SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I11P120

Volume 11 Issue 11, 244-256, November 2024
© 2024 Seventh Sense Research Group®

Original Article

Energy Distribution Based Dual Image Data Hiding with Weightage Mapping of Secret Data

A. I. Mujeebudheen Khan[1], K. Siva Sankar[2]

[1]*Department of CSE, Noorul Islam Centre for Higher Education, Tamil Nadu, India.*
[2]*Department of Information Technology, Noorul Islam Centre for Higher Education, Tamil Nadu, India.*

[1]*Corresponding Author : MujeebudheenKhan.A.I@outlook.com*

Received: 21 September 2024 Revised: 21 October 2024 Accepted: 19 November 2024 Published: 03 December 2024

Abstract - *The swift advancement of information and communication technologies provides exceptional facilities in the field of data transmission systems. Nowadays, confidential information, including national security, scholastics, personal information, and industrial commerce, is exchanged through the internet and within the cloud computing environment. In the wake of technology, especially multimedia, different processes have been developed recently for information hiding and data manipulation. The secret data hiding can be performed using steganography to communicate the authentication-specific, account-specific sensitive information even in the public domain. The current method proposes an energy distribution-based dual image data hiding to solve this problem. The proposed method is designed in two distinct phases: data embedding and data extraction. Each phase is executed with careful processing steps to ensure reversible steganography and preserve the cover image and secret data. The proposed steganography technique effectively preserves the visual quality of the cover images, as demonstrated by high average PSNR values (48.2269 to 48.4770), low MSE values (0.9215 to 0.9807), and high SSIM values (0.9923 to 0.9968), indicating minimal error introduced by the embedding process. This work offers a robust approach to steganography, balancing security and image fidelity.*

Keywords *- Dual image data hiding, Cover image, Energy distribution, Weightage mapping, Steganography.*

1. Introduction

Data communication and digital technology advancements have led to an increasingly interconnected world, resulting in the convergence of network services and computing functionalities. In this era of digital communication, secure data transfer is very crucial [1]. Data-hiding techniques, particularly in the realm of steganography, play a crucial role in enhancing data security. Steganography is a kind of encoding technique in which the information is hidden within the cover data [2]. This cover can be an image, video, audio, text or some other media file or data. Figure 1 illustrates the general process of embedding and extracting hidden data within a cover image. Unlike encryption, where data is simply scrambled and easily recognizable as protected, steganography conceals the very existence of the hidden data, hence diminishing the possibility of detection [3]. This technique is essential for secure communication, ensuring that sensitive information remains confidential without attracting attention. In the context of modern data security, steganography provides an additional layer of protection, particularly in scenarios where data transmission is critical [4]. Energy distribution-based methods for dual image data hiding stem from the need to balance data embedding capacity with the preservation of image quality [5]. By analyzing the energy distribution of pixels in the cover image, this approach identifies regions with optimal energy levels for embedding, avoiding areas that could either distort important visual features (like edges) or lead to noticeable changes in smooth regions [6].

Energy-based embedding allows more efficient use of the available space, enhancing the steganographic method's robustness and capacity. The major objectives of the paper are listed below:

- To design a steganographic method that leverages energy distribution for selecting optimal embedding regions in the cover image.
- To ensure minimal distortion to the cover image while maximizing data embedding capacity through efficient energy-based embedding techniques.
- To assess the efficacy of the suggested methodology for image quality, robustness, and resistance to detection using metrics such as PSNR, SSIM, and MSE.

The subsequent portion of the paper is organized as outlined below: Section two offers a comprehensive review of existing methods and identifies the research gap. The proposed methodology is detailed in section three, while section four delineates the results accompanied by commentary. Section five ultimately concludes the paper and delineates prospective future endeavors.

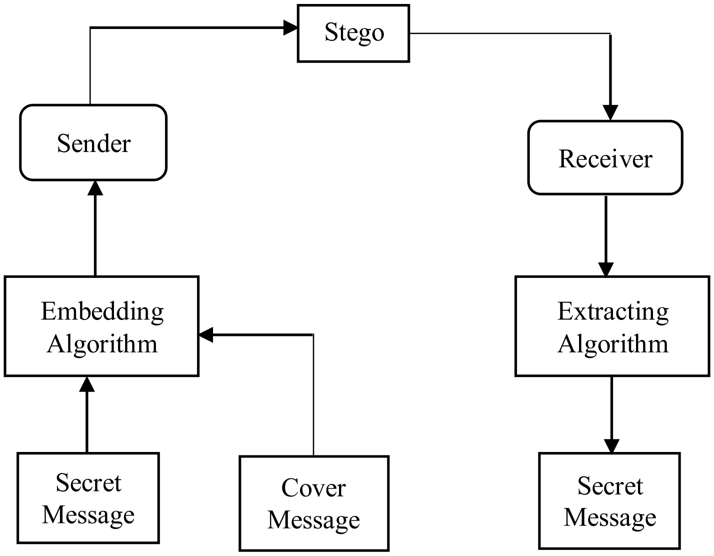


Fig. 1 General Steganography system

2. Related Works

Chen et al. [7] suggested a method for Reversible Data Hiding (RDH) utilizing multiple data-hiders based on secret sharing. It divides the original image into numerous identically sized encrypted images and distributes them to different data hiders to hide data. Each data-hider can independently embed data into the encrypted image to acquire the corresponding tagged encrypted image. A separable RDH-EI approach with high capacity was proposed based on the current paradigm, where data extraction was carried out in the encrypted domain.

Two enhanced RDH techniques were put forth by Sahu et al. [8] to support both image quality and EC. The methods proved useful in situations where both the secret data and the host medium are absolutely necessary. Next, the first two identical images and the secret data were embedded utilizing the n-rightmost bit substitution technique. In the final stage, the modified pixel value embedded two identical images with secure data. The RDH approaches with an interpolation-based strategy for data concealment were proposed by Hassan et al. [9]. The method was carried out to scale up the original image using the improved parabolic interpolation approach, and then the secret data was included using the embedding technique. Gull et al. [10] suggested a dual-image reversible data-hiding approach. The Huffman encoding technique was employed to preprocess the acquired secret data. A codebook of "d" bits is created so that indices can be used to encode the converted decimal values. To generate dual stego images, the indices were divided into two segments and inserted within two similar images. Wang et al. [11] suggested a Reversible Data Hiding in Encrypted Image (RDHEI) approach that utilized pixel correlation to perform embedding. Block-level permutations and block-level stream cipher were combined using a block-level encryption technique. All blocks are classified as useable or unusable while preserving the pixel correlation inside each block. Yin et al. [12] suggested a reversible RDHEI method utilizing pixel prediction and multi-MSB plane rearrangement. Initially, the predicted value was computed using the median edge detector predictor. Subsequently, the one-bit plane represents the absolute values of Prediction Errors (PEs), whereas the remaining bit planes indicate the signs of PEs.

Sanivarapu et al. [13] proposed a watermarking technique for concealing patient data within ECG signals as a rapid response image, utilizing the wavelet method. They first employ the Pan-Tompkins method to transform the one-dimensional ECG signal into a two-dimensional ECG image. A wavelet transform is employed to break down the 2D-ECG image. Wavelet analysis can extract the ECG's delicate underlying information. Lu et al. [14] analyzed and encrypted secure data while adjusting the amount of pixel distortion using the NC and MXD parameters. The NC parameter controls the number of codes utilized to re-encode a secure symbol, which also regulates the total number of code combinations. MXD limits image distortion by defining the maximum distortion for each code combination.

An approach for RDHEI based on adaptive Most Significant Bit (MSB) was proposed by Wang et al. [15]. In order to maintain the correlation of pixels inside a block, the cover image was first encrypted block by block. The upper left pixel in a block was used to forecast others during data embedding, freeing up the embedding. To guarantee reversibility, all of the available blocks are chosen and rearranged. The approach effectively utilized the correlation between pixels within a block by implementing adaptive MSB prediction to attain the desired capacity improvement.

