Multimedia Tools and Applications (2020) 79:18005–18031
https://doi.org/10.1007/s11042-020-08691-2

A Reversible Data Hiding Scheme for Interpolated Images Based on Pixel Intensity Range

Aruna Malik[1] · Geeta Sikka[1] · Harsh K Verma[1]

Received: 25 August 2018 / Revised: 28 December 2019 / Accepted: 28 January 2020 /
Published online: 25 February 2020

Abstract
In this paper, we propose a novel interpolation and a new reversible data hiding scheme for upscaling the original image and hiding secret data into the upscaled/interpolated image. This data hiding scheme considers the characteristics of the human visual system while embedding the secret data so that the existence of the secret data is not detected even after embedding a large amount of secret data. The proposed hiding scheme first divides pixel intensity ranges into groups and then adaptively embeds the secret data bits into the pixels based on the pixel intensity values. Therefore, the proposed scheme is able to maintain the visual quality of the stego-image. Experimental results show that the achieved PSNR by the proposed interpolation method is more than 30 dB for all the test images. Further, the results prove that the proposed data hiding scheme has superior performance than all the existing interpolation-based data hiding schemes.

Keywords Reversible data hiding · Pixel intensity · Image interpolation · PSNR · Embedding capacity

1 Introduction

Due to the advent of advanced network technologies, digital information in the form of text, image, audio or video is being distributed more conveniently via the public network like the Internet. However, the distribution or transmission of the confidential/sensitive information such as those used by the commercial businesses and by the military over the publicly

✉ Aruna Malik
arunacsrke@gmail.com

Geeta Sikka
sikkag@nitj.ac.in

Harsh K Verma
vermah@nitj.ac.in

[1] Department of Computer Science & Engineering, National Institute of Technology, Jalandhar, India

accessible network (Internet), makes them vulnerable to be attacked. Hence, the protection of such information has attracted the focus of many researchers. Some techniques have been developed to protect sensitive information from being intercepted or tampered. Basically, there are two techniques, namely cryptography and data embedding, which can easily verify whether the digital information is an original one or being illegally modified. Cryptography can be defined as an intuitional way to protect sensitive information, where sensitive information is encrypted by using some traditional Cryptographical methods, such as DES and RSA into a set of unreadable codes. By this, only the legal receiver with a key can decrypt and access the secret data while on the other hand, a person without a key is not able to extract the secret data. However, the meaningless encrypted codes may cause suspicion from the eavesdropper on covert communication. In order to address the meaningless problem, data embedding, as an alternative approach has been developed to reduce the suspicion among the invaders [4, 20, 35, 46, 54]. The data embedding technique is a process of inserting information bits into a host multimedia signal by introducing little distortions to the cover signal. These techniques are widely used for authenticity, verifying content ownership, and copyright violations. Nowadays, there is abundant literature about data embedding techniques. Inevitably, most of the existing data embedding schemes introduce some amount of distortions; even the distortion due to embedding is imperceptible to the human eye. However, there are some applications, such as medical, military imaging, and artwork preservation for which any distortion introduced to the content is not acceptable. As a result, reversible data hiding techniques emerge to recover the cover image without any loss [32]. In reversible data hiding, secret data is embedded into the cover image, and the cover image can be easily recovered without distortion after the extraction of the embedded secret data. Since it has low distortion, it can avoid an attacker's suspicion. Reversible data hiding has certain features like transparency, payload, and security. It can be effectively used for image authentication or copyright protection. Generally speaking, reversible data hiding cannot withstand any signal processing attacks. Currently, the reversible data hiding technique can be classified into the transform domain, compressed domain, and spatial domain methods. In the transform domain schemes [50], the host image is first transformed into a set of coefficients by utilizing a frequency-oriented mechanism such as discrete cosine transformation (DCT) [53] or discrete wavelet transformation (DWT) [52], then these coefficients are modified according to secret bits. After that, the modified coefficients are inversely transformed into marked pixels. The reversible data hiding technique under the compression domain is designed for images compressed by vector quantization [36], block truncation coding [5], etc. In the spatial domain [33] schemes, all pixel values are modified directly to embed secret data. The various techniques based on the above-mentioned schemes are discussed in [9–13, 21, 22, 26, 27, 39].

Generally, image interpolation [2] technique is used for generating a high-resolution image from a low resolution, i.e. it is a process by which a small image is resized or remapped to a larger one. Here, limited information is used to calculate and predict other pixel values [2, 28, 30, 31]. The limited information, or the known pixels, are called reference pixels and will leave unchanged while interpolating. In this paper, we propose a new interpolation method that considers all the proximate pixels by giving them different weights as per their closeness to the pixel being predicted. Thus, it provides a good quality interpolated image. Additionally, a reversible data hiding scheme is also proposed which embeds the secret data into the interpolated pixels based on their pixel intensity value. This scheme provides a good quality stego-image and high data hiding capacity both at the same time. The motivation and contribution of the proposed scheme are as follows:

1) The existing interpolation methods have not efficiently considered all the surrounding pixels while estimating the center pixel value. The proposed interpolation method makes use of a weighted technique for estimating the pixel values. The experimental results prove that the quality of the interpolated image is superior to the ones obtained using the existing methods.
2) The proposed data hiding scheme takes into account the human visual system characterizes for hiding the secret data into the cover image pixels. The method adaptively modifies the pixel values so that modification is not perceived by human eyes.
3) Further, the experimental results show that the proposed scheme has the highest performance in terms of both data hiding capacity and output image quality for all the test images. Additionally, the proposed hiding scheme is one of the simplest data hiding schemes as it only replaces the LSBs by the secret data bits.
4) Furthermore, the proposed data hiding method is a reversible data hiding method as it only modifies the interpolated pixel values while hiding the secret data. The interpolated pixel values can be recovered by the proposed interpolation method at the receiving end.
5) The applications which require the high-resolution images will be benefitted from the proposed interpolation and data hiding methods.

The rest of the paper is organized as follows. Section 2 discusses the related works. Section 3 discusses the proposed method and in section 4, experimental results are discussed. Finally, in section 5, the paper is concluded.

2 Related works

In this section, the Bilinear interpolation, Nearest Neighbor Interpolation, Neighbor Mean interpolation, Enhanced Neighbor Mean Interpolation, and existing interpolation-based data hiding schemes are briefly reviewed.

2.1 Bilinear interpolation

Bilinear Interpolation method uses the four nearest neighboring pixels, known as reference pixels located in diagonal directions from the given pixel. This method finds the gray level from the weighted average of the four closest pixels of the specified input coordinates and it assigns a value to the output coordinates. One of the main drawbacks of the bilinear interpolation method is that it generates a smoother image and has higher computation time as compared to the nearest neighbor method. Figure 1 shows an example of bilinear interpolation, where the pixel value of $P'(1,2)$ is calculated by weighting its reference neighbors which are pixels $P(0,0)$, $P(2,0)$, $P(0,3)$, and $P(2,3)$.

2.2 Nearest neighbor interpolation

The nearest neighbor method is a simple method, which finds the closest corresponding pixel in the source image P(i, j) for each pixel in the destination image pixel $P'(i,j)$. This method suffers from normally unacceptable aliasing effects with regard to enlarging and reducing images. Fig. 2 shows an example of nearest neighbor interpolation.

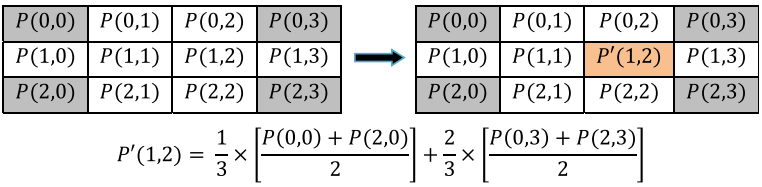


Fig. 1 Bilinear Interpolation

2.3 Neighbor mean interpolation

In 2018, Jung [16] and in 2009, Jung and Yoo [17] proposed a new data hiding scheme based on neighbor mean interpolation (NMI). The NMI method calculates the mean using neighboring pixel values and inserts it into pixels that have not been allocated yet. Fig.3 shows an example for neighbor mean interpolation. The NMI is calculated for 3 × 3 sub-block as$P'(0, 1) = (P(0, 0) + P(0, 2))/2$, $P'(1, 0) = (P(0, 0) + P(2, 0))/2$, and $P'(1, 1) = (P(0, 0) + P'(0, 1) + P'(1, 0))/3$. The data hiding schemes based on the NMI helps to embed a large amount of secret data while maintaining image quality due to its simple computation.

2.4 Enhanced neighbor mean interpolation

The ENMI (Enhanced Neighbor Mean Interpolation) scheme [6] is an improved version of the Jung and Yoo scheme [17].

Figure 4 shows an example of how to process the enhanced neighbor mean interpolation, where the pixel value of $P'(0, 1)$, $P'(1, 0)$, $P'(1, 1)$, $P'(1, 2)$,and $P'(2, 1)$ are computed by weighting its reference neighbors pixels.

2.5 Interpolation based data hiding schemes

In 2009, Jung and Yoo [17] discussed an interpolation technique popularly known as neighbor mean interpolation method. This method has a high calculation speed and low time complexity. It firstly scales down the input image to ¼ of its initial size which is called an original image. The NMI method is used to enlarge the original image and convert it into a cover image, having the same size as the input image. Finally, secret bits are hidden into the scaled-up cover image. Hong and Chen [14] discussed a reversible data hiding scheme using histogram shifting technique which classifies the cover image into smooth and complex

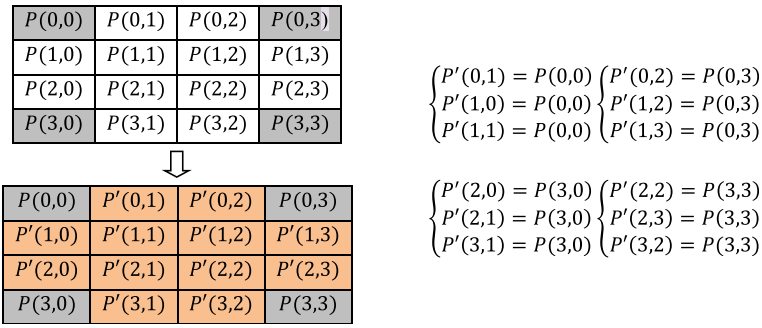


Fig. 2 Nearest Neighbor interpolation

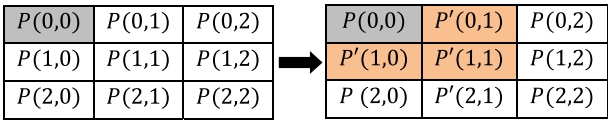


Fig. 3 Neighbor Mean Interpolation

regions. It builds a binary image that represents the locations of reference pixels. Firstly, fewer bits of the secret data are embedded into the complex regions since more reference pixels are chosen and thus image distortion is reduced. Secondly, it hides a number of secret data bits into the smooth regions since small numbers of reference pixels are chosen. Thus, it is able to manage the good data hiding capacity while maintaining the stego-image quality.

