ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse291032021.pdf
https://doi.org/10.30534/ijatcse/2021/291032021

An Improved Methodology for Data Hiding In Images Using Haar Transformed, LSB Replacement Method and Modified PVDMF 1

Laraib Naz[1], Qamar Nawaz[1], Isma Hamid[2], Ahmad Mateen[1], Salman Afsar[1],MushhadMustuhzar Gilani[3]
[1]Department of Computer Science, University of Agriculture Faisalabad, Pakistan.
[2]Department of Computer Science, National Textile University, Faisalabad, Pakistan.
[3]University Institute of Information Technology, PMAS-Arid Agriculture University, Rawalpindi, Pakistan.
Corresponding Author Email: laraibnaz243@gmail.com

ABSTRACT

Steganography is a technique of concealing secret text or image within another image. In this paper, abetter and efficient steganography method for hiding images and/or text into a color image is proposed. The proposed technique is based on two irreversible methods of spatial domain Least Significant Bit (LSB) and Pixel Value Differencing and Modulus Function (PVDMF 1) and one Haar Wavelet Transformation of the frequency domain. The proposed method works in four stages: at the first stage, Haar Wavelet Transformation is applied on the input image and transformed Haar coefficients are obtained. At the second stage, Haar coefficients and secret image are converted into binary form, before applying the LSB replacement method on the green channel by replacing the first two Most Significant Bits (MSB) of the input image with the last two LSB bits of the secret image. In the third stage, modified PVDMF 1 is applied on intermediate stego images after hiding the image by dividing the image into two non-overlapping consecutive pixels of pixels for hiding text. Inthe fourth stage, Inverse Haar Wavelet Transformation is applied to get the stego image. The proposed method offers high hiding capability with good visual quality. The visual quality of the stego image is measured by using three widely used objective quality assessment matrices PSNR, RMSE, and SSIM. Furthermore, Regular/Singular (RS) analysis is applied on stego images to check their resistance against RS attack. The hiding capacity and quality assessment results are compared with some existing methods. It is evident from the comparison that the proposed process is superior in terms of visual quality and hiding capacity.

Key words: Data hiding, Haar Wavelet Transformation, LSB replacement method, PVDMF, Steganography

1. INTRODUCTION

Today the internet plays a vigorous part in the growth of societies. Therefore, a huge volume of private data is being communicated through the internet. So this data is important to business, government, and for a single person. With new technology, data transmission becomes fast and convenient but not secure sometimes[1],[2]. This has drawn many researchers' attention to the establishment of a system that secures data through an insecure medium. To attain the objective of security of information transmitted through the internet is data hiding. Overcoming this problem, there are two methods; one is information encryption and the second is information hiding [3]. Figure 1 shows the hierarchical categorization of the data security system. In information encryption, the cryptography method is used, in which encryption and decryption are done for hiding the secret data. Cryptography is commonly used in a varied range of applications like computer passwords, electronic commerce, and ATM cards[4]. Like Chaotic Encryption process for secure and Store data[5]. Information hiding is a process by which private information is protected to make sure that its existence remains unnoticed. Data hiding works by secretly inserting data within a host (cover object). In addition, data hiding could be categorized into two main classifications, which are steganography and watermarking [6].

Watermarking prevents intellectual property or copyrights of contents [7]. For small data, watermarking is used such as company logo, author tags, and product information. This method also makes sure the strength of hiding. The process of changing a media object, in an unnoticeable way, to add data in that media is called watermarking.

Another method for data hiding is steganography; steganography originates as of two Greek words‘ steganos' means the cover and ‘graphei’ means writing [8].Steganography is subdivided into linguistic and technical steganography. Technical steganography contains hiding data in image, video, audio because in these objects secret data cannot be easily noticeable. The linguistic steganography to conceal secret data uses natural languages like dots and Kashia in the Arabic language.

Digital image steganography is more separated into spatial domains and frequency domains. The spatial domain is concerned with the image plane itself, while the frequency domain is concerned with the rate of change in pixels. The spatial domain is further divided into Reversible [9] and Irreversible. In reversible methods of data hiding, a cover image fully restored after secret information is getting from a stego image. Irreversible

means that the original data cannot be regained from the stego image after the covert image embedded on the original image has been destroyed, i.e. during the extraction process [10].

The basic irreversible methods are Least Significant Bit (LSB) [11] and difference in pixel value (PVD) [12].Basic reversible techniques are Histogram shifting [13],Modification of Prediction Error (MPE) [14] etc. Also, the frequency domain is further divided into Integer Wavelet Transform (IWT) [15], and Discrete Cosine Transform (DCT) [16]**,** etc.

