Discover Internet of Things

Discover

Research

Innovative image interpolation based reversible data hiding for secure communication

Riya Punia[1] · Aruna Malik[1] · Samayveer Singh[1]

Received: 5 May 2023 / Accepted: 8 November 2023
Published online: 04 December 2023

Abstract
In an increasingly digitized world, secure communication plays a pivotal role in safeguarding sensitive information and ensuring the confidentiality of data transmission. Conventional encryption techniques are robust but often result in a loss of data during transmission, making it challenging to achieve both security and image quality simultaneously. To address this issue, an innovative technique for interpolation-based reversible data hiding (RDH) within images is presented in this study. The interpolation scheme considers the Min function of the neighboring pixels and generates the cover image. After that, a data hiding method is applied to the cover image by considering the intensity range of the pixels using the least-significant bit (LSB) substitution method. The suggested embedding approach first encrypts the secret message, and then it encodes the encrypted secret message into interpolated pixels based on pixel intensity range groups. This technique enables the image to be consistently recreated once the data has been extracted. The percentage increment in the embedding capacity and peak signal-to-noise ratio (PSNR) is 40.00 and 8.64% for the proposed method as compared to the existing method. The experimental results indicate that the proposed technique enhanced the embedding capacity for all test pictures and produced higher PSNR values.

Keywords Embedding capacity · Reversible data hiding · Encryption · Interpolation · Least-significant bit

1 Introduction

In information security, encryption is vital for encoding confidential data before transmission, creating indecipherable ciphertext. This shields the content from unauthorized access. Data hiding, using methods like embedding in images or audio files, not only conceals content but also challenges third parties to detect the existence of secret data. Unlike encryption, data hiding weaves secret information into seemingly harmless digital files, enhancing overall data transmission security. This double concealment makes significant contributions to fortifying security measures. In essence, the fusion of encryption and data hiding forms a sophisticated defense, protecting sensitive information by rendering it unreadable and strategically embedding it in the digital landscape, bolstering the resilience of security protocols.

Data hiding has emerged as a prominent technique in contemporary times to safeguard audio, video, or text files transmitted over the internet, mitigating the risk of security breaches. Security breaches occur when unauthorized users or programs access a network. This technology facilitates the secure encapsulation of any multimedia format within another multimedia format. Safeguarding data over an open network poses a significant challenge, prompting the adoption of various data hiding techniques to ensure authenticity, integrity, and reliability. These techniques can be broadly

✉ Samayveer Singh, samays@nitj.ac.in; Riya Punia, puniariya850@gmail.com; Aruna Malik, malika@nitj.ac.in | [1]Department of Computer Science & Engineering, Dr B R Ambedkar National Institute of Technology Jalandhar, Punjab, India.

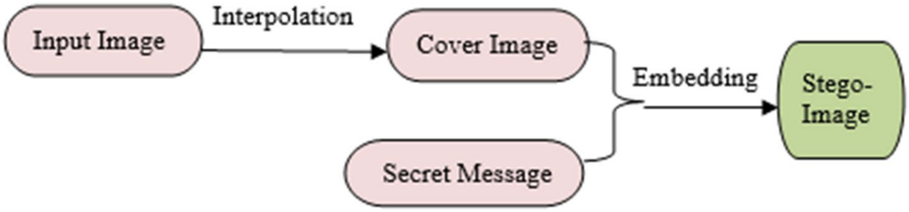
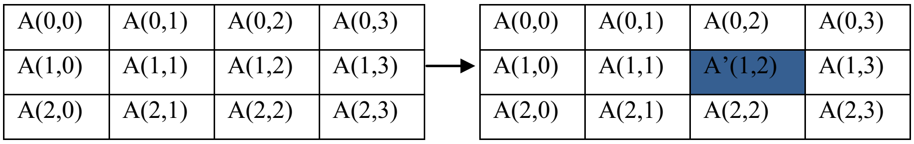


Fig. 1 Interpolation-based RDH Process [1]



A(0,0)	A(0,1)	A(0,2)	A(0,3)
A(1,0)	A(1,1)	A(1,2)	A(1,3)
A(2,0)	A(2,1)	A(2,2)	A(2,3)

→

A(0,0)	A(0,1)	A(0,2)	A(0,3)
A(1,0)	A(1,1)	A'(1,2)	A(1,3)
A(2,0)	A(2,1)	A(2,2)	A(2,3)

Fig. 2 BI example [2]

categorized into irreversible data hiding (IDH) and reversible data hiding (RDH), both commonly employed in securing information. In the context of irreversible data hiding, only the secret message can be retrieved, not the original image. Challenges may arise in certain scenarios, leading to the receiver's inability to accurately reconstruct the cover image. However, this limitation is context-dependent, and in fields such as medicine, the military, and crime scene investigation, preserving the cover image is imperative. The utilization of these data hiding techniques provides a multifaceted approach to fortifying data security over networks, addressing the intricate balance between concealing information and maintaining the integrity of the cover image.

In these situations, a remarkable type of data concealing technique known as reversible data hiding (RDH) is used. It can also be called as lossless data hiding as neither secret data nor the cover/original image is lost. Obtaining an unknown value based on known values or values is termed "Interpolation". This research paper is based on Interpolation based Reversible Data Hiding techniques. During interpolation, an original image is upscaled and new interpolated pixels are calculated using original/reference pixels. Then by using an embedding technique, a secret message can be concealed in the cover image resulting in a stego image which is illustrated in Fig. 1. Here, the entire embedded message is not visible to naked human eye.

Tamper detection in digital imagery, Image digital watermarking for copyright protection, embedding audio tracks in video signals, embedding subtitles in video signals, medical fields, military, and intelligence communication are a few of the applications of data hiding. The primary goal of researchers in the RDH field is to provide higher embedding capacity while increasing algorithmic performance. There are three metrics which are generally used for measuring the performance of a scheme (Fig. 2).

The mean squared error (MSE), peak signal to noise ratio (PSNR) and structural similarity index measure (SSIM) are the three basic image quality performance measurements. PSNR is a decibel (dB) based metric using Eq. (1) that is used to calculate the image quality.

$$PSNR = 10 * log10((256)^2 / MSE)$$

The mean squared error (MSE) is a measure of the average squared difference between corresponding elements of two images, typically the original image and a reconstructed image called stego-image. The formula for MSE is as follows:

$$PSNR = 10 * log10\left((256)^2 / \frac{1}{n \times n} \sum_{i=1}^{n} \sum_{j=1}^{n} (X_{ij} - Y_{ij})^2\right) \tag{1}$$

where n is the total number of pixels in the image, X_{ij} and Y_{ij} represent the pixel values in the ith row and jth column of the $n \times n$ sized cover image X and stego-image Y, respectively.

