Scientific Reports

https://doi.org/10.1038/s41598-025-28140-0

Article in Press

An improved hybrid image steganography method using AES algorithm

Received: 7 January 2025

Accepted: 7 November 2025

Published online: 08 December 2025

Cite this article as: Banoori S.Z., Khan W., Rahman S. *et al.* An improved hybrid image steganography method using AES algorithm. *Sci Rep* (2025). https://doi.org/10.1038/s41598-025-28140-0

Syeda Zahra Banoori, Wajidullah Khan, Shahid Rahman, Fahad Masood, Abdu Salam, Farhan Amin, Isabel Torre, Mónica Gracia Villar, Helena Garay & Gyu Sang Choi

We are providing an unedited version of this manuscript to give early access to its findings. Before final publication, the manuscript will undergo further editing. Please note there may be errors present which affect the content, and all legal disclaimers apply.

If this paper is publishing under a Transparent Peer Review model then Peer Review reports will publish with the final article.

scientific reports

An Improved Hybrid Image Steganography Method Using AES Algorithm

Syeda Zahra Banoori[1], Wajidullah Khan[1], Shahid Rahman[2], Fahad Masood[1], Abdu Salam[3], Farhan Amin[4,*], Isabel de la Torre[5,*], Mónica Gracia Villar[6] and Helena Garay[6] and Gyu Sang Choi[4]

[1]Department of Computer Science, Abasyn University Peshawar, Pakistan
[2]Department of Computer Science, University of Buner, Buner, Pakistan
[3]Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan
[4] School of Computer Science and Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea
[5]Department of Signal Theory and Communications, University of Valladolid, Valladolid, Spain
[6]Universidad Europea del Atlántico, Santander, Spain
* farhanamin10@hotmail.com (F.A); isator@uva.es (I.T)

Abstract

Image Steganography is the process of hiding information, which can be text, image, or video inside a cover image. Recent steganography literature hasn't addressed the problem of loss of secret information during extraction and reliability. Hence, to reduce information loss and provide reliability between in the basic criteria, Herein, we proposed a hybrid method that utilizes the Least Significant Bit (LSB) substitution, transppsition, magic matrix , key and Advance Encrytion Standard (AES) algorithm. The LSB method decreases embedding errors by implementing a new value difference algorithm. In addition, to improves the reliability between the basic criterion for image steganography we used transposition, magic matrix, key and AES. The proposed method ensures a high-quality image format in the RGB color model to conceal the hidden message within the cover image which is jpeg. The proposed hybrid method performed several experiments and these are mainly based on Quality Assessment Metrics (QAM) such as PSNR, SSIM, RMSE, NCC, etc which showed better results. The proposed method also analyzed with different perspectives in terms of different dimensions of images and different sizes of message text which showed better results. In addition, the performance of the proposed method showed better results based on (Regular and Singular) steganalysis, noise, and cropping attacks. The security analyses such as key space, differential, and statistical attacks show that the proposed scheme is secure and robust against channel noise and JPEG compression.

Keywords: Image Steganography, Image quality assessment metrics, Histogram analysis, Image, LSB, AES, Cryptography, Image steganography

Introduction

With the rapid growth in modern technology, millions or even billions of data are transferred over the internet within seconds. From this aspect, ensuring data protection from unauthorized access becomes a crucial issue. Different techniques are used to tackle these issues, and each has their own pros and cons but Steganography plays a vital role in secure communication, which means "secret writing" or "covered writing". It is the art and modern science of hiding sensitive information from unauthorized and third parties that no naked eye can detect. The steganography seeks to conceal data that no naked eye can suspect, the information that needs to be kept hidden is embedded in a carrier, such as an image, audio file, video, or text, to establish covert communication. Both cryptography and steganography terms are closely related, but they serve different purposes. During the literature review, we found that cryptography, watermarking, and steganography techniques are used to secure data transmission. However, the balance between the basic criteria used for image steganography is essential. Up to now many methods developed to tackle secure communication between end users. So, some are try to cover security and some struggle to get capacity or another criteria, but for image steganography it is essential to developed a reliable method in term of basic criteria which are robustness, captaincy, temper protection, transparency etc. [1].So, image steganography play a vital role and we proposed hybrid method that give the reliability between the criterion of steganography. In addition, also used Cryptography which shuffles messages to prevent deciphering, while steganography conceals the communication so that it remains undetected [2-6]. Before going to further discussion let explain some existing concepts which vital for the proposed method that make clear statement. So, in the spatial domain, the researcher's primary focus is to cover the image. This cannot have detected by the naked eye even if information is embedded in the image. In the spatial domain, bits from the original image's pixels are dispersed. The LSB (Least Significant Bit) is one of the popular strategies used in the spatial domain [7]. This technique involves embedding a hidden message by manipulating the least significant bit (LSB) of each pixel in the cover image. Each pixel has 8 bits and is assigned a binary value [11-12]. The most significant bit (MSB) determines the shape of the object in the image. If the MSB is altered significantly, the resulting image will differ greatly from the original. The LSB modification does not alter the shape of the object in a notable way up to 4 LSB [8]. Recently, the data transmission on the internet is a challenging task for both the sender and the receiver. Therefore, in steganography, the calculation of the image is very important for embedding a secret message into the image to meet the criteria of steganography. Because the resulting image must resist different attacks. However, reliability in Image steganography, the format of the image, and the dimension of the image remain a challenging task. Because the complexity of the Image (different dimensions, formats, etc.) can't give us a way to make the reliability in information security. That's why the proposed method used AES, key, magic matric, LSB, and some transposition comments are used to address secure communication issues up to some acceptable limits. However, several methods such as adaptive are [12], modified lsb modification technique [13], hybrid is method [14], hybrid using lsb [15], text security [16], chaos-based cryptography [19], Ransomware Hiding Model [28], Hybrid data security [29], and Hybrid EMI Edge [32] proposed but have differernt issues; for instance; balanced and tradeoffs, etc. These techniques are superior to LSB but do not satisfy the essential measures of steganography; limit/payload, robustness, perceptional frankness, temper insurance, calculation, etc. In addition, these techniques have high payloads and separate different models and some have accomplished two boundaries but not get the others. Our research aims to develop and design a very effective and efficient data hiding method using the steganography technique with encryption algorithms to ensure confidentiality and integrity and to increase the security of the stego image by a method that does not show any difference in the image using visual attack tools. Also, the proposed method is designed to generate a stego image with the lowest quality changes to avoid any visual attacks that can lead to a hidden message. The proposed method also has an encryption solution using AES to the hidden message to protect the content of the secret message. This research mainly addresses the problem of detecting an attacker's alteration of a concealed confidential message. It also addresses the issue of improving the unauthorized individual's steganography of a personal protection technique by attaching an unauthorized individual to verify integrity. Our proposed steganography method fulfills the need for security and covers these issues by combining AES, Magic matrix, transposition, MLEA, and LSB. Its purpose is to defeat steganography as well as to assess and enhance the security of steganographic systems using some concepts such as MLEA, AES cryptography, MM, Different perspectives, and steganalysis, etc [13].

The key contributions of our research are given below.

- This research proposes a method that combines steganography and encryption algorithms to ensure the confidentiality and integrity of the transmitted data. It works systematically by enabling the embedding procedure to enhance the security level.
- We propose an improved hybrid image steganography method using the AES algorithm supporting different operations such as magic matrix, and transposition for securing data or information.
- To ensure the security and quality of the stego image, we combined AES encrypts for sensitive data, and XOR operation before embedding the carrier image pixels.

- To show the efficiency of the proposed method, we compared our method with some of the state-of-the-art methods and also analyzed different perspectives in terms of different dimensions of RGB images, different sizes of secret messages, etc.
- We performed critical analysis using QAM'and RS, Histogram, and PDH of the proposed method which indicates better results.

The paper is organized into several sections. Section 2 provides an overview and critical analysis of related works. Section 3 presents the proposed work, which includes the use of the LSB, AES algorithm, Magic Matrix, Embedding Algorithm, and Extraction Algorithm. Experimental results and image quality assessment measurements are presented in Section 4, while Section 5 analyzes security performance. Finally, Section 6 concludes the paper conclusion and future work.

Literature Review

Due to the rapid use and researcher attention, people used image Steganographic techniques to hide messages for secure communication. For instance, in ancient Greece, messengers used to tattoo messages into their shaved heads and let their hair grow out to cover them. Similarly, during World War II, invisible ink was used to write information on seemingly blank paper. The paper had to be heated to reveal the message, and the ink would turn visible. Fruit juices, milk, and vinegar were used to make the ink, as they all turned dark when heated, making the message visible to the human eye [14]. Recently, different cover objects have been used to embed secret messages, such as images, audio, video, etc. Still, the concept and uses of digital images and their formats, types, and channels get attention for steganography. Because RGB images can be stored with 24 depth per pixel of 8 bits for each RGB color channel. A 24-bit image provides more space for hiding information using the Least Significant Bit (LSB) shown in Figure 1. So, LSB steganography is a type of image steganography that involves concealing messages inside an image by replacing the message's secret bits with the LSB of each pixel shown in Figure 1.

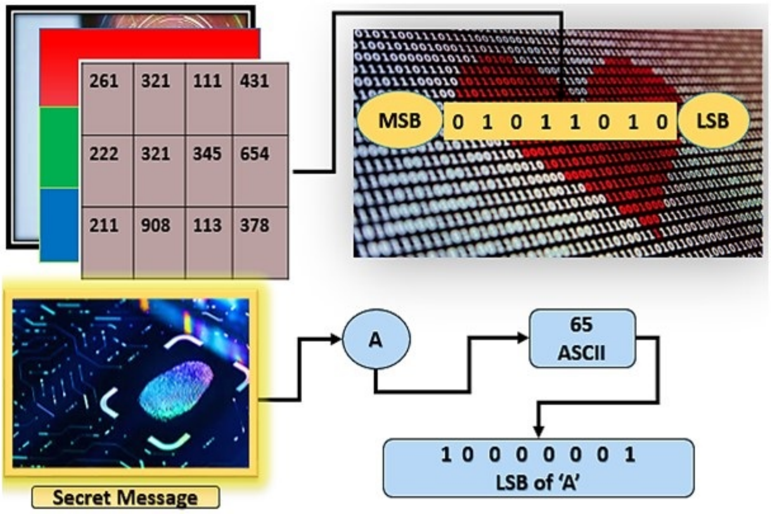


Figure 1: The Least Significant Bits operation

However, LSB steganography is the most common technique for hiding data by converting the message's values to decimal and then binary using the ASCII table. Once the pixel values are converted to binary, we replace every least significant bit in a sequence with the message bits [15]. We just used the reverse operation to extract the secret message. However, the LSB encoding is highly vulnerable to filtration or alteration of the stego image, one of its major drawbacks [16-18]. Any attack on the stego-image is likely to destroy the message. That's why we used the AES algorithm to tackle this issue. Before analyzing previous work, it is necessary to elaborate on some basic parameters used for any steganographic method. When developing any steganography method, it is important to consider objectives such as security, payload, robustness, imperceptibility, tamper protection, calculation complexity, and perceptual transparency. So, Payload refers to the concealed capacity of the hidden message inside the image, which is calculated in bits per pixel (bpp) [19-22]. It is important to ensure that the stego and cover images match transparency or visual quality, with no distortion or noise allowed. Perception requires identical cover and stego images, with no visible differences to the naked eye [23,24]. Considering these objectives is crucial to develop an effective and secure steganography method [25,26]. Temper Protection: It is difficult to modify the secret message in an implanted object after it has been protected. Calculation Complexity: How expensive is it computationally to embed & extract a covered message? [27]. Toughness: This describes the ability of the implanting and decrypting system to function, although the stego-image is deformed by a third party utilizing image processing techniques such as rotation, scaling, resizing, etc. Imperceptibility: Since concealing the hidden data in the digital image in a manner that retard it from being understood by the human eye is the primary characteristic and power of any Steganographic system or statistical algorithms, imperceptibility is the most top priority criterion for any data implanting [28-30]. Security: Security in a Steganographic system refers, in an oblique sense, to "un-noticeability" or "un-detectability “. As a result, any steganography method is considered safe if the concealed information cannot be found using statistical methods [31-34]. Below, Tables 1 and 2 below present a critical analysis of previous techniques developed for image steganography.