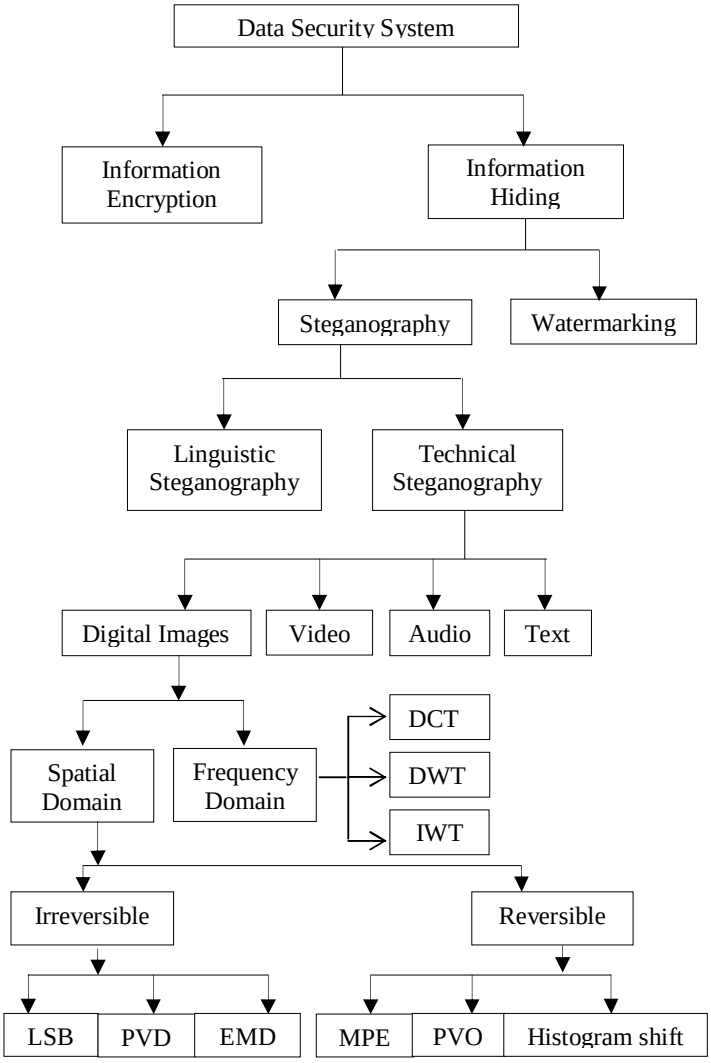


Figure 1: Hierarchical categorization of data security system for hiding data

The least significant bit (LSB) replacement is irreversible data embedding technique[11]. The LSB replacement scheme replaces the LSB bits with a hidden bit stream. LSB method needs more bits to change in pixels to achieve a higher payload. Visual output can be decreased by at least a bit of modification and may become susceptible to regular/singular (RS) statistical steganalysis. The development of steganography pixel value differentiation (PVD) [10] provided a new path to the field of image steganography to achieve the high visual quality of the stego image. PVD-based techniques, however, are constrained by fewer payloads and are susceptible to the analysis of histograms.

Hwang et al. [17], proposed a method to improve the hiding ability by combining PVD and LSB methods. In this proposed scheme, the cover image is split into levels of edge and smooth. Smooth and edge stages are added by LSB and PVD techniques respectively. The hiding ability of the previous method [12] was thus enhanced. However, this approach is unable to resist RS steganalysis. By adding a lower level readjustment technique, Yang *et al.*[18] Further improved the method [17]; visual quality was improved, and the object remains undetectable by regular and singular steganalysis [19] detect attacks. This method does not however increase the hiding ability. A new data hiding approach based on LSB and PVD for greyscale images was suggested by Khodaei and Faez [20].This technique combines PVD with Kbit LSB. The Kbit LSB is embedded in the middle pixel and the leftover right and left pixels of the block are added to PVD. Thus the capacity of embedding is increased, but the stego-image visual output is lower [18].

Popular reversible methods of embedding include differential expansion, histogram shifting [13], and prediction error modification (MPE) [14]. In general, reversible steganography methods have low embedding capacity. Hong *et al.*[14] Suggested MPE to achieve a high hiding capacity in reversible methods. In the MPE embedding process, a high visual quality achieves by more than 48 dB PSNR. However, the MPE approach has a lower hiding capacity than PVD and LSB methods. Reversible and irreversible data embedding techniques are distinguished by enhancing hiding capacities, yet integrating these techniques while achieving the same visual quality and payload can also be further improved. The threat of resistance against steganalysis is increased with the use of combined multiple steganography methods.

The proposed technique has three main objectives: (1) to create a stego image without affecting the visual quality of stego image; (2) to increase the hiding ability so that a huge volume of data can be transmitted; and (3) to improve protection to withstand an RS attack. In this study, an improved data hiding scheme was proposed by combining two irreversible steganography methods of the spatial domain which are the LSB replacement method and modified Pixel Value Differencing Modulus Function 1 (PVDMF 1) with a Haar wavelet of frequency domain to obtain a high visual quality and hiding capacity. Extended the PVDMF 1[21] data hiding method proposed by and LSB replacement [22].

The paper's contribution is as follows. At first, a Haar Wavelet Transformation is applying to the cover image. Second, the LSB replacement method is applied to hide an image in transformed coefficients (these are generated by Haar wavelet Transformation). Third, modified PVDMF 1 is applied to hide secret messages which are in the text files. Then inverse haar transformation is applied tothe image to obtain a stego image which is similar to the

cover image. In the extraction process, apply the inverse process of the proposed method to obtain secret image and text. Results show that the proposed scheme provides an improved hiding capacity with good visual quality and shows resistance against RS steganalysis attack.

2. RELATED WORK

1.1 Haar Wavelet Transformation

Haar functions have been used since 1910 when the Hungarian mathematician Alfred Haar[23]introduced them. A complete orthogonal system of functions in L^p [0, 1], $p \in [0, \infty]$ which take values from the set $\{0, 2^j : j \in N\}$ was defined by Haar [23]. Nowadays, there are several other meanings of Haar functions in the literature [24]. For example, in (1)[25], the original Haar definition is as follows.

$$\text{haar}(1,t) = \begin{cases} 1, & \text{for } t \in \left[0, \frac{1}{2}\right), \\ -1, & \text{for } t \in \left[\frac{1}{2}, 1\right) \end{cases} (1)$$

1.2 Least Significant Bit Replacement Method for 24 Bit Color Image

The most basic is LSB steganography, In which the least significant bits of digital data from the cover media are used to hide the hidden message[11]. The LSB replacement/LSB matching terminology was first discussed by T. Sharpness [26]. Rawat and Bhandari[22] suggested that 24-bit color image LSBs replace the least significant bit of every pixel of a specific color channel with a bit of secret data. This LSB replacement method for RGB replaces at least two significant bits of each green,red or blue channel with message bits.