In 2012, Lee and Huang [29] improved the performance of the data hiding scheme given by Jung and Yoo [17] by proposing a new method called Interpolation by Neighboring Pixels (INP). This method takes the benefits of maximum difference values. Experimental results reveal that Lee and Huang's method has large embedding capacity i.e., up to 2.28bpp. Later, Wang et al. [51] proposed a reversible data hiding scheme based on interpolation and direction order mechanism. In this scheme, all pixels are divided into two categories, namely wall pixels and non-wall pixels. In the case of wall pixel, the interpolation error is calculated and is used to embed secret data. For non wall pixels, the difference value between the non-wall pixel and its parent pixel is calculated, which is defined by the direction order and is used to hide secret data through histogram shifting. Chang et al. [6] discussed image interpolating based data hiding scheme in conjunction with the pixel-shifting of the histogram. This scheme employs a two-stage data hiding method. At the first stage, by using the enhanced neighbor mean interpolation, a high-quality cover image is generated and then difference values are calculated from the input and cover pixels to embed secret data. In the second stage, a histogram modification method is applied to the difference image to further increase the payload and maintain the image quality without distortion. In 2014, Tang et al. [48] modified Lee and Huang [29] approach by providing a high capacity reversible steganography using multilayer embedding (CRS). In the same year, Lu and Huang [37] proposed an enhanced hiding scheme to improve Hong and Chen's scheme [14]. In their scheme, Difference Expansion, histogram and bilinear interpolation strategies are used to embed a secret message in the reference pixels for increasing the hiding capacity. Later, Hu and Li [15] proposed a high payload image steganographic technique based on the extended interpolating method. In this scheme, the difference between neighboring pixels is maximized to increase the capacity. In 2015, Jung and Yoo [18] discussed a steganographic method based on interpolation and LSB substitution of digital images. Firstly, interpolation methods are used to scale up and down the cover image before hiding secret data. Secondly, the LSB substitution method is used to embed secret data.

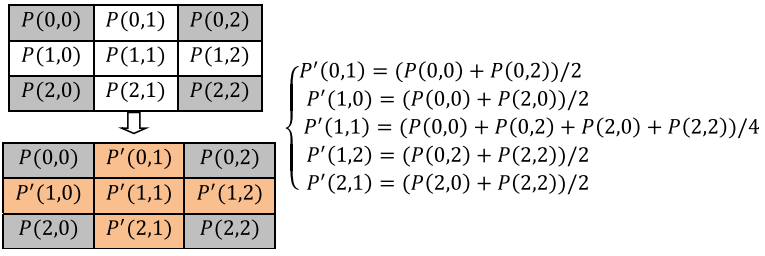


Fig. 4 Enhanced neighbor mean interpolation

In the same year, again Jung and Yoo [19] proposed an index based pixel value differencing method. By using an index function, the basis pixel is calculated for non-overlapping sub-blocks. In order to decide the number of embedding bits, the pixel-value differencing method is applied for other pixel-pairs of the sub-block. Finally, to keep the same basis pixel value, the pixel adjustment is used. Malik et al. propose an image interpolation based reversible data hiding scheme using the pixel value adjusting feature [38]. This scheme consists of two phases, namely: image interpolation and data hiding. The interpolation method takes into account all the neighboring pixels like the NMI method. However, it uses different weight-age as per their proximity. Thus, it provides a better quality interpolated image. In the case of the data hiding phase, secret data is embedded in the interpolated pixels in two passes. In the first pass, it embeds the secret data into the odd valued pixels and then in the second pass, the even-valued pixels are used to embed the secret data. Malik et al. propose an image interpolation based high capacity reversible data hiding scheme [40]. The proposed interpolation technique considers all the neighboring pixels as well as their impact on the reference pixels to provide better quality interpolated image and a new data hiding scheme which embeds the secret data in the interpolated pixels by taking into account the human visual system so that quality of the resultant image is maintained. The proposed data hiding scheme identifies the smooth and complex regions of the interpolated (or cover) image by dividing the same into blocks. It then embeds more bits into the complex regions of the image so that data hiding capacity, as well as the image quality, can be enhanced similar to [24, 25, 41, 42].

Meikap et al. propose a generalized directional pixel value ordering (DPVO) with varying block size [43]. The original image is partitioned into blocks and then enlarged using image interpolation. A new parameter (α) is introduced and added with maximum pixel value and subtracted from minimum pixel value to maintain the order of the rank which is dependent on the size of the image block. To improve data hiding capacity overlapped embedding has been considered in three different directions namely horizontal, vertical, and diagonal of each block. Lu discusses an interpolation based hiding scheme using the modulus function and re-encoding strategy [34]. It examines the probabilities for the position values and re-encodes the value according to its occurrence number. A re-encode function is used to obtain the rank of the position value in descending order. The most frequent position value is re-encoded to zero. The re-encoded codes are positive numbers, and the values of the codes are still large. To narrow down the value, the re-encoded codes are ciphered to generate mapping codes with negative and positive numbers. A mapping function is proposed to map the re-encoded code to the mapping code. The mapping code is half of the re-encoded code such that the image distortion becomes small. Kumar et al. propose a new reversible high capacity data hiding scheme using a combinatorial strategy which has very less distortion while hiding the secret data [22, 23]. It first builds a location map for the pixels of the cover image and then identifies the embeddable pixels. It divides the image into pairs of embeddable pixels and hides the secret data bits in each pair. The values of the embeddable pixels are updated according to prespecified rules. The pixel values get changed at most by one and some of them may remain unchanged. Wahed et al. discuss a new interpolation-based reversible data hiding scheme [49] which designs a capacity control parameter for high-quality stego-image. The scheme focusses to utilize the formula to determine a minimum set of embeddable bits in a pixel. Mohammad et al. [44] introduce a fast interpolation-based data hiding scheme for high payload. The scheme adaptively adjusts the level of tradeoff between data hiding capacity and image quality with an aim to maintain the stego-image quality while increasing the data hiding capacity. Zang et al. [55] suggest a parabolic interpolation-based data hiding to produce high quality

interpolated images, useful for medical applications. The scheme makes use of original as well as interpolated pixels for embedding the secret data. The utilization of a greater number of original pixels in the data hiding process improves the data hiding capacity while maintaining the good visual quality. Shaik et al. discuss another high capacity reversible data hiding using 2D parabolic interpolation [47]. In this paper, we also propose a new reversible data hiding scheme for interpolated image based on the pixel intensity range to further improve the embedding capacity and image quality. In the next section, the proposed method for the reversible data hiding scheme is discussed in detail.

3 Proposed method

In this section, we propose a reversible data hiding scheme for interpolated images based on pixel intensity range. In Section 3.1, the algorithm for the proposed data hiding scheme is provided. To demystify the proposed interpolation and embedding phase algorithm, examples are presented in Section 3.2 and 3.3 respectively. The algorithm for extraction of secret data and image restoration is discussed in Section 3.4 and an extraction example of the proposed algorithm is presented in Section 3.5.

3.1 Proposed data hiding algorithm

Input: Original image O with sized N × N.

Output: Stego-image S.

Step1: **(Interpolation step-)** Interpolate the original image O to cover image C as follows:

For i = 0 to N − 1 do.

For j = 0 to N − 1 do

$$C(i,j)=\begin{cases} O(i,j) \;\; if\ i\ mod\ 2=0, j\ mod\ 2=0\ and\ j<N-1 \\ O(i,j) \;\; if\ i\ mod\ 2=0\ and\ j=N-1 \\ O(i,j) \;\; if\ j\ mod\ 2=0\ and\ i=N-1 \\ \dfrac{O(i-1,j)*2+O(i+1,j)*2+O(i-1,j-2)+O(i+1,j-2)}{6} & if\ i\ mod\ 2=1\ and\ j=N-1 \\ \dfrac{O(i,j-1)*2+O(i,j+1)*2+O(i-2,j-1)+O(i-2,j+1)}{6} & if\ j\ mod\ 2=1\ and\ i=N-1 \\ \dfrac{O(i,j-1)*2+O(i,j+1)*2+O(i+2,j-1)+O(i+2,j+1)}{6} & if\ i\ mod\ 2=0, j\ mod\ 2=1\ and\ i<N-1 \\ \dfrac{O(i-1,j)*2+O(i+1,j)*2+O(i-1,j+2)+O(i+1,j+2)}{6} & if\ i\ mod\ 2=1, j\ mod\ 2=0\ and\ j<N-1 \\ \dfrac{O(i-1,j-1)+O(i-1,j+1)+O(i+1,j-1)+O(i+1,j+1)}{4} & otherwise \end{cases} \tag{1}$$

End For.

End For.

Step2: **(Encrypt step-)** Select a secret key of 8 bits and XOR this with all bytes of the secret message (SM).

Step3: **(Group construction step-)** Divide the intensity range into three groups as the first group (0–15 & 192–255), second group (16–31) and the third group (32–191).

Step4: **(Reversibility assurance step-)** Identify the interpolated pixels of the cover image to embed the secret message.

Step5: **(Embedding step-)** If the identified pixel belongs to the first group (wherein the pixel intensity is in the range of 192–255 or 0–15) then replace 4 LSBs of the identified pixel with the 4 bits of the secret message using a simple LSB substitution technique.

Else if the identified pixel belongs to the second group (wherein the pixel intensity is in the range of 16–31) then replaces 3 LSBs of the pixel with the 3 bits of the secret message using simple LSB substitution technique.

Else replace 2 LSBs of the pixel with the 2 bits of the secret message using a simple LSB substitution technique.

Step6: Repeat step 4 for all the interpolated pixels. Thus, proceeding the same the stego-image S is obtained.

3.2 Illustration of modified neighbor mean interpolation (MNMI)

An example to explain our proposed modified neighbor mean interpolation method for scaling the original image of size 3×3 is shown in Fig.5. Initially, we add one blank row and one column between two adjacent rows and columns, respectively, as shown in Fig.5 (b) and assign original pixel values to the old locations as follows: C(0, 0) = O(0, 0), C(0, 2) = O(0, 2), C(0, 4) = O(0, 4), C(2, 0) = O(2, 0), C(2, 2) = O(2, 2), C(2, 4) = O(2, 4), C(4, 0) = O(4, 0), C(4, 2) = O(4, 2), and C(4, 4) = O(4, 4).