Conventional steganographic techniques often face significant limitations, particularly regarding embedding efficiency, image quality preservation, and detection risk. Many traditional methods either lack the capacity to embed large amounts of data or introduce noticeable distortions in the cover image, which can easily alert attackers or detection algorithms. These techniques typically distribute hidden data uniformly without considering the characteristics of the image, leading to the alteration of important features such as edges or textures, which reduces visual quality. Moreover, by embedding data indiscriminately, these methods increase the likelihood of statistical anomalies, making it easier for steganalysis tools to detect the presence of hidden information, thus compromising the security of the steganographic process.

3. Materials and Methods

The proposed method is designed in two distinct phases, namely the data embedding and extraction. Each phase is executed with careful processing steps aimed at ensuring reversible steganography and preserving both the secret data and cover [16]. In the first phase, the data embedding phase, the secret image undergoes initial conversion to become the bit stream. This transformation ensures that the image data is represented in a binary format compatible with the embedding procedure. The primary focus of this phase is identifying optimum energy pixels in the cover image, which are computed and selected based on energy estimation techniques. These optimum energy pixels are crucial as they offer better embedding efficiency and minimize distortion in the cover image. Once the energy pixels are selected, the secret bit stream is embedded within these pixels. The embedding procedure utilizes optimal sites identified using energy computation to minimize the impact on the cover's overall appearance, preserving its quality and rendering the hidden data invisible. The second phase of the method deals with recovering the secret image and the cover image. During this phase, the same energy computation process is applied to extract the embedded data accurately. The image is converted into an 8-bit binary format, and these binary numbers are arranged sequentially to reconstruct the hidden secret data.

Once the 8-bit binary format is extracted, the pixels in the secret image are grouped into segments of bits. These bit segments are then converted into their corresponding decimal values. A constructed histogram of these decimal values plays a critical role in the extraction process. The histogram essentially acts as a weightage map, representing the secure data distribution and aiding in the precise reconstruction of the hidden image [17]. By using this two-phase process—embedding the secret data into optimum energy pixels and utilizing a histogram-based weightage mapping technique for extraction—the proposed method ensures a reversible and efficient steganographic process, allowing for the recovery of both the secret image and the original cover image.

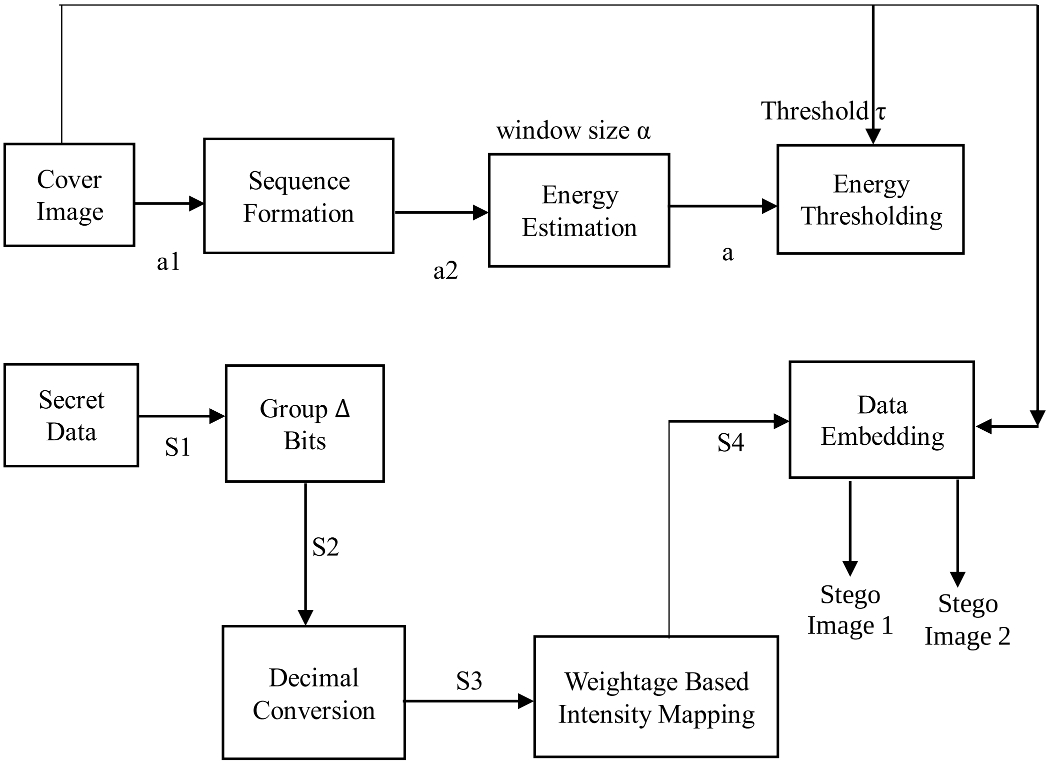


Fig. 2 Block diagram of proposed data embedding phase

3.1. Embedding Phase

In traditional embedding processes, the energy of pixels is often overlooked, leading to significant distortion in the cover image. If high-energy pixels, such as those located along edges and boundaries, are used for embedding, these critical areas of the image can be visibly degraded, leading to noticeable distortions. On the other hand, if low-energy pixels, typically found in smooth or plain regions of the image, are used for embedding, the uniformity of these regions may be compromised, resulting in a loss of visual quality. The suggested method's data embedding diagram is displayed in Figure 2.

Figure 3 illustrates the process of sequence formation in the cover image, where pixel values are systematically arranged to create a structured sequence for data embedding.

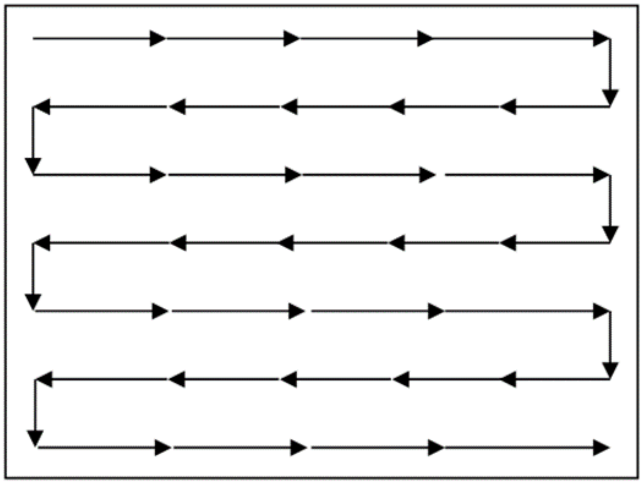


Fig. 3 Sequence formation in cover image

To avoid such issues, the proposed study calculated the optimum energy region, and it is essential to distribute the secret data in the intermediate regions of the cover. An image, $mg = X(p, q)$, where p and q are coordinates p =1, 2... T and q= 1, 2... S, the size of the image is $S \times T$, and *Img* is defined as the maximum pixel value *X*. Regarding an image with a unique coordinating position $(p\ , q)$ as $T_{pq}^{d} = \{p + u, q + v, (u, v) \in T^{d}\}$, T of order d is used to model the spatial association between surrounding pixels in a digital image, *Img*. Finding the energy of each pixel value in the image is the initial stage, after which a binary matrix is created, $Bin_X = \{bin_{pq}, 1 \le p \le S, 1 \le q \le T\}$, the $bin_{p,q} = 1$ if $X_{p,q} > X$; else $bin_{p,q} = -1$. Let $CE = CE_{pq}, 1 \le p \le S, 1 \le q \le T$ is another matrix provided as $CE_{pq} = 1, \forall(p, q)$. For every pixel X in the image, *Img* with an energy value ENR_X is calculated using Equation (1).

$$ENR_X = -\sum_{p=1}^{S}\sum_{q=1}^{T}\sum_{mn \in T_{pq}^{2}} bin_{pq}bin_{mn} + \sum_{p=1}^{S}\sum_{q=1}^{T}\sum_{mn \in T_{pq}^{2}} CE_{pq}CE_{mn} \tag{1}$$

The second term of the expression in the above equation is constant, confirming that the energy value $ENR_X \ge 0$. According to Equation (1), all of the pixel levels of Img_{pq} have pixel values that are either larger than or less than X. This means that the energy value at a given pixel value is equal to zero if every element of Bin_X is either 1 or -1. After calculating the energy values of pixels in an image, the next critical step is energy normalization. The goal of normalization is to scale the energy values so that they fall within a predefined range, typically between 0 and 1. This ensures that the energy values can be uniformly compared and processed for embedding purposes.

