

Secured Information Communication Exploiting Fuzzy Weight Strategy



Alok Haldar, Biswapati Jana, Sharmistha Jana, Nguyen Kim Sao,
and Thanh Nhan Vo

1 Introduction

Today, everyone in the world uses the internet and finds it to be quite useful. Digital data protection is both important and difficult. Using steganography and digital watermarking techniques is one way to protect the security of digital data. This is especially important for different types of multimedia data, such text, images, audio files, and video files. Information concealment using established and emerging scientific techniques such as steganography and digital watermark embedding. In order to secure and safeguard digital materials from any illegal access, this is the primary criterion. In order to defend the legitimate rights, it resolves copyright disputes, offers proof to counter illegal copying, and authenticates, ownership identification, detects copy move fraud, uses digital forensics, and detects tampering with multimedia content.

In steganography, extra information that is embedded in a digital cover entity is protected. Steganographic techniques' primary objective is to hide embedded data from an attacker. Because only the sender and recipient will be aware that the secret

A. Haldar · B. Jana (✉)

Department of Computer Science, Kharagpur College, Kharagpur, West Bengal, India
e-mail: biswapatijana@gmail.com

Department of Computer Science, Vidyasagar University, Midnapore, West Bengal, India

S. Jana

Department of Mathematics, Midnapore College [Autonomous], Midnapore, West Bengal, India

N. K. Sao

Department of Computer Science, University of Transport and Communication, Hanoi, Vietnam
e-mail: saonkoliver@utc.edu.vn

T. N. Vo

Department of Information Management, Chaoyang University of Technology, Taichung 41349,
Taiwan, ROC
e-mail: vtuhan@tdmu.edu.vn

information is included inside the transmitted cover object, this assertion allows for the safe transmission of sensitive information over an open communication channel [1].

The digital cover items themselves are protected via digital watermarking techniques. A digital object's integrity and authenticity are attested to by a digital watermark. Digital watermarks are used to control data integrity and to authenticate the origins of data in order to safeguard the authorship of multimedia files [2].

Secret communication, authentication, copyright protection, ownership identification, copy move forgery, digital forensics, and tamper detection of multimedia documents are just a few of the uses for data hiding. Digital watermarking, cryptography, steganography, data encryption, and other methods fall under the category of data concealing and are used to protect digital media and information. Data concealing is a technique of incorporating information in the form of signal that can withstand noise, such as an audio, video, or image file. The invisibility of embedding is typically the primary need for steganographic methods to be effective. These days, robust embedding algorithms that can find embedded data in a digital item are developed as data hiding algorithms. However, a number of authors are creating algorithms with additional quality markers.

Digital watermarking [4] and steganography [3] are two techniques to achieve this goal. Based on their level of robustness, we can classify digital watermarking techniques into three groups: fragile, semi-fragile, and robust. A minimal alteration to the watermarked signal would cause the detection of the message at the receiver end to fail in a fragile watermarking. This type of watermarking is helpful for integrity proof. Moderate alterations are resistant to semi-fragile watermarking. Therefore, we can use this kind of watermarking to protect against a certain type of attack. When using robust watermarking, the watermark message can withstand numerous attacks. For the protection of copyright, this is helpful.

Spatial and transform domain algorithm are two categories of data concealment or steganography [5]. Regarding hiding ability, visual quality, security, storage space, robustness, and execution time, each of these categories has advantages and disadvantages of their own. The cover image's pixels immediately encode the secret message in the spatial domain [7]. However, in the transform domain [8], the cover media must first undergo a transformation to acquire frequency coefficients and modified coefficients for data embedding, such as discrete fourier transform (DFT) [8], discrete wavelet transform (DWT) [11], or discrete cosine transform (DCT) [10]. The robustness is then achieved by embedding the secret message bits into significant coefficients. Despite the higher computational complexity of transform domain techniques, it is believed that watermarks inserted in transform domains withstand attacks better than those embedded in spatial domains.

A special focus has been placed on designing protocols that take advantage of the features included in the cover image in order to boost resilience.

The following are some important key features of data hiding schemes:

- (i) **Reversibility:** One approach to authentication is data concealment. Watermarking, however, has the potential to deteriorate the cover data that was present

in the original cover media after embedding. The receiver end makes it challenging to obtain a precise cover medium. However, in recent times, it has become crucial to retrieve original cover media in a variety of human-centric application fields like the military and medicine. Such programs use reversible data hiding as opposed to traditional data concealing.

