Discover Engineering
An International Journal
OPEN ACCESS
ISSN 3117-566X
Original Research Article
Check for updates

Development of an Enhanced LSB Image Steganography Algorithm with AES-GCM Encryption for Secure Digital Data Transmission

Pankaj Nandan

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

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

Citation: Pankaj Nandan (2023). Development of an Enhanced LSB Image Steganography Algorithm with AES-GCM Encryption for Secure Digital Data Transmission. *Discover Engineering: An International Journal.* **DOI: https://doi.org/10.51470/DE.2023.4.2.06**

Received 06 August 2023 | Revised 05 September 2023 | Accepted 04 October 2023 | Available Online 02 November 2023

Abstract

The increasing exchange of confidential information through digital communication networks has intensified the need for reliable techniques that ensure data confidentiality, integrity, and concealment during transmission. Conventional cryptographic approaches protect information by transforming readable messages into unintelligible ciphertext; however, the presence of encrypted data may attract the attention of unauthorized users and potential attackers. Image steganography provides an additional layer of protection by concealing confidential information within an ordinary digital image, thereby reducing the visibility of secret communication. Nevertheless, conventional Least Significant Bit (LSB) substitution techniques are vulnerable to statistical steganalysis, predictable embedding patterns, and unauthorized information extraction, particularly when data are embedded sequentially without considering image characteristics. The present study proposes an enhanced LSB-based image steganography framework integrated with Advanced Encryption Standard–Galois/Counter Mode (AES-GCM) encryption to improve the confidentiality, integrity, and concealment of digital information. The proposed framework introduces a dual-layer security mechanism in which the plaintext message is first encrypted using AES-GCM and subsequently embedded within adaptively selected image pixels using a key-dependent pseudorandom embedding sequence. Pixel selection is guided by local image complexity, including edge intensity and neighbourhood variation, to distribute the encrypted payload across suitable image regions while minimizing visual distortion. A corresponding extraction mechanism reconstructs the encrypted payload using the shared cryptographic key and authenticated decryption. The framework is designed to be evaluated using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), embedding capacity, embedding and extraction time, and resistance to statistical steganalysis. Comparative evaluation against conventional sequential LSB and encrypted sequential LSB methods will establish the effectiveness of adaptive pixel selection and authenticated encryption. The proposed approach provides a structured foundation for developing secure image-based communication systems for confidential document exchange, private digital communication, and sensitive information transmission.

Keywords: *Image steganography; Least Significant Bit; AES-GCM; data encryption; information security; adaptive pixel selection; digital image processing; secure data transmission.*

1. Introduction

The rapid expansion of digital communication technologies has transformed the way confidential information is generated, stored, and transmitted across interconnected networks. Digital platforms are increasingly used for exchanging personal documents, institutional records, financial information, research data, authentication credentials, and other sensitive materials. Although these technologies provide considerable advantages in terms of accessibility and communication efficiency, they also create opportunities for unauthorized interception, data manipulation, information theft, and cyberattacks [1]. Consequently, protecting digital information during transmission has become an important research concern in computer science, information technology, and cybersecurity.

Conventional encryption algorithms provide an established mechanism for protecting confidential information by converting plaintext into ciphertext through mathematically defined cryptographic operations. However, encrypted information may still be recognizable as protected or encoded data, potentially attracting attention during network monitoring or unauthorized inspection. This limitation has encouraged the development of information-hiding techniques that conceal the existence of confidential communication rather than merely transforming its readable contents.

Steganography is an information-hiding technique through which confidential data are concealed within an apparently ordinary digital medium, such as an image, audio recording, video file, or text document. Unlike conventional cryptography, which focuses primarily on protecting the meaning of information,

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

steganography attempts to conceal the presence of the communication itself [2]. Digital image steganography has received considerable attention because images contain large numbers of pixels and can accommodate hidden information through controlled modifications of their numerical representations. Among the available approaches, Least Significant Bit substitution remains one of the most widely investigated spatial-domain techniques because of its straightforward implementation, relatively low computational complexity, and ability to embed information without producing immediately noticeable visual changes. In conventional LSB substitution, the least significant bit of a pixel intensity value is replaced with a corresponding bit from the secret message. Since changing the least significant bit modifies the intensity value by only one unit, the resulting visual difference is generally limited under low embedding rates [3]. Despite these advantages, conventional LSB techniques present several limitations that restrict their suitability for security-sensitive communication. Sequential embedding, in which message bits are inserted into consecutive pixel locations, may generate detectable statistical patterns in the resulting stego-image. Such modifications can be investigated through statistical steganalysis methods, including chi-square analysis, Regular-Singular (RS) analysis, and other image-distribution-based detection approaches. Furthermore, conventional LSB substitution does not inherently provide encryption or authentication. Therefore, even when information is successfully concealed within an image, the embedded message may remain vulnerable if an attacker identifies the embedding mechanism or obtains access to the concealed payload. Fixed embedding strategies may also distribute modifications across visually sensitive image regions without considering local texture, edge characteristics, or neighbourhood complexity, potentially reducing the perceptual quality of the resulting stego-image at higher payload levels.