It then calculates the center pixel values of C(1, 1),C(1, 3),C(3, 1), and C(3, 3) with the help of original image pixels using Eq.(1).

It is basically the average value of all the surrounding pixels. After calculating the center pixel values, the value of the other pixels like C(0, 1), C(1, 0), C(0, 3), C(1, 2), C(1, 4), C(2,1),C(3, 0), C(2, 3), C(3, 2), C(3, 4), C(4, 1), and C(4, 3) are calculated i.e., 28, 32, 31, 28, 26, 35, 52, 25, 32, 46, 49, and 52, respectively. The scaled-up pixel values of the last row and column are computed with the help of the pixel values of the previous rows and columns, respectively as shown in Fig. 5. This process can be repeated for the entire image to get the final scaled up image.

3.3 Illustrative example for interpolating the original image and data embedding process

An example of the interpolating image and the embedding process is illustrated in Fig. 6. We have considered a 3 × 3 sub-block of an original image (7,12,95,8,6,82,40,43,35), and applied the proposed interpolating function $C(i, j)$ for scaling up the image. By using function $C(i, j)$, the 3 × 3 sub-block of the original image (7,12,95,8,6,82,40,43,35) is converted into new 5 × 5 sub-block of the cover image (7,9,12,50,95,8,8,36,49,62,8,19,6,42,82,24,24,36,41,47,40,30,43,41,35). Our interpolation method takes weightage based on the proximity of the current pixel into consideration while predicting the same since the value of the pixels is more likely to be close to the proximate pixels. However, the pixel values are also influenced by other surrounding pixels that's why we have considered four surrounding pixels and their weight is defined as per their proximity to the pixel. The proximate pixels are having double weight in comparison to the other pixels in consideration. Thus, the cover image is computed which is used to hide the secret data. Assume that the encrypted secret data bitstream is S_{db} = "10101110101110110001110101011100101011011O". The encryption of secret data is done to add one more layer of security. In this method, secret data will be hidden into

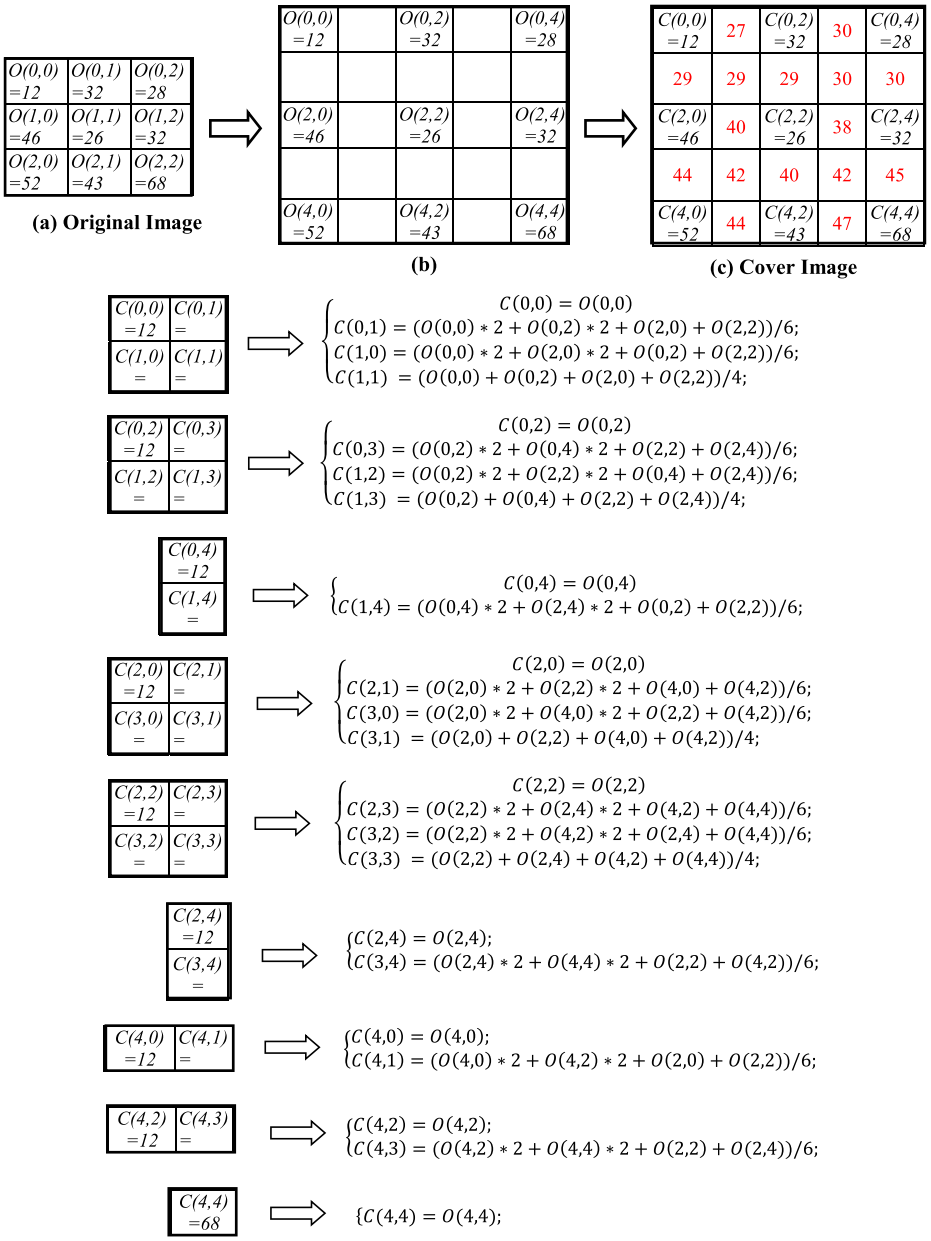


Fig. 5 An example of modified neighbor mean interpolation method

the interpolated pixels only that are (9,50,8,8,36,49,62,19,42,24,24,36,41,47,30,41). According to the data hiding rule, the number of bits to be hidden in each identified pixel is decided by the intensity of the pixel itself. In our example, the first interpolated pixel is 9, which lies in the range 0–15, so we can hide four bits in the pixel. The first four bits of the S_{db} are '1010' and the binary representation of 9 is '00001001' after replacing the secret data bits the pixel value will be '00001010' = 10. The next interpolated pixel is 50 which is

in the range of 32–191, so we can hide two bits in the pixel. The next two bits of the S_{db} are '11' and the binary representation of 50 is ′00110010′ after replacing the secret data bits the pixel value will be '00110011' = 51. The next interpolated pixel is 8 which is in the range of 0–15, so we can hide four bits in the pixel. The next four bits of the S_{db} are '1010' and the binary representation of 8 is '00001000' after replacing the secret data bits the pixel value will be '00001010' = 10. Thus, proceeding in the same manner, the secret data is embedded in the interpolated pixels. The complete process for the entire block is illustrated in Fig. 6.

3.4 Data extraction phase

The extraction phase is performed by the receiver. Here, the receiver reverses the embedding phase to extract the secret data and to recover the original image. In the end, 8 bits secret key with XOR operations is applied to the extracted message to regenerate the original message. By removing every interpolated pixel or the pixels which had secret data, the receiver can easily get the original image. The complete extraction algorithm is given as follows:

Input: Stego-image S
Output: Secret data
Step1: Identify the interpolated pixels in the stego-image.

Step2: (Secret data extraction step-) If pixel intensity of the identified pixel is in the range of 192 to 255 or 0 to 15 then extract 4 LSBs of the pixel and add it to the secret data stream.

Else if the pixel intensity of the identified pixel is in the range of 32 to 191 then extracts 2 LSBs of the pixel and adds it to the secret data stream.

Otherwise, the pixel intensity of the identified pixel is in the range of 16 to 31 then extract 3 LSBs of the pixel and adds it to the secret data stream.

Step3: Repeat the step2 for all the interpolated pixels.

Step4: (Decryption step:) XOR the obtained secret data in the bytes using the private key to obtain the original secret data bitstream.

Step5: Discard the interpolated pixels to get the original cover image.

3.5 Illustrative examples of extraction process

Suppose we have a 5 × 5 sub-block of stego-image, in order to extract the secret data from this stego-image, firstly, the interpolated pixels in the stego-image are identified which are 10,51,10,14,39,48,61,22,42,29,30,37,41,45,29, and 40. The first interpolating pixel is 10, which lies in the first group i.e., (0 to 15 and 192 to 255). So, according to our algorithm if the interpolating pixel lies in the first group then 4 LSB will be extracted and added to the secret data. So, after converting this interpolating pixel into binary form which is equal to$(00001010)_{2,}$ 4 LSB i.e. 1010 is extracted and is added to the secret data bitstream. Thus, we get the first 4 bits of secret data as 1010. Then, we check for the next pixel which is 51, now this pixel lies in the third group (32–191) similarly 2 LSB i.e. 11 will be extracted and added to the secret data bitstream. Thus, proceeding the same manner, we get the complete secret data bitstream as (10101110101110110001110101011100101010110110).