- (ii) **Security:** Security of a method is assessed by how well it defends against potential assaults. The data concealment technique utilised in real applications has been determined to have some security flaws based on the work that has already been done. Regarding unauthorised detection, the stego image should not provide any indications as to the existence of the hidden message.
- (iii) **Payload:** Payload is the quantity of information inserted within the cover image. It is a key component of data hiding schemes, therefore it was evident from the literature review that many researchers are attempting to boost embedding capacities while preserving image quality. The payload should be as high as possible while maintaining a discernible level of image quality.
- (iv) **Integrity/Tamper detection:** Tampering is the planned alteration of documents so that the consumer would be harmed. Therefore, it is crucial for the authorised user to expose both the secret information and the cover image throughout the extraction process.
- (v) **Imperceptibility/visual quality:** Any technique for hiding data must meet the imperceptibility criteria first and foremost. There shouldn't be any visual deterioration due to the embedding data that is included in the original image. For the hidden message to remain imperceptible and harmful, it must not be seen by humans, cannot be detected by their eyes, and must not cause any visual distortion in the stego image. Therefore, maintaining acceptable visual quality after embedding the hidden data is a crucial quality of any invisible data concealment strategy.
- (vi) **Robustness:** A media action, such as filtering, lossy compression, or alteration, is considered robust if the hidden message can still be discovered. There are times when delicate confidential data may be required. Fragile data means that it should not resist manipulation or would only resist to a limited degree. It is a critical prerequisite for data concealing.

2 Literature Survey

Wenyin and Shih [21] demonstrated a semi-fragile watermarking technique utilising Local Binary Pattern (LBP) operators, pixel contrast, and a multilevel picture watermarking system. A straightforward texture descriptor called the LBP operator which was developed by Ojala et al. [22]. With the help of suggested methodology, the author has demonstrated that the watermarking techniques can withstand standard image processing operations including JPEG compression, brightness alteration, contrast modification, and additive noise. The results, however, were not thoroughly compared

with any other LBP schemes and were not robust against significant geometrical attacks.

Fan et al. [23] developed a data concealing method that can only conceal four secret data bits within a (3×3) block using a weighted matrix for a grayscale image. Tseng et al. [24] suggested an effective binary image data embedding technique that makes use a weighted matrix W with key matrix K . There is only one modular sum of entry-wise multiplication that can be performed using a weighted matrix W and a (3×3) pixel block for both of these matrix-based data hiding methods. A significant research question is still how to achieve large capacity with reversibility in watermarking while preserving decent visual quality. Reversible data hiding (RDH) becomes a crucial and difficult issue in hidden data communication for authentication, copy right protection and ownership identification in medical and military applications. Through the use of picture interpretation, Jana et al. [25] created a weighted matrix-based reversible data hiding strategy that can conceal 2.97 bpp. However, Chowdhuri et al. [26] created a weighted matrix-based reversible data concealing method that uses the colour image and provides image authentication and tamper detection. To repeatedly embed the secret data in each block, they divided the original image into (3×3) pixel blocks and multiplied the sum of the entries using a modified weighted matrix. Additionally, the proposed data hiding strategy increased visual quality PSNR 50.03 and data embedding capacity up to 8.03 (bpp) (dB). Their technique was successful in detecting and authenticating tampered images, however it may only partially recover the original cover picture from a manipulated stego image. In their innovative method for image watermarking in the spatial domain [27], Kumar and Dutta combine the well-known LSB substitution technique with the idea of information theory. The watermark is positioned in the block with the highest entropy after dividing the cover image into a number of blocks. None of geometric attack difficulties were supported by the experimental findings. Cao et al. [28] developed hamming code-based data hiding techniques with high payload and embedding rates as high as 3 (bpp) and PSNR as low as 51(dB). Bai and Chang [29] have created a high payload steganographic technique for compressed images. They have a 2 (bpp) payload, however their PSNR is under 30(dB). Jana et al. [5, 30] recently developed a partial and dual image based reversible data hiding technique using the (7, 4) hamming code, which may improve data concealing capacity, visual quality, and accomplish reversibility. Su and Chen [31] presented an algorithm that combines frequency and spatial domain to protect copyright.

Watermarked images with good visual quality and good resistance to common image processing attacks, this technique ensures an appropriate compromise between the computational complexity and the authentication level of host images. Due to the watermark being embedded in multiple blocks, the technique's key value is giving the ability to retrieve the watermark either it cropping or rotation attacks. The goal of Hassan and Gutub [34] was to enhance the reversible data concealment strategy with interpolation. The proposed method scales up the original image utilising the existing enhanced neighbour mean interpolation (ENMI) and modified neighbour mean interpolation (MNMI) approaches before inserting the secret data.

Using a dual watermark approach and blind removal, Rangel-Espinoza et al. [39] suggested a removable visible data concealment system. The brightness and texture properties of the watermark and original images are taken into consideration when placing a visible watermark pattern in the DCT domain to create a visible watermarked image. Without other information, such as the original watermark or host image, the watermark could only be removed using the keys of the right user. The experimental findings demonstrate that the suggested system surpasses earlier comparable efforts with the help of blind removal, retention of the quality of the undamaged restored images, and higher visual degradation of the recovered the content of images in the event of an illegal removal attempt. In the value of the interpolation pixel, Jana et al. [40] presented an effective data hiding strategy that takes advantage of the Centre Folding Strategy (CFS) and Fuzzy Logic System (FLS).

