



Dynamic 8-bit XOR algorithm with AES crypto algorithm for image steganography

D. Madhu¹ · S. Vasuhi¹ · A. Samydurai²

Received: 23 February 2024 / Revised: 14 March 2024 / Accepted: 19 March 2024 / Published online: 25 April 2024
© The Author(s), under exclusive licence to Springer-Verlag London Ltd., part of Springer Nature 2024

Abstract

The proliferation of the Internet's infrastructure, extending even to rural areas, has propelled images to the forefront of multimedia content, necessitating the need for robust methods to safeguard confidential data. Image steganography has emerged as a pivotal technique for concealing sensitive information within images, amidst growing threats to copyright protection and content integrity. To address these challenges, this research proposes a novel approach that combines the dynamic 8-bit XOR algorithm with the AES crypto algorithm, aiming to fortify the outcomes of image steganography. The method entails encrypting messages using AES encryption, followed by embedding them within images using the dynamic XOR method, ensuring both security and imperceptibility. The study's objectives include assessing the impact of secret message size and stego image dimensions on algorithm efficiency, evaluating through metrics like PSNR, MSE, NPCR, and entropy. Notably, histogram analysis reveals minimal differences between original and stego images, underscoring the difficulty in detecting hidden information. Moreover, the study delves into the influence of secret message size on algorithm performance, highlighting a trade-off between text size and PSNR, where smaller sizes exhibit stronger concealment capabilities. Additionally, the impact of stego image dimension size is examined, revealing varied performance metrics based on different dimensions. Comparisons with existing encryption methods indicate favourable outcomes for the proposed algorithm in terms of PSNR, NPCR, and entropy. Notably, PSNR values range from 74.17 to 80.17 dB, while NPCR values vary from 87.98 to 99.81%. Moreover, MSE values range from 0.000621 to 0.04, and entropy values range from 7.39 to 7.64 dB. The study contributes valuable insights into image steganography, emphasizing the need for robust techniques to safeguard sensitive data in multimedia content. Through comprehensive evaluation and comparison, the proposed method demonstrates promising potential for real-world applications, addressing critical concerns surrounding content protection and data security in the digital age.

Keywords Image steganography · AES · NPCR · Histogram · PSNR · Entropy

1 Introduction

The evolution of the Internet has brought about profound changes in how we communicate and interact with information. Over the years, the Internet's infrastructure has expanded dramatically, reaching even the most remote rural areas [1]. As a consequence, various forms of multimedia content, particularly images, have emerged as dominant mediums of expression and communication [2]. This surge in the prominence of images has not only transformed the way we convey information but has also spurred the utilization of sophisticated techniques like image steganography for concealing sensitive data within these visual assets [3]. With the proliferation of hardware, software, and network technologies, the digital landscape has become rife

✉ D. Madhu
dmadhuknr@gmail.com
S. Vasuhi
vasuhi_s@annauniv.edu
A. Samydurai
asamydurai@gmail.com

¹ Department of Electronics Engineering, Madras Institute of Technology, Anna University, Chennai, India

² Department of Computer Science and Engineering, SRM Valliammai Engineering College, Kattankulathur, Chengalpattu, India

with threats to copyright protection and content integrity [4]. This escalating risk has necessitated the deployment of robust mechanisms to safeguard confidential information from malicious actors. In response, steganography systems have emerged as a clandestine means of communication, enabling the covert embedding of secret data bits within any communication medium [5]. To counter the pervasive threat posed by intruders seeking to compromise data integrity, information concealment techniques have become indispensable tools for securely exchanging sensitive data. Steganalysis, the process of detecting the presence or absence of hidden data in a stego medium, has become a vital component of modern security frameworks [6]. Steganography encompasses two fundamental schemes: spatial domain and transform or frequency domain techniques [7]. Spatial domain schemes directly manipulate the bits of pixel values within images, with the least significant bit (LSB) substitution method emerging as one of the most popular techniques [8–14]. In contrast, frequency domain schemes leverage transformations to embed data imperceptibly into images [4, 15–19]. The study of image steganography has undergone significant scrutiny and categorization, resulting in the classification of techniques as either reversible or irreversible [20, 21]. Reversible techniques prioritize the recovery of hidden data while ensuring the restoration of the original image, whereas irreversible methods primarily focus on retrieving the concealed data [22]. The safeguarding of sensitive data demands heightened attention from a security standpoint [23]. Images, often regarded as visual representations, possess the potential to convey intricate messages beyond what meets the eye. Without accompanying textual context, images risk being misinterpreted or misused, potentially leading to defamation or misinformation [24]. Thus, ensuring the protection and integrity of image content is paramount in today's digitally interconnected world.

2 Literature review

Liao et al. [25] proposed an inter-block technique for embedding patient records in medical JPEG images. The technique involves identifying adjacent discrete cosine transform (DCT) blocks of similar positions and calculating the difference between their coefficients. Sajjad et al. [26] focused on embedding a region of interest (ROI) in host images, which can be separated from the host image after decryption and used by concerned consultants. Alsaidi et al. [27] analysed the use of steganography in computer forensics and its potential to be used by criminals to hide evidence. Meanwhile, Elhoseny et al. [28] explored the use of level 1 and 2 2D discrete wavelet transform techniques to embed patient data in grayscale and colour images as cover media. Text data are encrypted before being embedded, and various

statistical measures are applied to ensure the imperceptibility of the cover medium. The statistical scoring method is found to be effective in concealing secret textual information, which outperforms other existing techniques [29]. Biometric systems face numerous challenges related to security and data integrity. Steganography can provide a valuable solution to improve the security of biometric data. LSB (least significant bit) and PVD (pixel value differencing)-based steganography methods are widely used to protect biometric data and resist various statistical attacks. Shehab et al. [30] have presented a refined watermark technique that ensures self-retrieval and authentication of images in medical applications. The authors utilized a singular value decomposition (SVD) scheme on the blocks of the broken image. They then substituted the SVD block-wise tracks to the host image LSBs. This approach has worked well in recovering the original data in case of tampering with the host image. Similarly, Lee [31] utilized a reversible watermark technique on the segmented image, the background region, and the object region to detect tampering or forgery in image modalities such as X-rays, computed tomography (CT), or MRI images. The proposed technique works well to detect tampering using the hash code. The reversible watermark techniques are particularly effective where medical systems are more vulnerable to forgery or tampering. Additionally, Kaw et al. [32] have offered a technique to integrate patient records into their clinical images by incorporating data based on optical pixel repetition. They divided the cover image into two-by-two blocks and integrated the electronic patient record into each block by substituting secret data bits to each block pixel bits. Finally, Parah et al. [33] proposed a technique to divide the host image into non-overlapping blocks of n th size based on both non-seed pixels and seed pixels. Only non-seed pixels were used for data embedding to achieve better imperceptibility and payload capacity. The selection of image pixels from the non-sequential least significant bits was based on pixel similarity and fuzzy logic, where pixels with similar intensity values were used to embed secret patient data. With the widespread use of the Internet, there is a growing demand for sharing various types of media, including images, videos, and documents. However, this has also led to a need for protecting the data from being lost or intercepted through digital steganography. In addition, with the increasing concern for information security in the digital market, there is a need for steganography techniques that offer a balance between imperceptibility and payload capacity, which are inversely proportional to each other [34].