2.3. Pixel value differencing Modulus function

Sahu and Swain[21] suggested a data hiding approach to embed hidden information based on an 7 range table by using the difference between a pair of consecutive pixels. To decrease the distortion in the stego-image, modulus operations with pixel readjustment were used.In Their technique is rem is obtained by (2).

$$(rem_1) = \begin{cases} (P_x mod 4, P_{x+1} mod\ 4), & if\ d \in R1 \\ (P_x mod 8, P_{x+1} mod\ 8), & if\ d \in R2 \\ (P_x mod 16, P_{x+1} mod\ 16), & if\ d \in R3 \end{cases} (2)$$

The new pixel values P'_x and P'_{x+1} can be get using (3).

$$P'_x = \begin{cases} P_x, & if\ rem_1 = dec_1 \\ P_x - x_1, & if\ rem_1 < dec_1\ and\ |x_1| < 2^{n-1} \\ P_x - x_2, & if\ rem_1 > dec_1\ and\ |x_2| < 2^{n-1} \\ P_x - z, & if\ rem_1 < dec_1\ and\ |x_1| \geq 2^{n-1}\ where\ z = 2^n + x_1 \\ P_x + z, & if\ rem_1 > dec_1\ and\ |x_2| \geq 2^{n-1}\ where\ z = 2^n + x_2 \end{cases} (3)$$

Now calculate another difference value $d' = |P'_x - P'_{x+1}|$. Apply (4) to obtain the stego-pixel pair P^*_x and P^*_{x+1}.

$$(P^*_x, P^*_{x+1}) = \begin{cases} (P'_x, P'_{x+1}), & if\ d' \in R1 \\ (P'_x - 2^n, P'_{x+1} + 2^n), & if\ d' \in R2\ and\ P'_x \geq P'_{x+1} \\ (P'_x + 2^n, P'_{x+1} - 2^n), & if\ d' \in R2\ and\ P'_x < P'_{x+1} \end{cases} (4)$$

3. PROPOSED METHODOLOGY

In this section, an improved method was developed by combining LSB replacement and PVDMF1 with Haar Wavelet for data hiding. The proposed method enhances the hiding capability with visual quality and remains unnoticed against RS steganalysis attack. The proposed method has been implemented on MATLAB 2016a software. Figure 2 shows the flow chart of the proposed method. The embedding and extraction processes are discussed below.

3.1. The embedding process

Input: A cover image of 512*512, the secret image of 256*256 and one text file

Output: The stego-image of 512*512

Step 1: Apply Haar wavelet transformation on the cover image

i. First, find the H value by using (5)

ii.

$$\boldsymbol{H(n) = 0.5 \begin{bmatrix} H(n-1) \otimes [1 \quad 1] \\ 2^{(n-1)/2} I(n-1) \otimes [1 \quad -1] \end{bmatrix}, H(0) = 1} \quad (5)$$

iii. After that this H value multiplies with each image pixel and gets transformed coefficients.

Step 2: Now take transformed coefficients and secret images for hiding a secret image in it.

i. Convert haar transformed coefficients and secret image pixels into binary values. Suppose the first 3pixels of the cover image are [11100010 11100010 11100010] and the first three pixels of the secret image are [10001011 10001100 10001101].

ii. Now take the only green plane of the cover image, because the visual perception of intensely green objects is less distinct than the perception of red. Now clear the last 2 LSB bits to 0 with multiplying $\text{bitand}(c(x, y, 2), \text{uint8}(252))$ or [111111100]. In Matlab "bitand" command, used for removing these bits, resulting original image pixels are [11100000 11100000 11100000]. Obtain next MSB i.e 7^{th} and 6^{th} bit of secret image and embedded it into green plane.

iii. After shifting secret image pixels by 2 bits to the right and applying these bits to the original image pixel by "bitor" command, then last 2 LSBs of cover image are exchanged by the first 2 MSBs of the secret image. Now we gotnew image after embedding secret image, whose first three pixels are: [11100010 11100010 11100010].

iv. Repeat the steps 2 and 3 until secret image embedded.

Step 3: Use previously generated pixels in step 2 for hiding the secret message which is in the text file.

i. Read the secret message that we want to hide and convert into binary numbers for further processing.

ii. Take P_x and P_{x+1} the pair of non-overlapping pixels of a block of the new image.

iii. Find the difference value $d = |P_x - P_{x+1}|$.

iv. Obtain the range of d from range Table 1 and find maximum bits n that can be embedded between 2 pixels by using (6).