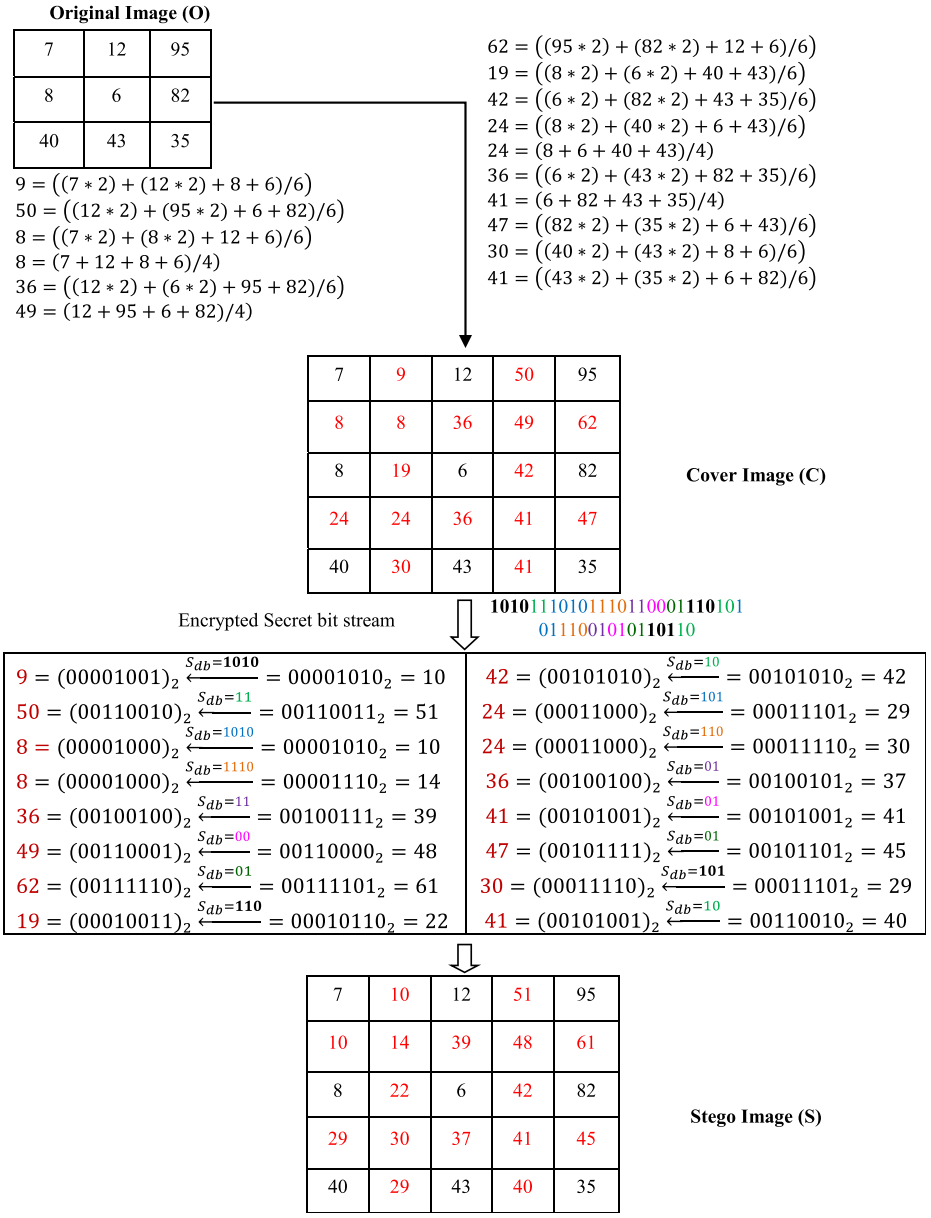


Fig. 6 An example of our proposed method for the interpolating image and embedding secret bitstream

4 EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we discuss and analyze the performance of our proposed scheme with respect to other popular and existing schemes. We have taken twelve images as the cover media for covering the maximum variance in the image characteristics. The twelve images, each of which is 512 × 512 pixels, namely Lena, Baboon, Airplane, Splash, Sailboat, Tiffany, House, Peppers, Couple, Elaine, Fishing Boat, and Man are shown in Fig. 7(a)-(l), respectively. We

have implemented the proposed scheme on the MATLAB tool running on the Intel® Core 2 (TM) i5 CPU 3.33 GHz and 4GB RAM hardware platform. The secret data used in the experiments are generated using a pseudo-random number generator. The performance analysis of the existing and proposed schemes is based on four commonly used parameters: hiding capacity, peak-signal-to-noise ratio (PSNR), embedding speed (in bits per second) and embedding time (in seconds). The hiding capacity refers to the number of secret data bits embedded in the cover image and the PSNR measure the stego-image quality with respect to the cover image. It is a commonly used metric to measure image reliability or conformity. The mathematical formula to calculate the PSNR value is as follows:

$$\mathrm{PSNR} = 10 \times \log_{10}\left[\frac{255^2}{\mathrm{MSE}}\right] \tag{2}$$

where MSE is the mean square error and is defined as follows

$$\mathrm{MSE} = \frac{1}{\mathrm{N} \times \mathrm{N}} \sum_{i=1}^{N} \sum_{j=1}^{N} \left(\mathrm{I_{ij}} - \mathrm{X_{ij}}\right)^2 \tag{3}$$

where, I_{ij} and X_{ij} indicate the pixel values of the i^{th} row and j^{th} the column of the $N \times N$ sized cover image I and stego-image X, respectively. In general, the larger PSNR value indicates the higher visual quality of the stego-image.

In the proposed scheme, we have introduced a new interpolation method which is an improvement of the existing NMI method and a new data hiding scheme for interpolated images. The performance of our modified NMI method and the data hiding scheme is discussed as follows.

4.1 Performance evaluation of the modified NMI method

In this section, the experimental results of our proposed and existing interpolation method for all the test images are illustrated in Table 1. For critical analysis, we have compared the performance of our method with the existing methods like NMI [17], Cubic spline Interpolation [3], Bi-cubic Interpolation [1], ENMI [6], Zhang et al. method [55], and 2D parabolic interpolation [47]. From Table 1, it is clearly evident that the proposed method performs much better than both the existing methods in terms of PSNR value. In fact, our interpolation method achieves a minimum 2.03% and maximum 50.39% increase in the PSNR value with respect to 2D parabolic interpolation [47] which is the best among the existing methods. The main reason for achieving better PSNR value is that our method uses all the proximate pixels while predicting the center pixel. Since different weights as per their closeness to the pixel are assumed by the proposed method, the performance is significantly better for complex images like Baboon and Tiffany than the existing methods which have good performance for smooth images like Lena, Airplane etc.

4.2 Data hiding results

This section illustrates the experimental results in terms of PSNR (dB) and embedding capacity (bits) of our proposed scheme with Jung &Yoo [17] method, Lu et al. [37] method, Mohammad et al. method [44], Zhang et al. method [55], and Shaik et al. method [47]. The PSNR is calculated between the original image and the stego-image. The image quality results

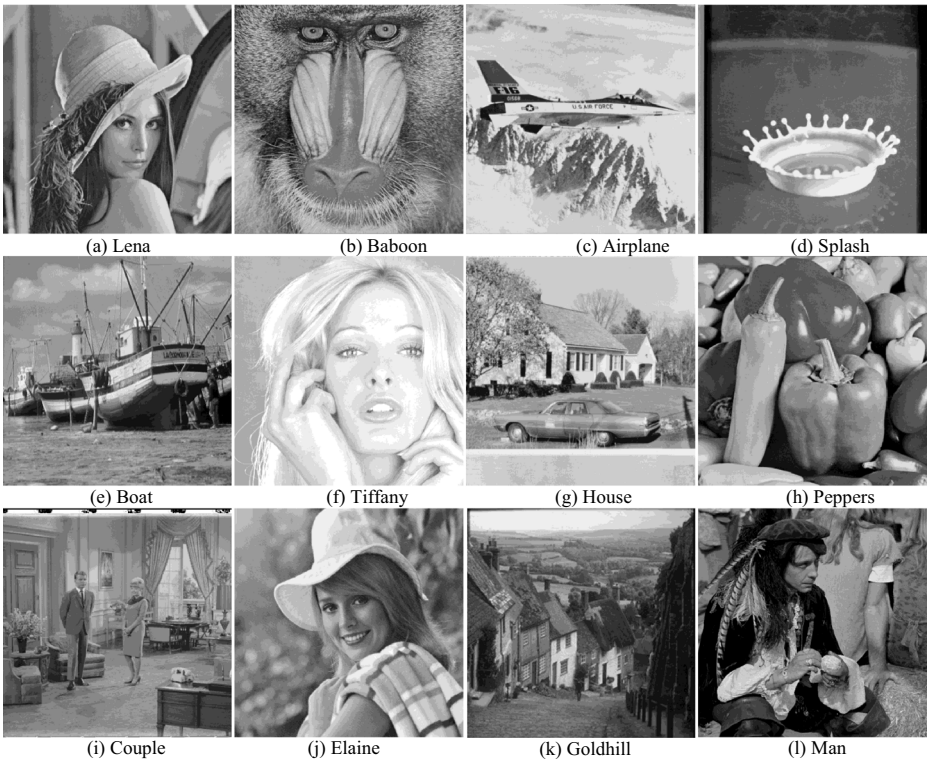


Fig. 7 Cover images

are presented in Fig. 8 by varying the embedding capacity so that comprehensive evaluation can be done. It is clear from Fig. 8 (a-l) the proposed scheme is far better than the existing schemes in terms of both the data hiding capacity and visual quality. In fact, it gains on the average 19.45% and 9.50% percent increment in the PSNR value and the data hiding capacity, respectively, with respect to Shaik et al. method [47]. We have calculated the increment percent with respect to Shaik et al. method [47] because its performance is better than all the available interpolation-based schemes in terms of both the data hiding capacity and image quality. The proposed scheme provides a better quality output-image because the proposed hiding scheme considers the characteristics of the human visual system and then embeds the secret data in the pixels of the cover image. Further, it basically makes lesser changes into the pixels having low-intensity value and more changes into the pixels of high-intensity value since, more change made to a low-intensity pixel might change its intensity value significantly, which in turn will raise suspicion, however, if the same amount of change is made in the high-intensity pixel then there is no chance of such suspicion among invaders. Additionally, it inherits the high-quality interpolated/cover image which helps tremendously in achieving performance goals. Thus, the proposed scheme is able to provide a good quality stego-image with high data hiding capacity. Further, the proposed scheme is a reversible data hiding scheme as it only modifies the interpolated pixels for hiding the secret data which can be recovered at the receiving end using the proposed interpolation method.

In Fig. 9 (a & b), we have presented the results of execution time and speed for the proposed scheme and other existing interpolation-based data hiding schemes like Jung & Yoo

Table 1 Comparison of PSNR (dB) of different existing and proposed interpolation method

Cover Image	Neighbor mean interpolation (NNI) [17]	Cubic spline Interpolation [3]	Bi-cubic Interpolation [1]	Enhanced NNI [6]	Zhang et al. method [55]	2D parabolic interpolation [47] (A)	Our interpolation method (B)	Percentage increment (B-A)/A %
Lena	31.79	35.74	35.38	33.47	33.91	34.11	37.01	08.50
Baboon	23.86	25.52	30.23	24.47	22.87	22.74	31.46	38.35
Airplane	31.45	35.23	33.42	33.37	28.34	30.65	34.89	13.83
Splash	30.01	31.02	31.02	31.23	31.58	34.54	39.13	13.29
Boat	29.51	28.85	29.45	30.83	28.21	29.22	34.13	16.80
Tiffany	32.41	33.47	33.78	23.71	26.54	24.61	37.01	50.39
House	29.89	30.87	31.25	31.11	28.65	30.87	34.58	12.02
Peppers	33.39	34.57	34.14	35.29	28.14	29.32	36.51	24.52
Couple	24.80	28.45	27.15	25.87	25.54	26.34	32.15	22.06
Elaine	29.87	29.76	29.36	30.87	29.58	31.52	32.16	02.03
Goldhill	31.80	32.47	32.14	33.06	28.91	30.57	34.72	13.58
Man	29.80	31.45	31.58	30.01	31.70	30.61	32.10	04.86