3 Proposed Method

This work uses the Fuzzy weight strategy to construct a novel image interpolation scheme. The interpolated pixel values are produced by taking into consideration each pair of pixels in a particular block's fuzzy weight value. Each input pixel pair's fuzzy membership values have been taken to represent the range between the block's minimum and maximum value. The input membership value is fed into the fuzzy output function, which calculates the fuzzy rule's strength using the Max–Min composite principle. Then, through a defuzzification process, interpolated pixel values are calculated from the fuzzy output function dependent on the fuzzy rule's strength. In actuality, fuzzy weight based interpolation algorithms create virtual pixels, which are superior to the interpolation techniques now in use.

FWS based interpolated method

To provide fuzzy interpolated pixel values, a fuzzy rule-based controller with four features—fuzzification, fuzzy rule base, fuzzy inference mechanism, and defuzzification—is developed. As Demirci (Demirci, 2006) demonstrated in his study for similarity calculation, the visual evaluation of a fuzzy interpolated pixel value may vary from one skillful person to another skillful person. Because fuzzy interpolated pixel values between the pixels are imprecise, it is advisable to employ fuzzy rule-based logic to handle them. Two variables, pixel P_i and pixel P_j , are taken into consideration as input for fuzzification in order to determine the fuzzy interpolated pixel value between the pixels. Each component is shown with the fuzzy set for the following fuzzy linguistic variables: Very Low (VL), Low (L), Medium (M), High (H), and Extremely High (VH). These language words can be modelled using a variety of membership functions, including trapezoidal, gaussian, triangular, etc. Nonetheless, due to its simplicity and symmetric representation, the selected representation of the provided linguistic words is a triangular fuzzy number (TFN). The range of possible values is 0–255, with 255 being the maximum. Figure 1 depicts the

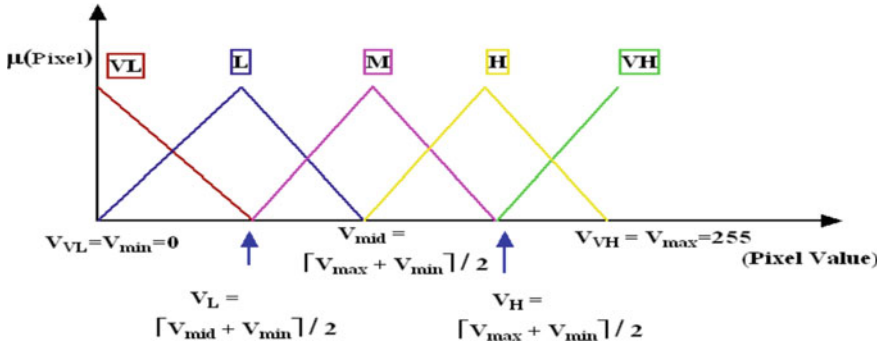


Fig. 1 Input pixel pair of a block’s membership functions

modelling for both of these factors. A fuzzy inference engine is set up after fuzzification and operates in accordance with predefined rules. A degree of association between two pixels is produced by combining the fuzzy inputs created during fuzzification with the rule basis. The degree to which a fuzzy interpolated pixel value exists is measured by this connection. The i th fuzzy rule according to Eq. (18) is thus expressed as: With n inputs such that $x_1X_1, x_2X_2, \dots, x_nX_n$ and one output $y Y$ R_i : If x_1 is 1, x_2 is 2, etc., then x_n must be n . The set of inputs in the rule base is also referred to as the antecedent, and the output is referred to as the subsequent, if y is B . Table 1 displays the most effective fuzzy rules that were successful for the recommended job. The linguistic words VVL, VL, L, ML, M, MH, H, VH, and VVH define the form in which the consequent is created. To create a fuzzy output set as the finished product, each rule’s actions are superimposed. The fuzzy output is produced by combining the results of the rules that have been shot. Further defuzzification techniques produce a crisp value on the fuzzy output. Two common defuzzification approaches are area and maxima based methods. The centroid approach is a well-liked area-based defuzzification method. The crisp value, as its name suggests, marks the location at which the output membership function divides the region in half.

The following is a list of the main steps in image interpolation:

Step-1: Imagine a colour cover image that is $(M \times N)$ pixels in size, divided into the three basic colours of Red (R), Green (G) and Blue (B), and then divided into $(n \times n)$ pixels for each colour block, where $n = 3, 5, 7, 9 \dots$

Step-2: Choose $V_{min} = 0$ as the block’s minimum and maximum pixel values, respectively, and use those values to calculate the fuzzy membership of each pair of pixels using V_{min} as the lower value and V_{max} as the higher value with the medium value is $V_{mid} = \lceil \frac{V_{min} + V_{max}}{2} \rceil$. Assume five linguistic inputs, such as VL for very low, low (L), medium (M), high (H) and very high (VL).

Consider of Fig. 1 as being very highly illustrated.