Structural similarity index measure (SSIM) is a metric used to quantify the similarity between two images. It takes into account luminance, contrast, and structure, providing a more comprehensive assessment than traditional methods like MSE or PSNR. The SSIM index produces a value between -1 and 1, where 1 indicates perfect similarity using Eq. (2). Higher SSIM values denote greater similarity between the compared images.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{2}$$

where, μ_x is the pixel sample mean of x, μ_y is the pixel sample mean of y, σ_x^2 the variance of x, σ_y^2 the variance of y, σ_{xy} the covariance of $x\text{and}y$, c_1 and c_2 are constant.

Contribution of the proposed work are as follows:

✓ The proposed scheme consists of two phases namely image interpolation and data hiding. The image interpolation method is based on the Min function which considers the neighboring pixels for generating the interpolated image.
✓ The secret data is embedded in the interpolated pixels during the data hiding phase by considering the intensity range of the pixels using the least-significant bit (LSB) substitution method. The use of the intensity range of the pixels enhances the capacity for hiding secret data within the image while maintaining image quality.
✓ The experimental results validate the effectiveness of the proposed scheme by showcasing improvements in data hiding capacity and image quality compared to existing methods.

This research paper flow is presented in the following order, the coming section discusses briefly several interpolation-based data hiding methods, followed by Sect. 3 demonstrating our proposed algorithm which is further categorized into two algorithms: one for interpolation and data hiding technique and a second for data extraction. Section 4 explains our proposed scheme with an illustrative example which is then followed by the experimental results section and hence at last we are concluding our research paper with further enhancements that can be made in the future.

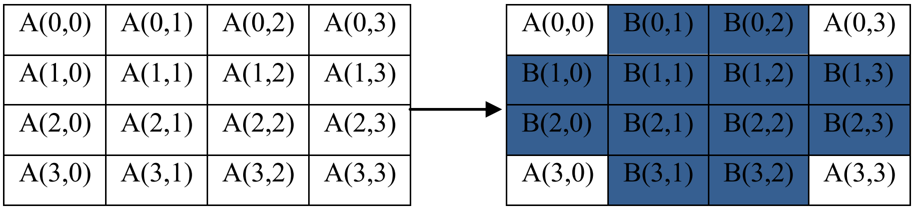
2 Literature review

Although interpolation-based reversible data hiding techniques have been studied, there is still a compromise between the ability to conceal data and the visual quality of the images. The next section discusses several interpolation techniques and data concealment strategies.

Liu et al. [2] introduced bilinear interpolation which uses the kernel method where non-overlapping blocks extracted from the original image are of equal sizes and then the weighted average of the reference (diagonally placed neighboring pixels) pixels is calculated using Eq. (3). Based on pixel block complexity, an adaptive pixel differencing method is used for embedding data. The final step is to embed the remaining pixels.

$$A'(1,2) = \frac{1}{3}x\left(\frac{A(0,0) + A(2,0)}{2}\right) + \frac{2}{3}x\left(\frac{A(0,3) + A(2,3)}{2}\right) \tag{3}$$

Rukundo et al. [3] used nearest-neighbor interpolation (NNI) where the pixel which is the nearest match is considered to produce a new interpolated pixel. NNI method takes the least computational time when compared to all other existing interpolation methods. In Fig. 3, the nearest pixel to the interpolated pixel $B(0,1)$ is $A(0,0)$ and similarly, the pixel nearest to $B(0,2)$ is $A(0,3)$. The entire pixel calculation for the block is shown in Eq. (4).



A(0,0)	A(0,1)	A(0,2)	A(0,3)
A(1,0)	A(1,1)	A(1,2)	A(1,3)
A(2,0)	A(2,1)	A(2,2)	A(2,3)
A(3,0)	A(3,1)	A(3,2)	A(3,3)

A(0,0)	B(0,1)	B(0,2)	A(0,3)
B(1,0)	B(1,1)	B(1,2)	B(1,3)
B(2,0)	B(2,1)	B(2,2)	B(2,3)
A(3,0)	B(3,1)	B(3,2)	A(3,3)

Fig. 3 NNI Example

$$\begin{array}{ll} B(0,1) = A(0,0) & B(0,2) = A(0,3) \\ B(1,0) = A(0,0) & B(1,2) = A(0,3) \\ B(1,1) = A(0,0) & B(0,3) = A(0,3) \\ B(2,0) = A(3,0) & B(2,2) = A(3,3) \\ B(2,1) = A(3,0) & B(2,3) = A(3,3) \\ B(3,1) = A(3,0) & B(3,2) = A(3,3) \end{array} \quad (4)$$

Jung et al. [4] found the neighbor mean interpolation (NMI) method where the mean of neighboring pixels is used to obtain interpolated pixels. Least significant method (LSB) is used for concealing secret messages. This method requires simple computation and hence, helps in concealing more amount of data without distorting the image quality. Figure 4 shows a 4 × 4 block for interpolation and Eq. (5) is used for pixel calculation.

$$\begin{array}{ll} B(0,0) = A(0,0) & B(1,0) = (A(0,0) + A(2,0))/2 \\ B(0,1) = (A(0,0) + A(0,2)/2) & B(1,1) = (A(0,0) + A(0,2) + A(2,0))/3 \end{array} \quad (5)$$

In Eq. (5), NMI formula is shown which is nothing but the average of the neighboring pixels, and the diagonal interpolated pixel is calculated with the help of reference pixels and two neighbor interpolated pixels. Another embedding scheme was proposed by Jung and Yoo et al. [5] wherein for non-overlapping sub-blocks, the pixel value is calculated using an index function using Eq. (6).

$$d = p(K.x + \beta, K.y + \delta) - p(K.x, K.y) \quad (6)$$

where β, δ = 0 or 1,

$$0 \leq x, y \leq 127$$

The number of bits to incorporate in the cover picture is determined using Eq. (7).

$$n = \lfloor Log2|d| \rfloor \quad (7)$$

NMI's improved version is enhanced neighbor mean interpolation (ENMI) where the weighted mean of reference pixels is calculated and then finds interpolated pixel values as shown in Fig. 5. Lee and Huang et al. [6] found this method. Here, the weighting of its reference neighbor pixels is used to determine the output pixel values. ENMI is an improved version of NMI wherein diagonal pixels are calculated using all the four reference pixels as shown in Eq. (8).

$$\begin{array}{ll} B(0,\ 0) = A(0,0) & B(1,0) = (A(0,0) + A(2,0))/2 \\ B(0,1) = (A(0,0) + A(0,2))/2 & B(1,1) = (A(0,0) + A(0,2) + A(2,0) + A(2,2)/4 \end{array} \quad (8)$$

In INP technique, difference values that are maximum are considered as shown in Fig. 6. This method has a huge embedding capacity. Interpolated pixels are calculated using Eq. (9).