The integration of cryptographic encryption with image steganography offers a potential solution to these limitations by separating information confidentiality from information concealment. Advanced Encryption Standard (AES) is a widely adopted symmetric-key encryption algorithm, while Galois/Counter Mode (GCM) provides authenticated encryption with associated data. AES-GCM combines confidentiality and authentication within a single cryptographic operation, allowing the receiver to verify the integrity and authenticity of the encrypted information before recovering the original message. According to the National Institute of Standards and Technology (NIST), GCM is designed to provide authenticated encryption and message authentication functionality for block ciphers. Its integration into image steganography can therefore strengthen the security of hidden information beyond the protection offered by conventional LSB embedding alone [4]. However, encryption and steganographic concealment address different security requirements and should not be treated as interchangeable mechanisms. AES-GCM protects the content of the message but does not independently prevent the detection of an image containing hidden information. Similarly, LSB embedding conceals data within an image but does not inherently guarantee message confidentiality or integrity. An effective framework should consequently combine authenticated encryption with an embedding strategy that considers image characteristics and avoids predictable pixel modification patterns. Adaptive embedding can provide a more controlled distribution of secret information by selecting pixel locations according to their local image properties. Textured and edge-rich regions may accommodate minor intensity modifications more effectively than uniform regions, although the relationship between image complexity and statistical detectability must also be evaluated experimentally [5], the present research proposes an enhanced LSB image steganography algorithm incorporating AES-GCM encryption and adaptive pixel selection for secure digital data transmission. The proposed framework initially encrypts the secret message using a cryptographic key and a unique initialization nonce. The resulting ciphertext, together with the authentication tag and necessary extraction information, is subsequently embedded into a cover image through a key-dependent pseudorandom pixel-selection mechanism. The selection process incorporates local image complexity to identify suitable embedding locations, while the pseudorandom ordering prevents the use of a simple sequential embedding pattern. A corresponding extraction procedure enables the intended recipient to recover the encrypted payload and authenticate it before decrypting the original message.

The primary contribution of this research is the development of an integrated security framework that combines authenticated encryption, adaptive image-based embedding, and key-dependent extraction within a unified algorithm. The proposed approach is intended to improve the balance between confidentiality, visual imperceptibility, embedding capacity, and computational efficiency. Rather than assuming that encryption alone makes an image steganographic system undetectable, the study considers cryptographic protection and steganographic detectability as separate evaluation dimensions. The framework is therefore designed to provide a systematic basis for comparative experimentation against conventional LSB techniques and encrypted sequential LSB approaches.

2. Related Work

2.1 Image Steganography and Information Hiding

Image steganography is an important branch of information hiding that enables confidential information to be embedded within digital images without substantially affecting their perceptual appearance. The technique generally involves three principal components: a cover image, a secret message, and a stego-image generated after the embedding process.

The cover image acts as the carrier medium, whereas the secret message represents the information intended for concealed transmission. The resulting stego-image is transmitted to the recipient, who applies the appropriate extraction procedure to recover the embedded information. Image steganography methods are broadly classified into spatial-domain, transform-domain, and adaptive or content-aware approaches. Spatial-domain methods directly modify pixel values, whereas transform-domain approaches embed information into image coefficients obtained through transformations such as the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). Spatial-domain methods are computationally efficient and relatively easy to implement, although their resistance to statistical detection and image-processing operations can be limited.

2.2 Least Significant Bit Substitution

The LSB technique operates by replacing the least significant bit of a pixel intensity value with a corresponding bit from the secret message. For an 8-bit grayscale image, each pixel is represented by an intensity value ranging from 0 to 255. Modification of the least significant bit changes the intensity by a maximum of one unit. In an RGB image, the red, green, and blue components can independently accommodate hidden information, increasing the theoretical embedding capacity. However, conventional LSB techniques generally use fixed or sequential pixel locations, which can create statistical irregularities and increase susceptibility to steganalysis. Modified and adaptive LSB methods have therefore been investigated to improve the relationship between embedding capacity and visual quality [6], for example, examined adaptive modified LSB embedding using pixel values and pixel-value differences, demonstrating the importance of image-dependent embedding strategies. These developments indicate that pixel selection and embedding allocation are important considerations in improving spatial-domain data-hiding techniques.

