Described by: Ilham Firman Ashari et al.

4.2.1 Technique Overview

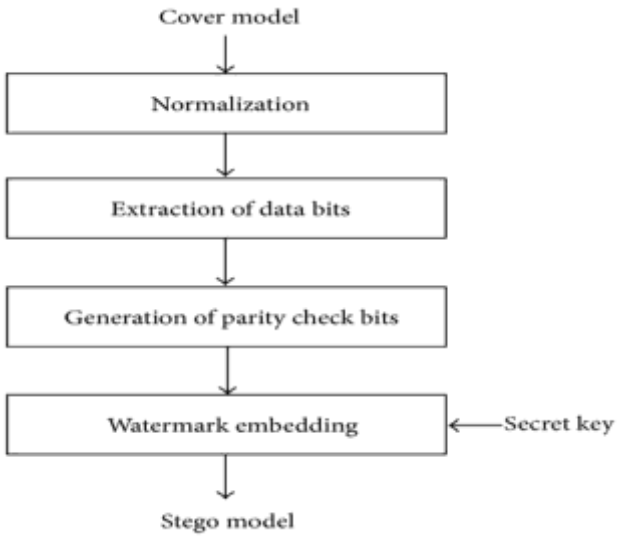
This method improves traditional LSB steganography by adding two cryptographic layers:

* To encrypt messages, use the Triple Data Encryption Standard (3DES).
* MD5 hashing for encryption key verification.

The resulting ciphertext is embedded into the LSBs of RGB image pixels, creating a secure stego image with minimal distortion.

4.2.2 System Architecture

Figure 2 below summarizes the embedding workflow.



4.2.3 Key Technical Components

* 3DES (Triple DES):

  * Uses a 168-bit key made from three 56-bit keys.
  * Supports EDE (Encrypt-Decrypt-Encrypt) and EEE (Encrypt-Encrypt-Encrypt) operation modes.
  * Provides high security through multiple encryption rounds, making brute-force decryption extremely difficult.

* MD5 Hashing:

  * MD5 is used to hash the 3DES encryption key, resulting in a 128-bit digest.
  * This hash is utilized during extraction for authentication and key verification, improving data integrity.

* LSB Embedding in RGB:

  * Encrypted message bits are embedded into the least significant bits of selected RGB pixels.
  * The method allows simple reverse extraction, assuming correct key and hash verification.

5. Background and Motivation

Today, we must transmit and store sensitive data securely in the digital world. Digital images are everywhere, high resolution, and have built-in redundancy. They are increasingly used not only for visual communication but also to carry confidential information discreetly. We often share these images through social media, websites, email, and cloud storage, many of which operate over untrusted networks where data can be intercepted and altered.

5.1 Digital Images as Steganographic Carriers

The easy availability of digital images and their large file sizes make them perfect for hiding information. Digital images, especially in uncompressed formats like BMP or lightly compressed formats like PNG, contain a lot of redundant bits that

can be changed without noticeable effects on the image quality. This allows secret data to be embedded in such a way that the modified image, known as the stego image, looks the same as the original to the human eye.

Among various steganographic methods, the Least Significant Bit (LSB) substitution method is the most commonly used because it is easy to understand and implement. This method works by changing the least significant bits of selected pixels to store parts of the secret message. In 24-bit RGB images, up to three bits per pixel, one for each color channel, can be used for data embedding without significantly distorting the image.

5.2 Limitations of Traditional LSB Techniques

Even though traditional LSB steganography is effective and hard to detect, it has several drawbacks that limit its use in real-world situations:

* Low robustness: LSB techniques are very sensitive. Any small changes to the image, such as cropping, rotating, filtering, resizing, or re-saving in a lossy format like JPEG, can corrupt the hidden data or make it unrecoverable.
* Susceptibility to steganalysis: Sophisticated statistical analysis methods can find irregularities caused by LSB changes. Tools like histogram analysis, chi-square testing, and RS steganalysis can uncover patterns that suggest hidden messages, putting secrecy at risk.

5.3 Research Motivation

The combination of steganographic and cryptographic methods creates a strong framework for secure covert communication. However, designing and optimizing these hybrid systems involves a complex balance among imperceptibility, payload capacity, robustness, and computational efficiency.

6. Comparative Analysis

A comparative evaluation of key techniques, including edge-based embedding, transform domain methods, and reversible data hiding, shows the **functional trade-offs in these systems. This section explores these limitations and explains how the proposed HC-LSBIS-MLE-AC model overcomes them by offering a well-rounded solution.

6.1 Review of Existing Steganographic Methods

6.1.1 Canny Edge Detector-Based Steganography:

Edge detection-based embedding techniques, such as those using the Canny Edge Detector, restrict data hiding to areas with high intensity variation. The idea is that changes in edge regions are less noticeable because of natural breaks in pixel values.

* Advantages: High imperceptibility, better resistance to detection by visual and statistical steganalysis due to careful pixel selection.
* Limitations: Very *low payload capacity since embedding is limited to edge pixels. This method is not suitable for large messages or complex encrypted payloads.
* Use Cases: Best for transmitting short messages in surveillance or watermarking systems where stealth matters more than capacity.

6.1.2 Huffman + AES with DWT (Discrete Wavelet Transform):

This hybrid approach uses Huffman coding for compression, **AES for encryption, and embeds the encrypted message in the **frequency domain through wavelet decomposition (DWT).