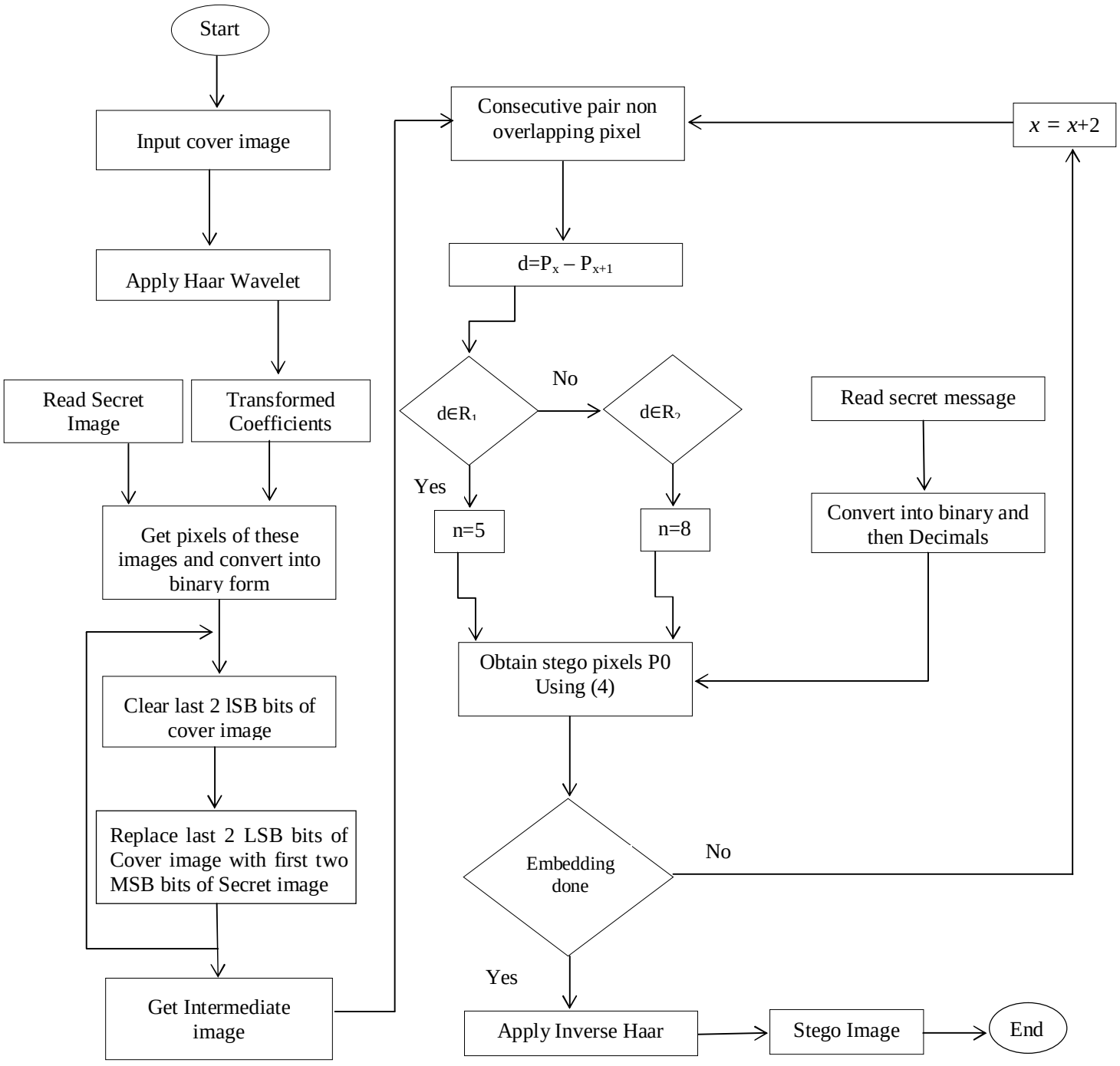


Figure 2: Flow chart of the proposed method

Table 1: Range Table for Proposed Method

Range	Embedding length (n)
R1=[0, 31]	5
R3= [32, 255]	8

$$n = ub(i) - lb(i) + 1, \quad n = \log2(n) \tag{6}$$

v. Find the remainder of two pixels P_x and P_{x+1} by using the modulus operation by using (7).

$$REM = \begin{cases} mod\big((P_x + P_{x+1})\big), 2^n * 4); & \text{if d}\epsilon\ \text{R1} \\ mod\big((P_x + P_{x+1})\big), 2^n * 8); & \text{if d}\epsilon\ \text{R2} \end{cases} \tag{7}$$

vi. After that find the value of variable m, m1 by (8)

$$m = |rem - n'|, \ m1 = n^2 - m \tag{8}$$

Where n' is the transform $n_i$into the decimal value.

vii. After finding REM, m, m1 use them and get Modified pixel value P^*_x and P^*_{x+1} after embedding secret message by using (9) and (10).

$$PO = (P^*_x, P^*_{x+1}) = \begin{cases} \left(P_x - \text{ceil}\left(\frac{m}{2}\right), P_{x+1} - \text{floor}\left(\frac{m}{2}\right)\right) & if\ rem > k\ and\ m \le \frac{2^n}{2}\ and\ P_x \ge P_{x+1} \\ \left(P_x - \text{ceil}\left(\frac{m}{2}\right), P_{x+1} - \text{floor}\left(\frac{m}{2}\right)\right) & if\ rem > k\ and\ m \le \frac{2^n}{2}\ and\ P_x < P_{x+1} \\ \left(P_x + \text{ceil}\left(\frac{m1}{2}\right), P_{x+1}1 + \text{floor}\left(\frac{m1}{2}\right)\right) & if\ rem > k\ and\ m > \frac{2^n}{2}\ and\ P_x \ge P_{x+1} \\ \left(P_x + \text{ceil}\left(\frac{m1}{2}\right), P_{x+1}1 + \text{floor}\left(\frac{m1}{2}\right)\right) & if\ rem > k\ and\ m > \frac{2^n}{2}\ and\ P_x < P_{x+1} \end{cases} \quad (9)$$

$$PO = (P^*_x, P^*_{x+1}) = \begin{cases} \left(P_x + \text{ceil}\left(\frac{m}{2}\right), P_{x+1} + \text{floor}\left(\frac{m}{2}\right)\right) & if\ rem \le k\ and\ m \le \frac{2^n}{2}\ and\ P_x \ge P_{x+1} \\ \left(P_x + \text{ceil}\left(\frac{m}{2}\right), P_{x+1} + \text{floor}\left(\frac{m}{2}\right)\right) & if\ rem \le k\ and\ m \le \frac{2^n}{2}\ and\ P_x < P_{x+1} \\ \left(P_x - \text{ceil}\left(\frac{m1}{2}\right), P_{x+1}1 - \text{floor}\left(\frac{m1}{2}\right)\right) & if\ rem \le k\ and\ m > \frac{2^n}{2}\ and\ P_x \ge P_{x+1} \\ \left(P_x - \text{ceil}\left(\frac{m1}{2}\right), P_{x+1}1 - \text{floor}\left(\frac{m1}{2}\right)\right) & if\ rem \le k\ and\ m > \frac{2^n}{2}\ and\ P_x < P_{x+1} \end{cases} \quad (10)$$

viii. Repeat the steps from 2 to 7 until the complete message embeds.