2.3 Cryptographic Encryption for Secure Data Embedding

Cryptographic encryption provides an additional security mechanism for protecting information before it is embedded within a digital image. AES is a symmetric-key block cipher that supports 128-bit, 192-bit, and 256-bit keys. When combined with GCM, AES provides authenticated encryption, enabling the receiver to verify whether the encrypted data have been modified or originated from a party possessing the appropriate secret key. Unlike encryption modes that provide confidentiality alone, AES-GCM also produces an authentication tag that must be verified before the decrypted information is accepted. This property is particularly important for image steganography because the embedded payload may be exposed to interception, accidental modification, or deliberate tampering. The integration of authenticated encryption can therefore provide protection even when the concealed information is extracted by an unauthorized party.

2.4 Steganalysis and Security Limitations

Steganalysis refers to the analysis of digital media to identify whether confidential information has been concealed within an apparently ordinary file. Statistical steganalysis techniques investigate changes in pixel distributions, correlations, intensity frequencies, and other image characteristics. Chi-square analysis and RS analysis are commonly used to examine the statistical properties of LSB-based stego-images. Recent research has emphasized that conventional spatial-domain embedding techniques remain susceptible to statistical detection, particularly when embedding is performed without considering image characteristics. Apau et al. (2024) systematically reviewed techniques for resisting statistical steganalysis and highlighted the importance of evaluating image-hiding methods against established detection mechanisms. [7] also reviewed image steganography approaches and detection strategies, emphasizing the continuing need to investigate the relationship between embedding techniques and steganalysis. These studies support the need for a framework in which cryptographic security and image-level concealment are evaluated independently.

2.5 Research Gap

Although encryption-based steganography has been investigated in different forms, several methodological issues remain relevant to the development of practical secure communication systems. Conventional LSB approaches frequently rely on sequential embedding, which may introduce recognizable statistical patterns. Encryption-only LSB frameworks improve the confidentiality of the hidden message but do not necessarily optimize the distribution of embedding modifications within the cover image. Similarly, adaptive pixel selection may improve perceptual quality, but it does not independently guarantee confidentiality or authentication of the embedded information. There is therefore a need for an integrated framework that combines authenticated encryption with content-aware pixel selection and reproducible key-dependent embedding positions. The proposed research addresses this requirement through an AES-GCM-based encrypted payload and an adaptive LSB embedding procedure designed to maintain synchronization between the sender and receiver.

3. Objectives of the Study

The principal objective of this research is to develop an enhanced LSB image steganography algorithm integrated with AES-GCM encryption for secure digital data transmission.

The specific objectives are:

1. To develop an AES-GCM-based encryption mechanism for protecting confidential information before image embedding.
2. To design an adaptive LSB embedding strategy that selects suitable pixel locations according to local image complexity and edge characteristics.
3. To incorporate a key-dependent pseudorandom embedding sequence to eliminate predictable sequential pixel selection.

4. To develop a synchronized extraction algorithm capable of recovering the encrypted payload and verifying its authenticity.
5. To evaluate the visual quality of the resulting stego-images using PSNR, MSE, and SSIM.
6. To investigate embedding capacity, computational efficiency, and resistance to statistical steganalysis.
7. To compare the proposed algorithm with conventional LSB and AES-GCM-encrypted sequential LSB methods.

4. Proposed Methodology

4.1 Overview of the Proposed Framework

The proposed algorithm consists of two interconnected security layers: cryptographic protection and image-based information concealment. During the embedding stage, the confidential message is first encrypted using AES-GCM. The encrypted output is then converted into a binary sequence and embedded into selected pixel channels of the cover image through an adaptive LSB substitution process. During extraction, the receiver reconstructs the same embedding sequence using the shared key and the transmitted nonce, recovers the encrypted binary payload, verifies its authentication tag, and decrypts the original message.

The overall framework includes the following stages:
1. Cover image acquisition and preprocessing.
2. Secret message preparation and AES-GCM encryption.
3. Image complexity estimation and adaptive pixel selection.
4. Key-dependent pseudorandom embedding-position generation.
5. Encrypted payload embedding using LSB substitution.
6. Stego-image generation and transmission.
7. Payload extraction and AES-GCM authentication.
8. Original message recovery.

The proposed system uses lossless image formats, particularly PNG or BMP, because lossy compression may modify pixel values and destroy the embedded LSB information. The same cover image content, cryptographic key, nonce, and embedding parameters must be available to the receiver for successful extraction.