To begin the normalization process, the minimum and maximum energy values among all pixels in the image are identified. These values represent the boundaries of the energy distribution within the image. The energy values are normalized according to the Equation (2).

$$Normalized_{\ E} = \frac{E(i) - E_{min}}{E_{max} - E_{min}} \tag{2}$$

Where $E(i)$ is the original energy value of the i th pixel, E_{min} is the minimum energy value across all pixels in the image, E_{max} is the maximum energy value across all pixels in the image. The energy values are normalized on a scale between 0 and 1, where 0 represents the least energy (plain areas), and 1 represents the highest energy (edges and boundaries). The rest of the pixels will have their energy values scaled proportionally between these two extremes. Optimum energy pixels strike a balance between high and low energy, ensuring that neither the edges nor the smooth regions are disproportionately affected.

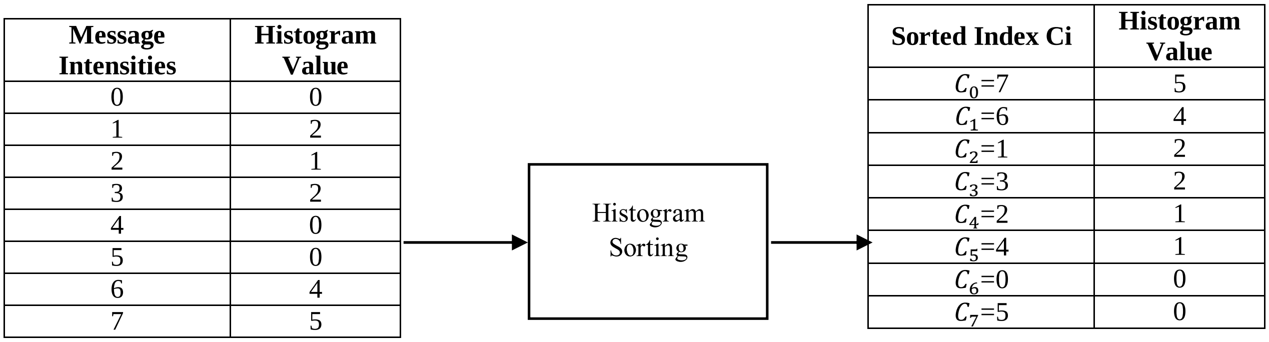
Energy thresholding is a technique used to determine whether a pixel in the cover image is suitable for data embedding based on its energy level [18]. This method uses a boundary factor, denoted as γ (gamma), to set the threshold for selecting carrier pixels. The gamma value can be adjusted between 0 and 1, allowing for flexible control over the embedding process and ensuring that data is embedded in the most suitable regions of the image. When energy thresholding is applied, the energy of each pixel is evaluated. Based on the comparison with the gamma threshold as measured in Equation (3), a decision is made on whether the pixel can be used as a carrier for embedding:

$$C(n) = \begin{cases} 1 & m_1 + \alpha(m_2 - m_1) \le a_3(n) \le m_2 - \alpha(m_2 - m_1) \\ 0 & Otherwise \end{cases} \tag{3}$$

If C(n) = 1, the pixel has an energy level that meets or exceeds the gamma threshold, meaning it can be used to carry embedded data.

If C(n) = 0, the pixel does not meet the required energy level, meaning it will not be used for embedding.

Where m_2 is the image's greatest energy value and m_1 is its minimum energy value. This selective process ensures that data is only embedded in pixels with appropriate energy levels, helping to minimize distortion and preserve the quality of the cover. Adjusting the gamma value controls how much data is embedded and in which regions, allowing for a more balanced trade-off between embedding capacity and image quality.



Message Intensities	Histogram Value
0	0
1	2
2	1
3	2
4	0
5	0
6	4
7	5

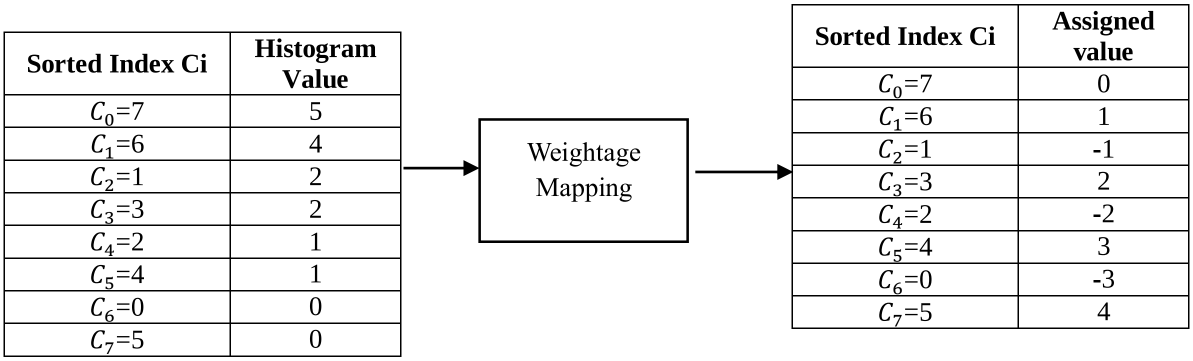
Sorted Index Ci	Histogram Value
C_0=7	5
C_1=6	4
C_2=1	2
C_3=3	2
C_4=2	1
C_5=4	1
C_6=0	0
C_7=5	0

Fig. 4 Histogram sorting of secret data

A decimal digit D is created from N secret bits using Equation (4) during the embedding process.

$$D = \sum_{i=1}^{K} 2^{i-1} Sec^{i} \quad (4)$$

The i^{th}secret bit in the sequence is indicated by Sec^i. As the number of secret bits rises, the parameter K is also increased. As illustrated in Figure 4, the suggested technique measures the histogram values of each decimal digit D and arranges the data in descending order to determine the order of each digit. The visual quality is reduced when a digit is directly embedded in an image if its histogram value is high. The proposed scheme converts the digit D, which has the maximum histogram value, with the smallest distortion code, d, as shown in Figure 5. The histogram value, in this case, is represented by $His(D)$. The values are sorted descendingly, and the index of the sorted results is shown by C_i.



Sorted Index Ci	Histogram Value
C_0=7	5
C_1=6	4
C_2=1	2
C_3=3	2
C_4=2	1
C_5=4	1
C_6=0	0
C_7=5	0

Sorted Index Ci	Assigned value
C_0=7	0
C_1=6	1
C_2=1	-1
C_3=3	2
C_4=2	-2
C_5=4	3
C_6=0	-3
C_7=5	4

Fig. 5 Weightage mapping of secret data

The code is then embedded in the pixel of the cover image by using weightage mapping to get stego pixels, namely $IMG'_{x,y}$ and $IMG''_{x,y}$ according to the Equation (5) and (6). For use in the recovery phase, the mapping relationship between the digits and indices needs to be noted.

$$IMG'_{x,y} = \begin{cases} A_1(x,y) + \lfloor 0.5 \times S_4 \rfloor & if\ C(n) = 1 \\ A_1(x,y) & if\ C(n) = 0 \end{cases} \quad (5)$$

$$IMG''_{x,y} = \begin{cases} A_1(x,y) + \lfloor 0.5 \times S_4 \rfloor & if\ C(n) = 1 \\ A_1(x,y) & if\ C(n) = 0 \end{cases} \quad (6)$$