Table 1: Analysis of the state of art methods using Data utilization, and image format

Methods	**Data**	**Image Format**
Depending on the secret code in this paper, concealed information is placed in various positions of the image's LSB [13]	RGB Image as cover object and secret message (image).	RGB
The RC4 technique was employed to achieve randomization in hiding message image bits into cover picture pixels instead of storing message image bits sequentially [14].	Grayscale Image as cover object and secret message (image).	Grayscale
To boost security, a Hue Saturation Intensity HSI color model employs an image's achromatic portion (I-plane) for embedding, which reduces the additional computational overhead [15].	Dimensional variation Images of 128x128,256x256,512x512, and 1024x1024 are utilized for secret message embedding.	Tiff
Triple XOR operation is implemented on the cover image's bits and the text message's bits [16].	Bitmap images of different dimensions are used to insert hidden messages.	Bitmap
Pseudo Random Number Generator used to produce random bit positions from the image's 7 most significant bits for every R, G, and B value [17].	Using Pseudo Random Number Generator and XOR operation. The paper focuses on security.	RGB
One-time pad (OTP) symmetric encryption algorithm used with a double XOR operation [18].	The paper targets security with a payload of up to 131072 bytes obtained for the cover image's 1024x1024 size.	Grayscale Image
A multi-level encryption algorithm and a blue channel are used in the RGB color model, which is less visible to the HVS (Human Visual System) [19].	Different dimensions of images, i.e., 128x128,256x256,512x512, and 1024x1024, are used for hidden message insertion.	Tiff

Methods	Data	Image Format
Four modules, i.e., encryption, encoding, decoding, and decryption proposed [20].	The AES algorithm is used for Encryption, and the encoding module takes the cipher text and input image using the LSB steganography method.	Jpg
A hybrid information security system uses discrete wavelength transform, advanced encryption standards, and LSB steganography. [21]	Compressing the hidden image utilizing the DWT algorithm, inscribing it with AES algorithms, and employing the LSB method to conceal hidden image data in the cover image.	Jpg
The author used a multi-level encryption algorithm, and for embedding purposes, a Blue channel is used in the RGB color model, which is less visible to the HVS (Human Visual System) [22].	Various sizes of a certain hidden message are present in various images, i.e., grey, RGB, texture, and aerial images.	Tiff
The author used the AES algorithm for encryption & for hiding data, a filtering-based algorithm that employs MSB bits for filtering [23].	The paper concentrates on the security of up to 4000 characters for a 512x512 cover image size.	Bitmap, jpg, png
The author used the Advance ES algorithm for encryption and filtering the image to decide the candidate pixel for data protection using LSB image steganography [24].	The paper's main focus is to strengthen the steganography process.	JPG

Table 2: Critical Analysis of previous methods used for steganography using basic parameters of image steganography

Approaches	Pros	Cons	Capacity	Security	Transparency	Temper Protection	Computation
Image steganography combination of the method and the secret key [13].	High Secure Payload	Time Taking	Yes	Yes	Yes	Yes	No
Image steganography using RC4 algorithm [14].	Excellent security and stego image quality	Time Taking	Yes	Yes	Yes	Yes	No
Using Multilevel Encryption Algorithm and HSI Color Model [15].	Enhancing security and safety	Payload & time taking	No	Yes	Yes	Yes	No
A combination of the LSB method and XOR operations is used	Imperceptible and robust	Time-Consuming	Yes	Yes	Yes	Yes	No

Approaches	Pros	Cons	Capacity	Security	Transparency	Temper Protection	Computation
[16].							
Using Random Number Generator and XOR operation [17].	Provide robustness and security	Time-Consuming	Yes	Yes	Yes	Yes	No
Image steganography using a one-time pad(OTP) symmetric encryption algorithm & double XOR operation [18].	Increasing safety and security	Low payload limit	No	Yes	Yes	Yes	No
Using Multilevel Encryption Algorithm, Magic matrix, and RGB color Model [19].	Payload and quality images	not able to resist all types of assaults	Yes	Yes	Yes	Yes	No
It uses four modules: encryption, encoding, decryption, and decoding [20].	Enhancing Safety and Security.	Time Taking	Yes	Yes	Yes	Yes	No
Using the DWT algorithm with the AES algorithm [21].	High security as well as capacity	Low-quality image	Yes	Yes	Yes	Yes	No
Using Multilevel Encryption Algorithms and Magic Matrix [22].	Enhanced security and higher embedding rate	Time Taking	Yes	Yes	Yes	Yes	No
Using AES Algorithm and filtering-based algorithm [23].	Enhancing Safety and Security.	Time-Consuming	Yes	Yes	Yes	Yes	No
Image Steganography using selected pixels for embedding & AES algorithm for encryption [24].	High Security & Safety	Low payload limit	No	Yes	Yes	Yes	No

To sum up this section first we explored the basic idea of LSB, RGB, and its importance in this research field. After that, we elaborate on the basic criterion (payload, robustness, temper, computation, perception) of image steganography for reliability. These parameters are used in Tables 1 and 2 for critical analysis of some existing methods. Therefore, Tables 1 and 2 elaborate on the advantages and disadvantages of various image steganography techniques, including their uses, cover objects, and embedding procedures, and also analyze the basic criteria of steganography achieved. The key issue in image steganography is that the cover object is visible for some time, making it crucial to maintain reliability between the fundamental parameters to ensure security. It is important to consider factors such as message size, image dimensions, cover object selection, image type, embedding techniques, and procedures to ensure successful steganography. Our proposed method aims to establish a dependable mechanism to meet the security requirements up to an acceptable standard which is discussed in the next section in detail.

Proposed Methodology

In this section, first, we briefly defined various mathematical notations and other concept terms used for proposed method. Finally, we explain the essential steps of embedding and extraction of proposed method concisely. The AES embedding algorithm used just after the stego image generated. first, we take a cover image and apply transposition function then divided into three channels and blue channels is further divided into four equals blocks. After that shuffled the bits of Blue chancel using magic matrix and apply xor. After that w rearranged the shuffled block and combine three channels once the stego image generated then AES algorithm performed. Equations 1 to 6 are used for the proposed method embedding parameters such as Ci denote cover image, Ti transpose image, Re, Gr, Bl respectively Red, Green, and Blue channel of the RGB image. While Mdv1 represents message bits, Mg Message, and Si show Stego image. So, extraction process is the reverse process of the embedding procedure and these parameters are set in equations 7 to 12.

Figure 2 elaborates the whole procedure of the proposed method. Firstly, taking secret data and cover images for embedding the data using LSB. Once the coded image was generated then we applied the AES and key to get the encrypted stego image. For in decrypted side first, we take the resulting stego encrypted image and apply AES and key to generate a decrypted stego image after that applying LSB the secret data extracted. Figure 2 elaborates the whole proposed method. It explains the steps handling from cover image to stego image and AES. Similarly, Figure 3 explains the LSB procedure from cover image to stego image before AES operation means the process is just ready to apply AES operation. Figure 4 shows the graphical representation Lsb data embedding. It is the transformed version of Figure 3. Figure 5 presents the whole AES encrypted and decrypted operations. Finally, Figure 6 elaborated on the way of encrypted bits such as the Transformation of Sub bytes, (b) Transformation of Shift Rows, (c) Transformation of Mix Column, (d)Transformation of Add Round Key.

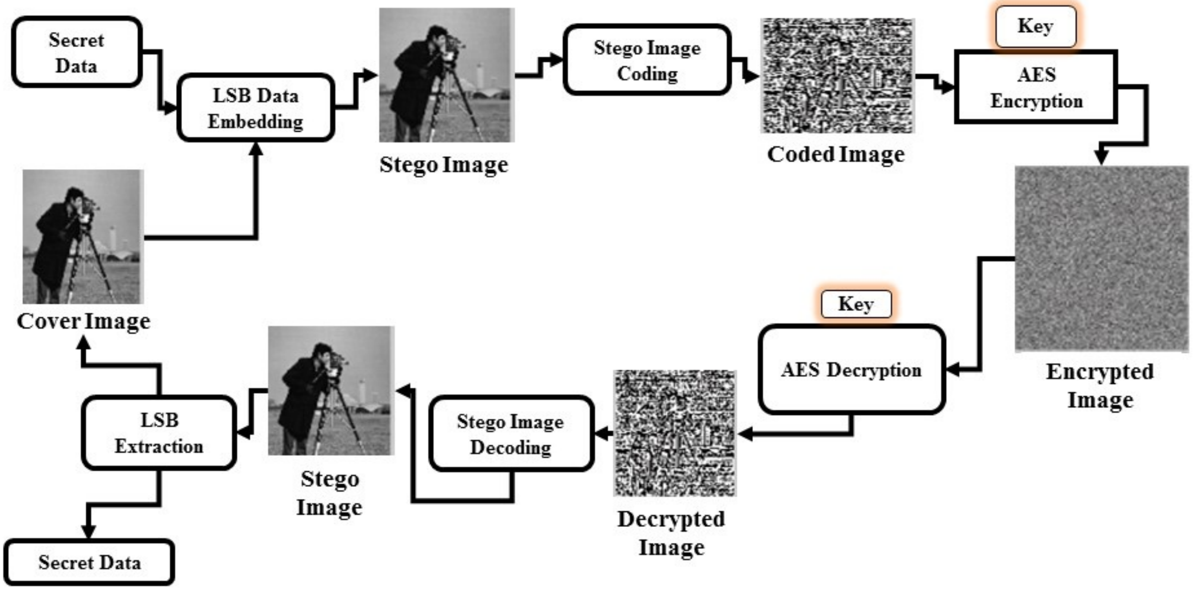


Figure 2: Proposed Methodology

Mathematical Foundation for LSB Data Embedding and Extraction

The hidden message is represented by Mg in the cover image (Ci). Ti shows the transposed Image. Re denotes the red, Gr the green, and Bl the blue channels, whereas Si denotes the encrypted image. Six functions named ε, π, ω, μ, η, and υ are used in the proposed method as a part of embedding in Equations (1)-(6) as stated.

$$Ti = \varepsilon(Ci) \tag{1}$$

$$Re,Gr,Bl = \pi(Ti) \tag{2}$$

$$Mdv1 = \omega(Mg) \tag{3}$$

$$Mdv1' = \mu(Mdv1) \tag{4}$$

$$Bl' = \eta(Bl) \tag{5}$$

$$Si = \upsilon(Mdv1', Bl') \tag{6}$$

The 1st function (ε) takes i as input & gets back (Ti) which is the transposed image. 2nd function (π) splits Ti into three channels that are red, green, and blue, where (Bl) is utilized for inserting the secret message. For providing more security XOR operation is applied on encrypted bits, which return (Mdv'). Before inserting the secret message into blue channel (Bl) it is shuffled utilizing magic matrix (Matlab function), then utilizing the 5th function (η) which provides (Bl') mean shuffled image of blue channel. Lastly, the stego image (Si) is generated utilizing the 6th function (υ) by inserting secret message bits (M dv') in the shuffled blue channel (Bl') utilizing LSB after that once the stego image generated then performed AES algorithm. On the receiver side, the reverse operation has to be applied to extract the original message. The original message can be extracted by utilizing the following six procedures in equations (7), (8), (9), (10), (11), and (12), as described below.

$$Ti = \varepsilon^{-1}(Si) \tag{7}$$

$$Re,Gr,Bl = \pi^{-1}(Ti) \tag{8}$$

$$Bl' = \omega^{-1}(Bl) \tag{9}$$

$$Mdv1' = \mu^{-1}(B') \tag{10}$$

$$Mdv1 = \eta^{-1}(Mdv1') \tag{11}$$

$$Mg = \upsilon^{-1}(M^{dv}) \tag{12}$$

In extraction side, we first apply the AES extraction procedure, then we apply LSB-based extraction on stego image. In the extraction process, function (ε^{-1}) put on to the encrypted image (Si) & returns a transposed image (Ti). Equation (8) divides (Ti) into three channels of RGB. function (ω^{-1}), will give the shuffled blue channel (Bl) randomized to produce the blue channel. after that applying XOR operation (M dv') and extracted the secret message from (Bl') by utilizing equation (10). To obtain the plaintext (Mdv), function (η^{-1}) is utilized. Lastly, the original message (Mg) is attained by utilizing equation (12).