$$\begin{array}{ll} B(0,\ 0) = A(0,0) & B(1,0) = (A(0,0) + A(2,0))/2 \\ B(0,1) = (A(0,0) + A(0,2))/2 & B(1,1) = (B(0,1) + B(1,0))/2 \end{array} \quad (9)$$

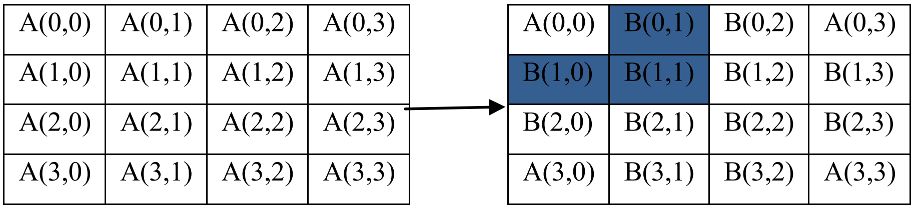
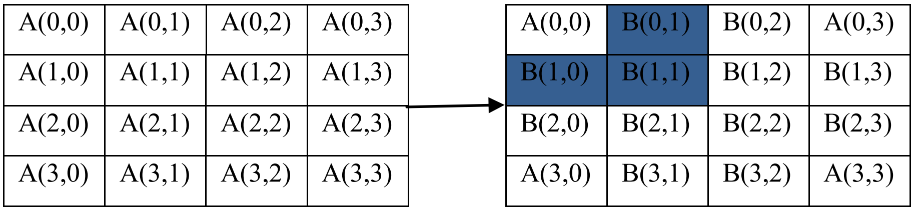


Fig. 4 NMI Example

A(0,0)	A(0,1)	A(0,2)	A(0,3)
A(1,0)	A(1,1)	A(1,2)	A(1,3)
A(2,0)	A(2,1)	A(2,2)	A(2,3)
A(3,0)	A(3,1)	A(3,2)	A(3,3)

A(0,0)	B(0,1)	B(0,2)	A(0,3)
B(1,0)	B(1,1)	B(1,2)	B(1,3)
B(2,0)	B(2,1)	B(2,2)	B(2,3)
A(3,0)	B(3,1)	B(3,2)	A(3,3)

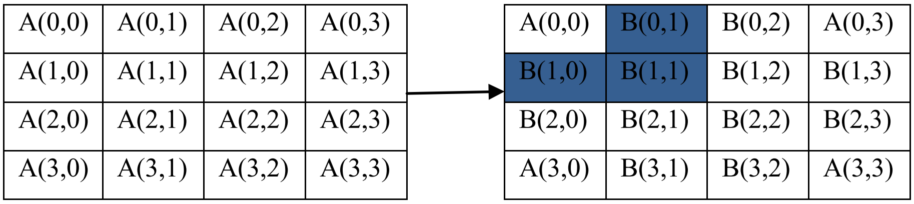
Fig. 5 ENMI Example



A(0,0)	A(0,1)	A(0,2)	A(0,3)
A(1,0)	A(1,1)	A(1,2)	A(1,3)
A(2,0)	A(2,1)	A(2,2)	A(2,3)
A(3,0)	A(3,1)	A(3,2)	A(3,3)

A(0,0)	B(0,1)	B(0,2)	A(0,3)
B(1,0)	B(1,1)	B(1,2)	B(1,3)
B(2,0)	B(2,1)	B(2,2)	B(2,3)
A(3,0)	B(3,1)	B(3,2)	A(3,3)

Fig. 6 INP Example



A(0,0)	A(0,1)	A(0,2)	A(0,3)
A(1,0)	A(1,1)	A(1,2)	A(1,3)
A(2,0)	A(2,1)	A(2,2)	A(2,3)
A(3,0)	A(3,1)	A(3,2)	A(3,3)

A(0,0)	B(0,1)	B(0,2)	A(0,3)
B(1,0)	B(1,1)	B(1,2)	B(1,3)
B(2,0)	B(2,1)	B(2,2)	B(2,3)
A(3,0)	B(3,1)	B(3,2)	A(3,3)

Malik et al. [7] proposed an even–odd data hiding scheme that works in two stages. Using odd and even valued pixels i.e., $bit - 0$ and $bit - 1$, location maps are created in stage one. And then in stage two, if secret message $bit = 0$ then the operation is taken else for $bit - 1$, even valued pixel is either incremented or decremented by 1. Zhang et al. [8] 's new data hiding methodology and parabolic interpolation technique add or delete hidden bit decimal values from interpolated pixels.

Modified neighbor mean interpolation [MNMI] is a more sophisticated variation of NMI that was introduced by Malik et al. [9]. The interpolation algorithm used here references pixels impact as well as all interpolated pixels, resulting in superior interpolated image quality. The cover image is segmented into smooth and complex region segments, with the complex portions containing more of the concealed secret message.

$$C(i,j) = \begin{cases} O(i,j) \ \ if \ \ i \ mod \ 2 = 0, j \ mod \ 2 = 0 \ \ and \ \ j < N - 1 \\ O(i,j) \ \ if \ i \ mod \ 2 = 0 \ \ and \ j = N - 1 \\ O(i,j) \ \ if \ j \ mod \ 2 = 0 \ \ and \ \ i = N - 1 \\ \frac{O(i-1,j) * 2 + O(i+1,j) * 2 + C(i,j-1)}{5} \ \ if \ i \ mod \ 2 = 1 \ \ and \ j = N - 1 \\ \frac{O(i,j-1) * 2 + O(i,j+1) * 2 + C(i-1,j)}{5} \ \ if \ j \ mod \ 2 = 1 \ \ and \ \ i = N - 1 \\ \frac{O(i-1,j) * 2 + O(i+1,j) * 2 + C(i,j+1)}{5} if \ i \ mod \ 2 = 1, \ j \ mod \ 2 = 0 \ \ and \ j < N - 1 \\ \frac{O(i-1,j-1) + O(i-1,j+1) + O(i+1,j-1) + O(i+1,j+1)}{4} \qquad otherwise \end{cases} \tag{10}$$

Equation (10) shows the MNMI formula, where O stands for the original picture and C for the cover image. Interpolation error and histogram shifting are used by Wang et al. [10] for embedding. Histograms are created using the FCM (Fuzzy C-Means) clustering algorithm. Peak, empty, and zero points are discernible from the cover image. The two phases of this system are as follows: in phase one, bin adjustments are performed between zero and peak points, and the secret message is concealed by modifications to peak and empty points. Malik et al. [11] proposed another novel weightage-based interpolation technique and reversible data hiding scheme which is based on range groups of pixel intensities. This scheme has better results than all other existing techniques.