3.2. Extraction Phase

The procedure involved in recovering the cover image and extracting secret bits from the stego image is described in this section. Two stego images have the encoded digit embedded in their pixels. Finding the cover image, as seen in Figure 6, is the first crucial step in the extraction process. The cover image serves as the foundation for retrieving the hidden secret data and re-estimating the energy values of the pixels involved in the embedding process. Both stego images are required to successfully recover the cover image without losing quality. Once the stego images are provided, the extraction process begins using a ceiling operator for value round-off, ensuring that pixel values are rounded up to the nearest integer, which helps accurately reconstruct the cover image. By computing the difference between two stego pixels, as shown in Equation (7), the correct digit can be recovered.

$$D' = \left|IMG'_{x,y} - IMG''_{x,y}\right| \quad (7)$$

Each secret digit is converted into K secret bits once the encoded digit D', has been obtained. Additionally, the average of two stego pixels can be used to retrieve the cover pixel $IMG_{x,y}$, as shown in Equation (8).

$$D = \left\lceil \frac{IMG'_{x,y}+IMG''_{x,y}}{2} \right\rceil \quad (8)$$

Following the initial cover image recovery, energy estimation and thresholding techniques are applied, just as they were applied during the embedding process. Energy estimation is necessary to identify the optimum regions of the cover image where the secret data was hidden. This step ensures that data is extracted from the same high-energy or low-energy regions used for embedding, preserving the cover's integrity.

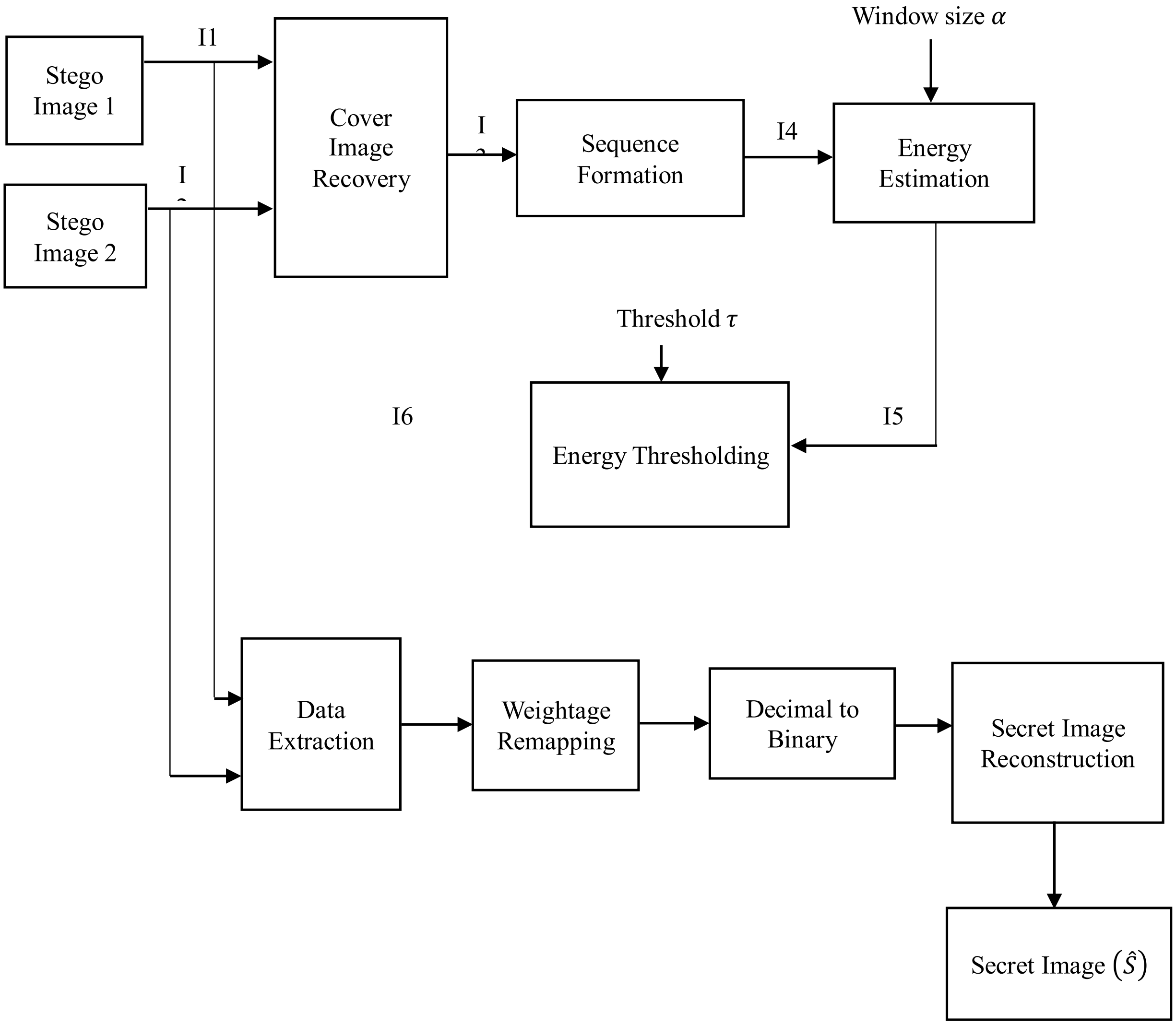
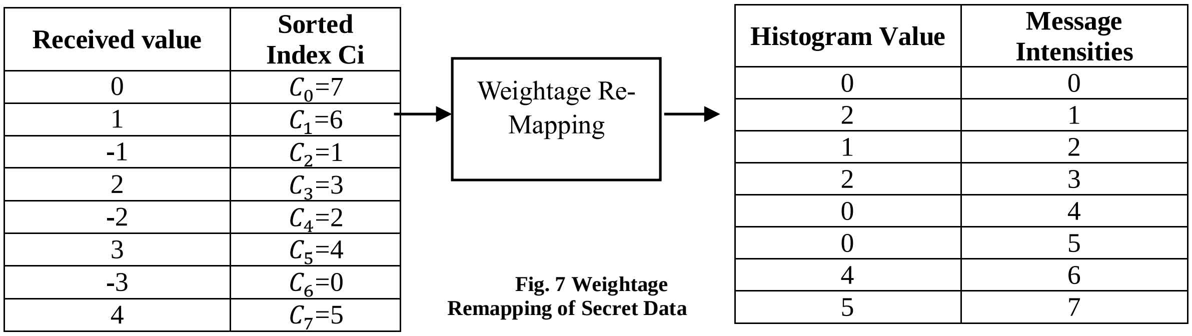


Fig. 6 Block diagram of proposed secure data and cover recovery

In the secret data extraction phase of the proposed technique, the process begins with extracting the weightage map sequence, as shown in Figure 7. The weightage map, created during the embedding phase using the energy distribution and histogram of the secret image, plays a vital role in ensuring accurate recovery of the hidden data. This acts as a guide, indicating the data distribution embedded in the cover image based on energy levels.



Received value	Sorted Index Ci
0	C_0=7
1	C_1=6
-1	C_2=1
2	C_3=3
-2	C_4=2
3	C_5=4
-3	C_6=0
4	C_7=5

Histogram Value	Message Intensities
0	0
2	1
1	2
2	3
0	4
0	5
4	6
5	7

Fig. 7 Weightage Remapping of Secret Data

Once the weightage map sequence is extracted, the next step is to extract the embedded data from the stego image. This is done by identifying the pixels that served as carriers during the embedding process based on earlier energy thresholding. The data retrieved at this stage is not yet in its original form; it is still encoded in the weightage sequence based on the energy distribution. The extracted data is then remapped using the weightage map sequence to reconstruct the actual secret data. This remapping step is critical, as it converts the extracted weightage data back into its original decimal form, undoing the transformation applied during embedding.

The weightage map helps to match the retrieved data points with their original locations and values in the sequence. After remapping, the decimal data is converted into its binary form, which was the format of the original secret image before embedding. This binary conversion restores the embedded data back to its original bit stream, providing the raw format of the hidden information.