4.2 AES-GCM-Based Message Encryption

The first stage involves converting the plaintext message into an authenticated ciphertext using AES-GCM. A 256-bit secret key is selected for the proposed implementation, while a unique 96-bit nonce is generated for each encryption operation. The nonce is not required to be secret and is transmitted alongside the encrypted payload. However, it must never be reused with the same key, as nonce reuse can seriously compromise the security of GCM. Let the original plaintext message be represented by (M), the encryption key by (K), and the nonce by (N). The AES-GCM encryption operation is expressed as:

[(C,T)=AES\text{-}GCM\text{-}Encrypt(K,N,M,A)]

Where:
- (C) represents the encrypted ciphertext.
- (T) represents the authentication tag.
- (K) represents the shared secret key.
- (N) represents the unique nonce.
- (M) represents the original plaintext.
- (A) represents optional additional authenticated data.

The ciphertext and authentication tag are combined with the nonce and a length field to construct the payload:
[P=L\parallel N\parallel C\parallel T]
Here, (L) represents the payload length, and (\parallel) denotes concatenation. The length field uses a fixed, explicitly defined encoding so that the receiver can determine the payload boundaries. The nonce, ciphertext, and authentication tag are embedded in the cover image as a single binary payload. The encryption stage ensures that even if an unauthorized individual successfully identifies and extracts the hidden information, the original plaintext cannot be recovered without the correct cryptographic key. The authentication tag further enables the receiver to reject modified or corrupted ciphertext before accepting the decrypted message.

4.3 Image Preprocessing and Pixel Representation

The cover image is represented as a three-dimensional RGB matrix:
[I(x,y,c)]
Where (x) and (y) represent the horizontal and vertical pixel coordinates, respectively, and (c) represents one of the three colour channels: red, green, or blue. Each colour-channel value is represented by an 8-bit integer ranging from 0 to 255. The embedding procedure modifies the least significant bit of selected channel values while retaining the remaining seven bits. The proposed algorithm uses lossless image input and verifies that the cover image has sufficient capacity for the complete encrypted payload. Images with insufficient embedding capacity are rejected rather than silently truncating the message.

4.4 Adaptive Pixel Selection Based on Local Image Complexity

A major component of the proposed framework is adaptive pixel selection. Instead of embedding information sequentially into every available pixel channel, the proposed method evaluates the local characteristics of the cover image and assigns embedding priority according to neighbourhood variation and edge intensity. To ensure that the receiver can reproduce the embedding positions after LSB modification, local image characteristics are calculated using the upper seven bits of the channel values. The quantized image is defined as:

[I_q(x,y,c)=\left\lfloor
\frac{I(x,y,c)}{2}\right\rfloor]

This representation removes the influence of the least significant bit, ensuring that the calculated selection characteristics remain unchanged after embedding.

The local intensity variation is estimated using a neighbourhood-based variance function:
[V(x,y)=\frac{1}{|\Omega|}
\sum_{(i,j)\in\Omega}
\left[I_q(i,j)-\mu_{\Omega}\right]^2]
Where (\Omega) represents a local neighbourhood surrounding pixel ((x,y)), (|\Omega|) represents the number of pixels within the neighbourhood, and (\mu_{\Omega}) denotes the corresponding local mean intensity.

Edge intensity is calculated using image-gradient operators:
[G(x,y)=\sqrt{G_x(x,y)^2+G_y(x,y)^2}]
Where (G_x) and (G_y) represent the horizontal and vertical gradient components, respectively.
The two characteristics are normalized and combined to generate an image-complexity score:
[S(x,y)=\alpha V_n(x,y)+\beta G_n(x,y)]
Where (V_n) and (G_n) represent normalized local variation and edge intensity, respectively, while (\alpha) and (\beta) represent weighting coefficients satisfying:
[\alpha+\beta=1]
Higher complexity scores indicate locations with greater local image variation. Such locations are assigned higher embedding priority, subject to the capacity constraints of the cover image.
For the initial experimental implementation, equal weighting may be adopted:
[\alpha=0.5,\qquad \beta=0.5]
The weighting parameters should subsequently be examined through sensitivity analysis to determine whether alternative combinations provide a better capacity–imperceptibility balance.

4.5 Key-Dependent Pseudorandom Embedding Sequence

Following adaptive pixel selection, the proposed framework generates a pseudorandom sequence of eligible pixel-channel locations. This mechanism prevents the embedding process from following a predictable sequential pattern. A cryptographic pseudorandom sequence can be generated using HMAC-SHA-256 with the shared key and nonce as inputs:
[R_i=HMAC\text{-}SHA256(K,N\parallel i)]
Where (i) represents a counter value and (R_i) represents the resulting pseudorandom output block.
The generated sequence is used to perform a deterministic, unbiased permutation of eligible embedding positions within the adaptive selection groups. The same key, nonce, cover-image content, and algorithm parameters allow the receiver to reconstruct the same ordering during extraction.
The proposed framework therefore combines two selection mechanisms:

- Content-adaptive prioritization based on local image complexity.
- Cryptographically keyed pseudorandom ordering of selected positions.