Sahu and Swain [20] proposed several data embedding techniques that improve peak signal-to-noise ratio (PSNR) and data embedding capability. These include the double layer reversible data embedding method, which embeds data in four images, and the reversible data embedding method using LSB match to embed data in pixels of similar images

[5]. Additionally, they proposed the rightmost n -bit replacement technique that uses a pair of similar pixels [3], the pixel value differencing technique with modulus function to minimize the fall of the boundary problem [35], and the rightmost n -bit embedding technique where n is between one and four [36]. They also introduced the pixel overlap block method based on five pixels from the right, which is divided into four sub-blocks (1st and 5th, 2nd and 5th, 3rd and 5th, 4th and 5th) [37]. Finally, they proposed the bit flipping method, which hides secret data in cover images by working on the 7th and 8th bits [38]. Other steganography techniques proposed by Wazirali and Chachzo [39] and Wang et al. [40] use edge detection and image compression techniques to divide the image into edge and non-edge regions and minimize image distortion caused by the embedding procedure. Li et al. [41] introduced batch steganography, which involves embedding data into multiple images instead of just one, allowing for secret data bits to be retrieved from more than one share in case of unusual conditions during data transmission. The use of compressed JPEG images is a popular communication channel for steganography. To ensure the similarity between the original stego image and the compressed image, Tao proposed a coefficient adjustment compression scheme [42]. In this approach, an intermediate image is created, which closely resembles the stego image. Similarly, Li and Zhang [43] introduced a novel technique for embedding secret data in a fingerprint image without requiring a cover signal. The secret message is incorporated into the construction of the fingerprint image as a piece of the hologram. The message is mapped to the polynomial and encoded at different polarities. This technique eliminates the need for a conventional cover signal used in conventional steganography schemes. Madhu and Vasuhi present a secure integration of cryptography and steganography using an image processing technique. It proposes a YCbCr-based 2-bit XOR LSB image steganography scheme, combining data concealment and encryption using a simple crypto algorithm. The proposed method achieves high security, high PSNR, and low MSE, demonstrating its effectiveness in concealing data within an image [44]. In as well as displaying very little block pattern versions, LEMARS acquired a PSNR value of 58.02 dB, an entropy value of 6.15 dB, an NPCR value of 99.84%, and a UACI value of 33.70 [90].

The peak point is used for data embedding in a picture in previous histogram shifting-based RDH algorithms [45, 46]. An enhanced RDH method that pre-processes host pictures using a Gaussian low-pass filter was proposed by Rajkumar et al. [47]. In this case, the histogram's highest peak point is selected for embedding. The stego image's authentication procedure is enabled by the secret key. The outcomes of the trial demonstrate improved resilience and quality of perception. The RDH approach of Zong et al. [48] provides improved imperceptibility. It initially divides the pixels of

the host picture into low- and high-frequency components using a low-pass filter.

Furthermore, a secret key that is produced at random is used to acquire the grey levels of the low-frequency components [49]. An RDH framework using the difference in a picture to increase the embedding capacity was developed by Aziz et al. [50]. Here, to improve the smoother areas, it additionally reorganizes the image's columns or rows in addition to calculating the difference between nearby pixels. After that, the data may be embedded into the altered picture using a difference-based method. A significant quantity of data may now be embedded in photographs with more space thanks to certain recent efforts [51–57].

In order to partition the cover picture using a dynamic blocking technique [59], Pan et al. [58] presented a unique method for reversible data concealing based on pixel value ordering (PVO) and dynamic pixel block partition. An enhanced RDH method using block-wise embedding and histogram shifting was proposed by Fallahpour et al. [60]. The zero and peak bins are found here. Next, the peak's neighbouring bins are moved. The peak bins are used for the data concealment. The recommended method is straightforward and offers very effective reversible data concealment. Regrettably, there are still some problems with this method. For instance, it has not been used appropriately to investigate the peak bin and the neighbouring peak bin because the right side of the peak bin is impacted if the peak bin value is even, and the left side of the peak bin is impacted if it is not. Furthermore, the histogram provides the zero and peak values needed for data embedding. The zero values on the left and right sides of the peak bins are, however, accessible in the majority of situations. Consequently, shifting-related volatility may be minimized if chosen wisely. To prevent bit mistakes, the authors in [61] used a block-wise substitution transposition approach. Next, to conceal the important information, a histogram shifting technique is used.

Ramesh et al. addresses security challenges in e-commerce transactions, highlighting issues with existing RSA and Rabin cryptosystems. It proposes a novel encryption method introducing a fake-modulus for enhanced security, validated through visual, histogram, and quantitative analyses. The proposed method demonstrates higher complexity against factorization attacks compared to recent Rabin variants [62].

Kallapu et al. studied the increasing volume of global information faces security challenges in existing cloud systems. Blockchain's attribute-aware encryption ensures real-time secure communication, offering fine-grained search permissions and secure access to encrypted data. Experimental evaluation validates key system capabilities [63].

Thomas et al. [64] proposed a medical image compression method using discrete wavelet transform, reduction operation, and Huffman coding, aiming for lossless encoding.

The approach demonstrates effectiveness with a PSNR of 54.66 dB, addressing storage and transmission challenges in medical imaging.

Khudhair et al. proposed a novel reversible data hiding (RDH) technique based on histogram shifting, LSB embedding, and dynamic block-wise embedding. It enhances robustness and security while achieving stego images with PSNR exceeding 58 dB for 0.9 BPP, validated through statistical tests [65].

Asmitha et al. highlight the importance of computer vision and deep learning in human authentication, addressing issues like fraud and limitations of existing methods. It introduces improved arc face combined with retina face for robust multi-face recognition, achieving 97% accuracy in real-time attendance tracking [91].

3 Aim and scope of the paper

According to recent research, image steganography has gained recognition as a highly efficacious method for securely transmitting confidential information. Various techniques, including the least significant bit (LSB), discrete cosine transform (DCT), spread spectrum (SS), phase coding (PC), XOR algorithm, and AES encryption algorithm, can effectively conceal information within images.

In this study, we propose a novel approach that combines the dynamic 8-bit XOR algorithm with the AES crypto algorithm to enhance the outcomes of image steganography. The proposed method comprises two pivotal phases. Initially, the message undergoes encryption using the AES encryption method, thereby augmenting the security of the concealed data. Subsequently, the dynamic XOR method is employed to embed the encrypted message within the image. Leveraging the dynamic properties of the XOR algorithm renders the concealed message more challenging to detect, while encryption ensures its protection. This integrated strategy ensures a more robust and secure steganographic solution.

To evaluate the effectiveness of the proposed technique, several objectives have been delineated. One objective entails investigating how the size of the secret message impacts the algorithm's efficiency. By varying the size of the secret message, we can assess the efficiency and efficacy of the proposed method. Another objective aims to explore how the dimensions of the stego picture influence the algorithm's effectiveness. Analysing the impact of different picture dimensions enables us to comprehend the algorithm's flexibility and resilience.

Furthermore, a histogram analysis of both the original picture and the stego image is conducted to assess the performance of the suggested strategy. This analysis, which is based on image dimensions, facilitates a comprehensive understanding of the distribution of pixel values in the images.

The main contribution of the work has been shown in below.

- The AES algorithm is used for symmetric key encryption and decryption. It operates by dividing data into fixed-size blocks and applying a series of mathematical transformations using a key.
- The Dynamic XOR algorithm is employed for image steganography, allowing the hiding of information within an image imperceptibly. It modifies pixel values through XOR operations with a dynamic key generated from the message to be concealed.
- The encryption process combines the AES crypto algorithm with the Dynamic XOR algorithm to hide messages within images effectively. The process involves converting messages into binary representation, generating dynamic keys based on message length, and iterating through image pixels to perform XOR operations.
- Several performance metrics are used to evaluate the effectiveness of the encryption technique, including PSNR, MSE, NPCR, and entropy. These metrics provide insights into the quality, security, and efficiency of the encryption algorithm under various conditions.
- The proposed encryption scheme is compared with other established methods using common encryption metrics. The results suggest that the proposed algorithm demonstrates favourable outcomes comparable to recent encryption methods.

4 Methodology

The proposed method is combination of dynamic 8-bit XOR with crypto algorithm to hide the image for the transfer from one place to another using image steganography. The proposed method has been shown as a schematic diagram in Figs. 1.

4.1 AES crypto algorithm

AES is a symmetric key encryption algorithm, which means that the same key is used for both encryption and decryption. It is widely used for securing data and communications and is considered to be one of the most secure encryption algorithms available today. AES works by dividing the data into fixed-size blocks and then encrypting each block using a series of mathematical transformations and a key. The algorithm allows for different key sizes (128-bit, 192-bit, or 256-bit), with longer keys providing stronger security.