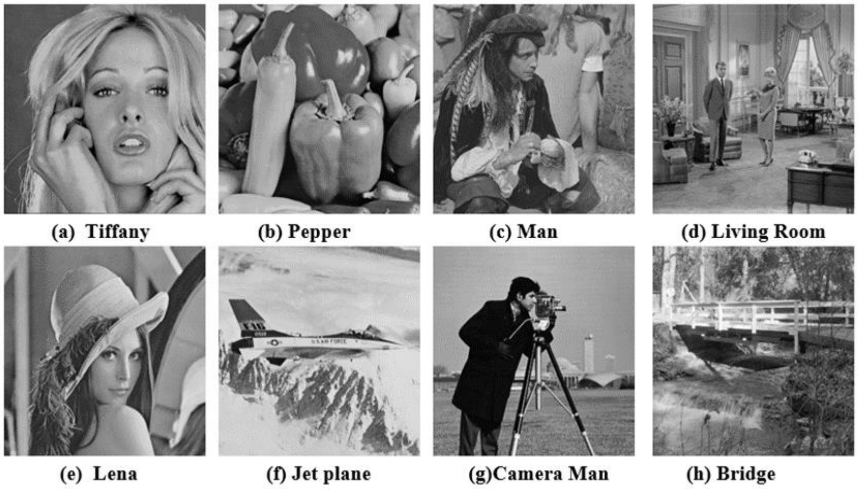
Extracted binary data is rearranged into the original sequence format in which the secret image was encoded during the embedding phase. This ensures the binary data is properly aligned and restored as the secret image, completing the extraction process. By following these steps, the original secret data is successfully recovered in its unaltered form, demonstrating the effectiveness of the reversible steganographic technique. The entire extraction process is designed to reverse the embedding process and ensure reversibility.

3.3. Experimental Setup

The proposed technique was implemented using MATLAB to perform the embedding and extraction processes. The experimental verification was conducted using a set of eight standard grayscale cover images, each with a resolution of 512x512 pixels. These cover images served as the carriers for the hidden data during the steganographic process. For embedding, the test secret images were also selected as grayscale images, each having a resolution of 178x178 pixels. These secret images were embedded into the cover images using the dual steganographic technique, utilizing the energy distribution of the cover image pixels to optimize the embedding process. The combination of grayscale cover images and grayscale secret images ensures a consistent evaluation of the steganographic technique.

4. Results and Discussion

Figure 8 shows eight cover images, namely, Lena, Tiffany, Jet plane, Peppers, man, Cameraman, living room and bridge and Figure 9 shows four secret images used in the proposed study. The size of the cover image is 512×512, and the secret image is 178 x178.



(a) Tiffany (b) Pepper (c) Man (d) Living Room

(e) Lena (f) Jet plane (g)Camera Man (h) Bridge

Fig. 8 Eight standard gray scale cover test images

Fig. 9 Secret images

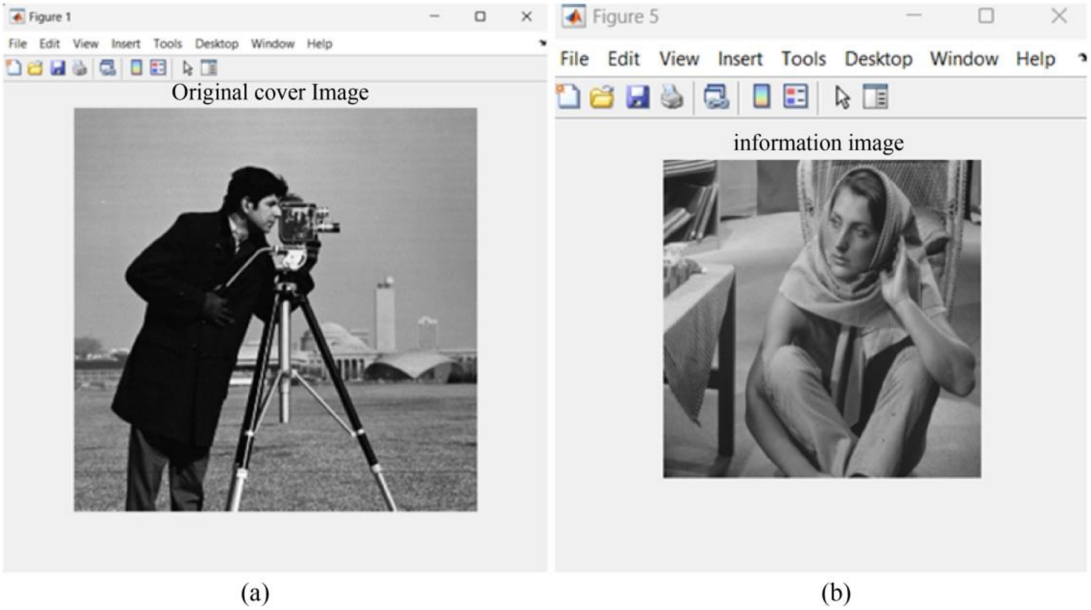


Figure 1
File Edit View Insert Tools Desktop Window Help
Original cover Image
Figure 5
File Edit View Insert Tools Desktop Window Help
information image
(a)
(b)

Fig. 10 Embedding process (a) Original cover image, and (b) Secret image.

Figures 10-11 illustrate key aspects of the steganographic process. Figure 10(a) shows the original cover image, which serves as the carrier for the secret data, while (b) represents the secret image to be embedded.

Figure 11 (a) depicts the intensity distribution of the cover image, showing how pixel intensities are distributed before embedding, and (b) demonstrates the intensity distribution after normalization, where the pixel values are scaled to a standardized range, ensuring uniformity in energy estimation.

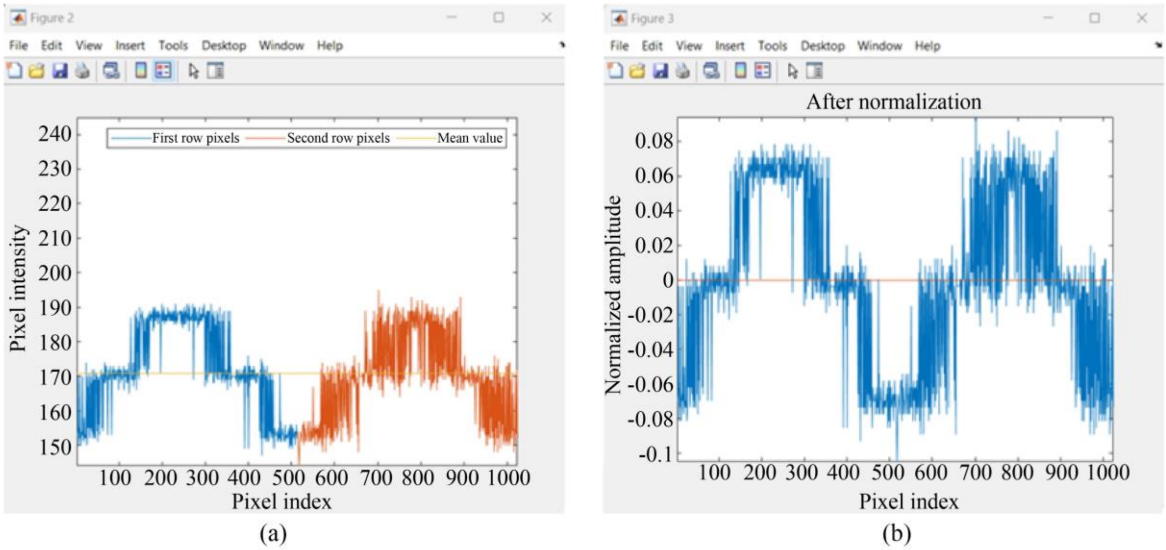


Fig. 11 Embedding process (a) Intensity distribution of cover image, and (b) Intensity distribution after normalization.