The complexity map is derived from LSB-independent pixel values, ensuring that embedding modifications do not alter the selection map needed during extraction.

4.6 LSB Embedding Procedure

After encryption and pixel selection, the encrypted payload is converted into a binary sequence:
[P={b_1,b_2,b_3,\ldots,b_n}]
Where each (b_i) represents a binary bit of the encrypted payload.
The LSB embedding operation for a selected pixel-channel value (p_i) is defined as:
[p_i'= (p_i\ &\ 254)\ |\ b_i]
Where:

- (p_i) represents the original pixel-channel value.
- (p_i') represents the modified pixel-channel value.
- (&) represents the bitwise AND operation.
- (|) represents the bitwise OR operation.
- (b_i) represents the encrypted payload bit.

The operation replaces only the least significant bit while preserving the remaining seven bits of the original channel value.
The maximum modification for an individual channel is one intensity level:
[|p_i'-p_i|\leq 1]
The embedding process continues until all bits of the encrypted payload have been embedded. The resulting image is saved in a lossless format to preserve the modified pixel values.

4.7 Payload Capacity Estimation

For an RGB image containing (W) pixels in width and (H) pixels in height, the total number of available colour-channel positions is:
[N_c=3WH]
When one LSB is used per selected channel, the theoretical maximum embedding capacity is:
[C_{\max}=3WH\text{ bits}]
However, the actual payload capacity is determined by the proportion of eligible locations selected by the adaptive embedding mechanism:
[C_a=\rho(3WH)]
Where (\rho) represents the proportion of selected channel positions.
The effective payload capacity must also account for the nonce, authentication tag, payload-length information, and other protocol metadata. Therefore, the available plaintext capacity is lower than the total number of embedded bits.
The embedding rate is calculated as:
[BPP=\frac{B_e}{WH}]
Where (B_e) represents the total number of embedded bits and (BPP) represents the embedding rate in bits per pixel.

4.8 Extraction and Decryption Process

At the receiving end, the stego-image is loaded without lossy transformation. The receiver uses the shared secret key and the transmitted nonce to regenerate the same pseudorandom embedding sequence. The local complexity map is reconstructed using the upper seven bits of the pixel-channel values, allowing the original selection pattern to be reproduced despite LSB modifications.
The receiver extracts the embedded bits from the selected pixel-channel positions and reconstructs the payload according to the predefined binary format:
[P=L\parallel N\parallel C\parallel T]

After separating the ciphertext, nonce, and authentication tag, the receiver performs AES-GCM authenticated decryption:

[M=AES\text{-}GCM\text{-}Decrypt(K,N,C,T,A)]

If the authentication tag is valid, the original plaintext is recovered. If the authentication check fails, the system rejects the payload and does not release the decrypted message. This process ensures that successful extraction alone is insufficient to recover accepted plaintext information. The authentication mechanism must also validate the integrity of the encrypted payload.

5. Proposed Algorithm

Algorithm 1: Enhanced AES-GCM-Based Adaptive LSB Embedding

Input: Cover image (I), plaintext message (M), secret key (K).
Output: Stego-image (I_s).
1. Read the input cover image and verify its dimensions and lossless format.
2. Generate a unique 96-bit nonce (N).
3. Encrypt the plaintext message using AES-GCM with key (K) and nonce (N).
4. Obtain ciphertext (C) and authentication tag (T).
5. Construct the payload using the length field, nonce, ciphertext, and tag.
6. Convert the payload into a binary sequence.
7. Generate the quantized image using the upper seven bits of each colour-channel value.
8. Calculate local neighbourhood variation and edge intensity.
9. Normalize the two image-complexity measures.
10. Calculate the combined adaptive selection score.
11. Identify eligible pixel-channel positions according to the predefined selection policy.
12. Generate a key-dependent pseudorandom permutation using HMAC-SHA-256.
13. Embed the encrypted binary sequence into the selected LSB positions.
14. Verify that the entire payload has been embedded.
15. Save the resulting stego-image in PNG or BMP format.
Return: Stego-image (I_s).

Algorithm 2: Authenticated Extraction and Message Recovery

Input: Stego-image (I_s), shared secret key (K).
Output: Original plaintext message (M), or authentication failure.
1. Read the received stego-image.
2. Reconstruct the quantized image using the upper seven bits of the pixel-channel values.
3. Recalculate the image-complexity scores.
4. Regenerate the key-dependent pseudorandom embedding sequence using (K) and the recovered nonce.
5. Extract the embedded binary sequence.
6. Read the payload-length information.
7. Separate the nonce, ciphertext, and authentication tag.
8. Perform AES-GCM authenticated decryption.
9. Verify the authentication tag.
10. If authentication succeeds, recover and display the original plaintext.
11. If authentication fails, reject the message and report an integrity-verification error.
Return: Verified plaintext or authentication failure.