Figure 3,4 and 5 … and apply the transport functior … nnels. The blue channel is furthe … x function. So after that the se … blue channel sub-blocks. Once … algorithm, the whole procedure

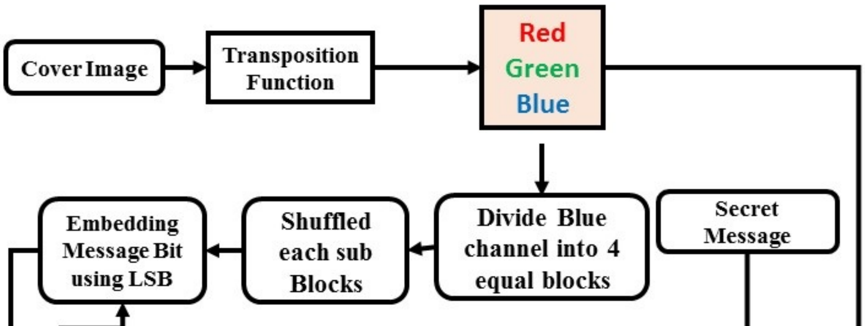


Figure 3: LSB Data Embedding

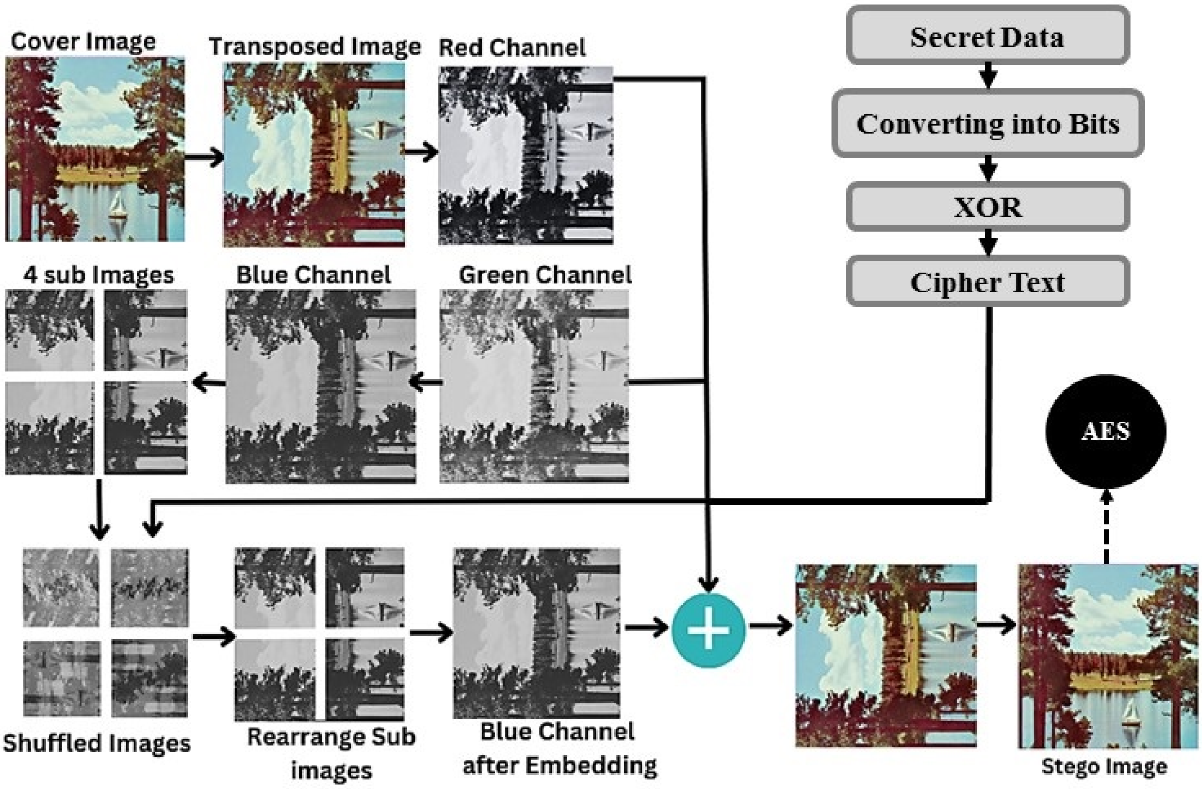


Figure 4: Graphical Representation LSB Data embedding

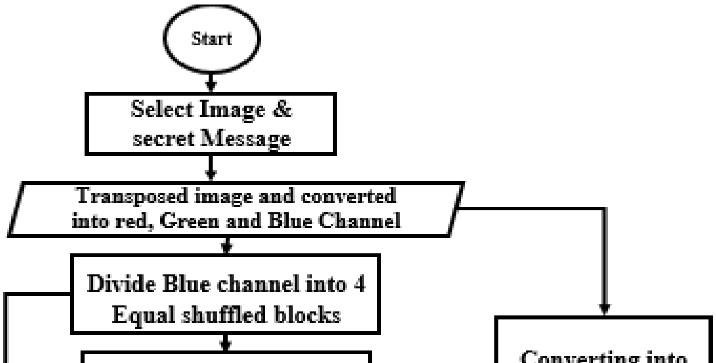

Start
Select Image & secret Message
Transposed image and converted into red, Green and Blue Channel
Divide Blue channel into 4 Equal shuffled blocks
Converting into

Figure 5: Flow Diagram of Embedding

Shuffling by magic matrix (MM)

An MM is a Matlab function called "magic matrix" that produces a matrix of a specified size with the characteristic that there are no duplicate numbers in the magic matrix. It is a magic matrix that the numbers cannot be larger than the sum of its rows and columns or diagonally. The results are the same by adding rows, columns, and diagonally. Considering the traits above, the pixels of a cover image can be easily rearranged in the right sequence after we shuffle them. A simple precedent is used to explain this rearranging method further. Imagine a 3x3 inch cover image (Ic), i.e., Ic= {95,25,10,36,21,48,88,33,62} to reposition. For this reason, we must create an enchantment framework (Mm) that is equivalent to the cover image dimensions and set (Is) as the repositioned image [34],[35].

$$Ic = \begin{matrix} 95 & 25 & 10 \\ 36 & 21 & 48 \\ 88 & 33 & 62 \end{matrix} \qquad Mm = \begin{matrix} 6 & 1 & 5 \\ 9 & 2 & 3 \\ 8 & 7 & 4 \end{matrix} \qquad Is = \begin{matrix} 48 & 95 & 21 \\ 62 & 25 & 10 \\ 33 & 88 & 36 \end{matrix}$$

The enchantment framework shows us where moving values of pixels, i.e., the first-pixel value 95 shifted to the 1 of mm (col 2, ro1), the second, 25 to (col 2, row 2), the third, 10 to (column 3, row 2), the fourth, 36 to (column 3, row 3), the fifth, 65 to (column 2, row 2), and so on. The MM Matlab function used in the proposed method on blue channel for shuffling the bits to gets more security and resistance to attackers.

Advanced Encryption Standard (AES)

AES is a symmetric encryption method and is considered an industry standard for keeping confidential data used in proposed method and applied once the stego image generated after LSB process. So, AES offers three different key sizes: a 128-bit key is used for 10 rounds, a 192-bit key is required for 12 rounds, and a 256-bit key is used for 14 rounds. The method resists various cryptographic attacks due to its use of multiple rounds of substitution, permutation, and mixing operations [36], [37]. Below are the main steps in the AES encryption process, as shown in Figures 6-7(A).

Step 1: Key Expansion: Each round of the method uses a different set of round keys created by expanding the original encryption key.

Step 2. Initial Key: The input data blocks, typically 128 bits each, are created. In the first round, each block byte and the matching byte of the round key are concatenated using a bitwise XOR operation.

Step 3. Rounds: The key size affects the number of rounds AES uses, which is fixed. During each round, the data block is subjected to many modifications. These changes to the bytes' structure include substitution, permutation, and mixing.

Step 4. Final Round: The mixing operation is absent from the final round, comparable to the earlier rounds. This ensures that the encryption procedure can be uncompleted.

The Advanced Encryption Standard (AES) is a highly secure encryption algorithm thoroughly researched by cryptographers globally. It resists known attacks when correctly implemented with a sufficiently long and random key. AES is widely used to protect network communication, data storage, cryptographic systems, and various applications and protocols. Figure 5 and Figure 6 elaborate both LSB and AES process used for embedded message bits in the proposed method.