In the 2022 study conducted by Benseddik et al. [12], the researchers focused on interpolation-based reversible data hiding in the transform domain. The emphasis on maintaining a tradeoff underscores the importance of finding an optimal balance between data hiding capacity and the preservation of data quality. In the study conducted by Mohammad et al. in 2023 [13], the authors introduced an interpolation-based reversible data hiding technique. The proposed technique demonstrated effectiveness in reducing cover image distortion, suggesting that the method was successful in minimizing the impact on the quality of the original image while providing a satisfactory capacity for hiding data. In the research conducted by Shastri et al. in 2023 [14], the focus was on the development of an interpolation-based dual-image reversible data hiding technique. The study aimed to enhance both the embedding capacity and PSNR of the process. The key improvement lay in maintaining a balanced tradeoff between embedding capacity (the amount of hidden data) and the quality of the images. This suggests that the proposed method achieved an improvement in the overall efficiency of reversible data hiding by optimizing the capacity for hidden information while simultaneously preserving the visual quality of the images. In the study conducted by Roselinkiruba et al. in 2023 [15], the authors focused on enhancing reversible data hiding, interpolation, and binary image encryption techniques. The research aimed to improve existing methods through the application of a combination of optimization techniques. The proposed approach demonstrated advancements PSNR and embedding capacity.

The paper [16] delves into spatial domain digital image steganography techniques, providing a comprehensive study. Moving on to the next [17], it centers around innovative methods for reversible data hiding, introducing a technique that employs block-wise histogram shifting to bolster data hiding security. The third paper [18] introduces a dual image-based reversible fragile watermarking scheme, emphasizing its utility in tamper detection and localization for enhanced digital image security. The fourth paper [19] focuses on tamper detection and localization in images, presenting a blind and fragile watermarking technique based on logistic maps. Lastly, the fifth paper [20] proposes a logistic-map-based fragile image watermarking scheme, with a primary objective of augmenting tamper detection and localization capabilities within the broader realm of multimedia security. The following research gaps have been identified after an exhaustive analysis of the existing literature:

As far as we know, there is no existing work which seems to consider the horizontal, vertical and/or diagonal edges as far as interpolation is considered. This overlook has impacted the performance of the existing works as far as PSNR is considered. For this, the proposed method takes a clue from the media edge detector which is predominantly used in RDH methods for predicting the pixel value. As experimental results also prove that the proposed method has been able to improve the performance in significant manner. The major challenge in the domain of interpolation-based data-hiding techniques revolves around the delicate balance between maximizing data embedding capacity and preserving the quality of the host media. This challenge arises from the inherent trade-off that exists between hiding substantial amounts of data within the host media and ensuring that the alterations made during the embedding process do not introduce perceptual artifacts or degrade the host media's quality. The major challenge is finding ways to maximize data embedding capacity without perceptually degrading the host media quality.

3 Proposed algorithm

In this section, a new image-based interpolation method for reversible data hiding schemes is proposed. The proposed work is divided into three different phases namely image interpolation, data embedding, and data extraction. Figure 7 illustrates the fundamental design of interpolation-based reversible data concealing. Interpolation and embedding methods are explained in Sect. 3.1 and data extraction is discussed in Sect. 3.2.

3.1 Proposed algorithm for image interpolation and data hiding

As far as we know, there is no existing work that seems to consider the horizontal, vertical, and/or diagonal edges as far as interpolation is considered. This overlook has impacted the performance of the existing works as far as PSNR is considered. For this, the proposed method takes a clue from the media edge detector which is predominantly used in RDH methods for predicting the pixel value. The algorithm for image interpolation and the embedding method to be used on the cover image created after applying the interpolation method to the original image are both illustrated in Sect. 3.1. When the original image of size $N \times N$ is used as an input, Stego-image S is produced as the output image.

Step 1 – The first step of the proposed methodology is interpolation where the source image O is interpolated as follows to create Cover Image C:

For i = 0 to N-1 do.
For j = 0 to N-1 do

$$Min\left[O(i,j-1), O(i,j+1)\right] \quad \text{if i mod 2 } = \text{ 0 and j mod 2 } = \text{ 1}$$

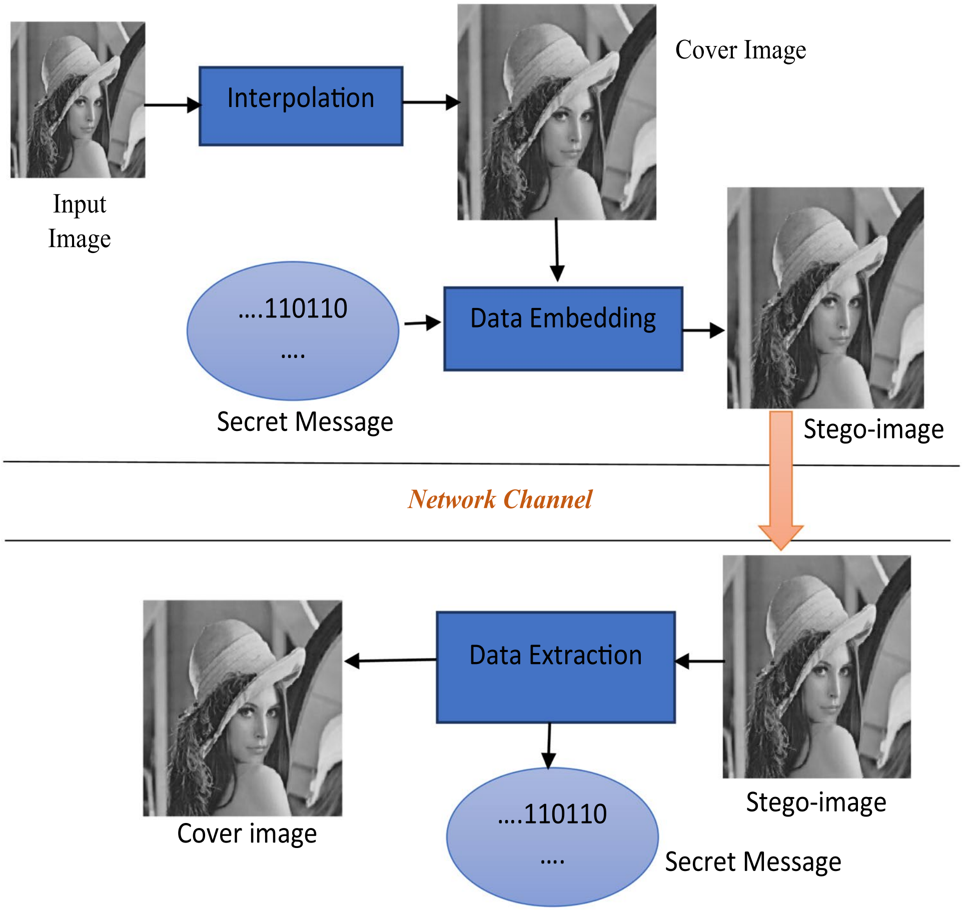


Fig. 7 Illustration of proposed technique

$$C(i,j) = Min\left[O(i-1,j), O(i+1,j)\right] \quad \text{if i mod 2} = 1 \text{ and j mod 2} = 0$$

$$Min\left[O(i,j-1), O(i,j+1), O(i-1,j), O(i+1,j)\right] \quad \text{if i mod 2} = 1 \text{ and j mod 2} = 1$$

End For.
End For.