In the code provided, the AES (advanced encryption standard) cryptography algorithm is used. Specifically, it is used

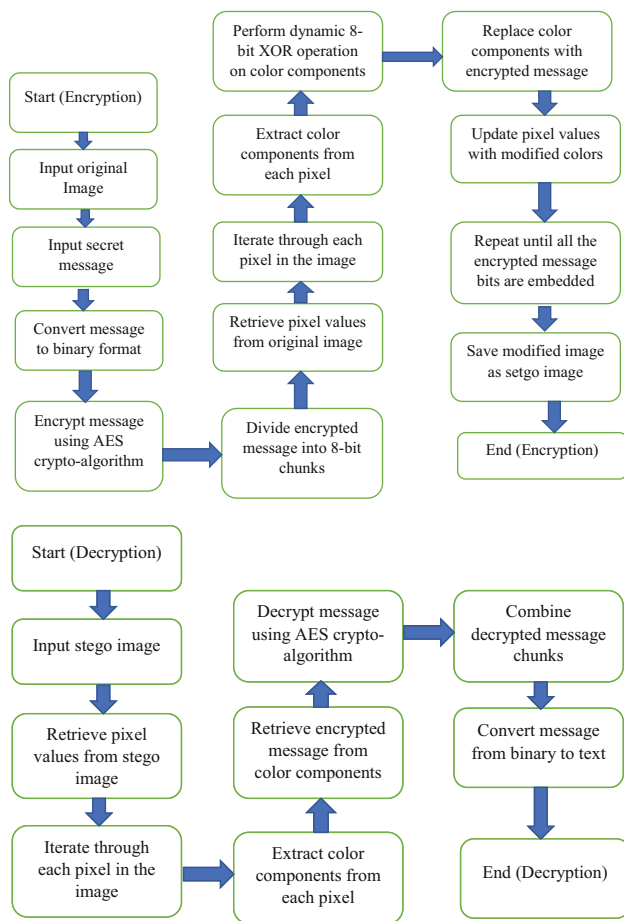


Fig. 1 Schematic diagram of encryption and decryption technology of the proposed method

for encrypting and decrypting messages in the functions `encrypt()` and `decrypt()`, respectively [66]

Here is an example of how AES encryption and decryption works with a key size of 256 bits:

Key Expansion: The 256-bit key is expanded to create a key schedule, which is a set of round keys used in the encryption and decryption process.

Initial round: The first round consists of a key addition step, where each byte of the plaintext is XORed with a byte of the round key.

Main rounds: The next 13 rounds (for a total of 14 rounds) consist of four operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. These operations are applied to each block of plaintext to create the ciphertext.

Final round: The final round consists of three operations: SubBytes, ShiftRows, and AddRoundKey. MixColumns is not applied in this round.

Here is an example of how encryption and decryption would work using AES:

4.1.1 Encryption

Suppose we want to encrypt the plaintext “Hello, world!” using AES with a 256-bit key. We’ll use the key “this is my secret key” for this example.

Key Expansion: The 256-bit key is expanded to create a key schedule.

Initial Round: The first round consists of a key addition step, where each byte of the plaintext is XORed with a byte of the round key.

Plaintext: 48 65 6c 6c 6f 2c 20 77 6f 72 6c 64 21.

Round Key: 74 68 69 73 69 73 6d 79 73 65 63 72 65 74 6b 65.

Result: 3c 0f 1b 15 1a 7f 4c 58 0e 0e 0f 70 7c 1e 51 7f.

Main Rounds: The next 13 rounds consist of four operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

Round 1:

SubBytes: 26 7c 3b 9c 04 3d d3 e5 33 8d 9e e3 8c 75 55 6b 65.

ShiftRows: 26 d3 9e 67 04 8d 55 e5 33 75 3b e3 8c 7c 3d 9c.

MixColumns: 7e d2 93 a4 5f fc 4b fa 4e d2 91 66 69 06 9b 25.

AddRoundKey: 96 56 a9 c1 f7 97 8e d8 63 a7 fc 64 e2 68 b4 99.

Round 2:

SubBytes: 59 66 f9 9a 25 c8 5f e6 c9 52 03 e8 a9 16 d7 4a 6e.

ShiftRows: 59 c8 03 6e 25 52 d7 e6 c9 16 f9 e8 a9 66 5f 9a 4a.

MixColumns: 19 d7 5d 6b 89 87 97 18 68 ab 24 f5 d5 be b2 73.

AddRoundKey: ec d9 46 1e d2 9f f5 d0 bd e1 17 8f aa 3b 60 5e.

...

Round 14:

SubBytes: d4 bf 5d 30 e0 b5 ff 8d 30 88 c8 96 8a 89 7c 54.

ShiftRows: d4 89 c8 54 e0 b5 7c 8d 30 bf 96 30 8a 88 ff 5d.

AddRoundKey: 19 d6 0e d4 1b 4a 07 b3 8f e8 32 9d 3a 27 e4 29.

Ciphertext: 19 d6 0e d4 1b 4a 07 b3 8f e8 32 9d 3a 27 e4 29.

4.1.2 Decryption

Now, let’s decrypt the ciphertext “19 d6 0e d4 1b 4a 07 b3 8f e8 32 9d 3a 27 e4 29” using the same 256-bit key.

Key Expansion: The 256-bit key is expanded to create a key schedule.

Initial Round: The first round consists of a key addition step, where each byte of the ciphertext is XORed with a byte of the round key.

Ciphertext: 19 d6 0e d4 1b 4a 07 b3 8f e8 32 9d 3a 27 e4 29.

Round Key: 74 68 69 73 69 73 6d 79 73 65 63 72 65 74 6b 65.

Result: 6d bc 11 68 67 6a 34 b5 85 0f 6e c6 7a a3 0f 5d.

Main Rounds: The next 13 rounds consist of four operations: InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey.

Round 1:

InvShiftRows: 6d a3 0f c6 67 0f 5d 68 85 6a 34 b5 6e bc 11 7a.

InvSubBytes: 25 0c 13 91 5b f2 85 44 15 8e 02 c2 10 d7 22 45.

AddRoundKey: 51 83 4a 9f 62 68 f0 b8 28 14 7c 37 8e aa 39 84.

Round 2:

InvShiftRows: 51 68 39 84 62 14 f0 9f 28 83 7c 37 8e 68 22 b8.

InvSubBytes: 33 3e 85 92 5f 22 f9 51 4a 5e 1f 84 b8 18 3a 1c.

AddRoundKey: 18 c9 fe dd c9 6f 69 e8 11 85 72 33 61 c9 68 95.

Round 14:

InvShiftRows: 47 40 a5 1d 69 c1 d5 c5 e9 29 24 9c 7b 6b 4b 77.

AddRoundKey: d4 bf 5d 30 e0 b5 ff 8d 30 88 c8 96 8a 89 7c 54.

Plaintext: 48 65 6c 6c 6f 2c 20 77 6f 72 6c 64 21.

The decrypted plaintext is “Hello, world!”.

4.2 The dynamic XOR algorithm

The dynamic XOR algorithm is a technique used in image steganography to hide information within an image. It involves modifying the pixel values of an image by performing an XOR operation with a dynamic key generated from the message to be concealed. The algorithm ensures that the changes made to the pixel values are imperceptible to the human eye.

Here is an example of the dynamic XOR algorithm for image steganography:

Let us consider a grayscale image with pixel values ranging from 0 to 255. We want to hide the binary message “10,110” within the image. The algorithm works as follows:

Convert the message “10,110” into individual bits:

1 0 1 1 0

Generate a dynamic key based on the message length. In this example, the key will be a repeating pattern of “0101” to match the length of the message.

Iterate through each pixel of the image:

- Retrieve the next bit from the message and the corresponding bit from the dynamic key.
- Perform an XOR operation between the pixel value and the key bit.
- Update the pixel value with the result of the XOR operation.

Repeat steps a to c for each pixel until all the message bits have been hidden.

Let us say we have the following grayscale image with pixel values:

[100, 150, 75, 200, 50]

And the dynamic key generated based on the message length is:

0101

Applying the dynamic XOR algorithm, we get the following modifications:

Pixel 1: 100 XOR 0 = 100.

Pixel 2: 150 XOR 1 = 151.

Pixel 3: 75 XOR 0 = 75.

Pixel 4: 200 XOR 1 = 201.

Pixel 5: 50 XOR 0 = 50.

The resulting modified pixel values become:

[100, 151, 75, 201, 50]

By applying the dynamic XOR algorithm, we have hidden the message “10,110” within the image.

4.3 Dynamic XOR algorithm combined with AES crypto algorithm

The encryption and decryption process of the dynamic XOR algorithm combined with AES crypto algorithm for image steganography involves two main steps:

4.3.1 Encryption

Convert the message to be hidden into binary representation.

Generate a dynamic key based on the length of the binary message.

Iterate through each pixel of the image.

Retrieve the next bit from the binary message and the corresponding bit from the dynamic key.

Perform an XOR operation between the pixel value and the key bit.

Update the pixel value with the result of the XOR operation.

Encrypt the modified image using the AES crypto algorithm with a secret key.

Output the encrypted image.