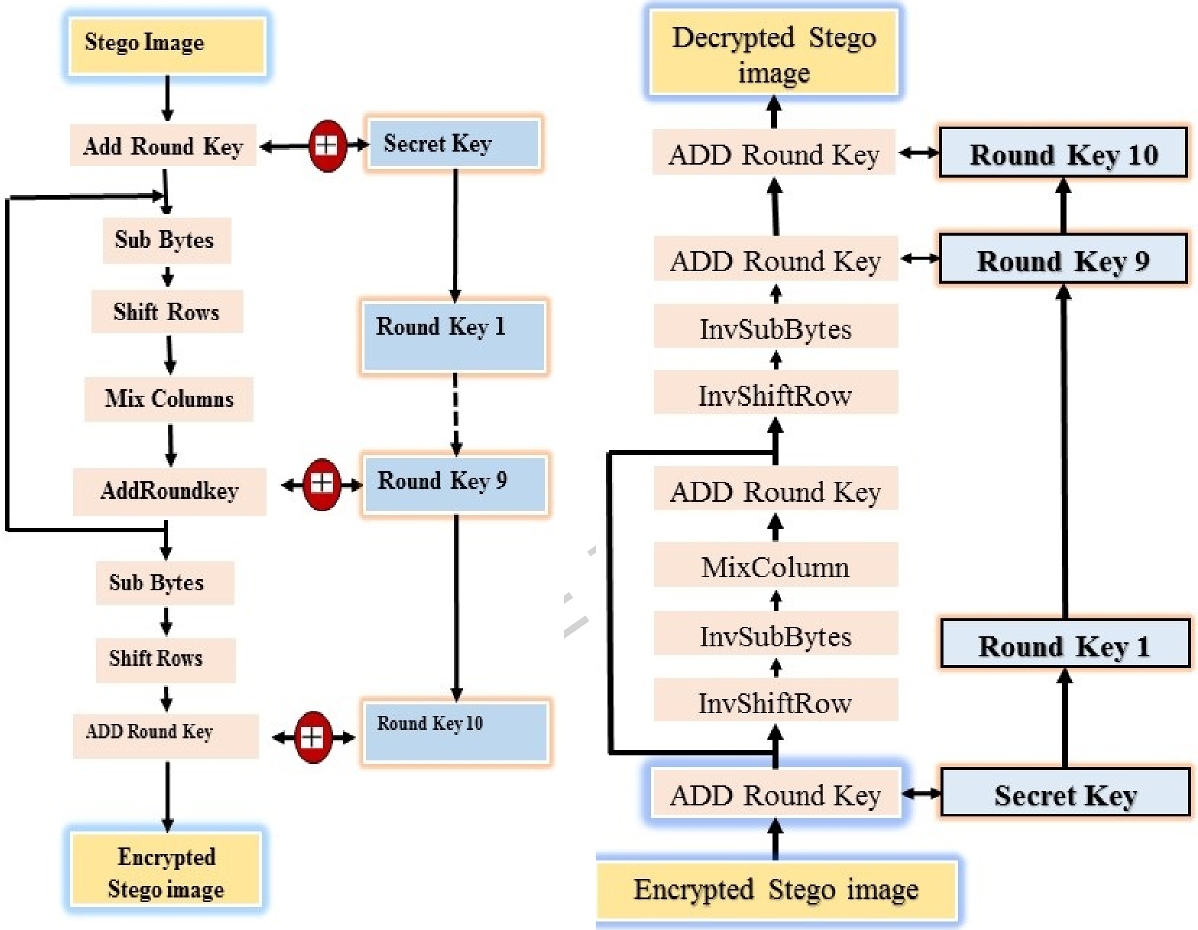


Figure 6: AES Encryption and Decryption

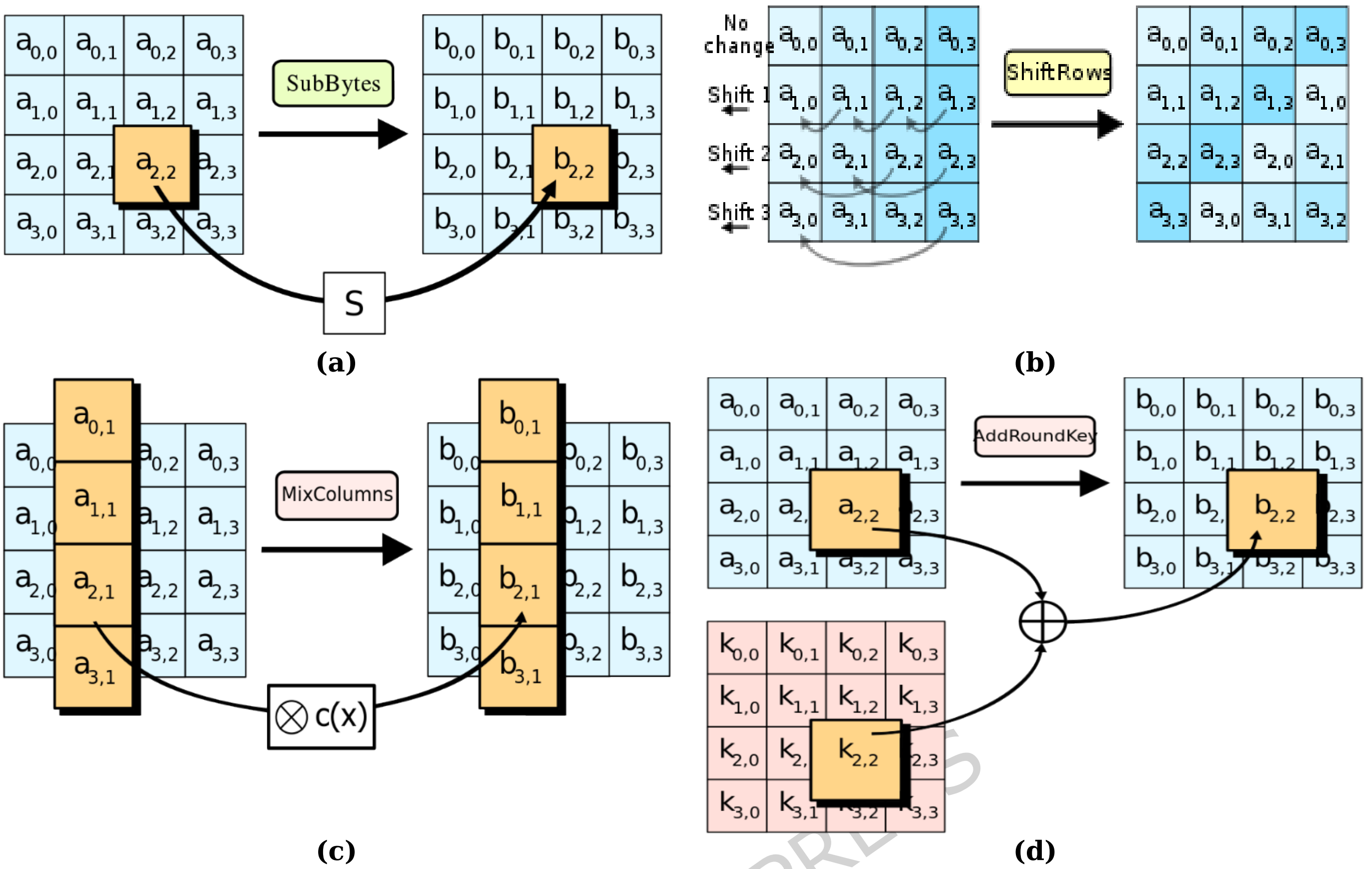


Figure 7: (a) Transformation of Sub bytes, **(b)** Transformation of Shift Rows, **(c)** Transformation of Mix Column, **(d)**Transformation of Add Round Key

AES Decryption Process

Decoding is the reverse of encoding and includes returning the code image to the decrypted image using a key. There is a backward substitute byte, a reverse blend section, an opposite shift column, and a converse box. Inverse Sub Byte Transformation: Acquiring the new framework, each byte from the frame is supplanted with the opposite s-box table. Inverse Shift Rows Transformation: The frame's column has been circularly correctly moved. Inverse Add Round Key Transformation: Capability is opposite to that of blend segment change. Opposite [37], [38], [39]. Add Round Key Change: The subsequent grid is XORed with the lengthy key from the earliest key shown in Figure 7 (a-d).

Simulation Results and Discussion

In this section, we present the experimental setup, analysis, and discussion in detail. The proposed method enables information to be concealed without causing noticeable visual alterations because the least significant bit has a minimal impact on the image up to 4 LSBs. The proposed method used MATLAB for experiments, a well-known programming, numerical, and technical computing language. It offers a convenient setting for working with images and putting the essential algorithms for concealing and obtaining sensitive information into practice. The experimental results are conducted based on different perspectives (to measure the method with different dimensions for getting better image type, dimensions, format, etc.) and also critically analyzed on some QAM and security analysis to show the importance of the research work. However, the overall analysis and discussion of the proposed method are discussed respectively, which are given below:

- Perspective 1: Same-size images and different-size text
- Perspective 2: Different dimensions' images with same text.
- Perspective 3: Analysis using QAM and Security Analysis

Image Quality Assessment Measurements (QAMs)

To assess the effectiveness of image steganography, various methods are utilized. All of these methods evaluate a different angle of the Steganographic method [34], [35]. A few renowned approaches include Mean Square Error (MSE), Peak Signal Noise Ratio (PSNR), Structured Similarity

Index Measure (SSIM), Normalized Cross Correlation (NCC), and Root Mean Square Error (RMSE). Peak Signal Noise Ratio (PSNR) are used. So, the Peak signal-noise ratio is a fundamental metric used to determine whether the resulted image is identical to the original image. PSNR is used to calculate the robustness of the suggested technique. Where C represents the cover media.

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{C_{max\ 2}}{\mathrm{MSE}}\right) \qquad (13)$$

Mean Square Error: The mean square determines the distinction between the original and the resulted image. It highlights the variations between the original and stego images. Where S denotes the stego media & C denotes the cover medium. The median dimensions are M and N.x & y are then the loop counters. MSE formula is:

$$\mathrm{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy}) \qquad (14)$$

Structural Similarity Index Measurement: Structural Similarity index measurement is utilized to compute the brightness, contrast, & structure of the original & stego mediums were calculated using this measurement.

$$\mathrm{SSIM(X,Y)} = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\left(\mu_x{}^2 + \mu_y{}^2 + C_1\right)\left(\sigma_x{}^2 + \sigma_y{}^2 + C_2\right)} \qquad (15)$$

SSIM assesses the decline in quality induced by certain activities. Where x and y are the mean values for μ_x & μ_y, the variances for x and y are $\sigma_x{}^2$ & $\sigma_y{}^2$, respectively, while the covariance for x and y is σ_{xy}.

Normalized Cross Correlation: Normalized Cross Correlation is the approach for calculating the original medium & stego medium quality. M & N denote the medium dimensions, C the cover medium & S the stego medium.

$$\mathrm{NCC} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}(S(x,y) * C(x,y))}{\sum_{x=1}^{M}\sum_{y=1}^{N} S(x,y)^2} \qquad (16)$$

Root Mean Square Error: RMSE calculates the variation among the stego & the original medium.

$$\mathrm{RMSE} = \sqrt{\left(\frac{1}{N}\right)\sum_{x=1}^{N}(C_x - S_x)^2} \qquad (17)$$

Mean Absolute Error: Mean Absolute Error is a criterion to assess how well a system resists assaults. Where $C(x, y)$ & $S(x, y)$ are the pixel's grey levels, M is the cypher medium, & N is the plain medium [29].

$$\mathrm{MAE} = \left(\frac{1}{MXN}\right)\sum M - 1 \sum N - 1|C(x, y) - S(x, y)| \qquad (18)$$

Correlation Coefficient: it is also used for linearity analysis of two random variables. Both variables are said to be equal if the value is 1 otherwise not equal if 0. Eq. 19 represent the formula of CC.

$$I = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2}\sqrt{\sum_i (y_i - y_m)^2}} \qquad (19)$$

Image Fidelity: it is also used for checking the image quality of both stego and the cover image. Equation 20 shows IF where P and S are both stego and cover images. While i and j represent upper and lower bonds.

$$\mathrm{IF} = 1 - \frac{\sum_{i,j}(P(i,j) - S(i,j))^2}{\sum_{i,j}(P(i,j) \times S(i,j))} \qquad (20)$$

To begin, a text of eight KB is inserted in color images of various formats with a size of 256x256 utilizing *Perspective 1*; On 50 images, this experiment is conducted. Second, in *Perspective 2*, conceal four different text sizes (i.e:2KB, 4KB, 6KB, 8KB) in separate images of the equal size (256x256). This investigation is focused on four standard shading images. In *Perspective 3*, we employ comparable images to those in Perspective 2 with varying resolutions (128x128, 256x256, 512x512, and 1024x1024) with an inserting hidden text size of 8 KB.