Step 2—The secret message (SM) is first converted to SM' in the second step of the proposed process, which is called encryption.
Step 3—In the third step, group construction is performed to categorize the intensity range into 4 groups.

G1 = 0 to 15.
G2 = 16 to 31.
G3 = 32 to 191.
G4 = 192 to 255.

Step 4—This step performs embedding on the cover image obtained after step 1. Take all the interpolated pixels of the cover image C to embed SM'.

If the recognized pixel is falling under G1 range, then use the straightforward LSB substitution approach to substitute four LSBs of the recognized pixel with four bits of SM'.
Else if the recognized pixel belongs to G2 range, then using the straightforward LSB substitution approach to substitute three LSBs of the recognized pixel with three bits of SM'.

Else if the recognized pixel belongs to G3 range, then using the straightforward LSB substitution approach to substitute two LSBs of the recognized pixel with two bits of SM'.

Else the recognized pixel is belonging G4 range, then using the straightforward LSB substitution approach to substitute one LSB of the recognized pixel with one bit of SM'.

Step 5—For every interpolated pixel, repeat step 4. As a result, we can get the stego-image S.

3.2 Proposed data extraction algorithm

In Sect. 3.2, the data extraction step of the proposed methodology, which is carried out at the receiver side, is discussed. By the end of this stage, the receiver side can obtain both the original image and the secret message. The stego image is used as the input, and a data extraction method is used to produce a secret message as the output.

Step 1—In the first step, identify all the interpolated pixels from S.
Step 2—This step helps in extracting SM' from the stego image S.

If identified pixel ∈ G1 then extract 4 LSBs of the identified pixel and add it to SM' stream.
Else identify pixel ∈ G2 then extract 3 LSBs of the identified pixel and add it to SM' stream.
Else identify pixel ∈ G3 then extract 2 LSBs of the identified pixel and add it to SM' stream.
Else identified pixel ∈ G4 then extracts 1 LSB of the identified pixel and adds it to SM's stream.

Step 3—For every interpolated pixel, repeat step 2.
Step 4—Decryption is performed in step 4 by applying 1's complement to SM' to obtain the final secret message SM.
Step 5 – In the final step, obtain the original image by discarding all interpolated pixels.

4 Illustrative example of proposed method

In this section, an image interpolation method and the complete steps of the data embedding method are discussed. This section is further categorized into Sects. 4.1 and 4.2 which explain the entire proposed scheme using an example.

4.1 Image interpolation and data embedding step

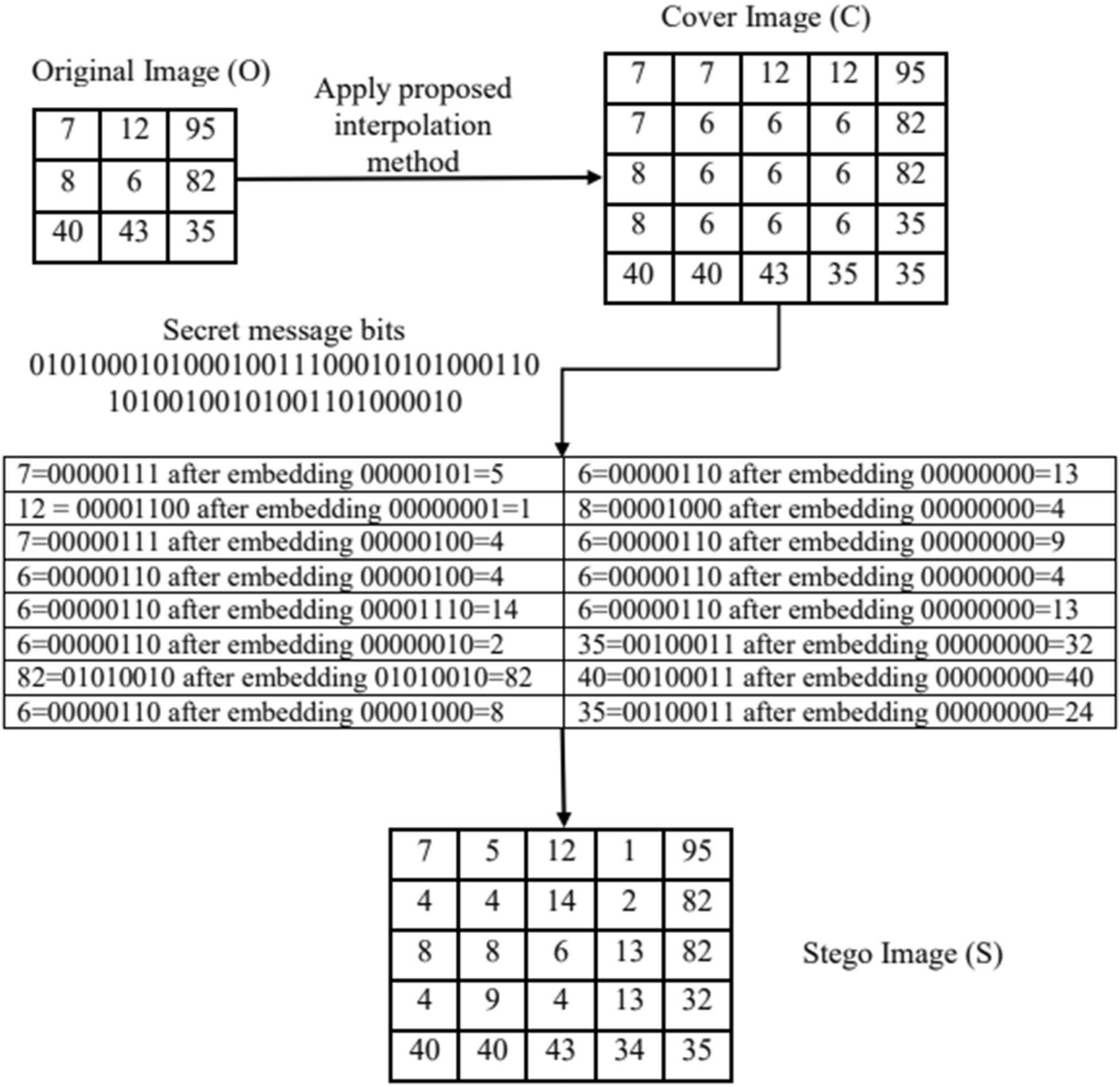
We get a 5 × 5 sub-block of the cover image by taking a 3 × 3 sub-block of the original image and using the interpolation function $C(i,j)$ to upscale the image as shown in Fig. 8. Usually, up-scaling is done by inserting rows and columns between adjacent rows and columns. So, the original image O is converted into the cover image C.