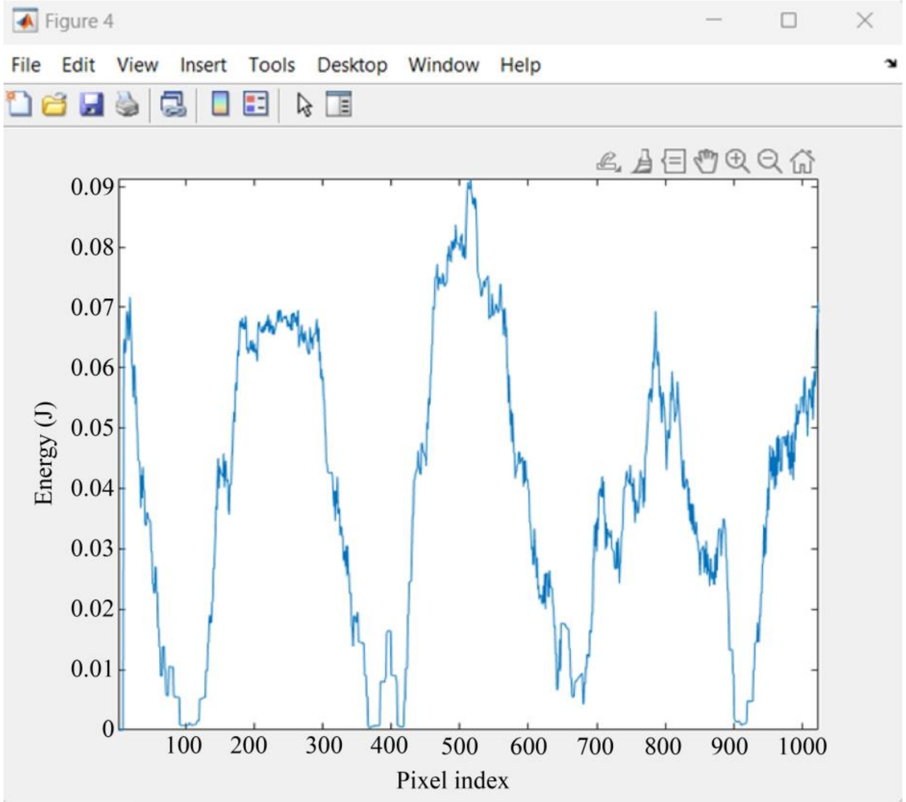


Fig. 12 Normalized energy distribution of cover image in embedding

Figure 12 presents the normalized energy distribution of the cover image, providing a visual representation of the energy levels across the image after normalization, which guides the optimal embedding of secret data into regions with appropriate energy levels.

Three important metrics were used to assess the performance of the suggested method. These metrics evaluate the data hiding technique's efficacy as well as the stego images' quality.

4.1. Mean Squared Error (MSE)

The MSE quantifies the average squared deviation between actual values and predicted values. It is computed by averaging the squared residuals, where each data point's residual is the difference between its expected and actual values. The model's accuracy can be examined using the MSE value. When the MSE is smaller, the model is more accurate since its predictions are more accurate when they are closer to the actual values. A greater MSE indicates a larger deviation between the model's predictions and actual values, which indicates worse performance. It is represented as per Equations 9-11.

$$MSE_1 = \frac{1}{P}\sum_1^P (ZE_m - Z\acute{E}_m)^2 \tag{9}$$

$$MSE_2 = \frac{1}{P}\sum_1^P (ZE_m - Z\acute{E}_m)^2 \tag{10}$$

$$MSE_{avg} = \frac{1}{2}(MSE_1 + MSE_2) \tag{11}$$

Where the number of observations in the dataset is denoted by P, the actual value of the observation is denoted by ZE_m and the extracted value is denoted by $Z\acute{E}_m$.

4.2. Peak Signal-to-Noise Ratio (PSNR)

The PSNR evaluates how much signal power is present at its maximum and how much noise is there to distort it and lower the quality of its representation. Because many signals have a very large dynamic range—the ratio between the greatest and smallest conceivable values of a variable quantity—the PSNR is often articulated using the logarithmic decibel scale. It computes the ratio of a signal's maximum potential power to the power of any noise or distortion that compromises the signal's integrity. PSNR is defined as per Equation (12),

$$PSNR\ _1 = 10\log_{10}\left[\frac{255^2}{\frac{1}{H\times W}\sum_{j=1}^{H}\sum_{k=1}^{W}(S-S_1)^2}\right] dB \tag{12}$$

$$PSNR\ _2 = 10\log_{10}\left[\frac{255^2}{\frac{1}{H\times W}\sum_{j=1}^{H}\sum_{k=1}^{W}(S-S_2)^2}\right] dB \tag{13}$$

Where $H \times W$ is the size of the cover, S_1 and S_2 are the two stego-images, and S is the cover image. A slight change between the cover image and the stego-image yields a higher PSNR, while a higher change between the cover and stego image yields a lesser PSNR value. The average PSNR between the two stego-images is as follows,

$$PSNR_{avg} = \frac{1}{2}(PSNR_{\ 1} + PSNR_{\ 2}) \tag{14}$$

4.3. Structural Similarity Index (SSIM)

The images' structure, contrast, and luminance are compared to measure SSIM. The brightness, contrast, and structural terms are computed to determine the quality assessment index for the SSIM.

$$SSIM_1(S, S_1) = \frac{(2\mu_S\mu_{S1}+C_1)(2\sigma_{SS1}+C_2)}{(\mu_S^2+\mu_{S1}^2+C_1)(\sigma_S^2+\sigma_{S1}^2+C_2)} \tag{15}$$

$$SSIM_2(S, S_2) = \frac{(2\mu_S\mu_{S2}+C_1)(2\sigma_{SS2}+C_2)}{(\mu_S^2+\mu_{S2}^2+C_1)(\sigma_S^2+\sigma_{S2}^2+C_2)} \tag{16}$$

$$SSIM_{avg} = \frac{1}{2}\{(SSIM_1(S, S_1)) + (SSIM_2(S, S_2))\} \tag{17}$$

The average pixel values of the images S and S_1 are μ_s and μ_{s1} respectively. The variance of the pixel values in images S and S_1 denoted by σ_s^2 and σ_{s1}^2, the covariance of the pixel values between images S and S_1 is denoted by σ_{SS1} and C_1 and C_2 are constants to stabilize the division when the denominator is close to zero. Figure 13 displays the stego images generated after the embedding process, showcasing the integration of hidden data into the cover images while maintaining visual similarity to the original images.