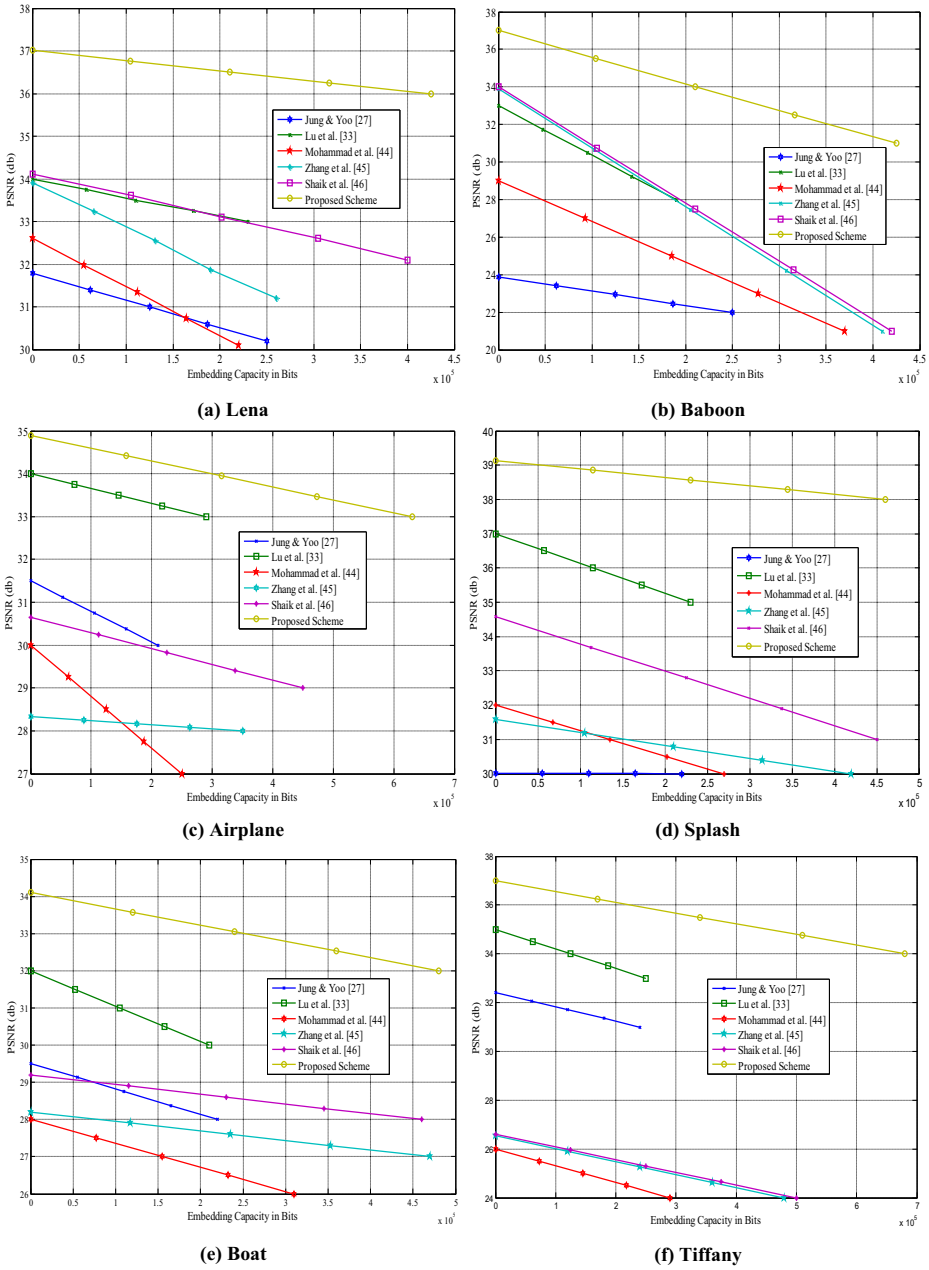
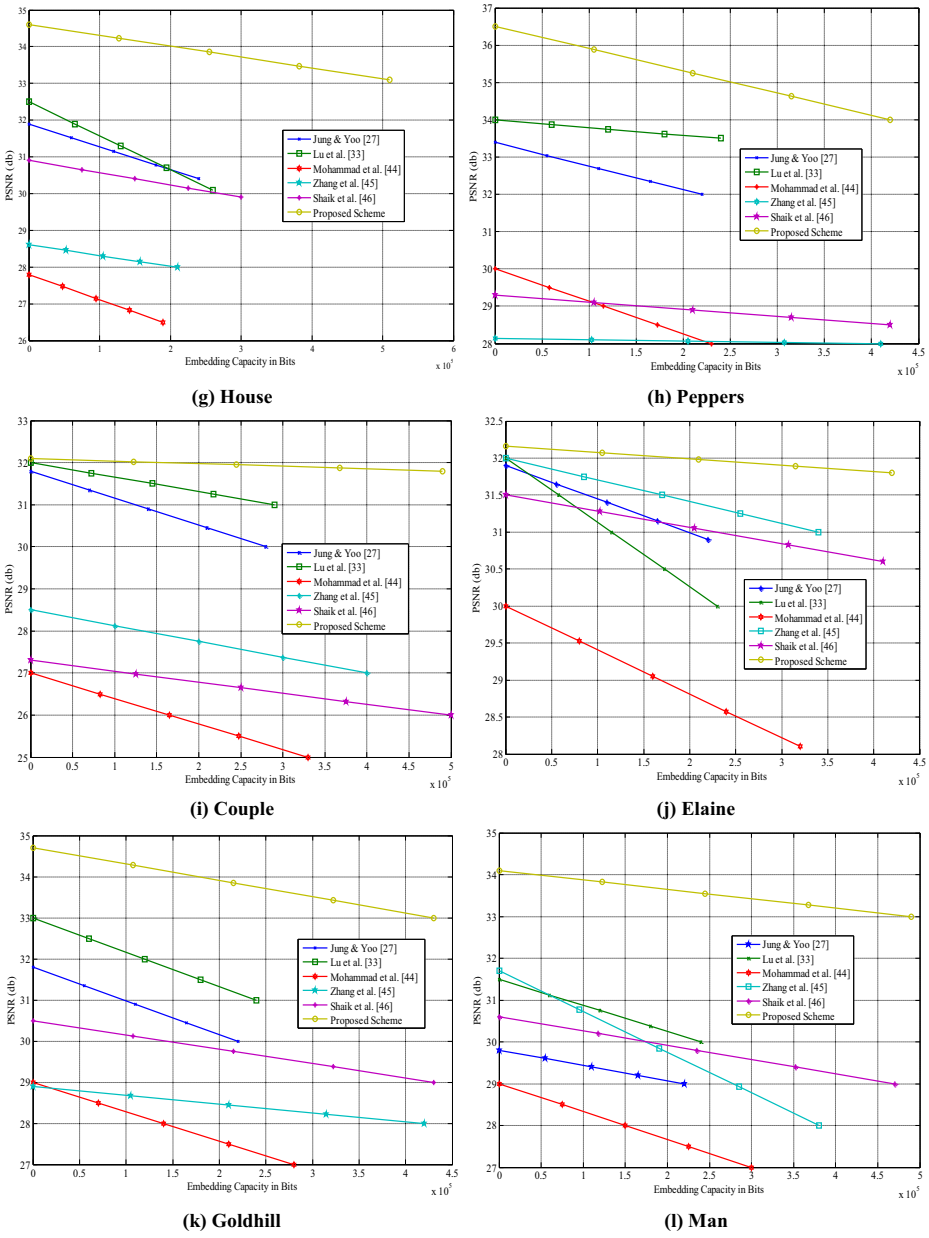


Fig. 8 Shows the comparison of PSNR (dB) and embedding capacity in bits for Jung & Yoo [17], Lu et al. [37], Mohammad et al. [44], Zhang et al. [55], Shaik et al. [47], and Proposed Scheme by considering different images

[17], Lu et al. [37], Mohammad et al. [44], Zhang et al. [55], Shaik et al. [47] methods. Fig. 9 shows that the proposed scheme has the highest embedding speed (bits/s) and the lowest minimum time (in seconds). The main reason behind the superior performance of the proposed scheme is its simplicity as it only replaces the LSBs of the pixels with the secret data bits unlike the complex calculation done by other methods [17, 37, 44, 47, 55].



(g) House **(h) Peppers**

(i) Couple **(j) Elaine**

(k) Goldhill **(l) Man**

Fig. 8 (continued)

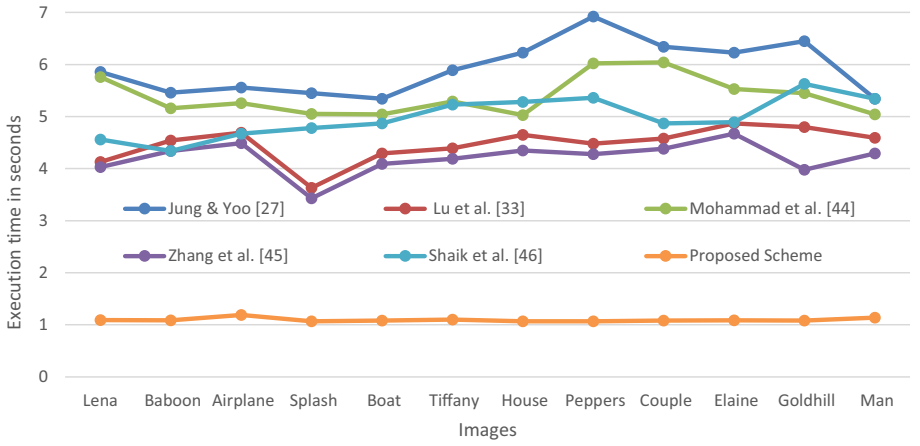
4.3 Steganalysis

Steganalysis is the art and science of detecting concealed information embedded through the practice of steganography. The steganalysis is an extremely challenging discipline as it is dependant on vulnerable steganography techniques and length of the hidden message. Generally, the secret data embedding in a cover image results in manipulations of pixel values,