Table 1 Proposed fuzzy rules

Rule	Antecedent	Consequent
R^1 :	If μ_{pi} is VL and μ_{pj} is VL	then μ_z is VVL
R^2 :	If μ_{pi} is VL and μ_{pj} is L	then μ_z is VL
R^3 :	If μ_{pi} is VL and μ_{pj} is M	then μ_z is L
R^4 :	If μ_{pi} is VL and μ_{pj} is H	then μ_z is ML
R^5 :	If μ_{pi} is VL and μ_{pj} is VH	then μ_z is M
R^6 :	If μ_{pi} is L and μ_{pj} is VL	then μ_z is VL
R^7 :	If μ_{pi} is L and μ_{pj} is L	then μ_z is L
R^8 :	If μ_{pi} is L and μ_{pj} is M	then μ_z is ML
R^9 :	If μ_{pi} is L and μ_{pj} is H	then μ_z is M
R^{10} :	If μ_{pi} is L and μ_{pj} is VH	then μ_z is MH
R^{11} :	If μ_{pi} is M and μ_{pj} is VL	then μ_z is L
R^{12} :	If μ_{pi} is M and μ_{pj} is L	then μ_z is ML
R^{13} :	If μ_{pi} is M and μ_{pj} is M	then μ_z is M
R^{14} :	If μ_{pi} is M and μ_{pj} is H	then μ_z is MH
R^{15} :	If μ_{pi} is M and μ_{pj} is VH	then μ_z is H
R^{16} :	If μ_{pi} is H and μ_{pj} is VL	then μ_z is ML
R^{17} :	If μ_{pi} is H and μ_{pj} is L	then μ_z is M
R^{18} :	If μ_{pi} is H and μ_{pj} is M	then μ_z is MH
R^{19} :	If μ_{pi} is H and μ_{pj} is H	then μ_z is H
R^{20} :	If μ_{pi} is H and μ_{pj} is VH	then μ_z is VH
R^{21} :	If μ_{pi} is VH and μ_{pj} is VL	then μ_z is M
R^{22} :	If μ_{pi} is VH and μ_{pj} is L	then μ_z is MH
R^{23} :	If μ_{pi} is VH and μ_{pj} is M	then μ_z is H
R^{24} :	If μ_{pi} is VH and μ_{pj} is H	then μ_z is VH
R^{25} :	If μ_{pi} is VH and μ_{pj} is VH	then μ_z is VVH

Step 3: The fuzzy output membership function has been developed using a certain range of pixel values and nine linguistic terms, including VVL-very very low, VL-very low, L-low, ML-medium low, M-medium, MH-medium high, H-high, VH-very high, and VVH-very very high. This function is shown in Fig. 2. The VVL will belong to the scale’s lower value, P_i , while the VVH will belong to the scale’s higher value, P_j .

Step 4: The fuzzy weighted strategy rule has been built using the nine output parameters VVL, VL, L, ML, M, MH, H, and VH displayed in Table 1 of the rule together with the five input parameters VL, L, M, H, and VH.

Step 5: The strength of the rule has been calculated using the Max–Min composite rule and the actual input values of each pair of pixels from the selected specified block.

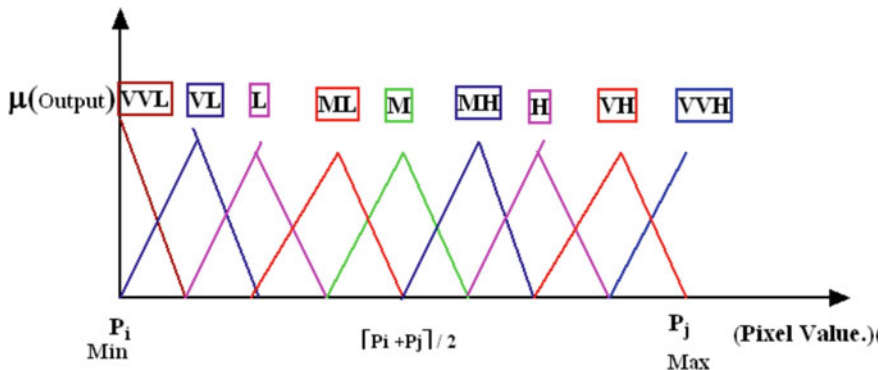


Fig. 2 Membership functions for block virtual pixel calculation

Step 6: The next step is to select the appropriate membership value from the fuzzy output function based on the rule’s strength. The weighted fuzzy function output is then used to construct the interpolated virtual pixel, and in cases where there are several values, the interpolated pixel value of that block for the selected pixel pair will be the average value.

Numerical Example

Think about the image block in Fig. 3b. As seen in Fig. 3c, We reduce the size of the block by removing one row and one column of pixels. Figure 1 shows the anticipated pixel block produced by the Fuzzy Weight Strategy (FWS). Now think about the pixel pair with the values $P_i = 70$ and $P_j = 120$ and $V_{min} = 0$ and $V_{max} = 255$. $VL = 0$, $L = 64$, $M = 128$, $H = 192$, and $VH = 255$ are the results.