* Advantages: High level of *data confidentiality and strong resistance to compression and noise attacks because of frequency-domain embedding.
* Limitations: *Computationally intense due to AES and DWT transforms; embedding in high-frequency bands can often cause reduced robustness against geometric transformations like rotation or scaling.
* Use Cases: Suitable for forensic applications where resilience in the frequency domain and cryptographic strength are vital, but computational cost is manageable.

6.2 Superiority of the Proposed HC-LSBIS-MLE-AC Method

Compared to the methods above, the HC-LSBIS-MLE-AC (Huffman Coding–LSB–Multi-Level Encryption–Achromatic Component) method introduces a multi-dimensional optimization that addresses the key weaknesses of earlier models:

.
6.2.1. Enhanced Structural Resilience:

The Magic Matrix scrambling mechanism introduces non-linear, block-level transformations that disrupt predictable embedding patterns. This:

* Defeats statistical steganalysis,
* Prevents reverse engineering of embedding locations, and
* Ensures greater robustness against histogram and entropy-based attacks.

Moreover, using HSI transformation separates color channels, eliminating RGB interdependencies that are often exploited in stego detection.

6.2.2 Empirical Performance:

Extensive experimental validation using objective quality metrics such as:

* PSNR (Peak Signal-to-Noise Ratio),
* MSE (Mean Squared Error),
* SSIM (Structural Similarity Index), and
* NCC (Normalized Cross-Correlation),

shows that the HC-LSBIS-MLE-AC method consistently outperforms conventional techniques regarding imperceptibility and robustness, even under light compression, resizing, or noise addition.

7. Future Work

The field of steganography, especially when combined with cryptographic systems, is continually changing due to new technology and developments from adversaries. Current research shows a secure and effective method for hiding encrypted information in digital images, but there are still areas that can be improved. Future work can expand on this research by including intelligent automation, quantum-resistant cryptography, and

increased robustness to image changes. This will help ensure steganographic systems remain useful in more challenging digital settings.

7.1 Integration of Generative Adversarial Networks (GANs)

One of the most exciting developments in machine learning and security is Generative Adversarial Networks (GANs). GANs consist of two neural networks, a generator and a discriminator, that work against each other to create more realistic data. GANs can be used in steganography in several ways:

* Learn the best embedding patterns that maximize invisibility and payload capacity.
* Adjust to image characteristics in real time to minimize distortion and detectability.

7.2 Adoption of Post-Quantum Cryptography

With the rise of quantum computing, traditional cryptographic methods like RSA, AES, and 3DES may soon be outdated. Quantum algorithms, such as Shor's and Grover's algorithms, can potentially crack current encryption methods quickly, putting the security of embedded messages in stego systems at risk.

* Key encapsulation methods that are quantum-resistant yet lightweight enough for inserting images.

7.3 Enhancing Robustness Against Image Transformations

While the current method shows good strength under ideal conditions, real-world use often puts digital images through changes such as:

* Resizing or scaling, which can change pixel resolution.
* Compression, especially in lossy formats like JPEG that remove less important data.

8. Conclusion

The changing world of digital communication requires data security solutions that are strong, dependable, and also subtle. Traditional encryption methods protect data effectively, but they often reveal the presence of sensitive information, making them targets for attacks. In contrast, steganography, particularly image-based steganography using **Least Significant Bit (LSB) techniques, provides a more discreet way to hide the message itself. However, LSB on its own is very vulnerable to statistical analysis and image processing attacks, rendering it inadequate as a sole security method.

This study explored combining cryptographic techniques with LSB-based steganography to improve both data confidentiality and stego-image durability. Specifically, we evaluated two hybrid methods:

1. HC-LSBIS-MLE-AC: Huffman Coded–LSB–Multi-Level Encrypted embedding into the Intensity component of the HSI color space.
2. 3DES+LSB with MD5 hashing: A symmetric encryption-based model applied to RGB image pixels.

REFERENCES

\[1] S. Rahman, M. A. Amin, and M. A. Hossain, “Secure and robust image steganography based on Huffman coding, multi-level encryption and intensity component embedding,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 5, pp. 1650, 1660, May 2022. doi: [10.1016/j.jksuci.2020.06.014]

\[2] I. F. Ashari and D. R. Rahardjo, “Secure LSB image steganography using 3DES encryption algorithm and MD5 hash function,” in Proc. International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, Nov. 2019, pp. 106, 110. doi: [10.1109/ICIMCIS48181.2019.8985197]

\[3] S. A. Khan, A. A. Memon, and M. A. Uqaili, “A review of modern image steganographic techniques,” International Journal of Computer Applications, vol. 110, no. 1, pp. 1, 7, Jan. 2015.

\[4] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in Proceedings of IEEE International Conference on Image Processing (ICIP), Thessaloniki, Greece, Oct. 2001, vol. 3, pp. 1019, 1022. doi: [10.1109/ICIP.2001.958943]

\[5] M. Hussain and M. Hussain, “A survey of image steganography techniques,” International Journal of Advanced Science and Technology, vol. 54, pp. 113, 124, May 2013.

\[6] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32, 44, May–June 2003. doi: [10.1109/MSECP.2003.1203220]

\[7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Transactions on Signal Processing, vol. 52, no. 10, pp. 2992, 3006, Oct. 2004. doi: [10.1109/TSP.2004.833906]

\[8] C. C. Lin and W. H. Tsai, “Secret image sharing with steganography and authentication,” Journal of Systems and Software, vol. 73, no. 3, pp. 405, 414, Dec. 2004. doi: [10.1016/S0164-1212(03)00267-5]