4.3.2 Decryption

Decrypt the encrypted image using the AES crypto algorithm and the secret key.

Retrieve the pixel values from the decrypted image.

Generate the dynamic key based on the length of the hidden message.

Iterate through each pixel of the image.

Retrieve the next bit from the dynamic key.

Perform an XOR operation between the pixel value and the key bit.

Update the pixel value with the result of the XOR operation.

Retrieve the hidden binary message from the modified pixel values.

Output the decrypted binary message.

Example Here is an example illustrating the encryption and decryption process of the dynamic XOR algorithm combined with AES crypto algorithm for image steganography:

4.3.3 Encryption

Message to be hidden: “Hello World”.

Convert the message to binary: “010010000110010101101100011011000110111100100000010101110110111101100100110110001100100”.

Generate dynamic key: “1010”.

Iterate through each pixel of the image and perform XOR operation:

Pixel 1: Original value = 150, binary value = “10,010,110”, XOR with first bit of the key (1), Result = 151.

Pixel 2: Original value = 200, binary value = “11,001,000”, XOR with second bit of the key (0), Result = 200.

Pixel 3: Original value = 100, binary value = “01100100”, XOR with third bit of the key (1), Result = 101.

Pixel 4: Original value = 50, binary value = “00110010”, XOR with fourth bit of the key (0), Result = 50.

(Repeat this process for all pixels).

Encrypt the modified image using the AES crypto algorithm with a secret key.

Output the encrypted image.

4.3.4 Decryption

Decrypt the encrypted image using the AES crypto algorithm and the secret key.

Retrieve the pixel values from the decrypted image.

Generate dynamic key: “1010”.

Iterate through each pixel of the image and perform XOR operation:

Pixel 1: Original value = 151, XOR with first bit of the key (1), Result = 150.

Pixel 2: Original value = 200, XOR with second bit of the key (0), Result = 200.

Pixel 3: Original value = 101, XOR with third bit of the key (1), Result = 100.

Pixel 4: Original value = 50, XOR with fourth bit of the key (0), Result = 50.

(Repeat this process for all pixels).

Retrieve the hidden binary message from the modified pixel values: “010010000110010101101100011011000110111100100000010101110110111101100100110110001100100”.

Convert the binary message back to text: “Hello World”.

Output the decrypted message.

4.4 Entropy analysis

Entropy is a statistical test used in image encryption to quantify the level of unpredictability and randomness in a cipher image. It provides valuable insights into the effectiveness of the encryption process, with higher entropy values indicating a greater level of obfuscation.

$$\text{ENTROPY}(I) = - \sum_{i=1}^{2^8} P(I_i) \log_b P(I_i) \quad (1)$$

ENTROPY(I) presents the entropy of the i -th stego image, while the corresponding intensity and the probability of intensity value I_i are given by I and $P(I_i)$, respectively.

4.5 MSE and PSNR Metrics

The peak signal-to-noise ratio (PSNR) is a metric used to evaluate the similarity or closeness between two images, indicating how well they match each other. On the other hand, the mean squared error (MSE) measures the difference or distortion between the pixel values of the two images. These metrics are widely utilized and highly popular in various image processing applications due to their simplicity and computational efficiency [67]. The mathematical definitions of MSE and PSNR are as follows, according to references [67, 68]:

PSNR (peak signal-to-noise ratio):

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{(\text{MAX}^2)}{\text{MSE}} \right) \quad (2)$$

MSE (Mean Squared Error):

$$\text{MSE} = \sum ((I1[i, j] - I2[i, j])^2) / (M \times N) \quad (3)$$

In the above equations, MAX represents the maximum pixel value of the image (e.g. 255 for an 8-bit image), MSE denotes the mean squared error between the corresponding pixels of the two images, $I1[i, j]$ and $I2[i, j]$ represent the pixel values at coordinates (i, j) in the two images, and M and N indicate the dimensions of the images in terms of width and height.

These metrics provide objective measurements to assess the quality and fidelity of image processing algorithms, such as image compression, denoising, or steganography. Higher PSNR values indicate a higher similarity or better match between the images, while lower MSE values indicate lesser difference or distortion between the images. The image quality is considered to be the best when the mean squared error (MSE) value is extremely small or close to zero. This is because a small MSE indicates that the difference between the original image and the reconstructed image is negligible or insignificant. In other words, the reconstructed image closely resembles the original image, resulting in higher image quality.

4.6 NPCR

Normalized Pixel Change Rate (NPCR) is a metric used to evaluate the quality and effectiveness of image steganography techniques. It measures the percentage of pixels that change between the original image and the stego image when a single bit is modified in the secret message.

The equation for calculating NPCR is as follows:

$$\text{NPCR} = \text{NPCR} = \frac{N_{\text{diff}}}{N_{\text{total}}} \times 100 \quad (4)$$

where

NPCR is the normalized pixel change rate, N_{diff} is the number of pixels that differ between the original and stego images, N_{total} is the total number of pixels in the image.

By comparing the number of differing pixels to the total number of pixels, NPCR provides a quantifiable measure of the level of pixel changes caused by embedding the secret message. A higher NPCR value indicates a greater level of pixel variation, which is generally desired for a successful steganographic technique as it helps to conceal the presence of the hidden information.

4.7 Software

The system used for the research study was a Dell-Inspiron laptop equipped with an Intel i5 processor. The Dell-Inspiron is a reliable and high-performance laptop that provided the necessary computing power for the research tasks. The Intel i5 processor ensured efficient processing capabilities, enabling smooth execution of complex algorithms and

simulations. This system was chosen for its reliability, performance, and compatibility with the research requirements.

In addition to the local system, the research also utilized the Google Colab platform for Python coding and simulation purposes. Google Colab offers a cloud-based environment that provides the necessary computational resources to execute code and perform simulations. By leveraging the power of Google's infrastructure, researchers can access high-performance computing capabilities without the need for expensive hardware investments. The Python programming language was used for coding and developing simulation models, and the Google Colab platform facilitated seamless collaboration and execution of the research code.

The combination of the Dell-Inspiron system and the Google Colab platform provided a robust and efficient simulation environment for the research study. The system's specifications ensured smooth performance and reliable execution of the research tasks, while the Google Colab platform enhanced the computational capabilities and facilitated collaborative coding and simulation.

5 Results and discussions

5.1 Histogram analysis

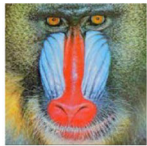
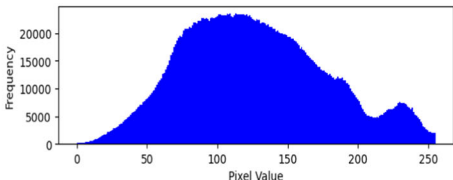
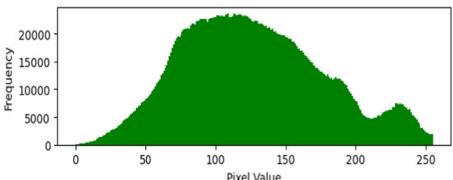
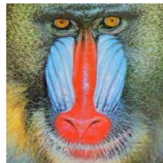

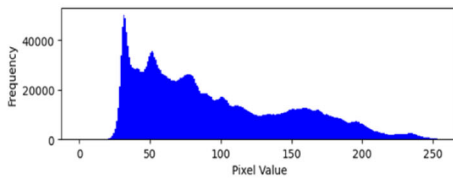
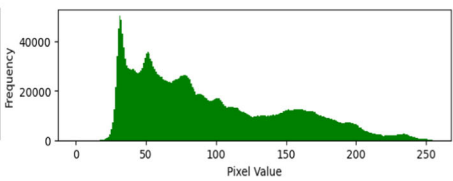


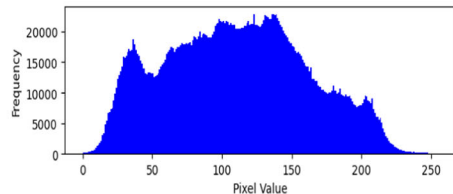
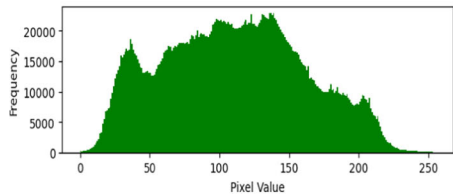


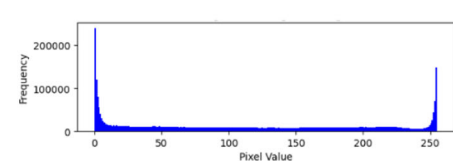
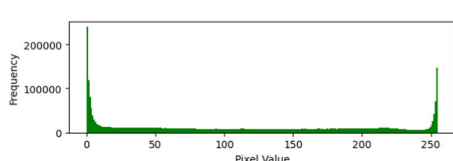

Histogram analysis is a crucial aspect of image steganography for transmitting secret text. It allows us to gain insights into the pixel value distribution and frequency in the original and stego images. By comparing the histograms, we can detect significant variations that suggest the presence of hidden information. When there is a higher frequency difference, it indicates noticeable alterations in pixel values, implying potential steganographic embedding. Conversely, a lower frequency difference signifies a closer resemblance between the original and stego images, making it harder to visually detect the hidden information. In Table 1, the histogram analysis demonstrates minimal differences between the original and stego images, indicating the difficulty in identifying pixel discrepancies and making it challenging for observers to discern the presence of a secret message. Table 2 shows the different parameters for different picture.