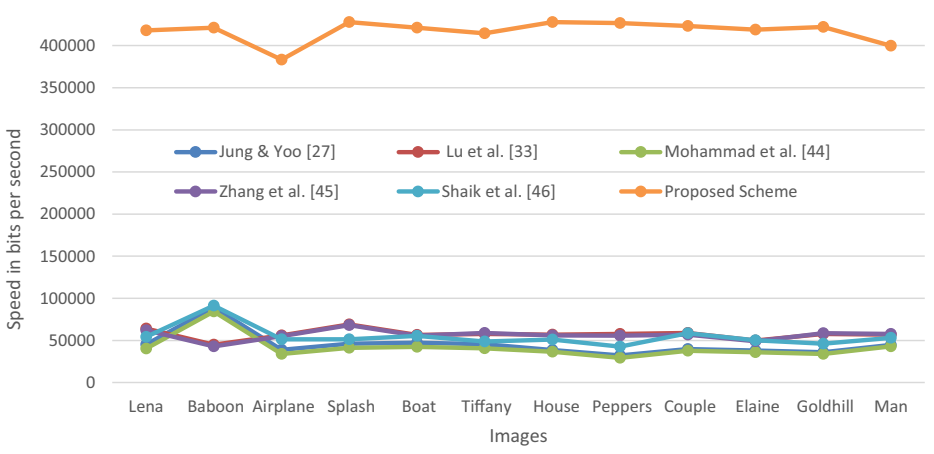
however, if the amount of embedded information is minute then the caused changes may be very limited which will be much more difficult to detect. For this, there are mainly two categories of steganalysis techniques, namely: targeted and blind, which are described as follows:

4.3.1 Targeted attacks

The targeted steganalysis method is used when the attacker has the clue about the steganography process as the embedding process usually leaves behind a specific pattern that can be investigated. In other words, the steganalyst is confident that secret communications have taken place and is also aware of an available process of embedding the information, then the targeted steganalysis based methods are considered as the method requires minimum effort to



(a) Execution time (seconds) for the existing method and proposed scheme by considering different images



(b) Speed (bit/seconds) for the existing method and proposed scheme by considering different images

Fig. 9 (a) Execution time (seconds) for the existing method and proposed scheme by considering different images. (b) Speed (bit/s) for the existing method and proposed scheme by considering different images

identify whether or not the image file consists of this kind of steganography or not. Three have been discussed multiple visual and statistical attacks relating to targeted steganalysis which are briefly reproduced in the context of the proposed data hiding scheme.

Visual attacks The visual attacks are the simplest form of steganalysis which are associated with the investigation of the stego media with the human eye in the hope that any occurrence of disparity is noticeable. An important rule of steganography is to ensure minimum degradation in the quality of image file, thus a good steganographic application will create stego objects that look quite similar to their cover object. However, when regions of the cover image that have not been altered during the embedding phase are removed, and the focus is put on probable regions having the embedded message, one is quite likely to detect traces of alterations. To counter this narrative of visual attack, the proposed data hiding scheme takes into account the human visual system while embedding the secret data into the interpolated image. The scheme makes the minimum changes into the low-intensity pixels and maximum changes into the high-intensity ones as it has been observed that the bigger changes in low-intensity pixels are quite perceivable to human eyes than the same amount of changes in the high-intensity ones and vice versa. Thus, the proposed scheme has decent protection against visual attacks.

Statistical attacks The statistical attacks are inspired by the concept of statistics in mathematics as the statistics make it viable to detect any random phenomenon within a data set by creating a hypothesis that apparently describes why this phenomenon happens. Then a statistical technique is applied to confirm the accuracy of the hypothesis. In the case of steganalysis, the data format for a stego object can be viewed with the lenses of statistics to determine whether or not an image includes secret information. For this, stego object is divided into two data sets namely image data, and message data. Generally, the image data relates to the facts of correlation whereas the message data (if coded) is usually more randomly constructed than image data. Thus, it can be derived that the message data is more random than image data, and this is where statistical attacks normally work. One of the most common and popular statistical steganalysis methods is RS steganalysis which is discussed in detail in the context of the proposed data hiding scheme.

a) **RS Steganalysis**

The regular singular (RS) steganalysis proposed by Fridrich et al. [8] is used to detect the presence of secret data within the stego-image. It is a technique for the detection of LSB embedding in colour and grey-scale. Fridrich et al. deliberate how statistical measures on LSBs for detecting the level of embedding, alone is inaccurate. They explain that this is mainly due to the lack of unrecognizable structure of the bit plane in a staged image. RS Steganalysis can manipulate this feature. Fridrich et al. method work by analyzing embedding capacity for lossless data insertion in LSBs. Randomizing LSBs minimizes this capacity. To inspect an image, the authors establish two groups of fixed shape. These groups are known as Regular (R) and Singular(S) groups of pixels and are based on particular attributes. For example, whether or not the pixel noise within the group (calculated using the mean absolute value of the differences between adjacent pixels) is increased or decreased after flipping the LSBs of a fixed set of pixels within each group. Subsequently, corresponding frequencies of both groups are then used to attempt to foresee the embedding degree, in the image retrieved from the

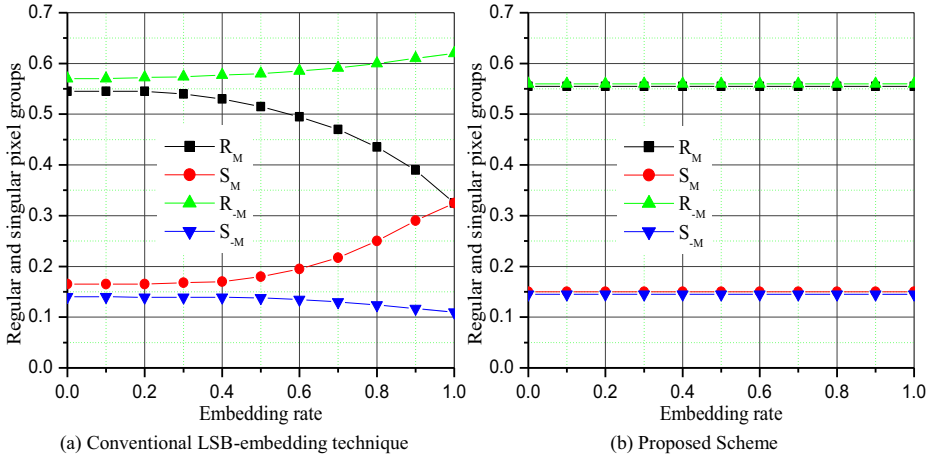


Fig. 10 RS steganalysis of the stego-image 'Peppers' with size of 512 × 512 (a) Conventional LSB-embedding technique, (b) Proposed scheme

initial image with flipped LSBs, and the image retrieved by randomizing the LSBs of the initial image.

Here, we check and analyze whether the proposed scheme can be detected by the RS steganalysis or not. In RS steganalysis method, all the stego-pixels are categorized into three-pixel groups namely: regular group (R_M or R_{-M}), singular group (S_M or S_{-M}), and unusable group. The stego-image will pass the RS detector when the relative number of R_M is equal to that of R_{-M} i.e., ($R_M \cong R_{-M}$) and the relative number of S_M is equal to that of S_{-M} i.e., ($S_M \cong S_{-M}$). Otherwise, the stego-image will be verified as a suspicious image which may reveal the presence of the secret data. For the proposed scheme verification, we have computed the detection results in terms of the percentage of hiding capacity with respect to the percentage of the regular and singular pixel groups with recommended masks M = [0 1 1 0] and –M = [0 − 1 − 1 0] as shown in Figs. 10, 11, 12. According to Fridrich et al. [8], if more and more LSBs are replaced with random data, then the percentages of R_M and S_M pixel groups will become

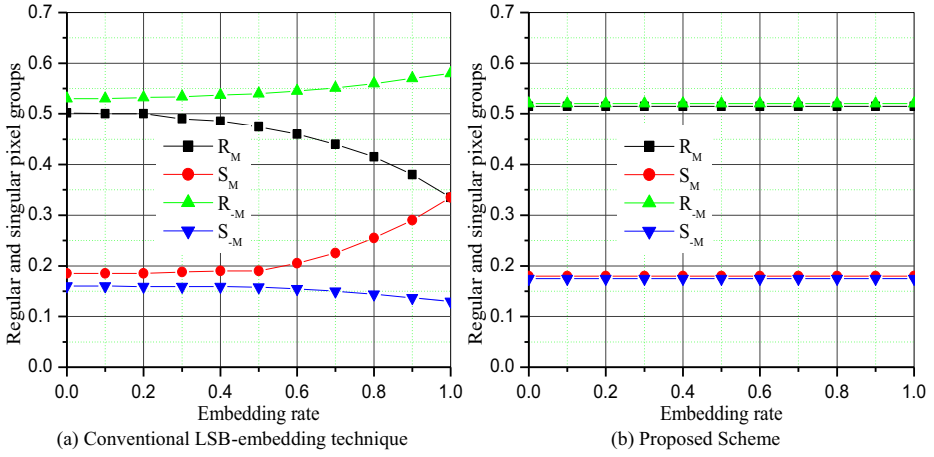
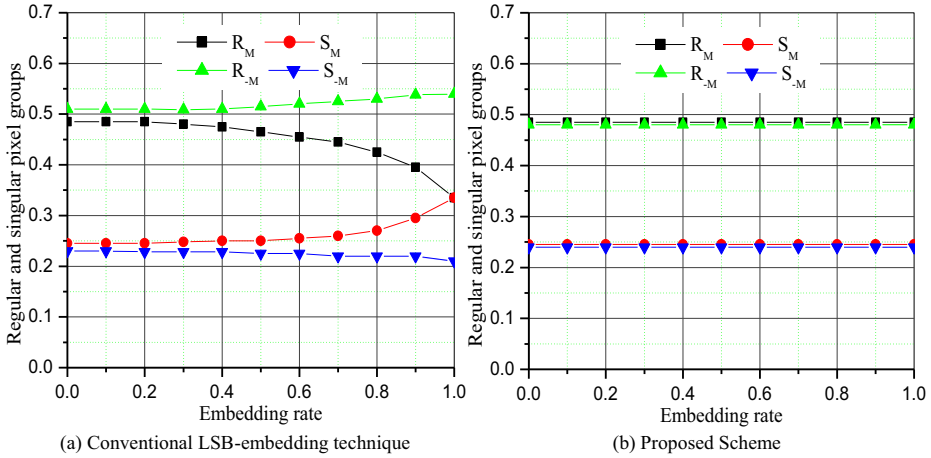


Fig. 11 RS steganalysis of the stego-image 'Lena' with size of 512 × 512 (a) Conventional LSB-embedding technique, (b) Proposed scheme



(a) Conventional LSB-embedding technique (b) Proposed Scheme

Fig. 12 RS steganalysis of the stego-image 'Baboon' with size of 512 × 512 (a) Conventional LSB-embedding technique, (b) Proposed scheme

gradually equal when the mask of M is adopted in the detection process, or the percentages of R_{-M} and S_{-M} will become more and more unequal when the mask of M is adopted. From the RS-diagram of Figs. 10, 11, 12(a) for Peppers, Lena and Baboon images, it is clearly evident that the secret data hidden through conventional LSB-embedding techniques in images is detectable as the value of R_M is more distant to that of R_{-M} and similar in the case of S_M and S_{-M}.