The proposed interpolation technique calculates the Min function for the neighboring pixels. To incorporate the data, the cover picture C that was produced following the interpolation phase is used. Let us consider the secret message as SM = "101 0111010111011000111010101110010101101101011001011110 1". The encryption of secret messages is done in two steps. Firstly, apply 1's complement to the secret message SM. As a result of this, we obtain an encrypted message, SM'=010100010 1000100111000101010001101010010010100110100001 0". The SM' is currently only incorporated in interpolated pixels. The number of bits to conceal in each recognized pixel is chosen depending on the pixel intensity range groups (G1, G2, G3, and G3).

According to the example, the first identified pixel from cover picture C is 7, which falls under group G1(0–15). As a result, we must conceal four bits of SM' in the identified pixel. The binary code for 7 is "00000111", while the four bits of SM are "0101". The new pixel value after embedding will be '00000101' = 5. The next recognized pixel is 12 which similarly falls under G1, therefore its four LSB bits are swapped with four SM' bits. '00000001' = 1 will be the new pixel value. Repeat the preceding steps for all of the remaining pixels from cover image C(7, 6, 6, 6, 82, 6, 6, 8, 6, 6, 6, 35, 40, 35). Thus, by repeating the whole procedure, SM' is incorporated into the interpolated pixels.

4.2 Data extraction process

Now, we have a 5 × 5 stego-image sub-block. For data extraction, firstly, the interpolated pixels 5,1,4,4,14,2,82,8,13,4,9 ,4,13,32,40,34 are identified from the stego-image S. The first interpolated pixel that is known to be in G1 is number 5.



Original Image (O)

7	12	95
8	6	82
40	43	35

Cover Image (C)

7	7	12	12	95
7	6	6	6	82
8	6	6	6	82
8	6	6	6	35
40	40	43	35	35

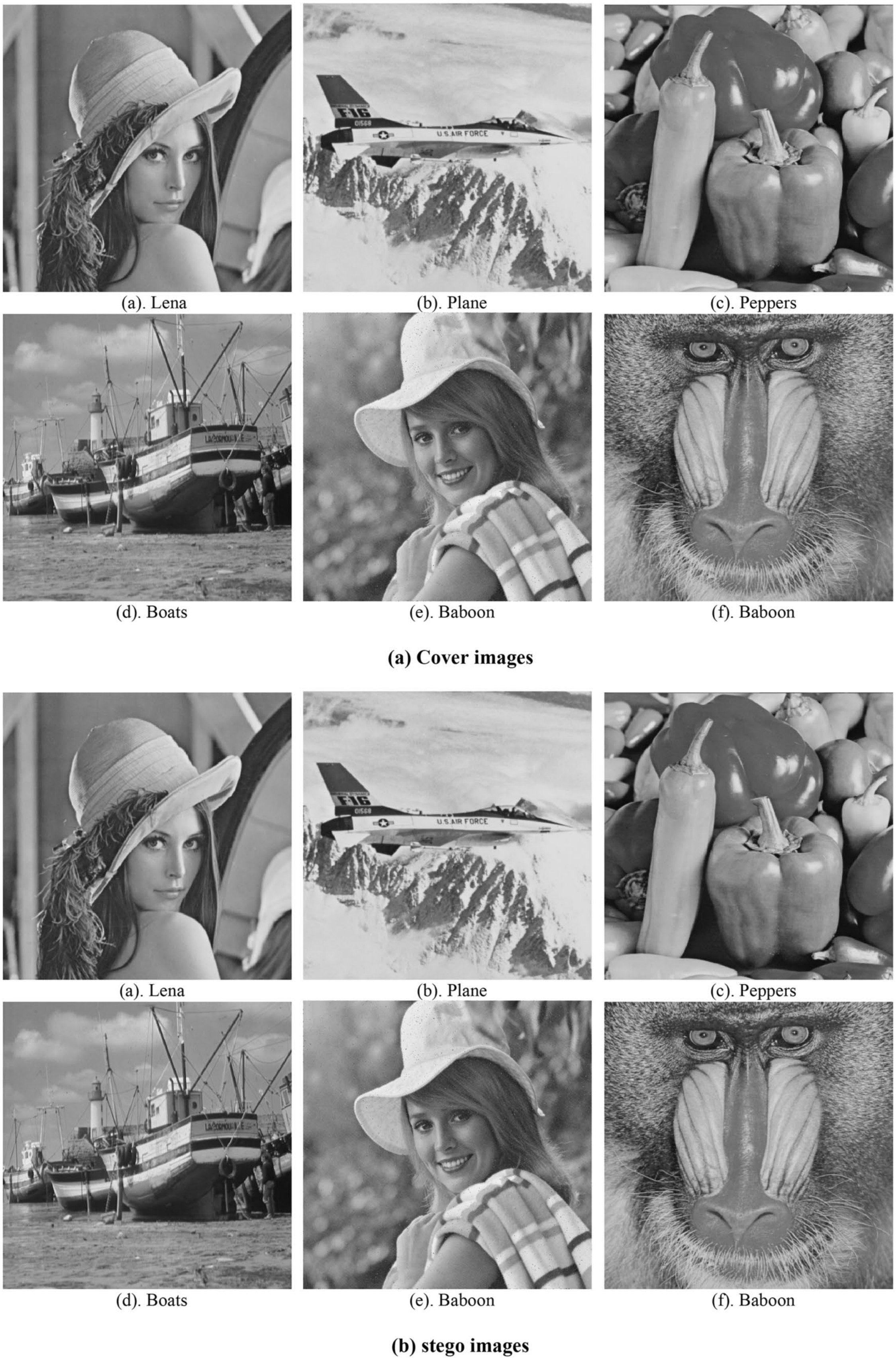
7=00000111 after embedding 00000101=5	6=00000110 after embedding 0000000=13
12 = 00001100 after embedding 00000001=1	8=00001000 after embedding 0000000=4
7=00000111 after embedding 00000100=4	6=00000110 after embedding 0000000=9
6=00000110 after embedding 00000100=4	6=00000110 after embedding 0000000=4
6=00000110 after embedding 00001110=14	6=00000110 after embedding 0000000=13
6=00000110 after embedding 00000010=2	35=00100011 after embedding 0000000=32
82=01010010 after embedding 01010010=82	40=00100011 after embedding 0000000=40
6=00000110 after embedding 00001000=8	35=00100011 after embedding 0000000=24

Stego Image (S)

7	5	12	1	95
4	4	14	2	82
8	8	6	13	82
4	9	4	13	32
40	40	43	34	35

Fig. 8 An example for a block of an image

Thus, in accordance with our algorithm's rule, four LSB are removed and then added to the data stream, because the binary representation of 5 is 00000101. The next interpolated pixel is 1(00000001), which is likewise under G1. Four LSB 0001 are thus extracted and appended to the data stream. The whole procedure is done in a similar manner for each interpolated pixel. Finally, the data stream is obtained as (0101000101000100111000101010001101010010010100110 1000010). Now, decryption is done by applying 1's complement to this obtained data stream. Hence, we can obtain a secret message. The secret message obtained is (1010111010111011000111010101110010101101101011001011110 1). By eradicating all interpolated pixels, the original image may be restored.