5.2 The impact of the secret message size on the algorithm's performance

In this analysis three different messages with various size have been used to check the algorithm's performance. The two different messages are.

- (i) 500B
- (ii) 1kB
- (iii) 2kB

Table 1 Histogram analysis

Image dimension (1024×1024)	Histogram of original image	Histogram of stego image	Stego Image (dimension 1024×1024)
			
			
			
			

To quantify the performance of the proposed method, various analytical parameters are considered, including peak signal-to-noise ratio (PSNR), mean square error (MSE), normalized pixel change rate (NPCR), and entropy. These metrics provide objective measures to assess the quality, security, and efficiency of the proposed algorithm.

5.2.1 Peak signal-to-noise ratio (PSNR) analysis

In this study, the PSNR performance of the proposed model was evaluated using different text payloads. Three different payload sizes, namely 500 B, 1 kB, and 2 kB, were used for embedding in all test cases. The proposed model aimed to achieve higher PSNR values while considering the adjustment metrics. The obtained PSNR values for various cases are presented in Table 3. The study analysed the efficacy of the proposed model by comparing the PSNR values for different image types and text sizes. The results indicated that using a 500 B secret message resulted in a notably high

PSNR value of 80.163. However, as the secret message size increased to 2 KB, the corresponding PSNR value decreased to 74.19, suggesting a trade-off between text size and PSNR performance.

5.2.2 MSE analysis

MSE (mean squared error) serves as a prominent metric within image steganography research, measuring the average squared disparity between the original image and the steganographic counterpart. A lower MSE value signifies improved quality and heightened imperceptibility of the steganographic image, while a higher MSE value indicates more noticeable distortion and compromised secrecy of the hidden message. Consequently, minimizing MSE is of paramount importance to achieve effective and visually inconspicuous image steganography. The obtained MSE values for various cases are presented in Table 4. Notably,

Table 2 Analysis of different parameters





Picture	PSNR (dB)	Entropy (dB)	MSE	NPCR (%)
	76.61	7.45	0.0014	99.575
	76.62	7.636	0.0014	99.57
	76.6	7.415	0.00141	99.574
	76.61	7.66	0.0014	99.57

Table 3 PSNR (dB) performance

Picture	Payload size		
	500 B	1 kB	2 kB
Lena	80.17	76.61	74.2
Barbara	80.16	76.62	74.17
Pepper	80.165	76.6	74.19
Baboon	80.16	76.61	74.2
Cumulative average	80.16375	76.61	74.19

Table 4 MSE performance

Picture	Payload size		
	500 B	1 kB	2 kB
Lena	0.0006	0.0014	0.0024
Barbara	0.00063	0.0014	0.0024
Pepper	0.000625	0.00141	0.0025
Baboon	0.00063	0.0014	0.0025
Cumulative average	0.000621	0.001403	0.00245

findings from this study reveal that employing a secret message size of 500B resulted in a notably low MSE value of 0.000621, whereas an increase in the secret message size led to a rise in MSE. For instance, when the secret message size was extended to 2 KB, the corresponding MSE value escalated to 0.00245.

5.2.3 NPCR analysis

The NPCR (normalized pixel change rate) is of great importance in the field of image steganography research. A higher

Table 5 NPCR (%) performance

Picture	Payload size		
	500 B	1 kB	2 kB
Lena	99.81	99.575	99.26
Barbara	99.81	99.57	99.258
Pepper	99.81	99.574	99.258
Baboon	99.81	99.57	99.258
Cumulative average	99.81	99.57225	99.2585

Table 6 Average entropy (dB) performance

Picture	Payload size		
	500 B	1 kB	2 kB
Lena	7.45	7.45	7.45
Barbara	7.64	7.636	7.636
Pepper	7.42	7.415	7.415
Baboon	7.66	7.66	7.66
Cumulative average	7.5425	7.54025	7.54025

NPCR value signifies that even a small modification in the original image will result in significant changes in the stego image, making it more difficult to detect any hidden information. Conversely, a lower NPCR value suggests that alterations in the original image have minimal impact on the stego image, potentially making it easier to uncover concealed data. NPCR serves as a quantitative metric to assess the effectiveness and security of steganographic techniques, with higher values indicating stronger concealment capabilities. The obtained NPCR values for various cases are presented in Table 5. Notably, a study demonstrated that utilizing a secret message size of 500 B resulted in an exceptionally high NPCR value of 99.81%, while increasing the secret message size led to a decrease in NPCR. For instance, when the secret message size was expanded to 2 KB, the corresponding NPCR value decreased to 99.258%.

5.2.4 Entropy analysis

Entropy serves a vital role in image steganography research as it quantifies the level of randomness or unpredictability within an image. The optimal entropy value is typically around 8 dB, and it is essential to maintain the entropy close to this ideal value. The obtained entropy values for various cases are presented in Table 6. A study observed that the cumulative average entropy for various picture secret message sizes ranged from 7.542 to 7.54 dB, indicating a remarkable proximity to the ideal entropy value.

5.3 The impact of the stego image dimension size on the algorithm's performance

In this particular section of study, a fixed payload text size of 500 B is used. However, the dimension of the stego image is varied to evaluate the performance of the proposed algorithm. By changing the dimensions of the stego image, the researchers aimed to assess how the algorithm performs under different image sizes and to analyse its effectiveness in concealing the fixed payload text.

5.3.1 PSNR analysis

PSNR (peak signal-to-noise ratio) plays a critical role in image steganography research. Higher PSNR values indicate superior image quality post-steganography, ensuring minimal visible distortion to the human eye. Conversely, lower PSNR values imply increased distortion, potentially compromising hidden data concealment. Researchers aim to maximize PSNR to enhance steganographic effectiveness and uphold visual fidelity for secure communication. In this study, various images were used to transmit secret messages and store them at different dimension. The obtained PSNR values for various cases are presented in Table 7. Findings revealed that average PSNR varied with stego image size. When the stego image dimension is high (1024×1024), the PSNR reached 80.16 dB, but decreased to 62.11 dB for a smaller size (128×128).

5.3.2 Entropy analysis

Entropy plays a crucial role in image steganography research as it measures the degree of randomness or unpredictability within an image. The desired entropy value is typically around 8 dB, and it is vital to maintain the entropy close to this optimal level. The obtained entropy values for various cases are presented in Table 8. In a study, the cumulative average entropy of different pictures saved as stego images exhibited values ranging from 7.54 to 7.52 dB, indicating a remarkable proximity to the ideal entropy value.

5.3.3 NPCR analysis

The normalized pixel change rate (NPCR) holds significant importance in image steganography research. A higher NPCR value signifies that even slight modifications in the original image yield substantial changes in the stego image, enhancing the concealment of hidden information. Conversely, a lower NPCR value indicates that alterations in the original image have minimal impact on the stego image, potentially making detection easier. NPCR serves as a quantitative metric to evaluate steganographic techniques, with higher values indicating stronger concealment capabilities.

The obtained NPCR values for various cases are presented in Table 9. Notably, a study demonstrated that a stego image size of (1024×1024) achieved an exceptionally high NPCR value of 99.81%, while reducing the stego image size to (128×128) resulted in a decrease to 87.98% NPCR.