6. Security Architecture and Threat Model

The proposed system is designed to address three primary security requirements: confidentiality, integrity, and concealment.

Confidentiality: AES-256-GCM encrypts the original message before it is embedded within the image. Therefore, unauthorized extraction of the ciphertext does not directly reveal the original information.

Integrity and authenticity: The authentication tag generated by AES-GCM allows the receiver to identify modifications to the encrypted payload. A modified or corrupted payload is rejected during authenticated decryption.

Concealment: Adaptive pixel selection and key-dependent pseudorandom embedding reduce dependence on predictable sequential pixel positions. The image-complexity mechanism is intended to minimize unnecessary modifications in relatively uniform image regions. The principal threat scenarios considered in the proposed study include unauthorized access to the transmitted image, attempted extraction without the secret key, modification of embedded information, statistical detection of hidden payloads, and accidental alteration of the image during transmission. It is important to distinguish resistance to unauthorized decryption from resistance to steganalysis. AES-GCM provides authenticated encryption, but it does not independently prevent an attacker from detecting that an image contains hidden information. Similarly, pseudorandom embedding positions do not guarantee resistance to advanced statistical or machine-learning-based steganalysis. These properties must be investigated separately during experimental evaluation.

7. Performance Evaluation Metrics

The proposed framework should be evaluated using established image-quality, capacity, computational, and security metrics.

7.1 Mean Squared Error

Mean Squared Error measures the average squared pixel-level difference between the cover image and the stego-image.

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

For RGB images, the calculation should additionally average over the three colour channels.
Lower MSE values indicate smaller numerical differences between the original and modified images.

7.2 Peak Signal-to-Noise Ratio

PSNR measures the reconstruction quality of the stego-image relative to the original cover image.

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

Where (MAX_I=255) for an 8-bit image.
Higher PSNR values generally indicate lower embedding distortion.

7.3 Structural Similarity Index

SSIM evaluates the similarity between the cover image and the stego-image in terms of luminance, contrast, and structural characteristics.

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

Where (\mu_x) and (\mu_y) represent mean intensity values, (\sigma_x^2) and (\sigma_y^2) represent variances, and (\sigma_{xy}) represents covariance.
SSIM values closer to 1 indicate greater structural similarity.

7.4 Embedding Capacity

Embedding capacity measures the amount of information that can be concealed within a cover image.
[EC=\frac{\text{Total embedded bits}}{\text{Total image pixels}}]
The result is expressed in bits per pixel.

7.5 Embedding and Extraction Time

Computational efficiency is evaluated by recording the time required for encryption, pixel selection, embedding, extraction, and decryption.
[T_{total}=T_{enc}+T_{select}+T_{embed}]
For extraction:
[T_{extract,total}=T_{reconstruct}+T_{extract}+T_{dec}]
The measurements should be performed under identical hardware and software conditions for all comparative methods.

7.6 Bit Error Rate

Bit Error Rate measures the proportion of incorrectly recovered bits:
[BER=\frac{N_e}{N_t]
Where (N_e) represents the number of incorrectly recovered bits and (N_t) represents the total number of transmitted bits. For an undamaged lossless transmission, the expected BER is zero.

Table 2: Comparative evaluation framework

Evaluation criterion	Method A: Conventional LSB	Method B: AES-GCM + LSB	Method C: Proposed method
Plaintext encryption	No	Yes	Yes
Authentication	No	Yes	Yes
Sequential embedding	Yes	Yes	No
Adaptive pixel selection	No	No	Yes
Key-dependent position selection	No	No	Yes
Confidentiality	Limited	AES-GCM protected	AES-GCM protected
Visual distortion evaluation	Required	Required	Required
Statistical steganalysis	Required	Required	Required

7.7 Statistical Steganalysis

The proposed method should be assessed against chi-square analysis, RS analysis, and, where feasible, modern machine-learning-based steganalysis. The detection performance should be reported using detection accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC). A suitable experimental dataset should include both cover and stego-images, with identical image sources and controlled payload rates.

8. Experimental Design and Comparative Evaluation

The experimental study should use a collection of standard RGB images with different spatial characteristics, including smooth surfaces, natural landscapes, buildings, textured objects, and complex scenes. A benchmark collection such as USC-SIPI or another appropriately documented image dataset may be considered. The images should be maintained in a lossless format throughout the experiment.
Three principal approaches should be implemented for comparison:

- **Method A:** Conventional sequential LSB embedding without encryption.
- **Method B:** AES-GCM encryption followed by conventional sequential LSB embedding.
- **Method C:** Proposed AES-GCM encryption with adaptive pixel selection and key-dependent pseudorandom embedding.