The following formula is used to determine fuzzy membership values:

Numerical Example

Table 2

120	68	70
181	177	124
200	165	180

(a): Original block

Table 3

120	70
200	180

(b): Reduced block

Table 4

120	89	70
170	151	139
200	196	180

(c): The Predicted block

Fig. 3 Numerical example of fuzzy weight strategy

$$\mu_{VL}(x) = \frac{64 - x}{64 - 0} = \frac{64 - x}{64}, \quad 0 \leq x \leq 64,$$

$$\frac{x - 64}{64 - 0} = \frac{x - 64}{64}, \quad 0 \leq x \leq 64,$$

$$\mu_L(x) = \frac{128 - x}{128 - 64} = \frac{x - 128}{64}, \quad 64 \leq x \leq 128$$

$$\frac{x - 64}{128 - 64} = \frac{x - 64}{64}, \quad 64 \leq x \leq 128$$

$$\mu_M(x) = \frac{192 - x}{192 - 128} = \frac{192 - x}{64}, \quad 128 \leq x < 192$$

$$\frac{x - 128}{192 - 128} = \frac{x - 128}{64}, \quad 128 \leq x < 192$$

$$\mu_H(x) = \frac{255 - x}{255 - 192} = \frac{255 - x}{63}, \quad 192 \leq x < 255$$

$$\mu_{VH}(x) = \frac{x - 192}{255 - 192} = \frac{x - 192}{63}, \quad 192 \leq x < 255,$$

Similar to that, each colour component of a particular block's membership values for the output fuzzy function were defined, taking into account the lower pixel value of 70 and the higher pixel value of 120, as shown below.

$$\mu_{vVL}(z) = \frac{77 - z}{77 - 70} = \frac{77 - z}{7}, \quad 70 \leq z < 77,$$

$$\frac{z - 70}{77 - 70} = \frac{z - 70}{7}, \quad 70 \leq z < 77$$

$$\mu_{VL}(z) = \frac{83 - z}{83 - 77} = \frac{83 - z}{6}, \quad 77 \leq z < 83$$

$$\frac{z - 77}{83 - 77} = \frac{z - 77}{6}, \quad 77 \leq z < 83$$

$$\mu_L(z) = \frac{89 - z}{89 - 83} = \frac{89 - z}{6}, \quad 83 \leq z < 89$$

$$\frac{z - 77}{89 - 83} = \frac{z - 83}{6}, \quad 83 \leq z < 89$$

$$\mu_{ML}(z) = \frac{95 - z}{95 - 89} = \frac{95 - z}{6}, \quad 89 \leq z < 95$$

$$\frac{z - 89}{95 - 89} = \frac{z - 89}{6}, \quad 89 \leq z < 95$$

$$\mu_M(z) = \frac{102 - z}{102 - 95} = \frac{102 - z}{7}, \quad 95 \leq z < 102$$

$$\frac{z - 95}{102 - 95} = \frac{z - 95}{7}, \quad 95 \leq x < 102$$

$$\mu_{MH}(z) = \frac{108 - z}{108 - 102} = \frac{108 - z}{6}, \quad 102 \leq z < 108$$

$$\frac{z - 102}{108 - 102} = \frac{z - 102}{6}, \quad 102 \leq z < 108$$

$$\mu_H(z) = \frac{114 - z}{114 - 108} = \frac{114 - z}{6}, \quad 108 \leq z < 114$$

$$\frac{z - 108}{114 - 108} = \frac{z - 108}{6}, \quad 108 \leq z < 114$$

$$\mu_{VH}(z) = \frac{120 - z}{120 - 114} = \frac{120 - z}{6}, \quad 114 \leq z < 120$$

$$\mu_{VVH}(z) = \frac{120 - z}{120 - 114} = \frac{120 - z}{6}, \quad 114 \leq z < 120$$

Then, assess the input for each pair of pixels you collected from the block's input fuzzy membership value. In this case, $P_i = 70$, which is between 64 and 128. Thus, it is necessary to calculate,

$$\mu_L(x) = \frac{128 - x}{64} = \frac{128 - 70}{64} = \frac{58}{64}$$

$$\mu_M(x) = \frac{x - 128}{64} = \frac{70 - 64}{64} = \frac{6}{64}$$

In this case, $P_j = 120$ which is between $64 \leq x < 128$. Thus, it is necessary to calculate,

$$\mu_L(x) = \frac{128 - x}{64} = \frac{128 - 120}{64} = \frac{8}{64}$$

$$\mu_M(x) = \frac{x - 64}{64} = \frac{120 - 64}{64} = \frac{56}{64}$$

The following formula has been used to determine the strength of the fuzzy rule formed by the first four values:

S_1 : P_i is (VL) Very Low and P_j is (L) Low, So,

$$S_1 = \min(\mu_L(70), \mu_M(120)) = \min\left(\frac{58}{64}, \frac{8}{64}\right) = \frac{8}{64}$$