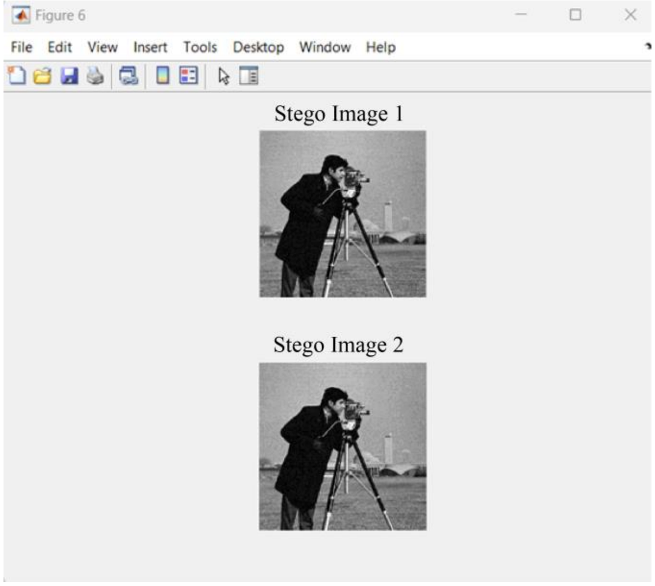


Fig. 13 Stego Images after embedding

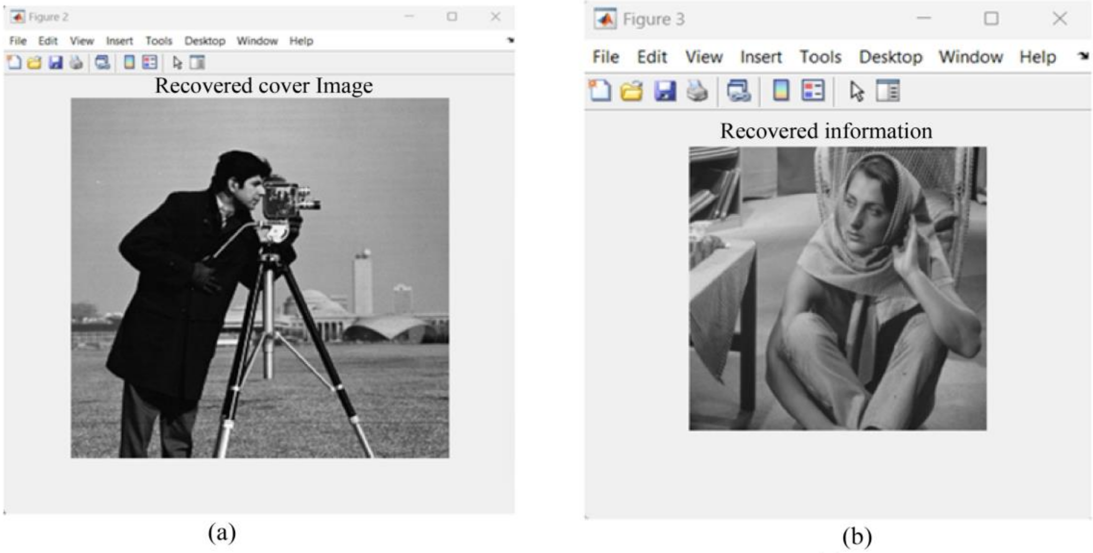


Figure 2
File Edit View Insert Tools Desktop Window Help
Recovered cover Image
Figure 3
File Edit View Insert Tools Desktop Window Help
Recovered information

(a)

(b)

Fig. 14 After extraction, (a) Recovered cover image, and (b) Recovered Secret image.

The cover and the secret image recovered after the extraction are shown in Figures 14(a) and (b).

The PSNR 1 and PSNR 2 values for different test images, including Cameraman, Bridge, Jet Plane, Peppers, and Tiffany, indicate the quality of the stego images after embedding the secret data. Table 1 provides a comparison of image quality using PSNR. The PSNR values are consistently high across all images, with slight variations between the two phases, showing minimal distortion in the cover images. The average PSNR values range from 48.2269 to 48.4770, demonstrating that the proposed steganography technique effectively preserves the visual quality of the cover images. The pictorial representation of the PSNR comparison is illustrated in Figure 15.

Table 1. Comparison of image quality using PSNR

Metric	Cameraman	Bridge	Jet plane	Peppers	Tiffany
PSNR 1	48.4683	48.4683	48.4349	48.2154	48.2465
PSNR 2	48.4856	48.4856	48.4479	48.2384	48.2698
Average PSNR	48.4770	48.4770	48.4414	48.2269	48.2582

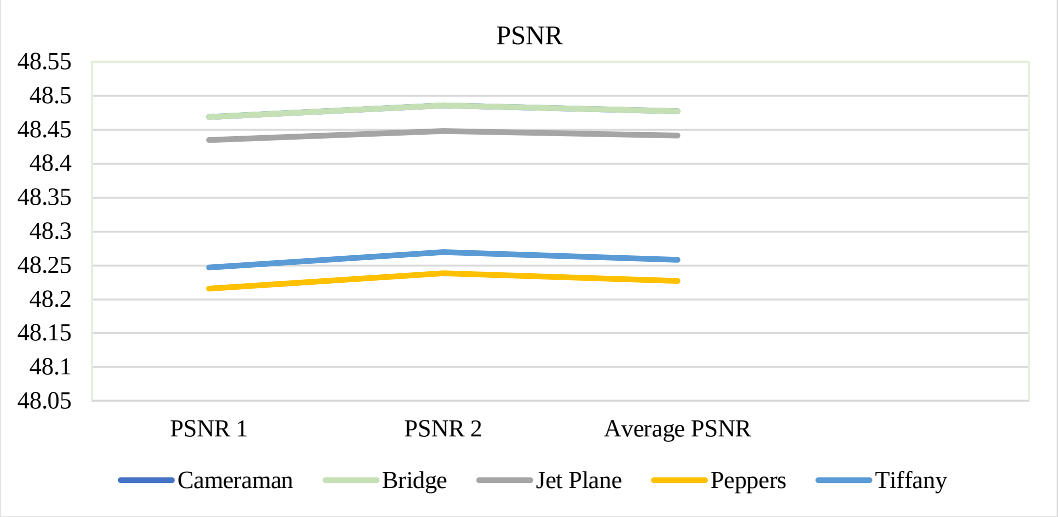


Fig. 15 PSNR comparison of the proposed method

The MSE 1 and MSE 2 values for the test images, including Cameraman, Bridge, Jet Plane, Peppers, and Tiffany, reflect the mean squared error between the original and stego images. Table 2 provides a comparison of image quality using MSE. The MSE values are low, ranging between 0.9215 and 0.9807, indicating minimal error introduced by the embedding process. The average MSE values, which range from 0.9233 to 0.9781, confirm that the proposed steganography technique maintains a high level of image fidelity, with only slight differences in pixel value between the original and modified image. The graphical representation of the MSE comparison is shown in Figure 16.

Table 2. Comparison of image quality using MSE

Metric	Cameraman	Bridge	Jet plane	Peppers	Tiffany
MSE 1	0.9252	0.9252	0.9324	0.9807	0.9737
MSE 2	0.9215	0.9215	0.9296	0.9755	0.9685
Average MSE	0.9233	0.9233	0.9310	0.9781	0.9711

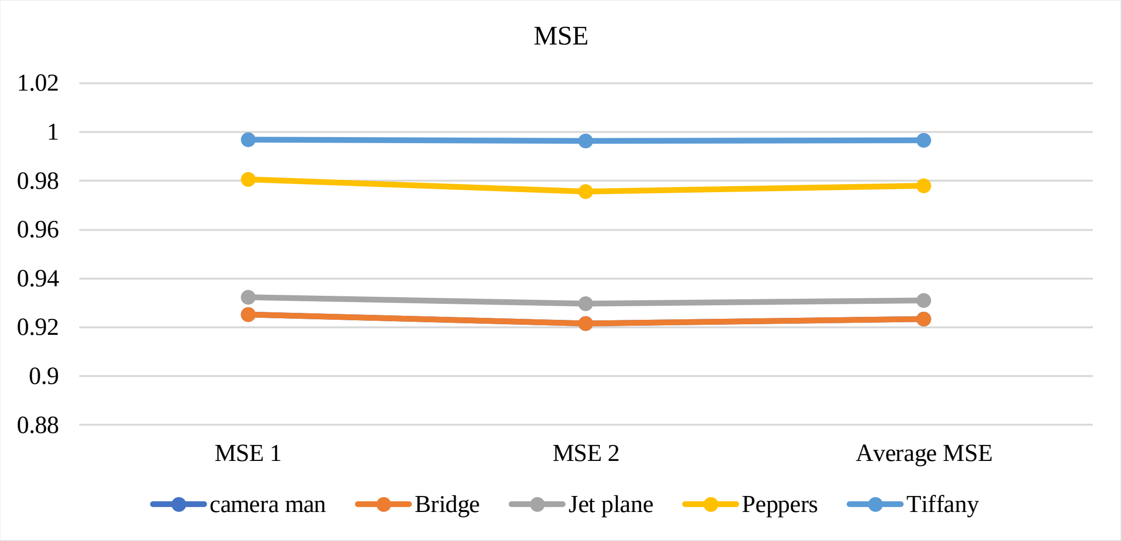


Fig. 16 MSE comparison of the proposed method

Table 3 provides the comparison of image quality using SSIM. For SSIM 1, the scores are very high across all images, with values ranging from 0.9934 to 0.9968, indicating excellent structural similarity between the original and processed images. Similarly, SSIM 2 shows slightly lower but still high similarity scores, ranging from 0.9923 to 0.9964. The average SSIM values, which aggregate the scores from both conditions, further confirm the overall high quality of the images, with values consistently above 0.9928 and reaching up to 0.9965. This demonstrates that image quality preservation is maintained effectively across different image types. The pictorial representation of the SSIM comparison is given in Figure 17.