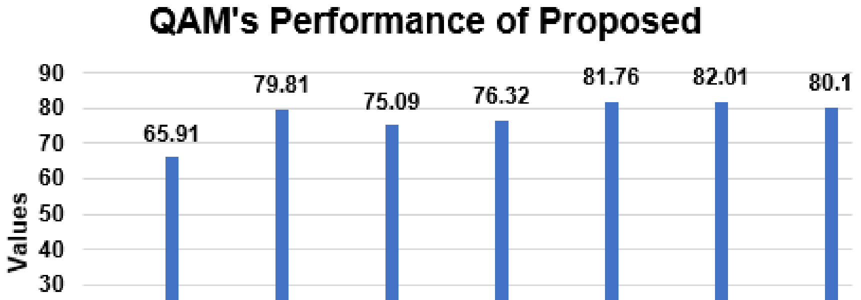
We used image datasets from SIPI as shown in Figure 8. For perspective 1 based on PSNR, the same text size (8 KB) is inserted in several images with the same dimensions (256x256). The average PSNR value over one hundred pictures (100) demonstrates the performance of this research work, shown in Figures and Tables 3-5 below.

Figure 8: Perspective1: Test of cover images

Table 3 and figure 9 represents the performing exploration of the proposed method based on some quality assessment metrics that shows better results.

Table 3: Perspective 1; our proposed strategy's PSNR, Different QAM’s correlation, on 8Kb message text size

S. No:	**Images**	**MSE**	**RMSE**	**NCC**	**SSIM**	**PSNR (dB)**
1	Baboon	0.101	0.039	0.999	0.999	65.91
2	F-16	0.123	0.048	0.999	0.999	79.81
3	Jelly Beans	0.012	0.149	0.989	0.999	75.09
4	Splash	0.041	0.139	0.999	0.998	76.32
5	Peppers	0.124	0.021	0.899	0.979	81.76
6	House 1	0.031	0.042	0.999	0.909	82.01
7	Lake	0.101	0.021	0.998	0.998	80.10



Different message text sizes (2-8 KBs) are inserted into three usual edgy & flat images (Peppers, Home, Lake, and Splash) of the same size (256x256) from the dataset, according to perspective 2. The average PSNR of the identical stego image with various text sizes is shown in Figures 10 and 11.

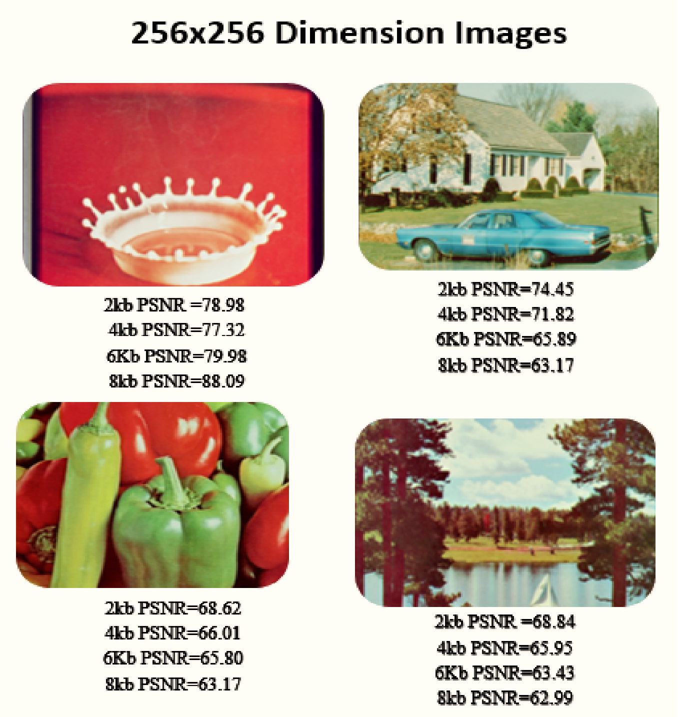


Figure 10: For perspective 2, PSNR values and image size (256x256)

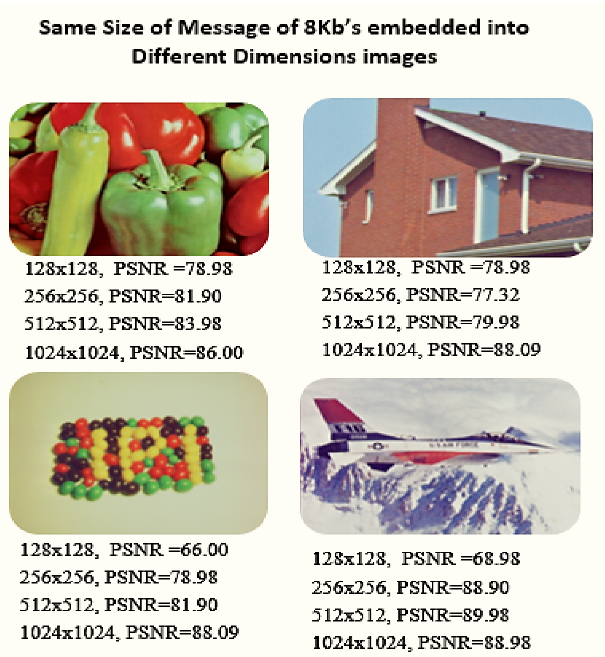


Figure 11: Perspective 3: Comparison based on PSNR and different size of text.

Table 4: Experimental Results of proposed method according to perspective 2 based on MSE, RMSE, NCC,CC,IF & SSIM

Images Name & Sizes	**Hidden Msg (KBs)**	**MSE**	**RMSE**	**NCC**	**SSIM**	**IF**	**CC**
Baboon 256x256	2	0.101	0.004	0.997	0.991	0.998	0.999
	4	0.002	0.010	0.891	0.999	0.989	0.997
	6	0.100	0.130	0.999	0.989	0.999	0.899
	8	0.102	0.120	0.891	0.987	0.997	0.899
F-16 256x256	2	0.020	0.003	0.997	0.998	0.799	0.998
	4	0.012	0.003	0.959	0.999	0.987	0.997
	6	0.100	0.040	0.899	0.999	0.999	0.987
	8	0.104	0.103	0.899	0.899	0.989	0.898
Jelly beans 256x256	2	0.011	0.142	0.987	0.989	0.899	0.999
	4	0.045	0.003	0.989	0.998	0.999	0.999
	6	0.100	0.101	0.899	0.989	0.998	0.998
	8	0.121	0.065	0.989	0.879	0.999	0.899
Splash 256x256	2	0.011	0.031	0.999	0.987	0.998	0.998
	4	0.101	0.010	0.999	0.998	0.988	0.999
	6	0.040	0.131	0.998	0.899	0.899	0.989

Images Name & Sizes	Hidden Msg (KBs)	MSE	RMSE	NCC	SSIM	IF	CC
	8	0.103	0.104	0.989	0.998	0.899	0.899

In light of perspective 3, 8KB text is inserted in images of various sizes (128x128, 256x256, 512x512, and 1024x1024), as shown in Figure 10. The data demonstrated improved presentation. Tab. 4's results using some QAM present the performance of the proposed method. Table 5 shows the results of the comparative analysis of the proposed method with some existing methods. The performance of proposed method can be clearly seen over the existing methods.

Table 5: Comparison of Proposed method with state-of-the-art methods

Image	**Comparative Analysis, resulted from PSNR value using Standard Images (12 kb text)**					
	Akhtar et.al. [14]	**Ahmad et al. [16]**	**W.awdah et al. [21]**	**Islam et. Al. [23]**	**Pabbi et al. [20]**	**Proposed Algorithm**
Jelly Bean	68.04	63.00	77.01	76.01	78.99	81.12
Peppers	66.21	68.01	64.99	71.92	76.89	79.09
Baboon	71.21	79.99	81.00	81.00	73.00	83.98
Lake	77.91	70.00	71.98	75.22	77.00	78.77
House	71.21	69.33	72.98	76.91	79.99	79.99
Lake	73.11	70.99	78.90	77.99	78.91	80.01
Average	71.28	70.22	74.48	76.51	77.46	80.49

However, performance analysis of the proposed method with different perspectives shows the better performance and reasonable results of this research work, highlighted in Figures 8-12, and Tables 3 and Table 4. After performance analysis of the proposed method, safety or critical breakdown analysis was also conducted, which shows the performance of the proposed method, which is elaborated in the given sub-sections. In Table 6, the bits per pixel is calculated using the standard formula, which is; bpp (bits per pixel) = total embedded bits/ number of pixels (image width and Height, i.e., W x H). So, in Table 6, 512x512 images with different hiding capacities, the bpp is shown in detail.

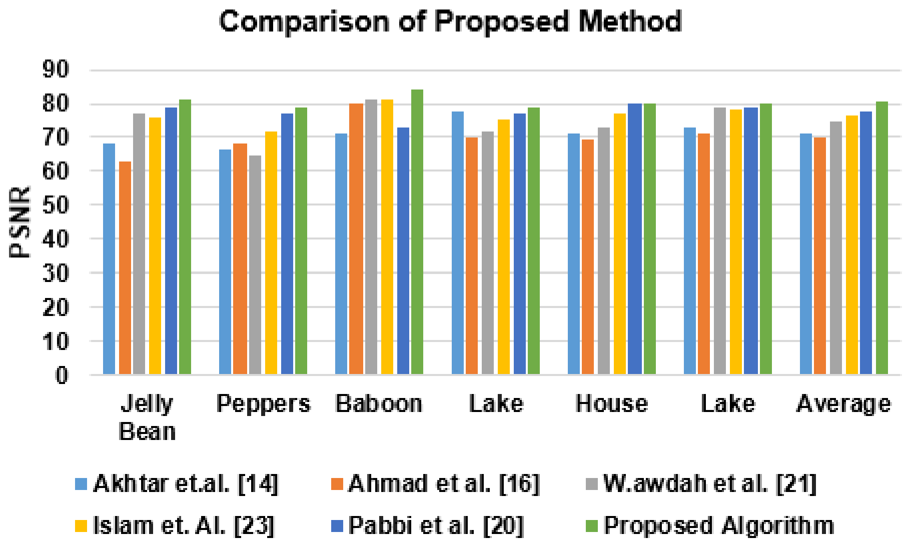


Figure 12: graphical representation of proposed method

Table: 6 shows embedding bits per pixel ratio for more than 10 images is **1.000**

Image 512x512	PM hiding capacity		
	bpp	Hiding Capacity	PSNR
House	142683	0.544	59.13
Peppers	143483	0.547	58.14
Lake	421462	1.608	53.21
Baboon	234574	0.895	56.21
Splash	232777	0.888	57.14
House1	411481	1.570	57.31
airplane	324421	1.238	57.34
Tree	145787	0.556	58.34
Girl	321421	1.226	56.99
Lena	243289	0.928	59.01
Average	**262138**	**1.000**	**57.282**

Discussion

In this section, we explain a critical analysis of the proposed results and performance, examining how it can resist some attacks using RS Steganalysis. The proposed method was analyzed using security RS analysis, noise, and cropping attacks. The proposed method also analyzed up to 4 LSB’s to check the tranparencey of the images, either the cover image and resulted image is identical or not and the bits how much effected. The proposed method also analyzed with historgram analysis. However, after performing this analysis, attacks on the proposed method with some standard images show better results and can resist any attacks. The RS analysis explains modifications in singular & regular groups via collective volume from a small inserting (5%) to the highest inserting of 50%. An encrypted picture can effectively shield against the RS attack under the condition that Rm Equivalents R−m and Sm Equivalents S−m. The RS examination finds no restricted information if Rm≈ R−m> Sm≈ S−m. Tab.6. displays the outcomes of the suggested method's RS-steganalysis for the stego-images at varied embedding rates. The statement Rm ≈ R−m >Sm=S-m is accurate. In other words, even when the embedding capacity is increased to 50%, the distinction between Rm, Rm & Sm, and Sm remains the same. Hence, the probability of finding hidden data inserted within cover images is very weak. Differences in the RS detection values for the suggested approach are reported at K = 4. Moreover, there is a maximum embedding capacity Between Rm and R-m on one side and between Sm and S-m on the other. The outcome demonstrates that the suggested method keeps relatively few average discrepancies between the singular group and the regular group, as shown in Table 7. It also shows that very few objects can be found. It demonstrates the suggested method's capacity to withstand RS-steganalysis by preventing contact with the attack and achieving the necessary level of security.