However, in the case of the proposed scheme, the Figs. 10, 11, 12(b) indicate that the stego-image seemingly does not contain any embedded data in their LSBs, because of the expected value of R_M is seen close to that of R_{-M} and same in the case of S_M and S_{-M}, i.e.,$R_M \cong R_{-M}$ and $S_M \cong S_{-M}$. Accordingly, the RS steganalysis detector is not able to detect the presence of secret data into the stego-images. Therefore, we can conclude that the proposed embedding scheme is able to resist against the RS detector attack. We have carried out experiments for all the twelve input images, however, their behavior is similar. So, to avoid redundancy of behavior, the

Table 2 Standard Deviation (SD) and Correlation Coefficient (CC) for different images

Cover & Stego-images	Correlation Coefficient	Standard Deviation (SD)		
		Cover image	Stego-image	Difference
Lena	0.9958	47.86	48.076	0.216
Baboon	0.9183	42.37	42.624	0.254
Airplane	0.9946	46.41	47.065	0.655
Splash	0.9976	51.51	51.721	0.211
Boat	0.9739	47.26	48.042	0.782
Tiffany	0.9863	29.11	29.651	0.541
House	0.9899	47.97	48.754	0.784
Peppers	0.9960	53.76	54.600	0.840
Couple	0.9491	40.68	40.894	0.214
Elaine	0.9781	46.58	46.834	0.254
Goldhill	0.9983	55.37	55.792	0.422
Man	0.9840	57.94	58.481	0.541

results for three different characteristics images i.e. Peppers, Lena & Baboon, are presented to prove our point.

The statistical attack is measured to test the robustness and innocuousness of the proposed scheme. The generated stego-images protect original information by hiding secret data through the proposed scheme. We embed original information within marked pixels in stego-images. The scheme is secure to preclude possible malicious attacks due to its innocuousness. Table 2 shows the correlation coefficient and the standard deviation between the interpolated cover image and interpolated stego-image. It shows that the correlation coefficient is nearer to one and the difference of standard deviation is nearer to zero indicate good concealment. The proposed scheme achieved stronger robustness against several attacks. Furthermore, the secret information can be retrieved without encountering any loss of data and recovered original image successfully from stego-images.

4.3.2 Blind attacks

The blind attacks do not depend on prior knowledge of any specific embedding procedures like targeted attacks. However, a steganalyst also does not think that any form of secret communications has transpired. Based on these observations, a series of algorithms are generally created to enable suspected image files to be investigated for indications of manipulations. If the algorithms find any clue of modification, then it is quite possible that the image file contains the hidden information. In the next sections, the procedure is to produce an estimate of the cover image using only a suspected image file is explained.

SPAM and SRM Steganalysis Subtractive Pixel Adjacency Matrix (SPAM) method is well known that values of neighboring pixels in images are not independent. This is not only caused by the inherent smoothness of images, but also by the image processing (de-mosaicking, sharpening, etc.) in the image acquisition device. This processing makes the noise, which is independent in the raw sensor output, dependent on the final image. The latter source of dependencies is very important for steganalysis because steganographic changes try to hide within the image noise. The SPAM features model dependencies between neighboring pixels

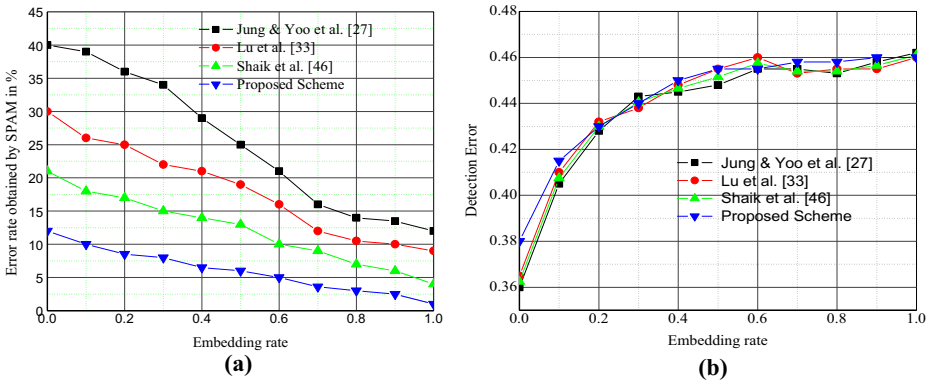


Fig. 13 Steganalysis of the stego-image 'Peppers' with size of 512 × 512 for proposed scheme, Shaik et al. [47], Lu et al. method [37], and Jung & Yoo [17] method (a) Error rate obtained by SPAM with respect to embedding rate, (b) Comparison of the detection error by SRM with respect to embedding rate

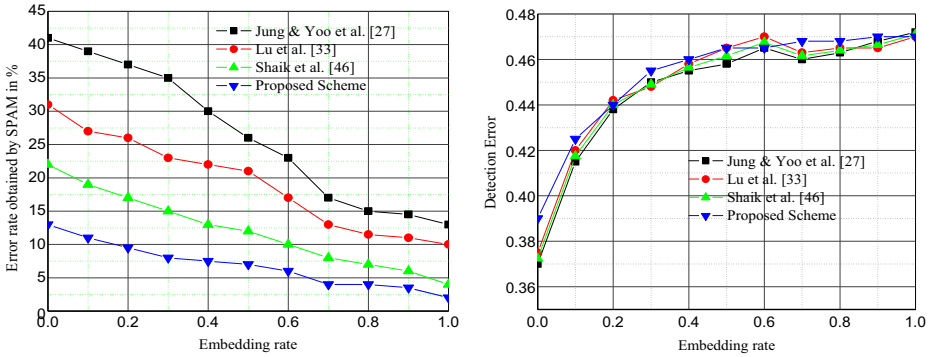


Fig. 14 Steganalysis of the stego-image 'Lena' with size of 512 × 512 for proposed scheme, Shaik et al. [47], Lu et al. method [37], and Jung & Yoo [17] method (a) Error rate obtained by SPAM with respect to embedding rate, (b) Comparison of the detection error by SRM with respect to embedding rate

by means of higher-order Markov chains. They have been designed to provide a low dimensional model of image noise that can be used for steganalysis purposes. The calculation of differences can be viewed as an application of high-pass filtering, which effectively suppresses the image content and exposes the noise. The success of SPAM features in detecting a wide range of steganographic algorithms suggests this model be reasonable for steganalysis and steganography. Whereas the spatial rich model (SRM) steganalysis method is a very effective steganalysis method. It uses statistics of neighboring noise residual samples as features to capture the dependency changes caused by embedding. Because the noise residuals are the high-frequency components of the image and closely tied to image content, the residuals of different types of image regions have different statistical properties and effectiveness for steganalysis.

Thus, one of the main focus points of blind steganalysis is to create an accurate estimation of the cover image. Generally, the attacks that succeed in this process will measure up the statistics in the supposed cover image with that of the suspect image. Additionally, we evaluate the performance of our proposed scheme with Shaik et al. [47], Lu et al. [37] and Jung & Yoo

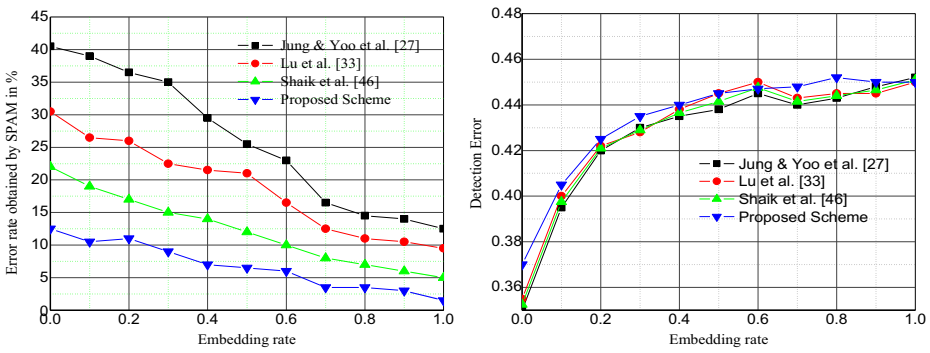


Fig. 15 Steganalysis of the stego-image 'Baboon'with size of 512 × 512 for proposed scheme, Lu et al. method [37], and Jung & Yoo [17] method (a) Error rate obtained by SPAM with respect to embedding rate, (b) Comparison of the detection error by SRM with respect to embedding rate. Shaik et al. [47]

[17] methods on the basis of modern steganalysis tools i.e., subtractive pixel adjacency matrix (SPAM) [45] and spatial rich model (SRM) [7] for Peppers, Lena and Baboon images. The steganalysis for the SPAM test is provided in Figs. 13-15(a). ".

From Figs. 13, 14, 15(a) it is clearly evident that the proposed scheme is having the least error rate for all the three test images. The lower error rate shows that the difference between the stego-image and the cover image is smaller which in turn means that the hidden secret data cannot be detected by the SPAM attack. The reduction in error rate is achieved by the proposed scheme by selectively embedding the secret data into the pixels based on their intensity values. Thus, we can say the proposed scheme is resistant enough against the SPAM attack. The steganalysis for the SRM test is provided in Figs. 13, 14, 15(b). It is clearly indicated from the Figs. 13, 14, 15(b) that the average detection error of our proposed scheme is higher than those of Shaik et al. [47], Lu et al. [37] and Jung &Yoo [17] methods by varying the embedding rate. Thus, our proposed scheme has higher resistance against the SRM steganalysis [7] than the Shaik et al. [47], Lu et al. [37], and Jung & Yoo [17] methods.

5 Conclusions

In this paper, a novel interpolation method and a new reversible data hiding scheme have been proposed. The interpolation method extends the existing NMI method for improving the quality of interpolated images. The proposed data hiding scheme takes into account the characteristics of the human visual system for adaptively embedding the secret data into the interpolated pixels so that high hiding capacity with good quality stego-image is obtained. The number of bits to be embedded in the secret data in a pixel is dependent on its intensity value. Since the secret data is hidden only in the interpolated pixels, the reversibility of the cover image is guaranteed. Experimental results show that the proposed data hiding scheme gains on the average 19.45% and 9.50% increment in the PSNR value and the data hiding capacity, respectively, with respect to the best existing method [47]. Therefore, it can be clearly stated that the proposed scheme has superior performance than all the existing schemes in terms of both the image quality and data hiding capacity. In the future work, research can be focused on the development of adaptive interpolation methods and new reversible data hiding scheme which can embed the secret data on both original and interpolated pixels for increasing the data hiding capacity without compromising the reversibility.