5.3.4 MSE analysis

MSE (mean squared error) plays a significant role in image steganography research, quantifying the average squared difference between the original and steganographic images. A lower MSE indicates enhanced quality and imperceptibility, preserving the secrecy of the hidden message. Conversely, a higher MSE implies more noticeable distortion and compromised concealment. The obtained MSE values for various cases are presented in Table 10. Notably, a study demonstrated that a stego image size of (1024×1024) yielded an impressively low MSE value of 0.000621, whereas reducing the stego image size to (128×128) resulted in an elevated MSE of 0.04.

5.3.5 SSIM and Q-index analysis

Quality index (Q) and structural similarity index measure (SSIM).

The SSIM determines how similar two photographs are to one another. Its value ranges from 0 to 1. Equation (13) is the basis for the estimation. The means and variances for the photographs in this case are A_{mn} , A_{mean} , B_{mn} , and B_{mean} .

$$SSIM = \frac{\sum_{m=1}^J \sum_{n=1}^K (A_{mn} - A_{mean})(B_{mn} - B_{mean})}{\sqrt{\sum_{m=1}^J \sum_{n=1}^K ((A_{mn} - A_{mean})^2) \sum_{n=1}^k \sum_{n=1}^k (B_{mn} - B_{mean})^2}} \quad (5)$$

The quality index (Q) is one of the metrics that finds the similarity between the cover.

and stego images. The highest value for Q is one. This can be achieved when two images are entirely equal. Q can be obtained using below equation:

$$Q = \frac{4 \sigma_{xy} \bar{a} \bar{b}}{(\sigma_x^2 + \sigma_y^2)[(\bar{a})^2 + (\bar{b})^2]} \quad (6)$$

Here, σ_x and σ_y are the standard deviations, and a and b denote the means for the individual images.

Tables 11 and 12 present the SSIM (structural similarity index) and Q-index performance metrics for stego images generated from different original pictures (Lena, Barbara, Pepper, and Baboon) at various saving dimensions (1024×1024 , 512×512 , 256×256 , and 128×128). Generally,

Table 7 PSNR (dB) performance

Picture	Stego image saving dimension			
	(1024 × 1024)	(512 × 512)	(256 × 256)	(128 × 128)
Lena	80.17	74.14	68.12	62.10
Barbara	80.16	74.144	68.12	62.103
Pepper	80.165	74.144	68.12	62.10
Baboon	80.16	74.14	68.12	62.12
Cumulative average	80.16375	74.142	68.12	62.10575

Table 8 Average entropy (dB) performance

Picture	Stego image saving dimension			
	(1024 × 1024)	(512 × 512)	(256 × 256)	(128 × 128)
Lena	7.45	7.44	7.42	7.39
Barbara	7.64	7.636	7.63	7.61
Pepper	7.42	7.43	7.45	7.466
Baboon	7.66	7.66	7.648	7.60
Cumulative average	7.5425	7.5415	7.537	7.5165

Table 9 NPCR (%) performance

Picture	Stego image saving dimension			
	(1024 × 1024)	(512 × 512)	(256 × 256)	(128 × 128)
Lena	99.81	99.248	96.995	87.98
Barbara	99.81	99.249	96.99	87.98
Pepper	99.81	99.247	96.99	87.98
Baboon	99.81	99.248	96.995	87.98
Cumulative average	99.81	99.248	96.9925	87.98

higher SSIM values indicate better similarity between the stego image and the original, while higher Q-index values indicate better visual quality. From the analysis, it is evident that as the saving dimension decreases, both SSIM and Q-index tend to decrease. This suggests that reducing the image dimensions leads to a loss of visual quality and similarity to the original image. However, even at lower dimensions (128 × 128), the SSIM values remain relatively high, indicating a

reasonable preservation of structural information. The cumulative average SSIM and Q-index also demonstrate the overall performance across all images and dimensions. These findings highlight the trade-off between image resolution and visual fidelity, emphasizing the importance of selecting an appropriate balance to achieve acceptable steganographic results. Additionally, these results underscore the potential

Table 10 MSE performance

Picture	Stego image saving dimension			
	(1024 × 1024)	(512 × 512)	(256 × 256)	(128 × 128)
Lena	0.0006	0.0025	0.01	0.04
Barbara	0.00063	0.0025	0.01	0.04
Pepper	0.000625	0.0025	0.01	0.04
Baboon	0.00063	0.0025	0.01	0.04
Cumulative average	0.000621	0.0025	0.01	0.04

Table 11 SSIM performance

Picture	Stego image saving dimension			
	(1024 × 1024)	(512 × 512)	(256 × 256)	(128 × 128)
Lena	0.99	0.994	0.989	0.989
Barbara	1	0.999	0.997	0.995
Pepper	.998	0.994	0.991	.989
Baboon	0.99	0.997	0.994	0.992
Cumulative average	0.99	0.99	0.988	0.988

Table 12 Q-index performance

Picture	Stego image saving dimension			
	(1024 × 1024)	(512 × 512)	(256 × 256)	(128 × 128)
Lena	93.625	86.65	82.31	74.077
Barbara	92.895	86.077	82.256	74.126
Pepper	93.264	86.245	81.956	74.056
Baboon	92.954	86.587	82.124	74.215
Cumulative average	93.657	86.354	82.098	73.898

utility of steganography techniques in scenarios where maintaining high-resolution images may not be critical, such as certain covert communication applications, where reducing image size could aid in efficient transmission or concealment.

6 Performance comparison with recent encryption algorithms

In this section, we compare the average performance of the proposed model with other existing methods. It is important to note that the cover image data and payload may differ between the reference systems and the proposed model. Therefore, we consider the average performance of both the reference methods and the proposed model for a fair comparative analysis. To evaluate the effectiveness of the proposed encryption algorithm, we compare it with recently developed techniques, as presented in Table 13. We assess the performance using commonly used encryption metrics such as PSNR, NPCR, and entropy. These metrics allow us to compare the proposed algorithm with other methods effectively.

The results indicate that the proposed encryption scheme outperforms most of the evaluation metrics. It demonstrates favourable outcomes comparable to those of recently developed encryption methods in terms of PSNR, NPCR, and entropy. These findings suggest that the proposed algorithm holds great potential in the field of steganography.

7 Conclusion

The proposed image steganography method, combining the dynamic 8-bit XOR algorithm and the AES crypto algorithm, exhibits promising results in terms of concealing confidential data within images while maintaining information security. The encryption step enhances the overall security, and the dynamic XOR algorithm adds an additional layer of complexity, making it challenging for adversaries to detect hidden messages. The evaluation metrics, including PSNR, MSE, NPCR, and entropy, demonstrate the algorithm's effectiveness, security, and efficiency. The histogram analysis reveals minimal differences between original and stego images, emphasizing the difficulty in visually detecting concealed information. The impact of secret message size on algorithm performance illustrates a trade-off between text size and PSNR, where larger messages lead to lower PSNR values. Additionally, the influence of stego image dimensions indicates that higher dimensions correlate with higher PSNR values, while entropy values remain close to the ideal 8 dB. Comparative analysis with recent encryption algorithms indicates that the proposed method outperforms existing works in terms of PSNR, NPCR, and entropy. These results suggest the algorithm's potential in the field of steganography. Implementation of the proposed algorithm showcases promising outcomes, surpassing existing methods in PSNR, NPCR, and entropy metrics. The study provides a foundation for further exploration in real-world scenarios and against advanced steganalysis techniques. Future research avenues include scalability testing for larger images, optimization

Table 13 Performance comparison

Parameters	Proposed system value				Existing established works	
	Dimension	Payload			Existing results	Ref
		500 B	1 kB	2 kB		
PSNR (dB)	(1024 × 1024)	80.16	76.61	74.19	43.23 dB	[69]
					41.60 dB	[70]
					38.85 dB	[71]
					46.76 dB	[72]
					42.90 dB	[73]
					40.27 dB	[74]
					42.50 dB	[75]
					42.23 dB	[76]
					45.22 dB	[77]
NPCR (%)	(1024 × 1024)	99.81	99.57	99.26	48.00 dB	[78]
					99.6127%	[79]
					99.5987%	[80]
					99.6200%	[81]
					99.6100%	[82]
					99.5865%	[83]
					99.5893%	[84]
					99.6239%	[85]
					99.6059%	[86]
Entropy (dB)	(1024 × 1024)	7.542	7.54	7.54	99.5743%	[87]
					99.6269%	[88]
					99.6100%	[89]
					7.9024 dB	[84]
					7.9991 dB	[85]
					7.9992 dB	[86]
					7.9971 dB	[87]
					7.9985 dB	[88]
					7.9969 dB	[89]

for faster processing, and integration with emerging encryption standards. Additionally, exploring adaptive techniques to dynamically adjust hiding strategies based on image characteristics could enhance concealment effectiveness. Overall, the proposed approach holds significant potential in securing confidential data within images while maintaining visual integrity, paving the way for advanced applications in secure communication and data protection.