Table 7: Differences between regular & singular groups using RS-Steganalysis with k=4 bits

Cover Images	Regular groups	Singular groups
Baboon	0.0234	0.0213
F-16	0.2136	0.2136
Jelly beans	0.3313	0.2710
Splash	0.0458	0.2710

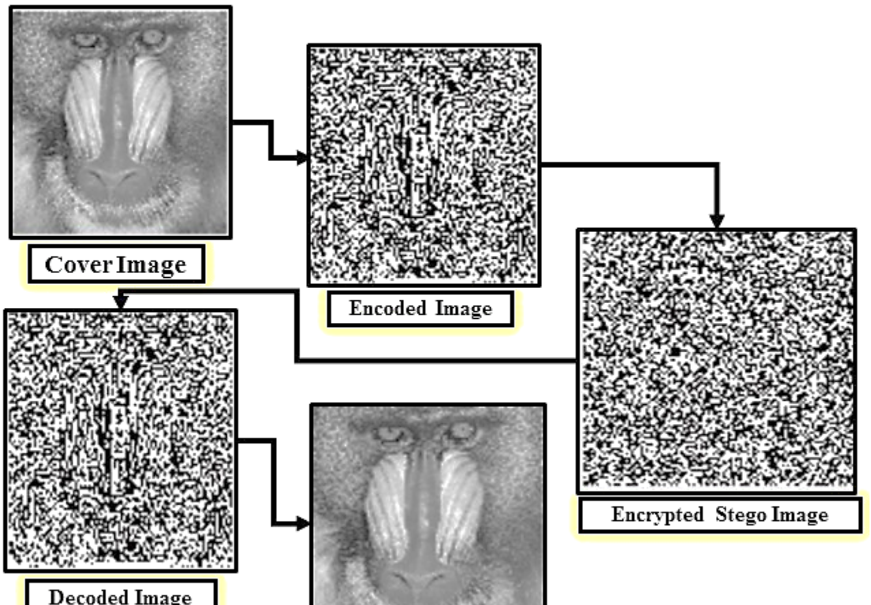


Figure 12: Baboon; Cover, Encoded, Encrypted, Decoded, and Recon-Stego Images

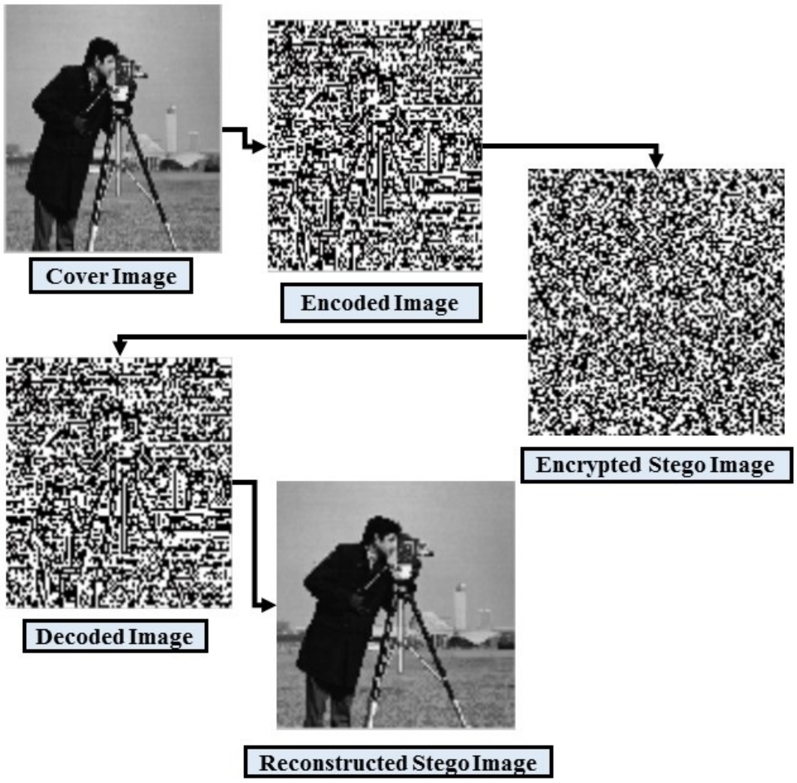


Figure 13: Cameraman; Cover, Encoded, Encrypted, Decoded, and Recon-Stego Images

Figures 12, and Figure 13, show the experimental results of the proposed method using 2 testing images. In each figure, the first line shows the cover and encoded image; the second line shows the stage image encrypted by AES, and the third line shows the Decoded and reconstructed stego image. We conducted both objective and subjective analysis for our proposed method, and it can be seen that the QAM values are from the 50-90 range, which is acceptable and shows the quality of images. It can be strongly supported using histogram analysis of the proposed method by the following Histogram analysis of both cover and stego images shown in Figure 14, Figure 15, and Figure 16.

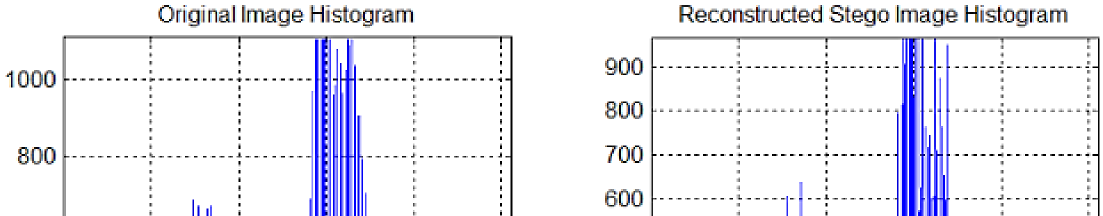


Figure 14: Bird image Histogram of cover and Reconstructed Stego Images

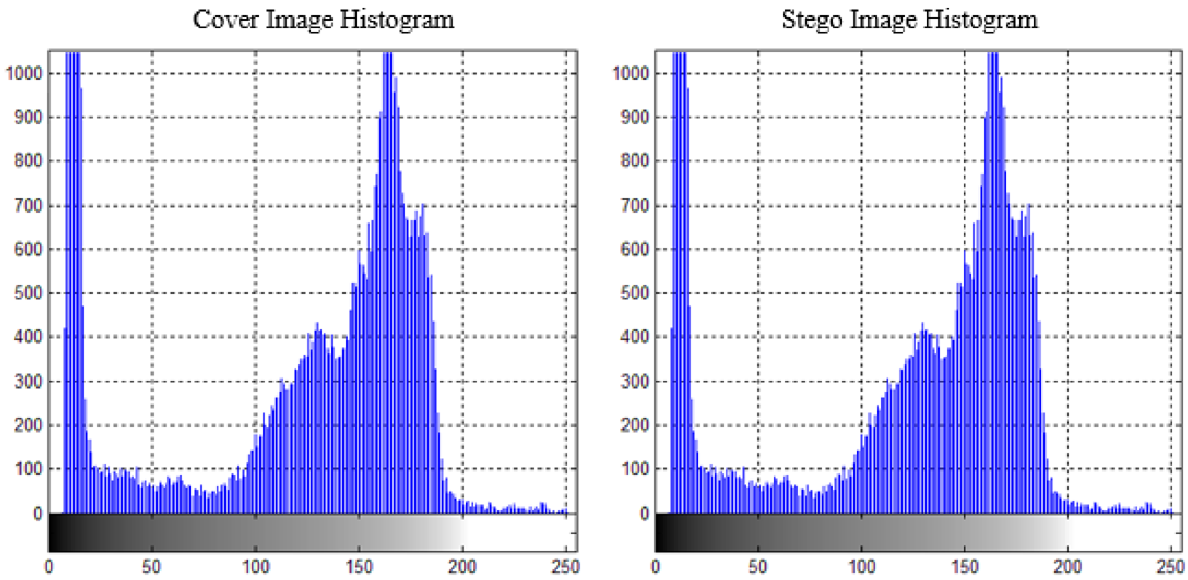


Figure 15: Cameraman; image Histogram of cover and Reconstructed Stego Images

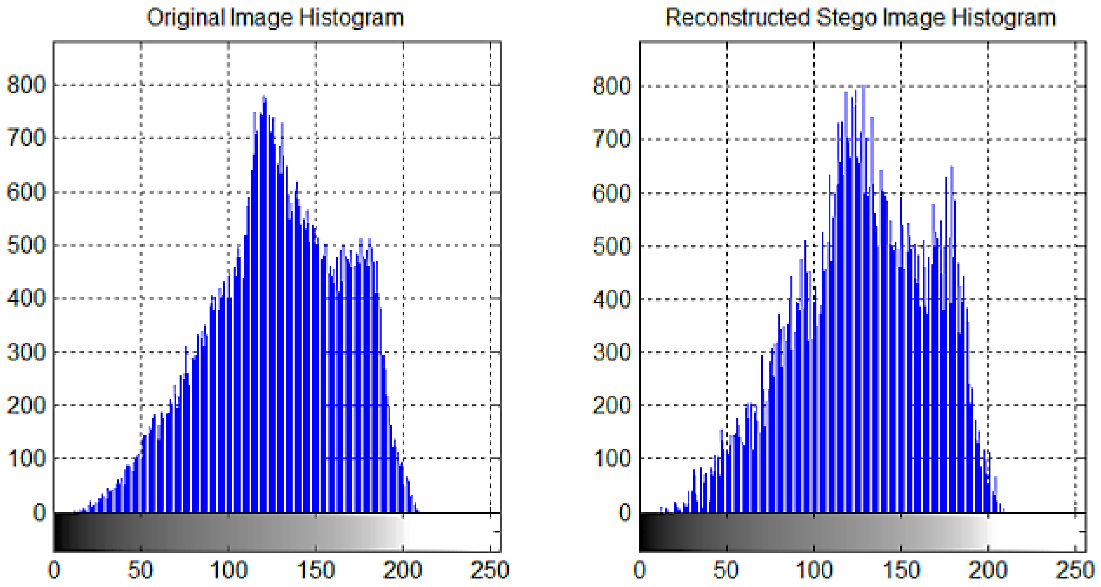


Figure 16 : Baboon; image Histogram of cover and Reconstructed Stego Images

We have experimented with the proposed method that analyzes the embedding LSB from 1-4 LSBs. It can be seen in Table 8 and Figures 16-21, the impact of the 1st LSB to 4th LSB embedding. In Figure 19, it is seen that we exceeded the embedding bits into more than 4th Lsb, and then the image quality degraded. So the feasible LSB for embedding message bits is up to the 4th LSB. Figure 21 shows the result of the cropping attack (ca) analysis.