(a). Lena (b). Plane (c). Peppers

(d). Boats (e). Baboon (f). Baboon

(a) Cover images

(a). Lena (b). Plane (c). Peppers

(d). Boats (e). Baboon (f). Baboon

(b) stego images

Fig. 9 (**a**) Cover and (**b**) stego images

Table 1 Comparative PSNR (dB) values of several existing and the proposed technique

Images	Metrics	Jung et al. method [4]	Zhang et al. method [8]	Shaik et al. method [21]	Malik et al. method [11]	Proposed Method
Lena	PSNR	31.79	33.91	34.11	37.01	38.82
	Embedding capacity	2.2×10^5	2.25×10^5	3.8×10^5	4.2×10^5	7.9×10^5
	SSIM	0.9854	0.9887	0.9878	0.9954	0.9985
Airplane	PSNR	31.45	33.37	30.65	34.89	38.51
	Embedding capacity	2.2×10^5	3.8×10^5	4.1×10^5	6.3×10^5	7.8×10^5
	SSIM	0.9874	0.9887	0.9854	0.9987	0.9954
Boat	PSNR	29.51	28.21	29.22	34.13	36.68
	Embedding capacity	2.25×10^5	4.8×10^5	4.7×10^5	4.9×10^5	7.6×10^5
	SSIM	0.9812	0.9854	0.9854	0.9898	0.9968
Elaine	PSNR	29.87	29.58	31.52	32.16	37.64
	Embedding capacity	2.3×10^5	3.8×10^5	4.2×10^5	4.5×10^5	7.9×10^5
	SSIM	0.9857	0.9852	0.9868	0.9887	0.9941
Peppers	PSNR	33.39	28.14	29.32	36.51	39.20
	Embedding capacity	2.3×10^5	4.1×10^5	4.2×10^5	4.4×10^5	7.7×10^5
	SSIM	0.9868	0.9845	0.9812	0.9897	0.9968
Baboon	PSNR	23.86	22.87	22.74	31.46	33.38
	Embedding capacity	2.4×10^5	4.05×10^5	4.1×10^5	4.2×10^5	7.9×10^5
	SSIM	0.9857	0.9824	0.9857	0.9877	0.9924

5 Experimental results

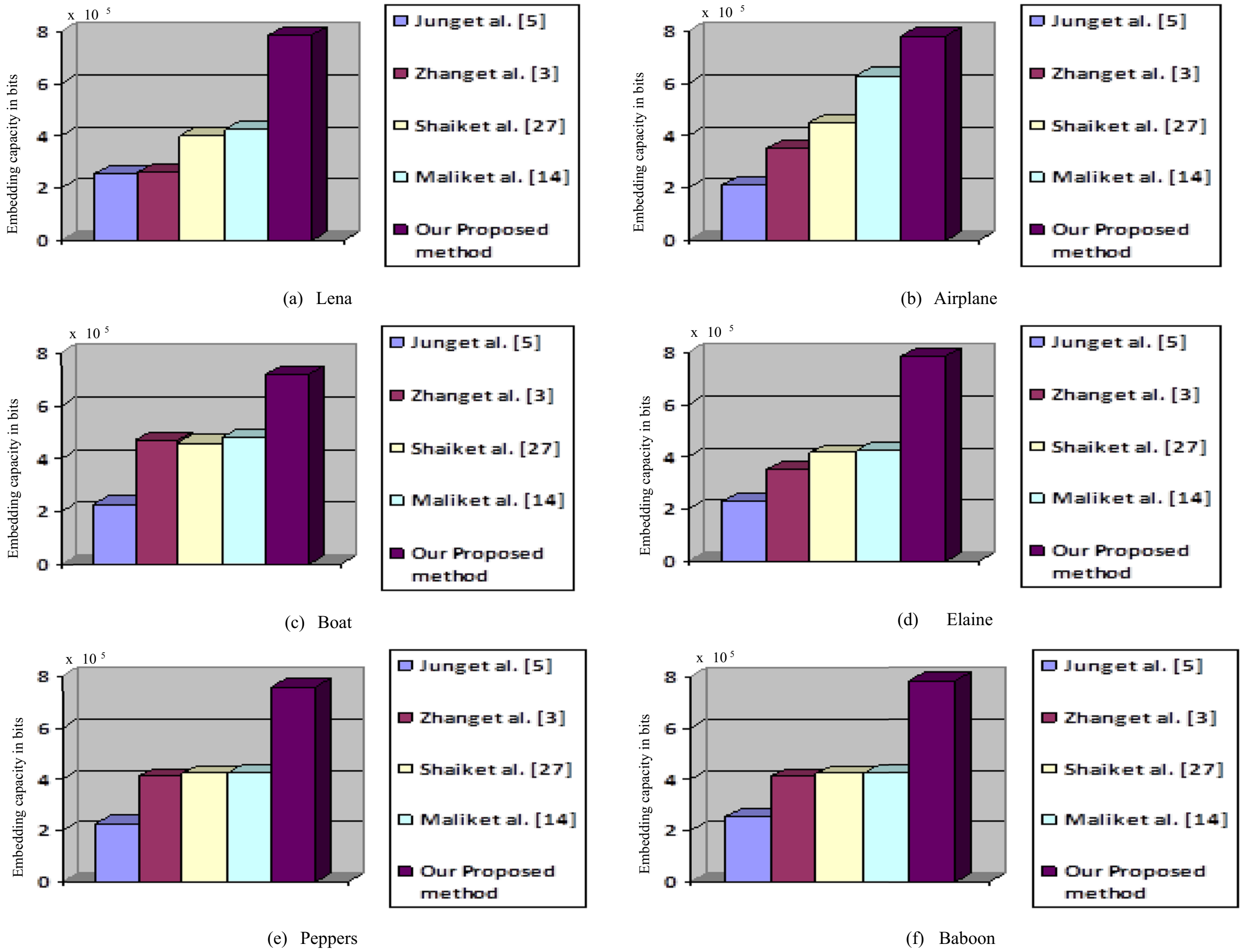
This section discusses the outcomes of experiments conducted by utilizing cover images. The six cover images are used of size 256 × 256 pixel such as lena, airplane, peppers, boat, elaine, and baboon as shown in Fig. 9. These images are then upscaled, after which interpolation method is used to generate cover images. The embedding procedure is then applied to cover images, yielding stego images.