S_2 : P_i is (VL) Very Low and P_j is (M) Medium, So,

$$S_1 = \min(\mu_L(70), \mu_M(120)) = \min\left(\frac{58}{64}, \frac{56}{64}\right) = \frac{56}{64}$$

S_3 : P_i is (VL) Very Low and P_j is (M) Medium, So,

$$S_1 = \min(\mu_L(70), \mu_M(120)) = \min\left(\frac{6}{64}, \frac{8}{64}\right) = \frac{6}{64}$$

S_4 : P_i is (VM) Very Medium and P_j is (M) Medium, So,

$$S_1 = \min(\mu_L(70), \mu_M(120)) = \min\left(\frac{6}{64}, \frac{56}{64}\right) = \frac{6}{64}$$

The first four numbers together create a fuzzy rule and the following formula has been used to determine the strength of this rule:

MAX $\{S_1, S_2, S_3, S_4\}$, that is

$$\text{MAX}\left(\frac{8}{64}, \frac{56}{64}, \frac{6}{64}, \frac{6}{64}\right) = \frac{56}{64} \text{ i.e } S_2$$

As a result, S_2 , which correlates to P_i being low and P_j being medium, is the rule with the highest strength out of the four. Now, using the defuzzification technique and analyze the fuzzy function that results to determine the virtual pixel:

$$\frac{z - 83}{6} = \frac{56}{64} \text{ i.e } z_1 = 88.25$$

$$\frac{95 - z}{6} = \frac{56}{64} \text{ i.e } z_2 = 89.75$$

Therefore $z = \lceil \frac{z_1 + z_2}{2} \rceil = \lceil \frac{88.25 + 89.75}{2} \rceil = 89$.

We have determined the projected values 158 and 144 for the diagonal input sets 120,180 and 70,200 respectively, for the central value 151 of the Fig. 1c.

```

if ( interpol > origin )
    m = interpol - origin
    s = ceil(m/2)
    new_interpol = interpol -s
else
    m = origin - interpol
    s = ceil(m/2)
    new-interpol = interpol + s.

```

Lastly, the average between 158 and 144, or $\lceil \frac{158+144}{2} \rceil = 151$, is used to get the centre predicted value. In Fig. 3c displays the final, identical-sized predicted pixel block that was produced using FWS.

4 Experimental Results with Comparative Analysis

We conducted the following investigation [41] using the six common benchmark photos from the tests: (a) aeroplane, (b) sailboat, (c) Lena, (d) baboon, (e) peppers, and (f) Tiffany in Fig. 4. These 512×512 -pixel images are fed into the suggested system to evaluate the effectiveness of the suggested research. Several comparisons are used in this part to demonstrate the viability of the created strategy. Secondly, five previously developed strategies are compared to the suggested interpolation technique.

To evaluate the advantages and disadvantages of the suggested innovative interpolation method, NMI, INP, ENMI, CRS, and MNMI were used. The suggested embedding strategy is then evaluated using the outcomes of the experiments, and various comparisons are used to investigate the scheme.

The PSNR is computed as follows:

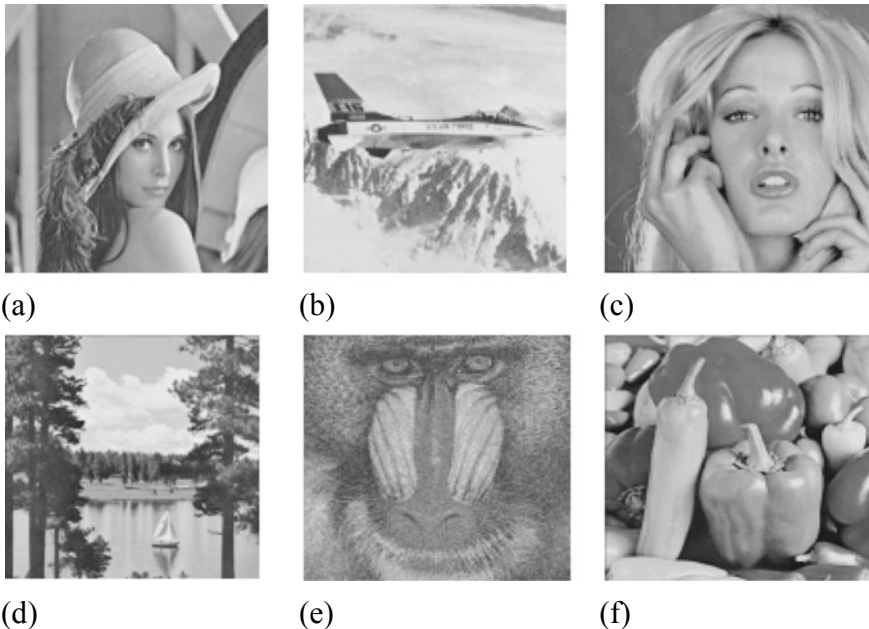


Fig. 4 Experimental images: **a** Lena, **b** Airplane, **c** Tiffany, **d**, Lake, **e** Baboon, **f** Peppers