Author contributions D & S did the research work . A prepared paper work and supported in results . D prepared Literature survey , S prepared Introduction in paper & A prepared tables.

Declarations

Competing interests The authors declare no competing interests.

References

1. IJ Kadhim P Premaratne PJ Vial B Halloran 2019 Comprehensive survey of image steganography: techniques, evaluations, and trends in future research *Neurocomputing* 335 299 326
2. D Artz 2001 Digital steganography: hiding data within data *IEEE Internet Comput.* 5 3 75 80
3. AK Sahu G Swain 2019 High fidelity based reversible data hiding using modified LSB matching and pixel difference *J. King Saud Univ. Comput. Inf. Sci.* <https://doi.org/10.1016/j.jksuci.2019.07.004>
4. H Noda M Niimi E Kawaguchi 2006 High-performance JPEG steganography using quantization index modulation in DCT domain *Pattern Recognit. Lett.* 27 5 455 461
5. A Sahu G Swain 2019 Dual stego-imaging based reversible data hiding using improved LSB matching *Int. J. Intell. Eng. Syst.* 12 5 63 73

6. H Sajedi M Jamzad 2010 BSS: Boosted steganography scheme with cover image preprocessing *Expert Syst. Appl.* 37 12 7703 7710
7. W-J Chen C-C Chang THN Le 2010 High payload steganography mechanism using hybrid edge detector *Expert Syst. Appl.* 37 4 3292 3301
8. A Ioannidou ST Halkidis G Stephanides 2012 A novel technique for image steganography based on a high payload method and edge detection *Expert Syst. Appl.* 39 14 11517 11524
9. D-C Wu W-H Tsai 2003 A steganographic method for images by pixel-value differencing *Pattern Recognit. Lett.* 24 9–10 1613 1626
10. C-H Yang C-Y Weng S-J Wang H-M Sun 2008 Adaptive data hiding in edge areas of images with spatial LSB domain systems *IEEE Trans. Inf. Forensics Secur.* 3 3 488 497
11. Naor, M., Shamir, A.: Visual cryptography II: improving the contrast via the cover base, in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer, 1996, pp. 197–202. [Online]. Available: https://link.springer.com/chapter/https://doi.org/10.1007/3-540-62494-5_18#citeas
12. A Shamir 1979 How to share a secret *Commun. ACM* 22 11 612 613
13. C-K Chan LM Cheng 2004 Hiding data in images by simple LSB substitution *Pattern Recognit.* 37 3 469 474
14. M Hussain AWA Wahab YIB Idris ATS Ho K-H Jung 2018 Image steganography in spatial domain: a survey *Signal Process Image Commun.* 65 46 66
15. A Khamrui JK Mandal 2013 A genetic algorithm based steganography using discrete cosine transformation (GASDCT) *Procedia Technol.* 10 105 111
16. SK Bandyopadhyay TU Paul A Raychoudhury 2010 A novel steganographic technique based on 3D-DCT approach *Comput. Inf. Sci.* 3 4 229
17. B Kaur A Kaur J Singh 2011 Steganographic approach for hiding image in DCT domain *Int. J. Adv. Eng. Technol.* 1 3 72
18. P-Y Chen H-J Lin 2006 A DWT based approach for image steganography *Int. J. Appl. Sci. Eng.* 4 3 275 290
19. W-Y Chen 2008 Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques *Appl. Math. Comput.* 196 1 40 54
20. AK Sahu G Swain 2020 Reversible image steganography using dual layer LSB matching *Sens. Imag.* 21 1 1
21. M Li S Yu Y Zheng K Ren W Lou 2013 Scalable and secure sharing of personal health records in cloud computing using attribute based encryption *IEEE Trans. Parallel Distrib. Syst.* 24 1 131 143
22. H Sajedi 2018 Applications of data hiding techniques in medical and health care systems: a survey *Netw. Model. Anal. Health Inform. Bioinf.* 7 1 6
23. S Arunkumar V Subramaniaswamy V Vijayakumar N Chilamkurti R Logesh 2019 SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images *Measurement* 139 426 437
24. RJ Anderson FAP Petitcolas 1998 On the limits of steganography *IEEE J. Sel. Areas Commun.* 16 4 474 481
25. X Liao J Yin S Guo X Li AK Sangaiah 2018 Medical JPEG image steganography based on preserving inter-block dependencies *Comput. Electr. Eng.* 67 320 329
26. M Sajjad K Muhammad SW Baik S Rho Z Jan S-S Yeo I Mehmood 2017 Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices *Multimed. Tools Appl.* 76 3 3519 3536
27. N Alsaidi M Alshareef A Alsulami M Alsafri A Aljahdali 2020 Digital steganography in computer forensics *Int. J. Comput. Sci. Inf. Secur.* 18 5 54 61
28. M Elhoseny G Ramírez-González OM Abu-Elnasr SA Shawkat N Arunkumar A Farouk 2018 Secure medical data transmission model for IoT-based healthcare systems *IEEE Access* 6 20596 20608
29. Mansor, N.K., Asraf, S.M.H., Idrus, S.Z.S.: Steganographic on pixel value differencing in iris biometric, *J. Phys., Conf. Ser.*, vol. 1529, no. 3, Apr. 2020, Art. no. 032078.
30. A Shehab M Elhoseny K Muhammad AK Sangaiah P Yang H Huang G Hou 2018 Secure and robust fragile watermarking scheme for medical images *IEEE Access* 6 10269 10278
31. H-Y Lee 2019 Adaptive reversible watermarking for authentication and privacy protection of medical records *Multimed. Tools Appl.* 78 14 19663 19680
32. JA Kaw NA Loan SA Parah K Muhammad JA Sheikh GM Bhat 2019 A reversible and secure patient information hiding system for IoT driven e-health *Int. J. Inf. Manage.* 45 262 275
33. SA Parah F Ahad JA Sheikh NA Loan GM Bhat 2017 A new reversible and high capacity data hiding technique for e-healthcare applications *Multimed. Tools Appl.* 76 3 3943 3975
34. K Rabah 2004 Steganography—the art of hiding data *Inf. Technol. J.* 3 3 245 269
35. AK Sahu G Swain 2019 An optimal information hiding approach based on pixel value differencing and modulus function *Wireless Pers. Commun.* 108 1 159 174
36. AK Sahu G Swain 2019 A novel n-rightmost bit replacement image steganography technique *3D Res.* 10 1 2
37. AK Sahu G Swain 2018 Pixel overlapping image steganography using PVD and modulus function *3D Res.* 9 3 40
38. AK Sahu G Swain ES Babu 2018 Digital image steganography using bit flipping *Cybern. Inf. Technol.* 18 1 69 80
39. R Wazirali Z Chachzo 2016 Hyper edge detection with clustering for data hiding *J. Inf. Hiding Multimedia Signal Process.* 7 1 1 10
40. Z Wang Z Qian X Zhang M Yang D Ye 2018 On improving distortion functions for JPEG steganography *IEEE Access* 6 74917 74930
41. F Li K Wu X Zhang J Yu J Lei M Wen 2018 Robust batch steganography in social networks with non-uniform payload and data decomposition *IEEE Access* 6 29912 29925
42. J Tao S Li X Zhang Z Wang 2019 Towards robust image steganography *IEEE Trans. Circuits Syst. Video Technol.* 29 2 594 600007A
43. S Li X Zhang 2019 Toward construction-based data hiding: From secrets to fingerprint images *IEEE Trans. Image Process* 28 3 1482 1497
44. Madhu, D., Vasuhi, S.: Image steganography: 2-Bit XOR algorithm used in YCbCr color model with crypto-algorithm, 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), 2020.
45. K Patel S Utareja H Gupta 2013 Information hiding using least significant bit steganography and blowfish algorithm *Int. J. Comput. Appl.* 63 24 28
46. M Jain SK Lenka SK Vasistha 2016 Adaptive circular queue image steganography with RSA cryptosystem *Perspect. Sci.* 8 417 420
47. R Rajkumar A Vasuki 2018 Reversible and robust image watermarking based on histogram shifting *Clust. Comput.* 22 12313 12323
48. T Zong Y Xiang I Natgunanathan S Guo W Zhou G Beliakov 2014 Robust histogram shape-based technique for image watermarking *IEEE Trans. Circuits Syst. Video Technol.* 25 717 729
49. AK Rai N Kumar R Kumar H Om S Chand KH Jung 2021 Intra-block correlation based reversible data hiding in encrypted images using parametric binary tree labeling *Symmetry* 13 1072
50. S Xu J-H Horng C-C Chang 2021 Reversible data hiding scheme based on VQ prediction and adaptive parametric binary tree labeling for encrypted images *IEEE Access* 9 55191 55204
51. F Aziz T Ahmad AH Malik MI Uddin S Ahmad M Sharaf 2020 Reversible data hiding techniques with high message embedding capacity in images *PLoS ONE* 15 e0231602