As a result, Table 1 demonstrates that the proposed strategy outperforms previous strategies by yielding higher PSNR, embedding capacity and SSIM values for all test images. It can be also observed from Table 1 that the highest PSNR value is obtained for the peppers test image and the lowest PSNR obtained is for the baboon test image using the proposed interpolation based reversible data hiding scheme. Also, the proposed method has improved the embedding capacity for all the test cases. This has been represented in the bar graphs in Fig. 10 with embedding capacity in bits taken on the y-axis. The graph shows the comparison between existing techniques and our proposed method. It can be observed from the graphs that the highest embedding capacity is for the baboon image and the lowest is for the boat image using our proposed scheme.

Over this, it is evident from the graphs that the embedding capacity has been greatly improved by at least 40% for the majority of the test case images. As a result, the performance of the proposed method for interpolation and embedding is superior to that of existing methods. The outstanding performance of the proposed approach is primarily attributed to its simplicity. In contrast to other methods that entail complex calculations, the proposed approach excels by directly substituting the least significant bits (LSBs) of the pixels with the relevant secret data bits. In addition to that, interpolation method in image data hiding also enhances capacity as well as preserves visual quality.

6 Conclusion

This research paper discusses a rapid overview of contemporary steganographic techniques applied in the spatial realm along with the architecture of the interpolation-based data hiding process. A new image-based interpolation method for reversible data hiding scheme is discussed. In this proposed work, a new interpolation method for the images is discussed.



(a) Lena

(b) Airplane

(c) Boat

(d) Elaine

(e) Peppers

(f) Baboon

Fig. 10 Embedding data load result graphs for test images

After that, a reversible data hiding scheme is proposed. The PSNR of the proposed method has improved the embedding capacity for all the test cases. Moreover, it is evident from the results that the embedding capacity has improved by at least 40 percent for the majority of the test case images as compared to the proposed method. The future scope of the proposed work opens up several avenues for further research and development such as the enhancement of interpolation techniques, optimization of data hiding algorithms, security analysis, exploration of multi-pass techniques, application in multimedia security, and real-world implementations. Thus, continued research in these directions could contribute to the evolution and practical deployment of the proposed reversible data hiding scheme, making it a valuable tool in the field of secure data communication.

Author contributions RP: Methodology, Software, Investigation, Writing original draft. AM: Conceptualization, Methodology, Writing–review & editing. SS: Conceptualization, Methodology, Writing–review & editing, Validation.

Data availability No data has been used in this study. Moreover, all the information will be available on request to Riya Punia (puniariya850@gmail.com).

Declarations

Competing interests The authors declare that they have no competing interests.

References

1. Hussain Mehdi, Wahab Ainuddin Wahid Abdul, Idris Yamani Idna Bin, Ho Anthony TS, Jung Ki-Hyun. Image steganography in spatial domain: a survey. Signal Process Image Commun. 2018;65:46–66.
2. Liu Y-C, Hsien-Chu Wu, Shyr-Shen Yu. Adaptive DE-based reversible steganographic technique using bilinear interpolation and simplified location map. Multimed Tools Appl. 2011;52(2):263–76.
3. Chang Y-T, Huang C-T, Lee C-F, Wang S-J. Image interpolating based data hiding in conjunction with pixel-shifting of histogram. J Supercomput. 2013;66(2):1093–110.
4. Jung K-H, Yoo K-Y. Data hiding method using image interpolation. Comput Stand Interfaces. 2009;31(2):465–70.
5. Cox, Ingemar, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. Digital watermarking and steganography. Morgan kaufmann, 2007.
6. Chan C-K, Cheng L-M. Hiding data in images by simple LSB substitution. Pattern Recogn. 2004;37(3):469–74.
7. Malik Aruna, Sikka Geeta, Verma Harsh Kumar. An image interpolation based reversible data hiding scheme using pixel value adjusting feature. Multimed Tools Appl. 2017;76(11):13025–46.
8. Zhang X, Sun Z, Tang Z, Chunqiang Yu, Wang X. High capacity data hiding based on interpolated image. Multimed Tools Appl. 2017;76(7):9195–218.
9. Malik A, Sikka G, Verma HK. Image interpolation based high capacity reversible data hiding scheme. Multimed Tools Appl. 2017;76(22):24107–23.
10. Wang J, Mao N, Chen X, Ni J, Wang C, Shi Y. Multiple histograms based reversible data hiding by using FCM clustering. Signal Process. 2019;159:193–203.
11. Wu D-C, Tsai W-H. A steganographic method for images by pixel-value differencing. Pattern Recogn Lett. 2003;24(9–10):1613–26.
12. Benseddik ML, Zebbiche K, Azzaz MS, et al. Interpolation-based reversible data hiding in the transform domain for fingerprint images. Multimed Tools Appl. 2022;81:20329–56.
13. Mohammad AA. A high quality interpolation-based reversible data hiding technique using dual images. Multimed Tools Appl. 2023. https://doi.org/10.1007/s11042-023-15092-8.
14. Shastri S, Thanikaiselvan V. Interpolation based dual image reversible data hiding using trinary encoding. Multimed Tools Appl. 2023. https://doi.org/10.1007/s11042-023-15574-9.
15. Roselinkiruba R. Reversible data hiding using optimization, interpolation and binary image encryption techniques. Multimed Tools Appl. 2023;82:35757–80.
16. Sahu AK, Sahu M. Digital image steganography techniques in spatial domain: a study. Int J Pharm Technol. 2016;8(4):5205–17.
17. Kamil Khudhair S, Sahu M, R KR, Sahu AK. Secure reversible data hiding using block-wise histogram shifting. Electronics. 2023. https://doi.org/10.3390/electronics12051222.
18. Sahu AK, Sahu M, Patro P, et al. Dual image-based reversible fragile watermarking scheme for tamper detection and localization. Pattern Anal Applic. 2023;26:571–90.
19. Sahu AK. A logistic map based blind and fragile watermarking for tamper detection and localization in images. J Ambient Intell Human Comput. 2022;13:3869–81.
20. Sahu AK, Hassaballah M, Rao RS, et al. Logistic-map based fragile image watermarking scheme for tamper detection and localization. Multimed Tools Appl. 2023;82:24069–100.
21. Al-Dmour H, Al-Ani A. A steganography embedding method based on edge identification and XOR coding. Expert Syst Appl. 2016;46:293–306.

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