Table 5 Six picture interpolation methods have been compared in terms of the visual attributes assessed by PSNR (dB)

Cover image	PSNR of both original and interpolated image					
	NMI	INP	ENMI	CRS	MNMI	FWS
Lena	28.06	26.41	25.64	26.29	22.64	33.95
Airplane	27.30	27.16	25.48	25.24	25.11	34.15
Tiffany	21.82	26.29	28.18	26.64	25.70	35.05
Lake	26.56	22.81	27.54	27.12	25.49	31.13
Mandrill	25.30	25.25	22.07	26.39	24.81	32.88
Pepper	22.09	21.44	23.84	21.51	24.45	33.34
Average	26.06	25.18	26.24	25.27	29.18	33.41

$$\text{MSE} = \frac{1}{h \times w} \sum_{i=1}^h \sum_{j=1}^w C(i, j) - S(i, j)^2$$

$$\text{PSNR} = 10 \log_{10}(255^2/\text{MSE})(\text{dB})$$

Where $C(i, j)$ is the cover image's pixel value, $S(i, j)$ is the stego image's pixel value at position, and MSE is the mean square error. To assess the effectiveness of the interpolation approaches, the PSNR is calculated. The NMI, INP, ENMI, CRS, and MNMI interpolation techniques are compared to the FWS methodology. Table 5 displays the outcomes. The NMI, INP, ENMI, CRS, and MNMI recommended interpolation approaches are all inferior than the FWS based image interpolation scheme. The suggested method showed that, in nearly all of the tested input images, the FWS methodology achieved the greatest PSNR, according to the results reported in Table 5. The PSNR average is roughly estimated to be 33 dB. As a result, the FWS was employed in the suggested technique to produce the enhanced cover image.

5 Conclusion

In this study, after performing picture interpolation with fuzzy weight, an innovative, efficient, and reversible data hiding strategy was created using the centre folding approach. The fuzzy weight of each pair of pixels in a particular image block is taken into account to produce the interpolated pixel values. Subsequently, data hiding operations were carried out in each interpolated pixel by centre folding and comparison with the signal of the secret data. The suggested technique reverses the folded value to match the secret data if the signal differs from that of the interpolated pixel in order to lessen the difference in image distortion between the interpolated picture and the stego-image. You can figure out the hidden data using the discrepancy between the outputs of these interpolated values and the receiver's centre folding scheme.

Experimental results and their analysis from many angles show that the suggested method is superior than state-of-the-art approaches. Additionally, security research of RS assaults reveals that the stego image has less noise, which makes it difficult to use it to detect the existence of secret information. The proposed technique may be utilised for authentication or secret data exchange in military, medical, and academic institutions. This method can be applied in the future for image authentication, copyright protection, and ownership identification using cellular automata, local binary patterns, and other methods.

References

1. Fridrich J (2009) *Steganography in digital media: principles, algorithms, and applications*. Cambridge Univ. Press, Cambridge, UK
2. Panah AS, Van Schyndel R, Sellis T, Bertino E (2016) On the properties of non-media digital watermarking: a review of state of the art techniques. *IEEE Access* 4:2670–2704. <https://doi.org/10.1109/ACCESS.2016.2570812>
3. Singh S, Singh AK, Ghreera SP (2017) A recent survey on data hiding techniques. In: 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE, pp 88–886
4. Chowdhury FS, Dhar PK, Deb K, Koshiba T (2020) Blind image watermarking in canonical and cepstrum domains based on 4-connected t-o'clock scrambling. *Symmetry* 12(2):266
5. Jana B, Giri D, Mondal SK (2017) Partial reversible data hiding scheme using (7, 4) hamming code. *Multimedia Tools Appl* 76(20):21691–21706
6. Jana B (2016) High payload reversible data hiding scheme using weighted matrix. *Optik* 127(6):3347–3358
7. Jana M, Jana B (2020) An improved data hiding scheme through image interpolation. In: *Computational intelligence in pattern recognition*. Springer, pp 157–169
8. Gunjan R, Pandia P, Mohnot R (2017) Secure extraction of image data based on optimized transform method. In: 2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud). IEEE, pp 217–222
9. Gonge SS, Ghatol AA (2017) An enhancement in security and copyright protection technique used for digital still image. In: 2017 international conference on nascent technologies in engineering (ICNTE). IEEE, pp 1–9
10. Pushpad A, Potnis AA (2017) Improved image security scheme using combination of image encryption and reversible watermarking. In: 2017 4th international conference on signal processing and integrated networks (SPIN). IEEE, pp 293–297
11. Rasti P, Anbarjafari G, Demirel H (2017) Colour image watermarking based on wavelet and qr decomposition. In: 2017 25th signal processing and communications applications conference (SIU). IEEE, pp 1–4
12. Kelkar V, Mehta JH, Tuckley K (2018) A novel robust reversible watermarking technique based on prediction error expansion for medical images. In: *Proceedings of 2nd international conference on computer vision and image processing*. Advances in intelligent systems and computing, vol 703, pp 131–143
13. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images. *IEEE Access* 6:10269–10278
14. Liu J, Li J, Ma J, Sadiq UN, Yang A (2019) A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon map. *Appl Sci* 9(4):1–23
15. Rehman A, Sultan K, Aldhafferi N, Alqahtiani A, Mahmood M (2018) Reversible and fragile watermarking scheme for medical images. *Comput Math Methods Med* 18:7