Table 8: Analysis of Proposed Method on 1st LSB to 4th LSB

Image		Lena	Baboon	Splash	Cameraman	Peppers
LSB-1	SSIM	0.999	0.998	0.9897	0.9977	0.9979
	PSNR	65.65	73.343	77.545	87.876	78.987
LSB-2	SSIM	0.977	0.9943	0.8955	0.9958	0.9769
	PSNR	64.75	72.333	76.554	86.876	77.966
LSB-3	SSIM	0.895	0.9855	0.8956	0.9577	0.9878
	PSNR	64.65	71.243	74.643	85.836	75.967
LSB-4	SSIM	0.899	0.9782	0.9892	0.9934	0.9879
	PSNR	62.55	70.553	73.764	82.656	71.547

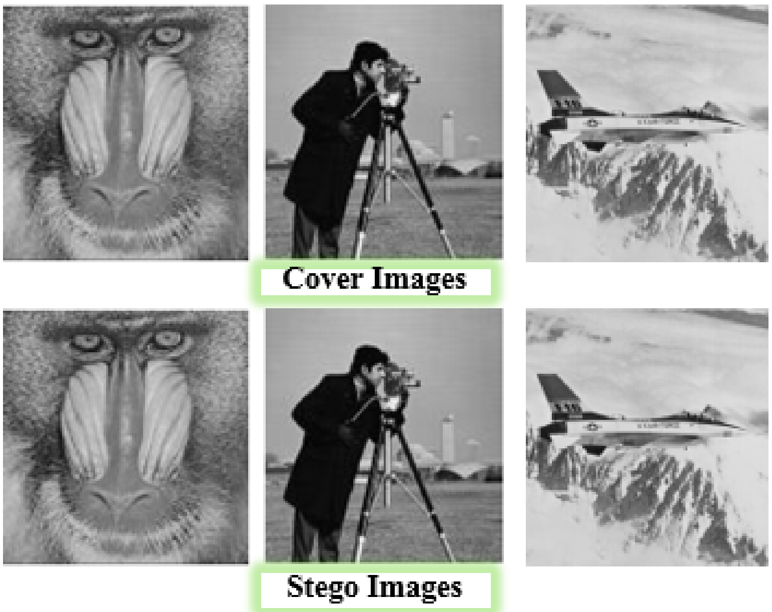


Figure 17: 1st LSB cover and Stego Images

Figure 18: 2nd LSB cover and Stego Images

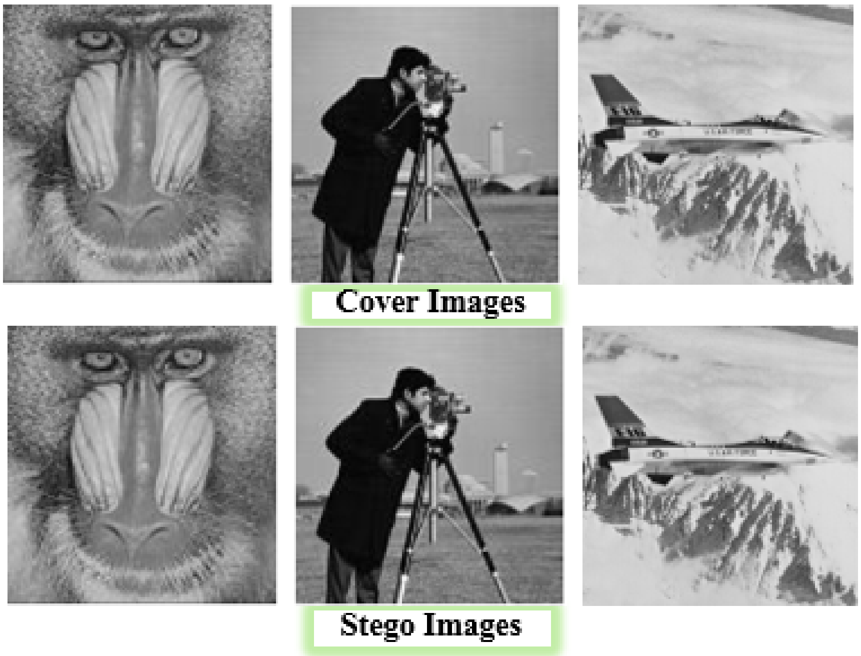


Figure 19: 3rd LSB cover and Stego Images

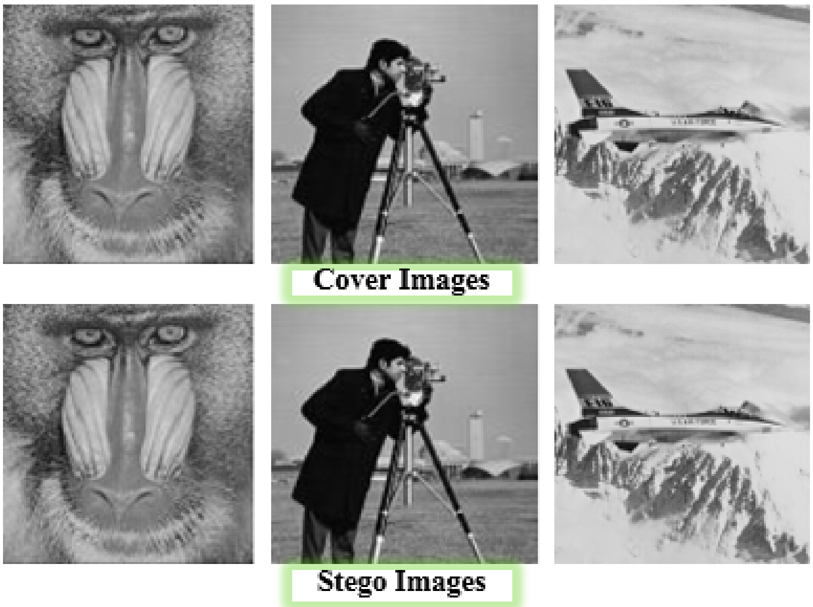


Figure 20: 4th LSB cover and Stego Images

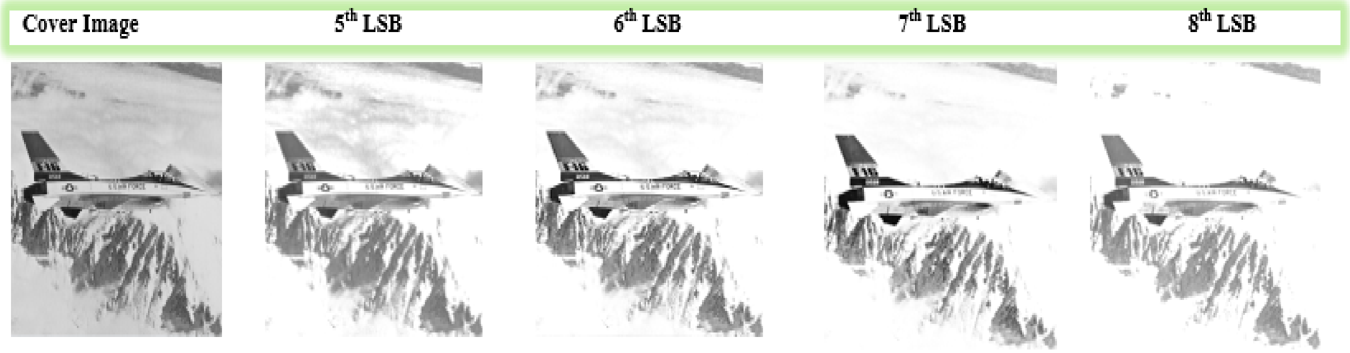


Figure 21: From 5th to 8th LSB cover image and corresponding Stego Images

Several standard images were analyzed using noise attacks with salt and pepper noise values of 0.01, 0.1, and 0.5. The results showed that 0.1 salt and pepper noise is still detectable. To protect against Cropping Attacks (CA), a good cryptosystem should be able to resist both transmission and storage-based data. To evaluate its resistance to cropping attacks, sections of size 64 x 64, 64 x 128, 128 x 128, and 128 x 256 were removed from the "Lake" image embedded in Figure 22. The resulting images are displayed in Figure 15 they are still recognizable. This demonstrates that our algorithm is capable of resisting data manipulation attacks. In this way, our proposed method shows has great durability and can capably go against upheaval attacks. This is demonstrated in Figures 14-21.

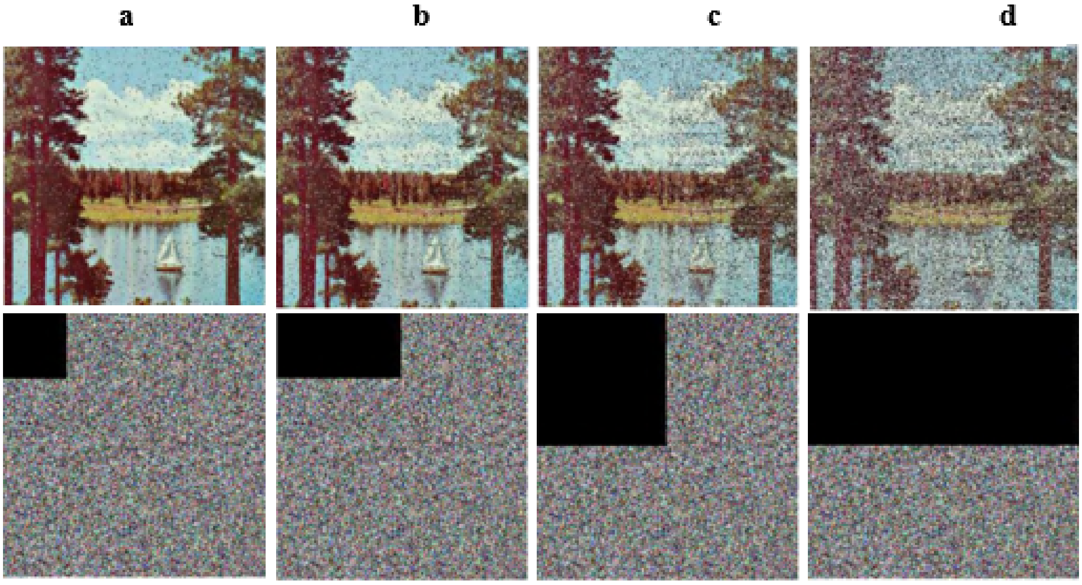


Figure 22: Cropping Attack (CA) analysis

The proposed algorithm has felt empirical testing from diverse perspectives using assessment metrics, showing improvement, efficiency, and effectiveness. Our method upgrades the payload, undeniable level of security, and temper assurance, and works on the visual nature of pictures [23]. The limitations in our method regarding format, color model, and some compression attacks. If attackers attempt to use techniques such as LSB or steganalysis to extract the contents of the secret message, they will not be able to succeed due to the use of AES, MLE, key, and Magic matrix. Even if they partially succeed, the extracted contents are useless without using AES, MLE, and other techniques to retrieve the actual message.

In order to test the strength of the proposed approach, the security analysis was performed in detail to determine the possible ambiguities and the measures adopted to address the ambiguities. The system is highly resistant to the attacks based on statistics because the xor process of embedding effectively randomizes the pixel intensity distributions with the help of group of bits' substitution and key permutation and reduces the statistical differences that can be detected. When compared to brute-force key attacks, there is an important complexity contribution of both a large key space and multi-level permutation, which makes exhaustive key search unfeasible. Moreover, the technique proves to be very resistant to steganalysis-based detection because the pixel level randomness brought about obscures embedding patterns and lowers the possibilities of detecting hidden data. The comparative analysis against the current methods reveals that the given scheme has a better confidentiality, imperceptibility, and resistance to different attacks. These findings reaffirm that the bit-group substitution coupled with the key-controlled pixel permutation operation is effective in enhancing the overall backlash in the security of the entire steganographic process. So the proposed method is embedded the secret message in a such a way that fulfill the need of image steganography and make a reliable method in terms of basics criteria. That's why we used a hybrid concept to achieve some criteria using cryptography and some are steganpragphy based and such a way that can easily achieve a better image steganography method. so we also tried to embeds the message in such a way that cover the need of steganography and the proposed method also analyzed using different statistically attacks (singular and regular groups, cropping and checking up to 4 LSB's (because according to literature and our experiment it can be clearly seen that we can embed a secret message up to 4 LSB)) to checks the resistance against attackers. The Proposed method also analyzed using different quality assessment metrics to shows the strengthen of the method.   After a detail analysis and experiment on different perspectives of the proposed method, it is found that Jpeg format is best format and dimensions is 512x512 for image steganography and the cropping analysis clearly shows the performance of the method but still need some compression i.e. Huffman etc. technique to more strengthen the steganography. Because image steganography needs reliability between the criterion and in the best of my knowledge they can only achievable only a hybrid model of both cryptography and steganography.