Table 3. Comparison of image quality using SSIM

Metric	Cameraman	Bridge	Jet plane	Peppers	Tiffany
SSIM 1	0.9966	0.9966	0.9934	0.9944	0.9968
SSIM 2	0.9962	0.9962	0.9923	0.9934	0.9964
Average SSIM	0.9964	0.9964	0.9928	0.9939	0.9965

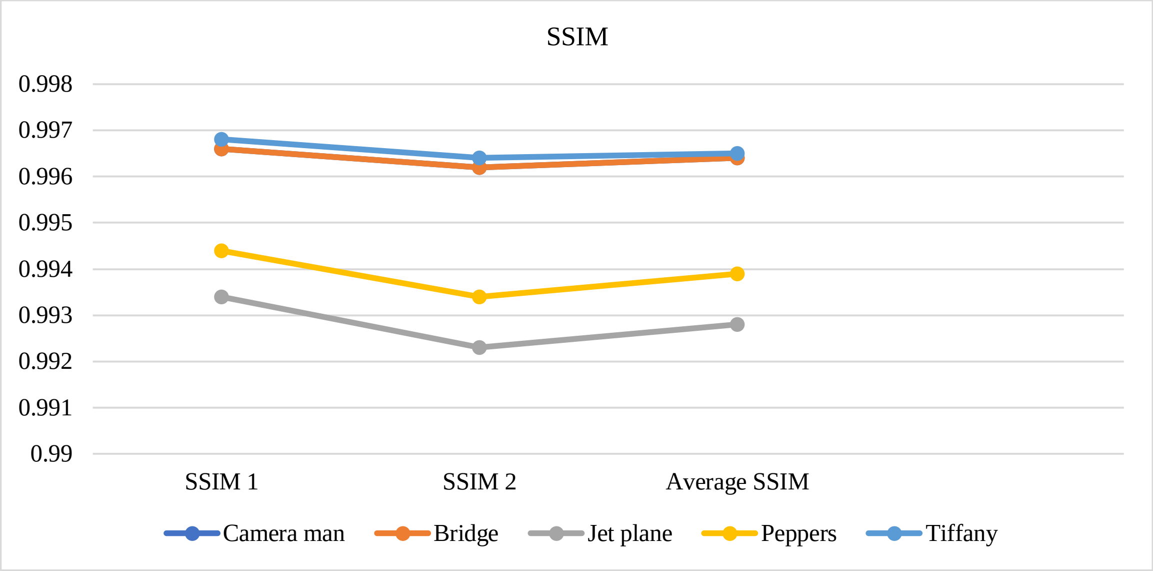


Fig. 17 SSIM comparison of the method

5. Conclusion

This work developed a reversible steganography technique using dual stego-images, incorporating energy distribution and weightage mapping to enhance the data-hiding process. The proposed method demonstrated impressive performance, particularly in terms of preserving image quality, as evidenced by the well-maintained edges and boundaries of the cover images. By selecting optimum energy pixels for embedding, the technique effectively minimized visual distortions in the cover image while ensuring accurate data extraction. The proposed steganography technique effectively preserves the visual quality of the cover images, as demonstrated by high average PSNR values (48.2269 to 48.4770), low MSE values (0.9215 to 0.9807), and high SSIM values (0.9923 to 0.9968), indicating minimal error introduced by the embedding process. The results validated the method's effectiveness, confirming that it offers a reliable and efficient approach for data hiding in grayscale images. The reversibility of the process ensures that both the secret data and the cover image can be fully recovered without loss of information. As a future direction, this work opens up the possibility of integrating machine learning techniques into the steganography process to further improve image quality and embedding efficiency. By leveraging advanced learning algorithms, the technique could become more adaptable and capable of handling larger datasets while maintaining the robustness and reversibility of the current approach.

Acknowledgements

The author conveys deep gratitude to the supervisor for offering guidance and persistent support during this study.

References

[1] Krishna Chaitanya Nunna, and Ramakalavathi Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography," *SoutheastCon*, Raleigh, NC, USA, pp. 1-5, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Osama F. AbdelWahab et al., "Hiding Data in Images Using Steganography Techniques with Compression Algorithms," *Telecommunication Computing Electronics and Control*, vol. 17, no. 3, pp. 1168-1175, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Camille B. Smith, "*The Comparison of Steganography and Cryptography: Concealing Information*," Master of Science in Cybersecurity, Utica College, pp. 1-10, 2019. [Google Scholar]

[4] Digvijay Pandey et al., "Secret Data Transmission Using Advanced Steganography and Image Compression," *International Journal of Nonlinear Analysis and Applications*, vol. 12, pp. 1243-1257, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ferda Ernawan, and Dhani Ariatmanto, "A Recent Survey on Image Watermarking Using Scaling Factor Techniques for Copyright Protection," *Multimedia Tools and Applications*, vol. 82, pp. 27123-27163, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Lin Wu et al., "Deep Adaptive Feature Embedding with Local Sample Distributions for Person Re-Identification," *Pattern Recognition*, vol. 73, pp. 275-288, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Bing Chen et al., "Secret Sharing Based Reversible Data Hiding in Encrypted Images With Multiple Data-Hiders," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 978-991, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Aditya Kumar Sahu, and Gandharba Swain, "High Fidelity Based Reversible Data Hiding Using Modified LSB Matching and Pixel Difference," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 4, pp. 1395-1409, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Fatuma Saeid Hassan, and Adnan Gutub, "Novel Embedding Secrecy within Images Utilizing an Improved Interpolation-Based Reversible Data Hiding Scheme," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 2017-2030, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Solihah Gull, Shabir A. Parah, and Khan Muhammad, "Reversible Data Hiding Exploiting Huffman Encoding with Dual Images for IoMT Based Healthcare," *Computer Communications*, vol. 163, pp. 134-149, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yaomin Wang, Zhanchuan Cai, and Wenguang He, "High Capacity Reversible Data Hiding in Encrypted Image Based on Intra-Block Lossless Compression," *IEEE Transactions on Multimedia*, vol. 23, pp. 1466-1473, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Zhaoxia Yin et al., "Reversible Data Hiding in Encrypted Images Based on Pixel Prediction and Multi-MSB Planes Rearrangement," *Signal Processing*, vol. 187, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Prasanth Vaidya Sanivarapu et al., "Patient Data Hiding into ECG Signal Using Watermarking in Transform Domain," *Physical and Engineering Sciences in Medicine*, vol. 43, pp. 213-226, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Tzu-Chuen Lu, Ting-Chi Chang, and Jau-Ji Shen, "An Effective Maximum Distortion Controlling Technology in the Dual-Image-Based Reversible Data Hiding Scheme," *IEEE Access*, vol. 8, pp. 90824-90837, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Yaomin Wang, and Wenguang He, "High Capacity Reversible Data Hiding in Encrypted Image Based on Adaptive MSB Prediction," *IEEE Transactions on Multimedia*, vol. 24, pp. 1288-1298, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jie Hu, and Tianrui Li, "Reversible Steganography Using Extended Image Interpolation Technique," *Computers & Electrical Engineering*, vol. 46, pp. 447-455, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[17] Shaswata Saha et al., "Extended Exploiting Modification Direction Based Steganography Using Hashed-Weightage Array," *Multimedia Tools and Applications*, vol. 79, pp. 20973-20993, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] R. Srikanth, and K. Bikshalu, "Multilevel Thresholding Image Segmentation Based on Energy Curve with Harmony Search Algorithm," *Ain Shams Engineering Journal*, vol. 12 no. 1, pp. 1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]