52. AK Sahu 2021 A logistic map based blind and fragile watermarking for tamper detection and localization in images J. Ambient. Intell. Humaniz. Comput. 13 3869 3881
53. Volume 2: Aerials. Available online: <http://sipi.usc.edu/database/database.php?volume=aerials&image=5#top> (accessed on 19 August 2022).
54. S Ayyappan C Lakshmi 2018 A review on reversible data hiding techniques Int. J. Appl. Eng. Res. 13 2857 2864
55. AK Sahu M Hassaballah RS Rao G Suresh 2022 Logistic-map based fragile image watermarking scheme for tamper detection and localization Multimed. Tools Appl. 82 1 32
56. J Wang N Mao X Chen J Ni C Wang Y Shi 2019 Multiple histograms based reversible data hiding by using FCM clustering Signal Process 159 193 203
57. AK Sahu M Sahu P Patro G Sahu SR Nayak 2022 Dual image-based reversible fragile watermarking scheme for tamper detection and localization Pattern Anal. Appl. 26 1 20
58. K Zhou Y Ding W Bi 2020 High-capacity PVO-based reversible data hiding scheme using changeable step size Multimed. Tools Appl. 80 1123 1141
59. Z Pan E Gao 2019 Reversible data hiding based on novel embedding structure PVO and adaptive block-merging strategy Multimed. Tools Appl. 78 26047 26071
60. IJ Cox ML Miller JA Bloom J Fridrich T Kalker 2007 Digital watermarking and steganography Morgan Kaufmann Burlington
61. M Fallahpour D Megias M Ghanbari 2011 Reversible and high-capacity data hiding in medical images IET Image Process 5 190 197
62. RK Ramesh R Dodmane S Shetty G Aithal M Sahu AK Sahu 2023 A Novel and secure fake-modulus based Rabin-3 cryptosystem Cryptography 7 44 <https://doi.org/10.3390/cryptography7030044>
63. KR Raghunandan Bhavya Kallapu Radhakrishna Dodmane NS Krishnaraj Rao Srinivasarao Thota Aditya Kumar Sahu 2023 Enhancing cloud communication security: a blockchain-powered framework with attribute-aware encryption Electronics 12 3890 <https://doi.org/10.3390/electronics12183890>
64. S Thomas 2023 A novel image compression method using wavelet coefficients and Huffman coding J. Eng. Res. 1 1 10
65. S Kamil Khudhair M Sahu KR Raghunandan AK Sahu 2023 Secure reversible data hiding using block-wise histogram shifting Electronics 12 5 1222 <https://doi.org/10.3390/electronics12051222>
66. ME Hameed MM Ibrahim NA Manap 2018 Review on improvement of advanced encryption standard (AES) algorithm based on time execution, differential cryptanalysis and level of security J. Telecommun. Electron. Comput. Eng. 10 1 139 145
67. Z Wang HR Sheikh AC Bovik 2018 “Objective Video Quality Assessment” in The handbook of video databases: design and applications CRC Press Florida 1041 1078
68. Stoica, A. Vertan, C., Fernandez-Maloigne, C.: Objective and subjective color image quality evaluation for JPEG 2000 compressed images, presented at International Symposium on Signals, Circuits and Systems, SCS 2003, 10–11 Jul, 2003.
69. GF Siddiqui 2020 A dynamic three-bit image steganography algorithm for medical and e-healthcare systems IEEE Access 8 181893 181903
70. NA Loan SA Parah JA Sheikh JA Akhoun GM Bhat 2017 Hiding electronic patient record (EPR) in medical images: a high capacity and computationally efficient technique for e-healthcare applications J. Biomed. Informat. 73 125 136
71. A Rehman T Saba T Mahmood Z Mehmood M Shah A Anjum 2019 Data hiding technique in steganography for information security using number theory J. Inf. Sci. 45 6 767 778
72. K Muhammad J Ahmad H Farman Z Jan M Sajjad SW Baik 2015 A secure method for color image steganography using gray-level modification and multi-level encryption Trans. Internet Inf. Syst. 9 5 1938 1962
73. K Bailey K Curran 2006 An evaluation of image-based steganography methods Multimed. Tools Appl. 30 1 55 88
74. Masud Karim, S.M., Rahman, M.S., Hossain M.I.: “A new approach for LSB based image steganography using secret key,” in Proc. 14th Int. Conf. Comput. Inf. Technol. (ICCIT), Dec. 2011, pp. 286–291.
75. Jassim, F.A.: “A novel steganography algorithm for hiding text in image using five modulus methods,” 2013, [arXiv:1307.0642](https://arxiv.org/abs/1307.0642).
76. ST Kamal KM Hosny TM Elgindy MM Darwish MM Fouda 2021 A New image encryption algorithm for grey and color medical images IEEE Access 9 37855 37865
77. SE El-Khamy NO Korany AG Mohamed 2020 A new fuzzy-DNA image encryption and steganography technique IEEE Access 8 148935 148951
78. R Wazirali W Alasmery MMEA Mahmoud A Alhindi 2019 An Optimized Steganography Hiding Capacity and Imperceptibility Using Genetic Algorithms IEEE Access 7 133496 133508
79. X Wang J Yang 2021 A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient Inf. Sci. 569 217 240
80. H Liu B Zhao L Huang 2019 A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map IEEE Access 7 65450 65459
81. X Zhang X Wang 2018 Remote-sensing image encryption algorithm using the advanced encryption standard Appl. Sci. 8 9 1540
82. Sedighi, M., Mahmoudi, S.K., Amini, A.S.: “Proposing a new method for encrypting satellite images based on hash function and chaos parameters,” Proceedings of the 2019 GeoSpatial Conference 2019—Joint Conferences of SMPR and GI Research, pp. 949–953, University of Tehran, Tehran, Iran, 12–14 October 2019.
83. X Wang L Liu Y Zhang 2015 A novel chaotic block image encryption algorithm based on dynamic random growth technique Opt. Lasers Eng. 66 10 18
84. Z Hua Y Zhou CM Pun CP Chen 2015 2D Sine Logistic modulation map for image encryption Inf. Sci. 297 80 94
85. A Alanezi B Abd-El-Atty H Kolivand A El-Latif A Ahmed A El-Rahiem S Sankar S Khalifa 2021 Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment Secur. Commun. Netw. <https://doi.org/10.1155/2021/6615512>
86. J Arif MA Khan B Ghaleb J Ahmad A Munir U Rashid A Al-Dubai 2022 A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution IEEE Access 10 12966 12982
87. Q Lu C Zhu X Deng 2020 An efficient image encryption scheme based on the LSS chaotic map and single S-box IEEE Access 8 25664 25678
88. M Samiullah W Aslam H Nazir MI Lali B Shahzad MR Mufti H Afzal 2020 An image encryption scheme based on DNA computing and multiple chaotic systems IEEE Access 8 25650 25663

89. A Qayyum J Ahmad W Boulila S Rubaiee F Masood F Khan WJ Buchanan 2020 Chaos-based confusion and diffusion of image pixels using dynamic substitution IEEE Access 8 140876 140895
90. D Madhu S Vasuhi 2023 Lightweight encryption assisted man-in-the-middle attack-resilient steganography model for secure satellite imagery services: LEMARS' J. Intell. Fuzzy Syst. 45 2 2847 2869
91. P Asmitha C Rupa S Nikitha 2024 Improved multiview biometric object detection for anti spoofing frauds Multimed. Tools Appl. <https://doi.org/10.1007/s11042-024-18458-8>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.