Conclusions

This research work presented an enhaced image steganography on LSB, AES, and Magix matrix, transposition and key based method to make a reliable method in term of basic criterion such as robustness, tranparecney, temper protection and computation etc in spaital domian. So, to cover reilablity, we used hybrid different concepts to fullfill the need of image steganography. First way make a embedding procedure based on LSB's in such a way to improves visual quality and embedding efficencey compared to exsiting methods while mainting great resistance against common attacks on steganpgraphy. Once the stego image generated, then applied AES algorithm to stego images to improve the security layers of secret data. The propoded research work also tested on different perspectives in terms of different dimensions images, and different sizes of message text which shows the performance of the method. The proposed work also tested based on quality assesment matrices, and it can be seen that the values of PSNR, MSE, RMSE, MAE, NCC, and SSIM shows better results fulfill the need for image steganography. After a details experiment it is identified that: JPG format, 512x512 dimenion, and 64 kb message size is best and recemended for future uses. In addition, we also assessed the proposed method's based on tamper resistance, robustness, and resistance against known attacks through Histogram and PDH analysis, etc. which generates high-quality images and increases level the security level when embedding up to the first 4 LSB in the ratio of 5.035 embedding capacity. It technical merits, the proposed method has meangfull effects on data secuirty healthcare and others sensitive domians where security and privacy are critical. In the future, the proposed method can be extended for mulimedia formats, noise, frequencey domian, differernt image formats, others attacks models, lossey compression and uses of deep learning for optimal cover steganography and smooth embedding processes. In our analysis, we found that our proposed method is best supported using JPG Images, but we observed that repeated compression of JPEG images loses the quality. Thus, to address these issues by adopting advanced compression procedures, for instance; Huffman coding or other deep learning optimization for better embedding process that make a secure communication in healthcare and data management.

Acknowledgments: This research is funded by the European University of Atlantic.

Competing interests: The authors declare no competing interests.

Data availability: Data is provided within the manuscript

References

[1]. Laishram and D.T. Tuithung," A Survey on Digital Image Steganography: Current Trends and Challenges",3rd International Conference on Internet of Things and Connected Technologies, pp.1-17.

[2]. R.Doshi, P.Jain and L.Gupta.(2012, Dec). "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), 2(6), pp.4634-4638.

[3]. Ye, J. (2024). Advancements in Spatial Domain Image Steganography: Techniques, Applications, and Future Outlook. *Applied and Computational Engineering*, *94*, 6-19.

[4]. Shamsi, Z., Waikhom, L., Saha, A. K., Patgiri, R., Singha, M. F., & Laiphrakpam, D. S. (2024). Visually meaningful cipher data concealment. *Digital Signal Processing*, *155*, 104717.

[5]. Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. *Open Computer Science*, *10*(1), 296-342.

[6]. Anfal, S. A., & Saeed, M. J. (2024). A Deep Dive into Deep Learning-Powered Steganography for Enhanced Security. *International Research Journal of Innovations in Engineering and Technology*, *8*(3), 79.

[7]. G.Borse,V.Anand, and K. Patel.(2013). "Steganography: Exploring an ancient art of Hiding Information from Past to the Future", International Journal of Engineering and Innovative Technology (IJEIT), pp.192-94.

[8]. Majumder, S., Tanu, M. D., Faisal, S. M., Sristy, M. R., & Paul, R. (2023). *Enhanced and secured hybrid steganography model for hiding large data* (Doctoral dissertation, Brac University)..

[9]. D.Ratnasari and A.S.Aji.(2019,Sept)."Text to Color Image Steganography Using LSB Technique and XOR Operations",03(2),pp.59-63

[10]. Y.B.J. Chanu, T.Tuithung and K.M. Singh"A Short Survey on Image Steganography and Steganalysis Techniques", 3rd National Conference on Emerging Trends and Applications in Computer Science.IEEE, 2012, pp.52-55.

[11]. V.K.Sharma, D.D.K.Srivastava,D.P.Mathur.(2017)"A Study of Steganography Based Data Hiding Techniques", International Journal of Emerging Research in Management &Technology,06(04),pp-145-150.

[12]. L.Y.POR,B.Delina." Information Hiding: A New Approach in Text Steganography", Proceedings of the International Conference on Applied Computer and Applied Computational Science, World Scientific and Engineering Academy and Society (WSEAS 2008), 2008,pp-689-695.

[13]. Kadhim, I. J., Premaratne, P., & Vial, P. J. (2020). High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. Cognitive Systems Research, 60, 20-32.

[14]. Shah, P. D., & Bichkar, R. S. (2021). Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure. Engineering Science and Technology, an International Journal, 24(3), 782-794.

[15]. Sahu, A. K. (2022). A logistic map based blind and fragile watermarking for tamper detection and localization in images. *Journal of Ambient Intelligence and Humanized Computing*, *13*(8), 3869-3881.

[16]. Roy, S., & Islam, M. M. (2022). A hybrid secured approach combining LSB steganography and AES using mosaic images for ensuring data security. *SN Computer Science*, *3*(2), 153.

[17]. Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. *Applied Sciences*, *13*(21), 11771.

[18]. Bima, A., Irawan, C., Krismawan, A. D., & Isinkaye, F. O. (2023). A text security evaluation based on advanced encryption standard algorithm. *Journal of Soft Computing Exploration*, *4*(4), 250-261.

[19]. S.M.M.Karim, Md.S. Rahman, Md. I. Hossain, "A new approach for LSB based image steganography using secret key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011),2011, pp. 286-291.

[20]. N.Akhtar,P.Johri and S.Khan, "Enhancing the Security and Quality of LSB based Image Steganography",International Conference on Computational Intelligence and Communication Networks,2013,pp. 385-390.

[21]. Aiswarya, S., & Gomathi, R. (2023). CHAOS BASED CRYPTOGRAPHY AND RECTANGULAR SHAPE BASED STEGANOGRAPHY TECHNIQUE USING LSB. *Malaysian Journal of Computer Science*, *36*(4), 368-380.

[22]. A.Ahmed and A.Ahmed,(2020,May)."A Secure Image Steganography using LSB and Double XOR Operations",IJCSNS International Journal of Computer Science and Network Security, 20(5),pp.139-144.

[23]. U.A.M.E. Ali,M.Sohrawordi and M.P. Uddin.(2019,Feb). "A Robust and Secured Image Steganography using LSB and Random Bit Substitution",American Journal of Engineering Research (AJER), 8(1), pp-39-44.

[24]. A.Ahmed and A.Ahmed,(2020,May)."A Secure Image Steganography using LSB and Double XOR Operations",IJCSNS International Journal of Computer Science and Network Security, 20(5),pp.139-144.

[25]. S.Rahman, F.Masood, W.Khan, N.Ullah, F.Q.Khan, G.Tsaramirsis, S.JanandM.Ashraf. (2020, May).“A Novel Approach of Image Steganography for Secure Communication Based on LSB Substitution Technique”, 64(1), pp.31-6.A.Pabbi,R.Malhotra and M.K“Implementation of Least Significant Bit Image Steganography Advanced Encryption Standard”, International Conference on Emerging Smart Computing and Informatics (ESCI) AISSMS Institute of Information Technology,2021, pp.363-366.

[26]. Yamni, M., Daoui, A., & Abd El-Latif, A. A. (2024). Efficient colour image steganography based on a new adapted chaotic dynamical system with discrete orthogonal moment transforms. *Mathematics and Computers in Simulation*.

[27]. W.A.Awadh,A.S.Alasady, and A.K.Hamoud(2022,Dec)."Hybrid information security system via a combination of compression, cryptography, and image steganography," International Journal of Electrical and Computer Engineering,12(6), pp. 6574-6584.

[28]. Abunadi, I., Abdullah Mengash, H., S. Alotaibi, S., Asiri, M. M., Ahmed Hamza, M., Zamani, A. S., ... & Yaseen, I. (2022). Optimal multikey homomorphic encryption with steganography approach for multimedia security in Internet of Everything environment. *Applied Sciences*, *12*(8), 4026.

[29]. K.Muhammad, M.Sajjad,I.Mehmood,S.Rho, S.W.Baik,” A Novel Magic LSB Substitution Method (M-LSB-SM) using Multi-Level Encryption and Achromatic Component of an Image”,pp.1-27, 2016.

[30]. Almomani, I., AlKhayer, A., & El-Shafai, W. (2022). Novel Ransomware Hiding Model Using HEVC Steganography Approach. *Computers, Materials & Continua*, *70*(1).

[31]. M.R.Islam, A.Siddiqa, M.P.Uddin, A.K.Mandal and M. D.Hossain,"An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography",3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014,2014,pp.1-6.

[32]. Ghrare, S. E., Abouras, M. A., & Akermi, I. A. (2024). Development of Hybrid Data Security System using LSB Steganography and AES Cryptography. *African Journal of Advanced Pure and Applied Sciences (AJAPAS)*, 86-95.

[33]. M.R.Islam,T.R.Tanni,S.Parvin, M.J.Sultana and A.Siddiqa, "A modified LSB image steganography method using filtering algorithm and stream of password", Information Security Journal: A Global Perspective, pp.359-370.

[34]. Sharma, D., & Prabha, C. (2024). Hybrid security of EMI using edge-based steganography and three-layered cryptography. In *Applied Data Science and Smart Systems* (pp. 278-290). CRC Press.

[35]. S.Rahman, J.Uddin, H. Hussain, S. Jan, I. Khan, M. Shabir and S.Musa(2023, Feb)."Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats”15(5),pp. 4252.

[36]. S.Rahman, F.Masood, W. U. Khan, A. Salam, S.I. Ullah(2019,Jun). "Investigation of LSB-based Image SteganographicTechniquesin Spatial Domainfor Secure Communication” , Sukkur IBA Journal of Emerging Technologies,02(01), pp. 1-12.

[37]. I.J.Kadhim, P.Premaratnea,P.J.Vial , B. Hallorana(2019,Nov). "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research”, pp. 299-326.

[38]. P.P.Bandekar and S.GC2, “LSB BASED TEXT AND IMAGE STEGANOGRAPHY USING AES ALGORITHM” Proceedings of the International Conference on Communication and Electronics Systems (ICCES 2018),2018, pp. 782-788

[39]. F.Q. A.Alyousuf, R.Din and A.J.Qasim(2020,April). "Analysis review on spatial and transform domain technique in digital steganography”, Bulletin of Electrical Engineering and Informatics,9(02), pp.573-581.

[40]. https://es.wikipedia.org/wiki/Advanced_Encryption_Standard#

[41]. M.Hassaballah, M.A. Hameed, A.I.Awad, and K. Muhammad, "A Novel Image Steganography Method for Industrial Internet of Things Security”, IEEE Transactions on Industrial Informatics,2021, pp. 7743-7751.