Step 4: Now perform inverse Haar wavelet transformation to get the final stego image.

i. First, find the H value by using Equation 5.
ii. Then the value of H is divided by 0.5.
iii. Take the transpose of H then H' value multiplies with each newly generated pixel in step 3 and gets stego image.

Step 5: Embedding done

2.2 The extraction process:

In the extraction process, extract the secret data without the original image.

Step 1:Read the stego image and apply Haar Wavelet Transformation to obtain haar coefficients.

i. Read and take the size of transformed coefficients generated in step 1.
ii. Get first file-obtained by clearing LSB bits by "bitand" command
iii. Get 2nd file right shifting by 2 bits in stego image by "bitshift" command.
iv. After combining these two files get the secret image.
v. Reduce the resolution to half so that it becomes the original image's resolution.

Step 3: Get Secret message:

i. Let P^*_x and P^*_{x+1}will be block's pixels of the stego image.
ii. Find the difference between two non-overlapping pixels, Test R boundary.
iii. Find REM by (7) and convert it into a binary value.
iv. Convert these binary bits into decimal to getting our secret message.
v. Extraction is done.

4. RESULTS AND COMPARISION

The proposed method has been implemented using MATLAB 2016a software. In experimental work collections of benchmark, dataset is used as cover images. Figure 3 shows experimental cover images Airplane, House, Lena, Boat, Baboon,and Peppers with a size of

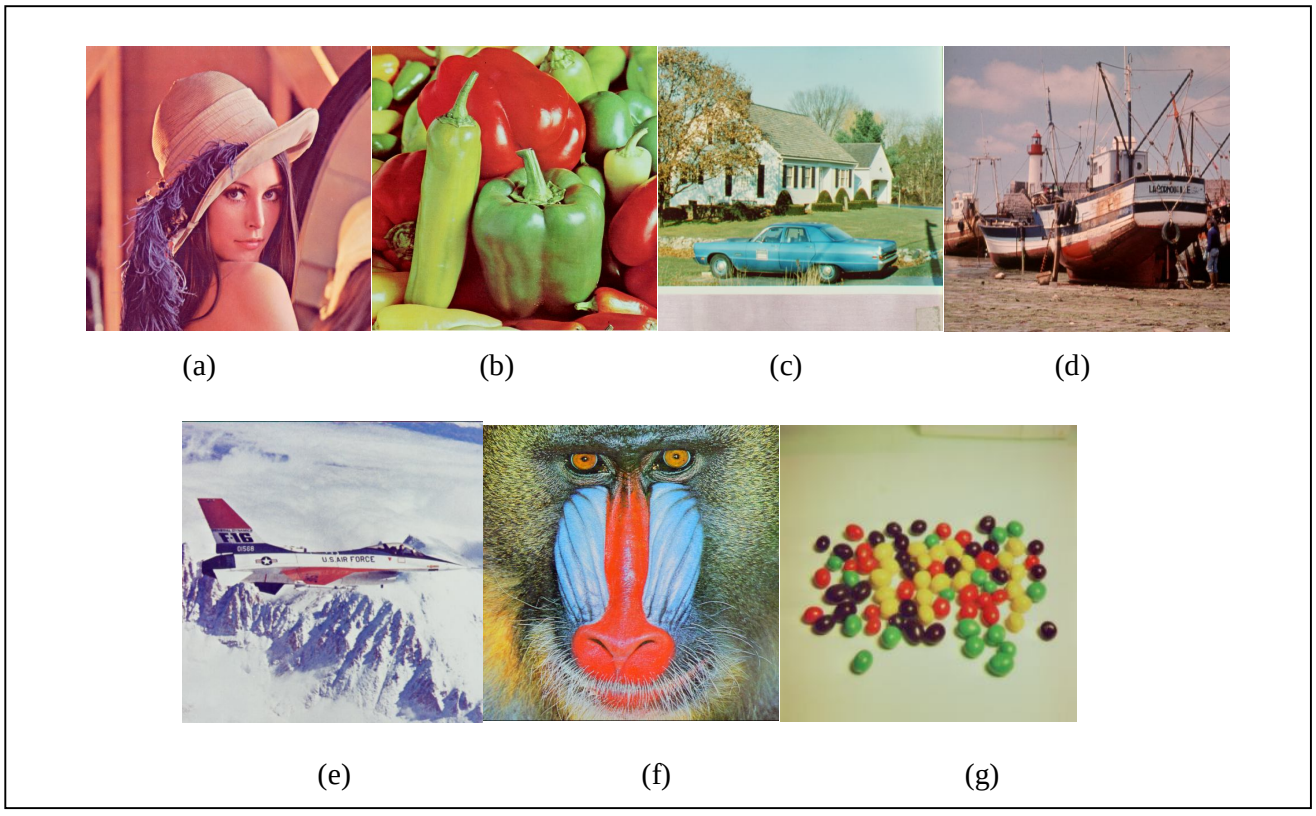


Figure 3: Cover images (a) Lena (b) Peppers (c) House (d)Boat (e) Airplane (f) Baboon, Secret image (g) Bunties

512*512 and secret image Bunties with a size of 256*256 were taken from USC-SIPI [27]. These images are widely used in a lot of publications concerning compression of images, image processing, and data hiding method. The proposed approaches are compared with LSB, PVD Shift, and MPE [28],PVD and LSB on bit plane [29] and Adaptive PVD and LSB [30], n-Rightmost Bit Replacement Image [31] by Peak Signal to Noise Ratio (PSNR) and hiding capacity. The assessment is based on hiding capability and invisibility. Stego-image quality can be measured using PSNR, RMSE, and SSIM.