All three approaches should use equivalent plaintext payload sizes and identical cover images. The comparison should consider the additional overhead introduced by encryption metadata and the authentication tag, rather than comparing only the original plaintext length. The experiments should be conducted at multiple payload rates to examine how embedding intensity influences visual quality, capacity, and detection probability. Each method should be evaluated under identical processing conditions.

Table 1: Experimental parameters of the proposed framework

Parameter	Proposed configuration
Image format	PNG/BMP
Image representation	RGB
Pixel depth	8 bits per channel
Encryption algorithm	AES-256-GCM
Cryptographic key	256 bits
GCM nonce	96 bits
Authentication tag	128 bits
Embedding technique	Adaptive LSB substitution
Pixel selection	Local variation and edge intensity
Position randomization	HMAC-SHA-256-based permutation
Embedding depth	1 LSB per selected channel
Evaluation metrics	PSNR, MSE, SSIM, BPP, BER
Security evaluation	Chi-square, RS, and steganalysis

9. Results and Discussion

9.1 Visual Quality Assessment

The visual quality of the generated stego-images should be examined by comparing the original cover images with the corresponding images obtained after embedding. PSNR, MSE, and SSIM measurements will be used to quantify the degree of image distortion introduced by the proposed framework. The comparison between conventional sequential LSB, AES-GCM-encrypted sequential LSB, and the proposed adaptive embedding method will help determine whether content-aware pixel selection provides a measurable improvement in visual quality. Since all three methods use one-bit substitution, encryption itself should not substantially influence pixel distortion when the embedded payload length is held constant. Differences in image quality are expected to arise primarily from the distribution of modified pixel locations and the actual embedded payload bits.

9.2 Embedding Capacity Analysis

Embedding capacity represents an important factor in evaluating the practical usefulness of an image steganography technique. The proposed framework uses adaptive pixel selection, which may restrict the number of available embedding positions compared with unrestricted sequential LSB substitution. This trade-off should be investigated by measuring the maximum successfully embedded payload under different selection thresholds. The results should distinguish between total encrypted payload capacity and the original plaintext capacity because nonce and authentication-tag information introduce additional overhead.

9.3 Computational Performance

The computational performance of the proposed framework should be evaluated by measuring the time required for encryption, image analysis, embedding, extraction, and decryption. AES-GCM is expected to contribute relatively low overhead compared with the overall image-processing procedure, although actual performance will depend on message size, hardware, and implementation. Adaptive pixel selection and pseudorandom position generation introduce additional computations compared with conventional sequential LSB embedding. Therefore, the evaluation should establish whether the additional processing cost is justified by measurable improvements in visual quality and security-related performance.

9.4 Security and Steganalysis Evaluation

The security evaluation should investigate whether the proposed embedding mechanism reduces the detectability of hidden information compared with conventional sequential LSB methods. Chi-square and RS analyses should be applied to both cover and stego-images at equivalent embedding rates. Where a suitable trained steganalysis model is available, additional classification experiments should be performed to determine whether the resulting stego-images can be distinguished from ordinary images. The results should be interpreted carefully because pseudorandom embedding alone does not eliminate statistical traces created by LSB replacement. AES-GCM provides strong protection of the message content, but its contribution should be evaluated separately from the detectability of the stego-image.

Table 3: Security evaluation framework

Security parameter	Conventional LSB	AES-GCM + LSB	Proposed method
Message confidentiality	No inherent encryption	Yes	Yes
Authentication	No	Yes	Yes
Resistance to unauthorized decryption	No cryptographic protection	AES-GCM protected	AES-GCM protected
Sequential embedding patterns	Present	Present	Reduced
Chi-square detection	To be tested	To be tested	To be tested
RS analysis	To be tested	To be tested	To be tested
Machine-learning steganalysis	To be tested	To be tested	To be tested
Tampering detection	No	Yes	Yes

9.5 Reliability of Message Extraction

The reliability of the proposed system should be evaluated by transmitting stego-images through controlled communication conditions and examining whether the receiver can reconstruct the original message. Under lossless transmission, the extracted payload should match the embedded ciphertext exactly, and AES-GCM authentication should succeed. Any modification to the authenticated ciphertext or tag should result in authentication failure. The system should also be tested with incorrect cryptographic keys, incomplete payloads, and corrupted images to verify that unauthorized or unreliable extraction attempts are rejected.