16. Zhang H, Wang C, Zhou X (2017) Fragile watermarking for image authentication using the characteristic of SVD. *Algorithms* 10(1):1–12
17. Konstantinides K, Natarajan B, Yovanof GS (1997) Noise estimation and filtering using block-based singular value decomposition. *IEEE Trans Image Process* 6(3):479–483
18. Liu R, Tan T (1997) An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans Image Process* 6(3):479–483
19. Roy S, Pal AK (2017) An indirect watermark hiding in discrete cosine transform singular value decomposition domain for copyright protection. *Roy Soc Open Sci* 4(6). Art. no. 170326
20. Makbol NM, Khoo BE, Rassem TH (2016) Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Process* 10(1):34–52
21. Wenyin Z, Shih FY (2011) Semi-fragile spatial watermarking based on local binary pattern operators. *Opt Commun* 284(16–17):3904–3912
22. Ojala T, Pietikainen M, Maenpaa T (2002) Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Trans Pattern Anal Mach Intell* 24(7):971–987
23. Fan L, Gao T, Cao Y (2013) Improving the embedding efficiency of weight matrix-based steganography for grayscale images. *Comput Electr Eng* 39(3):873–881
24. Tseng YC, Chen YY, Pan HK (2002) A secure data hiding scheme for binary images. *IEEE Trans Commun* 50(8):1227–1231
25. Jana B (2016) High payload reversible data hiding scheme using weighted matrix. *Optik-Int J Light Electron Opt* 127(6):3347–3358
26. Chowdhuri P, Pal P, Jana B (2019) Improved data hiding capacity through repeated embedding using modified weighted matrix for color image. *Int J Comput Appl* 41(3):218–232
27. Kumar S, Dutta A (2016, April) A novel spatial domain technique for digital image watermarking using block entropy. In: 2016 international conference on recent trends in information technology (ICRTIT). IEEE, pp 1–4
28. Cao Z, Yin Z, Hu H, Gao X, Wang L (2016) High capacity data hiding scheme based on (7, 4) Hamming code. *Springer Plus* 5(1):1–13
29. Bai J, Chang CC (2016) A high payload steganographic scheme for compressed images with hamming code. *Int J Netw Sec* 18(6):1122–1129
30. Jana B, Giri D, Mondal SK (2018) Dual image based reversible data hiding scheme using (7, 4) hamming code. *Multimedia Tools Appl* 77(1):763–785
31. Su Q, Chen B (2018) Robust color image watermarking technique in the spatial domain. *Soft Comput* 22(1):91–106
32. Laouamer L (2019, March) A new image watermarking technique in spatial domain using DC coefficients and graph representation. In: International conference on advanced machine learning technologies and applications. Springer, Cham, pp 633–644
33. Peng F, Zhao Y, Zhang X, Long M, Pan WQ (2020) Reversible data hiding based on RSBEMD coding and adaptive multi-segment left and right histogram shifting. *Sig Process Image Commun* 81:115715
34. Hassan FS, Gutub A (2021) Efficient image reversible data hiding technique based on interpolation optimization. *Arab J Sci Eng* 46(9):8441–8456
35. Maheswari S, Rameshwaran K, Malarselvi KM (2015) DCT-PCA based watermarking on E-governance documents. *Res J Appl Sci Eng Technol* 9(7):507–511
36. Abbas NH, Ahmad SMS, Ramli ARB, Parveen S (2016) A multi-purpose watermarking scheme based on hybrid of lifting wavelet transform and Arnold transform. In: International conference on multidisciplinary in IT and communication science and applications
37. Ghazvini M, Hachrood EM, Mirzadi M (2017) An improved image watermarking method in frequency domain. *J Appl Sec Res* 12(2):260–275
38. Yuan Y, Huang D, Liu D (2006) An integer wavelet based multiple logo-watermarking scheme. In: First international multi-symposiums on computer and computational sciences, Hanzhou, vol 2, pp 175–179

39. Rangel-Espinoza K, Fragoso-Navarro E, Cruz-Ramos C, Reyes-Reyes R, Nakano-Miyatake M, Perez-Meana HM (2018) Adaptive removable visible watermarking technique using dual watermarking for digital color images. *Multimedia Tools Appl* 77(11):13047–13074
40. Jana S, Jana B, Lu T-C, Vo TN (2022) Reversible data hiding scheme exploiting center folding with fuzzy weight strategy
41. USC-SIPI (2017). University of Southern California. The usc-sipi image database. <http://sipi.usc.edu/database/database.php>. Accessed 20 Sept 2017