PSNRis an engineering concept for the ratio in between the full potential power of a signal and the corrupting noise power that affects its representational fidelity. Strong PSNR means low sego image distortion [32]. That ratio assesses the consistency of cover picture embedded through hidden data and frame of the location.

MSE reflects the average change in squares between a distorted image and a reference image[33]. MSE's small value reflects fewer variations between 18 of the two images, resulting in higher PSNR by equation (1). The value of MSE is calculated pixels by pixels by inserting all the squared pixel variations and dividing by the total pixel number. If y_{ij} and x_{ij} are respectively the pixels of stego-image and cover image at the ith and jth coordinates, then MSE and PSNR can be determined using (11) and (12).

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=0}^{n-1}(Y_i - \hat{Y}_i)^2 \quad (11)$$

$$PSNR = 10 * \log 10 \frac{255*255}{MSE} (12)$$

A relatively modern metric called the Structural Similarity (SSIM) Index is the consistency metric that we have used [34]. To find a resemblance between the the stego-images and original, the SSIM metric is used.The value can vary from −1 to 1 for SSIM.The Structural Similarity Index (SSIM) is a perceptual metric, such as data compression or data transmission losses that quantifies image quality. This new similarity measure focuses on structural data similarity, rather than pixel-based comparison. Equation (13) calculates from.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2+\sigma_y^2+c_2)} (13)$$

Where $\bar{m}^2$,σ_x^2, $\bar{m}$, and $\bar{n}$, $\bar{n}^2$, σ_y^2 are the variance, standarddeviation, and mean pixel values for stego-image and cover image respectively.

The root mean square error (RMSE) is a statistical formula to measure model quality in research studies[35].It is a square root of the average collection of the square differences between the coordinate values of the dataset and the coordinate values for similar points from an independent source of higher precision. If y_{ij} and x_{ij} are respectively the pixels of the stego image and cover image at the ith and jth coordinates, then RMSE can be determined using (14).

$$RMSE = \sqrt{MSE} (14)$$

Now the results of the proposed steganographic method will discuss. Hidden data is the same in all test images. After that, compare the results from the literature with four current steganographic techniques. In addition, the benchmark image dataset tests the capacity, invisibility, and safety against the attacks of the histogram, Regular/Singular attack. The PSNR, RMSE, and SSIM will be used as performance metrics for efficiency. Table 2 shows the results of the proposed steganography method as hiding capacity, PSNR, SSIM, and RMSE.

Table 2: Results of data samples

Cover Image	Hiding Capacity	PSNR	SSIM	RMSE
Lena	1980500	38.89	0.99	2.89
Boat	1989500	38.05	0.96	3.19
Peppers	1976400	37.83	0.98	3.27
House	1984300	37.73	0.97	3.30
Airplane	1978200	39.04	0.93	2.84
Baboon	2002100	34.67	0.95	4.70

4.1. Comparing Hiding Capacity and PSNR with other methods

Table 3 shows, capacity comparison in bits between existing methods (LSB, PVD Shift, and MPE [28],PVD and LSB on bit plane [29]**,** Adaptive PVD and LSB [30], n-Rightmost Bit Replacement Image [31]), and proposed method. Tables 4 show comparisons of existing steganographic methods with the proposed process using the PSNR. The data inserting capacity of the proposed system is 1,985,167 bits, PSNR is 37.70 db, SSIM is 0.97and RMSE is 3.370 on average.

The capacity of Hussain and Wahab's technique [28], Jung's technique[29], Samayveer's technique [30],Kumar and Gandharba's technique [31] are 814,003, 1,051,369, 1,190,133 and 1,048,576 respectively on average bases. It can be noticed from the comparison that the proposed methods have the highest embedding capacities as compared with the other four techniques. It has the highest embedding capacity without alterationto human visual system. Figure 4 shows the average embedding capacity.

The PSNR of Hussain and Wahab's technique [28], Jung's technique[29], Samayveer's technique [30],Kumar and Gandharba's technique [31] are 37.54, 32.87, 34.32, and 34.82 respectively on average bases. Stego object quality could be measured by the use of PSNR. Higher PSNR in the stego picture means low distortion. Results show that the PSNR of the proposed method is better than [29], [30], [31]. The embedding capacity of LSB, PVD Shift, and MPEHussain and Wahab's technique [28] technique is very low but in some test images, it has good PSNR as compared to the proposed method. For example, data set images baboon and

TABLE 3: Comparison of proposed method's hiding capacity (bytes) with current methods

Cover Images	Algorithms				
	Hussain et al'stechnique[28]	Jung's technique[29]	Singh's technique [30]	Kumar's technique[31]	Proposed Method
Lena	820,370	1,049,742	1,195,376	1,048,576	1,980,500
Baboon	804,380	1,054,327	1,192,755	1,048,576	2,002,100
Airplane	827,529	1,050,973	1,179,648	1,048,576	1,978,200
Pepper	810,501	1,050,571	1,192,755	1,048,576	1,976,400
Boat	810,735	1,051,124	1,184,890	1,048,576	1,989,500
House	810,500	1 051 474	1,195,376	1,048,576	1,984,300