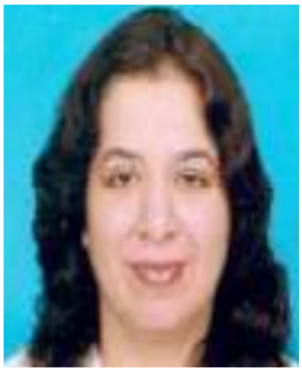
References

1. Ajeeshvali N, Rajasekhar B (2012) Steganography Based on Integer Wavelet Transform and Bicubic Interpolation. *I. J. Image, Graphics and Signal Processing* 12:26–33
2. Allebach J, Wong PW (1996) Edge-directed interpolation. International conference on image processing: 707–710
3. Benhfid A, Ameur EB, Taouil Y (2016) High Capacity Data Hiding Methods Based On Spline Interpolation, *In: 5th International Conference on Multimedia Computing and Systems (ICMCS),* pp. 157–162
4. Chang CC, Hsiao JY, Chan CS (2003) Finding optimal LSB substitution in image hiding by dynamic programming strategy. Pattern Recogn 36:1583–1595
5. Chang CC, Lin CY, Fan YH (2008) Lossless data hiding for color images based on block truncation coding. Pattern Recogn 41(7):2347–2357

6. Chang YT, Huang CT, Lee CF, Wang SJ (2013) Image interpolating based data hiding in conjunction with pixel shifting of histogram. J Supercomput 66:1093–1110
7. Fridrich J, Kodovsky J (2012) Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security 7:868–882
8. Fridrich J, Goljan M, Du R (2001) Reliable detection of LSB steganography in color and grayscale images. Proceedings of ACM workshop on multimedia and security:27–30
9. Gutub AA (2008) "Pixel Indicator high capacity Technique for RGB image Based Steganography", 5th *IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah
10. Gutub A and Al-Juaid N (2018) Multi-Bits Stego-System For Hiding Text in Multimedia Images Based on User Security Priority, *Journal of Computer Hardware Engineering*, vol. 1, no. 2, EnPress Publisher
11. Gutub A, Al-Qahtani A, and Tabakh A (2009) Triple-A: Secure RGB Image Steganography Based on Randomization, *7th ACS/IEEE International Conference on Computer Systems and Applications*, pp. 400–403
12. Gutub A, Al-Juaid N, Khan E (2017) Counting-Based Secret Sharing Technique for Multimedia Applications. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-017-5293-6
13. Gutub A, Alsaidi A, Al-lehaibi K, Alzahrani H, Al Ghamdi M (2018) Compression multi-level crypto Stego-security of texts utilizing colored email forwarding. Journal of Computer Science & Computational Mathematics 8(3):33–42
14. Hong W, Chen TS (2011) Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism. Journal of Visual Communications and Image Representation 22: 131–140
15. Hu J and Li T (2015) "Reversible steganography using extended image interpolation technique", Computer and Electrical Engineering
16. Jung KH (2018) A survey of interpolation-based reversible data hiding methods. *Multimedia Tools and Applications* 77(7):7795–7810
17. Jung KH, Yoo KY (2009) Data hiding using image interpolation. *Computer standards and interfaces* 31: 465–470
18. Jung KH, Yoo KY (2015) Steganographic method based on interpolation and LSB substitution of digital images. Multimed Tools Appl 74:2143–2155
19. Jung KH, Yoo KY (2015) High capacity index based data hiding method. Multimedia Tools and Appllications 74:2179–2193
20. Katzenbeisser S, and Petitcolas FAP (2000) Information hiding techniques for steganography and digital watermarking, Artech House, Norwood
21. Kumar R, Malik A, Singh S, Kumar B, Chand S (2016) Reversible data hiding scheme for LZW codes using even-odd embedding strategy, *International Conference on Computing, Communication and Automation (ICCCA)*, pp. 1399–1403
22. Kumar R, Chand S, Singh S (2018) A reversible high capacity data hiding scheme using combinatorial strategy. International Journal of Multimedia Intelligence and Security 3(2):146–161
23. Kumar R, Chand S, Singh S (2018) An efficient text steganography scheme using Unicode space characters. International Journal of Forensic Computer Science 10(1):8–14
24. Kumar R, Chand S, Singh S (2018) A reversible data hiding scheme using pixel location. Int Arab J Inf Technol 15(4):763–768
25. Kumar R, Chand S, Singh S (2018) "An Improved Histogram-Shifting-Imitated reversible data hiding based on HVS characteristics," *Multimedia Tools and Applications*, vol. 77, vol. 11, pp. 13445–13457
26. Kumar R, Chand S, Singh S (2019) An optimal high capacity reversible data hiding scheme using move to front coding for LZW codes. Multimed Tools Appl 1-25:22977–23001. https://doi.org/10.1007/s11042-019-7640-2
27. Kumar R, Singh S, Jung KH (2019) Human Visual System Based Enhanced AMBTC for Color Image Compression Using Interpolation. *6th International Conference on Signal Processing and Integrated Networks (SPIN)*:903–907
28. Lee CF, Chang WT (2010) Recovery of color images by composed associative mining and edge detection. Journal of Information Hiding and Multimedia Signal Processing 1:310–324
29. Lee CF, Huang YL (2012) An efficient image interpolation increasing payload in reversible data hiding. Expert Syst Appl 39:6712–6719
30. Lee CF, Chang CC, Pai PY, Huang WH (2010) "An effective demosaicing method for CFA image". *International Journal of Innovative Computing*. Inf Control 6:5485–5499
31. Lehmann TM, Gonner C, Spitzer K (1999) Survey: interpolation methods in medical image processing. IEEE Trans Med Imaging 18:1049–1075
32. Lin CC, Tai WL, Chang CC (2008) Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn 41:3582–3591

33. Lin IC, Lin YB, Wang CM (2009) Hiding data in spatial domain images with distortion tolerance. Computer Standards & Interfaces 31(2):458–464
34. Lu TC (2018) Interpolation-based hiding scheme using the modulus function and re-encoding strategy. Signal Process 142:244–259
35. Lu ZM, Pan JS, Sun SH (2000) VQ-based digital image watermarking method. Electronics Letter 36:1201–1202
36. Lu ZM, Wang JX, Liu BB (2009) An improved lossless data hiding scheme based on image VQ-index residual value coding. J Syst Softw 82(6):1016–1024
37. Lu TC, Chang CC, Huang YH (2014) High capacity reversible hiding scheme based on interpolation, difference expansion. Multimed Tools Appl 72:417–435
38. Malik A, Sikka G, Verma HK (2007) An image interpolation based reversible data hiding scheme using pixel value adjusting feature. Multimed Tools Appl 76(11):13025–13046
39. Malik A, Kumar R, Singh S (2016) Reversible data hiding scheme for LZW codes using LSB flipping strategy, *Proceedings of the International Conference on Advances in Information Communication Technology & Computing*, pp. 58–62
40. Malik A, Sikka G, Verma HK (2017) Image interpolation based high capacity reversible data hiding scheme. Multimed Tools Appl 76(22):24107–24123
41. Malik A, Kumar R, Singh S (2018) A New Image Steganography Technique Based on Pixel Intensity and Similarity in Secret Message, *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 828–831
42. Malik A, Singh S, Kumar R (2018) Recovery based high capacity reversible data hiding scheme using even-odd embedding. Multimed Tools Appl 77(12):15803–15827
43. Meikap S, Jana B (2018) Directional PVO for reversible data hiding scheme with image interpolation. *Multimedia Tools and Applications*:1–31
44. Mohammad AA, Al-Haj A, Farfoura M (2018) An improved capacity data hiding technique based on image interpolation. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-018-6465-8
45. Pevny T, Bas P, Fridrich J (2010) Steganalysis by subtractive pixel adjacency matrix. IEEE Trans on Info Forensics and Security 5:215–224
46. Podilchuk CI, Delp EJ (2001) Digital watermarking: algorithms and applications. IEEE Signal Process Mag 18:33–46
47. Shaik A, Thanikaiselvan V (2018) High capacity reversible data hiding using 2D parabolic interpolation. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-018-6544-x
48. Tang M, Hu J, Song W (2014) A high capacity image steganography using multilayer embedding. Optik 125:3972–3976
49. Wahed MA, Nyeem H (2019) High capacity reversible data hiding with interpolation and adaptive embedding. PLoS One 14(3):e0212093. https://doi.org/10.1371/journal.pone.0212093
50. Wang ZH, Lee CF, Chang CY (2013) Histogram-shifting-imitated reversible data hiding. J Syst Softw 86:315–323
51. Wang XT, Chang CC, Nguyen TS, Li MC (2013) Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. Digital Signal Processing 23:569–577
52. Xuan G, Shi YQ, Yao Q, Ni Z, Yang C, Gao J (2006) Lossless data hiding using histogram shifting method based on integer wavelets. International Workshop on Digital Watermarking, Lect Notes Comput Sci 4823:323–332
53. Yang B, Schmucker M, Funk W, Brush C, Sun S (2011) Integer DCT-based reversible watermarking for images using companding technique. Proceeding of International Journal of Electron Communication 65:814–826
54. Yu YH, Chang CC, Hu YC (2005) Hiding secret data in images via predictive coding. Pattern Recogn 38:691–705
55. Zhang X, Sun Z, Tang Z et al (2016) High capacity data hiding based on interpolated image. Multimed Tools Appl 9195–9218

Aruna Malik received her B. Tech. in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow, India and M. Tech. in Computer Science and Engineering from National Institute of Technology, Jalandhar, Punjab, India. She did her doctoral degree in Computer Science and Engineering from National Institute of Technology, Jalandhar, Punjab, India. Now, she is working as an Assistant Professor in the Department of Computer Science & Engineering at National Institute of Technology, Jalandhar, Punjab, India. Her research areas lie in the area of Data hiding and Image processing.



Geeta Sikka is presently working as an Associate Professor in the Department of Computer Science & Engineering and Associate Dean Faculty Welfare at National Institute of Technology, Jalandhar, Punjab, India. She received her Ph.D in Computer Science and Engineering, form National Institute of Technology, Jalandhar, Punjab, India. She did her Master's degree in Computer Science from Punjab Agricultural University, Ludhiana, Punjab, India. Her research interests are Software Engineering, Databases, Data hiding and Data mining.

Harsh Kumar Verma is working as a Professor and Head of Computer Centre at National Institute of Technology, Jalandhar, Punjab, India. He has done his Bachelor's degree in computer science and engineering in 1993 and Master's degree in Software Systems from Birla Institute of Technology, Pilani, in 1998. He received his Ph.D. degree from Punjab Technical University, Jalandhar, Punjab, India in 2006. He has many publications of international and national level to his credit. His research interests include Information security, Data hiding, Computer networks, Image processing and Scientific computing.