10. Discussion

The proposed framework combines two distinct information-security mechanisms to improve the protection of confidential digital communication. The cryptographic component provides authenticated encryption, whereas the steganographic component conceals the encrypted information within a digital image. This separation is important because encryption and steganography address different vulnerabilities. An attacker who identifies the presence of embedded information may potentially extract the ciphertext, but the encrypted message remains protected by the AES-GCM authentication and encryption mechanism. Conversely, the adaptive embedding process attempts to reduce predictable modification patterns that are commonly associated with conventional sequential LSB substitution. The introduction of local image-complexity analysis represents an important methodological component of the proposed approach. Pixel regions containing greater intensity variation or edge information may provide greater perceptual tolerance for small intensity modifications than uniform image regions.

Nevertheless, the suitability of such regions should not be assumed to guarantee statistical undetectability. In fact, indiscriminate concentration of modifications in highly textured areas may create detectable distribution patterns [6-7]. Consequently, the weighting coefficients, selection threshold, embedding rate, and position-randomization mechanism should be optimized and examined through controlled experiments. Another important consideration is the synchronization of the embedding and extraction procedures. Adaptive image analysis can create difficulties if the receiver calculates pixel-selection scores from the modified image and obtains a different ordering from the sender. The proposed use of upper-seven-bit quantization addresses this issue by ensuring that the local complexity calculations remain independent of the modified least significant bits. This provides a reproducible embedding map when the image is transmitted without lossy transformations. The framework also introduces additional computational requirements because it involves cryptographic processing, image-gradient calculation, neighbourhood-based statistical analysis, and pseudorandom position generation. Although these operations increase processing complexity compared with basic LSB embedding, they provide additional functionality that conventional approaches do not inherently offer. The overall suitability of the proposed system should therefore be determined through experimental comparison rather than through theoretical assumptions alone.

11. Limitations and Future Research Directions

The proposed algorithm has certain limitations that should be considered during implementation and evaluation. First, LSB-based embedding is inherently sensitive to lossy image compression, resizing, filtering, and other pixel-modifying transformations. Consequently, the initial implementation is intended for lossless image transmission rather than communication systems that automatically recompress uploaded images. Second, adaptive pixel selection may reduce the number of available embedding locations, particularly in images containing large uniform regions [8]. Third, the use of a shared cryptographic key requires an appropriate key-distribution and management mechanism. Fourth, the framework does not claim immunity against advanced steganalysis, because statistical and machine-learning-based detection techniques may still identify modifications introduced by spatial-domain embedding.

12. Conclusion

The present study proposes an enhanced image steganography framework that integrates AES-GCM authenticated encryption with adaptive Least Significant Bit embedding for secure digital data transmission. The proposed method is designed to address important limitations of conventional LSB approaches by introducing cryptographic protection, image-complexity-based pixel selection, and key-dependent pseudorandom embedding positions.

The encryption mechanism protects the confidentiality and integrity of the hidden information, while adaptive embedding is intended to minimize unnecessary image modifications and reduce dependence on predictable sequential pixel selection. A synchronized extraction procedure enables the receiver to reconstruct the embedded payload and authenticate the ciphertext before recovering the original message. The proposed framework establishes a systematic approach for evaluating the relationship between cryptographic protection, image imperceptibility, embedding capacity, computational efficiency, and statistical detectability. The comparative experimental design provides a basis for determining whether adaptive LSB embedding offers measurable advantages over conventional and encryption-based sequential embedding methods. The actual effectiveness of the algorithm must be established through implementation, benchmark testing, and statistical steganalysis rather than assumed from its design. Overall, the integration of authenticated encryption and adaptive image-based information hiding represents a promising direction for developing secure and efficient digital communication systems.

References

1. Dworkin, M. (2007). *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication 800-38D. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38D
2. Chefranov, A. G., & Öz, G. (2022). Adaptive to pixel value and pixel value difference irreversible spatial data hiding method using modified LSB for grayscale images. *Journal of Information Security and Applications, 70*, 103314. https://doi.org/10.1016/j.jisa.2022.103314
3. Apau, R., Asante, M., Twum, F., Hayfron-Acquah, J. B., & Peasah, K. O. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PLOS ONE, 19*(9), e0308807. 1. https://doi.org/10.1371/journal.pone.0308807
4. Kombrink, M. H., Geradts, Z. J. M. H., & Worring, M. (2025). Image steganography approaches and their detection strategies: A survey. *ACM Computing Surveys, 57*(2), Article 33. https://doi.org/10.1145/3694965
5. Ghadi, Y. Y. (2023). Enhanced payload volume in the least significant bits image steganography using hash function. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.1606
6. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information Hiding: Steganography and Watermarking—Attacks and Countermeasures*. Kluwer Academic Publishers.
7. Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press.
8. Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.). (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House.