TABLE 4: Comparison of proposed method's PSNR with current methods

Cover Images	Algorithms				
	Hussain et al'stechnique[28]	Jung's technique[29]	Singh's technique [30]	Kumar's technique[31]	Proposed Method
Lena	38.20	33.21	34.83	34.86	38.89
Baboon	36.02	31.74	33.36	34.65	34.67
Airplane	38.59	33.19	34.69	34.95	39.04
Pepper	38.56	33.55	34.81	34.75	37.83
Boat	37.54	32.84	33.98	34.82	38.05
House	36.35	32.73	34.29	34.79	37.73

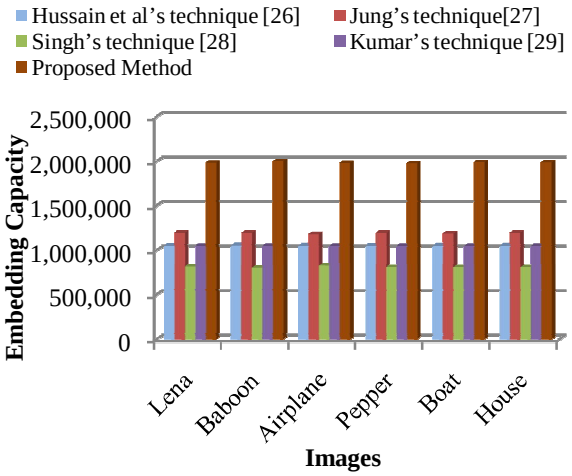


Figure 4: Average Hiding Capacity

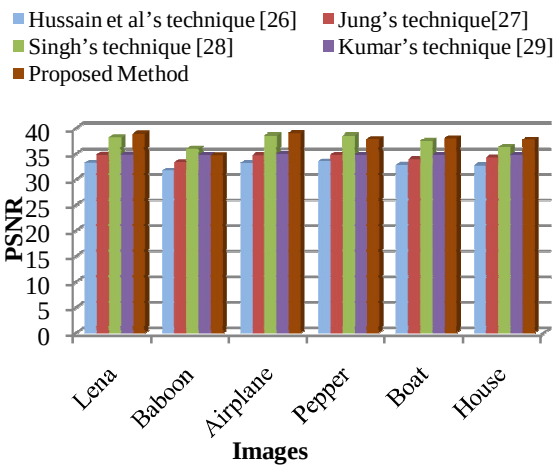


Figure 5: Average PSNR

peppers have high PSNR in Hussain and Wahab's technique [28] which are 36.02 and 38.56 respectively but in the proposed method these images have low PSNR which are 34.67 and 37.83 respectively due to haar transformed coefficients. Figure 5 shows the average PSNR.

4.2. Security Evaluation and Invisibility Comparison

Figure 6 shows the cover image and the corresponding stego images and the histogram for the cover and stego image. Distortions arising from embedding are imperceptible to human eyes, as the figures indicate.It can be seen from the figure that the histogram's form is preserved.The values of all image pixels are determined in this test,and then the histogram for that value is plotted for stego images and cover images.

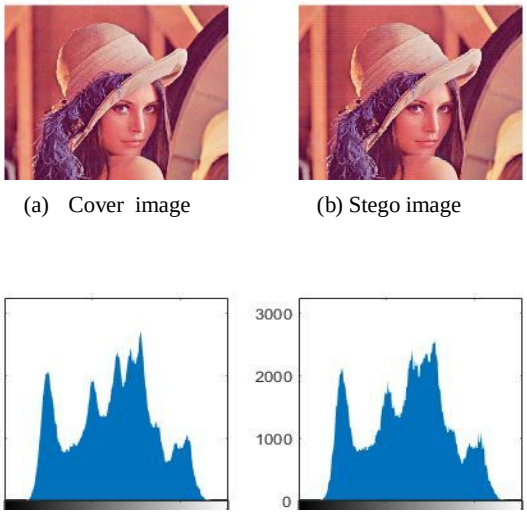
It's noted that in all cover images and stego images, there are no visual artifacts found. Therefore human eyes can't

recognize the stego image.The analysis of the histograms is used to verify protection. Analysis of the histogram is conducted on the image of Cover and Stego. Figure 6shows that as compared to the original image histogram with stego image histogram. This indicates a steganalyst won't be able to quickly figure out the secret message.

It is noticed that the proposed system histogram method is approximately identical to the cover image. Its results show fewer pixel distortions in the stego image. It also offers more security because various bits have been hidden in various non-overlapping pixels, so it is difficult to track how many bits within a pixel are hidden. As a result, there will be less distortion in the value of stego image pixel so image visual quality remains good.

4.3. Assessment of Robustness against RS Analysis

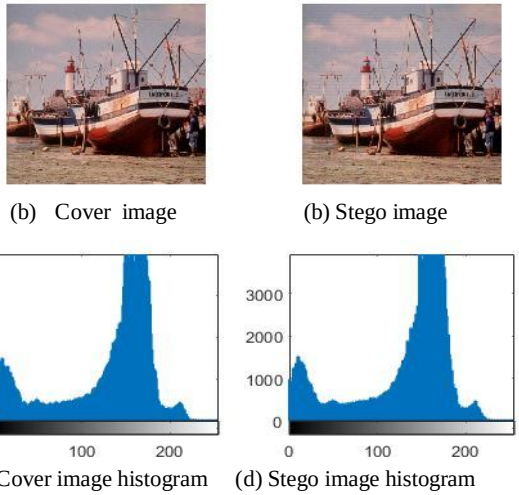
In the steganalysis domain, RS steganalysis is afamous research method [36]. Figure 7 shows the security of proposed technique against RS attacks, two stego-images of the RS analysis graph: Lena and boat images. The discrimination feature (DF) and masks M and −M can beused to do this. The value of masks are considered as [0 1 1 0] and [0 −1 −1 0] , respectively. For the proposedmethodology, the Regular and Singular analysis was implemented to check the attack on the stego image. In the case of LSB-based techniques, a statistical study wasmainly used toclassifying the rare behavior of stegoimages. The stego-pixels are first divided into three groups, like (1) the regular R_{-M} and R_M group, (2) the singular S_{-M} and S_M group, and (3) the useless group. Stego image obtained with an embedding rate increase of approximately 30 percent.The state in the plot$R_M \approx R_{-M} > S_M \approx S_{-M}$ implies that this method has acted against the attack successfully. On the opposite, the presence of hidden data is detected if condition R_{-M}-S_{-M} > R_M-$S_M$true. The Lena and boat images RS plot of the proposed technique are shown in Figure7.



(a) Cover image (b) Stego image

(c) Cover image histogram (d) Stego image histogram

(a) Lena

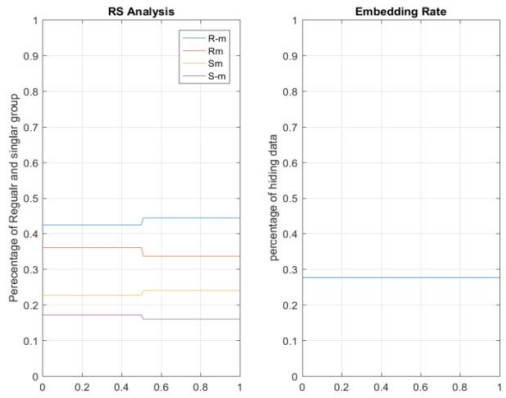


(b) Cover image (b) Stego image

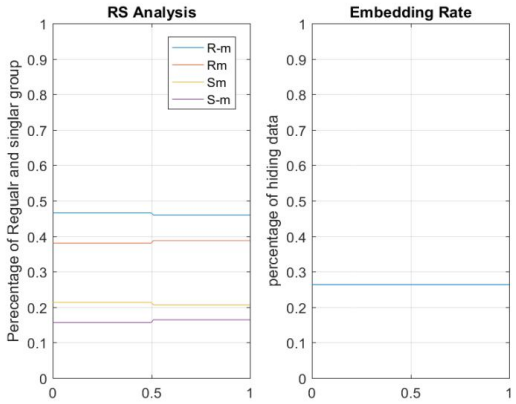
(c) Cover image histogram (d) Stego image histogram

(a) Boat

Figure 6: Cover and stego image & Histogram of cover and stego image (a) Lena (b) Boat



(a)



(b)

Figure 7: RS analysis (a) Lena Image RS analysis (b) Boat image RS analysis

Where the condition $R_M \approx R_{-M} > S_M \approx S_{-M}$ is satisfied in the case of the proposed scheme. It is therefore determined that the proposed scheme fights against the regular and singular attack successfully.

5. CONCLUSION

This study presented a recent study on hiding data. It addresses the basic functions of hiding information. For hiding the presence of secret data in a cover medium has been steganography. In this study, animproved steganography technique has been proposed based on Haar Wavelet, LSB, and PVDMF 1 to enhance the embedding capacity. First, Haar transformed coefficients obtained by haar transformation then image hide through LSB replacement method and text message by PVDMF1. The capacity of embedding ofthe proposed system is 1,985,167 bits, PSNR is 37.70 db, SSIM is 0.97, RMSE is 3.370. Results display that the proposed scheme has high PSNR and embedding capacity. Stego image resistance against many steganalysis assaults for protection, including RS attack, image histogram. The proposed method has high embedding capacity, good visual quality, and provided robustness against RS.

ACKNOWLEDGMENT

This research was supported by the Department of Computer Science, University of Agriculture Faisalabad (UAF).

REFERENCES

[1] M. S. Subhedar and V. H. Mankar, "**Current status and key issues in image steganography: A survey,**" *Comput. Sci. Rev.*, vol. 13–14, no. C, pp. 95–113, 2014.

[2] H. B. Abdalla, J. Lin, G. Li, and S. M. M. Gilani, "**NoSQL: Confidential on Data Security and Data Management by Using a Mobile Application,**" *Int. J. Inf. Electron. Eng.*, vol. 6, no. 2, pp. 84–88, 2016.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "**Digital image steganography: Survey and analysis of current methods,**" *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] P. V. S. Govind, M. K. Sajila, and B. M. Varghese, "**A Two Stage Data Hiding Scheme with High Capacity Based on Interpolation and Difference Expansion,**" *Procedia Technol.*, vol. 24, pp. 1311–1316, 2016.

[5] P. Manisekaran, P. Dhankhar, and P. Kumar, "**Approaches of Chaotic Image Encryption models in Enlightening Image Storage and Security systems,**" *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 2, p. 997-1005, 2021.

[6] A. Smajdor, A. Stöckl, and C. Salter, "**The limits of empathy: Problems in medical education and practice,**" *J. Med. Ethics*, vol. 37, no. 6, pp. 380–383, 2011.

[7] S. Atawneh, A. Almomani, and P. Sumari, "**Steganography in digital images: Commonapproaches and tools,**" *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 30, no. 4, pp. 344–358, 2013.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "**Information hiding - a survey,**" *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[9] J. Tian, "**Reversible Data Embedding Using a Difference Expansion,**" vol. 13, no. 8, pp. 890–896, 2003.

[10] T. Sarkar and S. Sanyal, "**Reversible and Irreversible Data Hiding Technique,**" 2014.

[11] C. K. Chan and L. M. Cheng, "**Hiding data in images by simple LSB substitution,**" *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, 2004.

[12] D. Wu and W. Tsai, "**A steganographic method for images by pixel-value differencing,**" vol. 24, pp. 1613–1626, 2003.

[13] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, "**An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism,**" *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 7, pp. 1109–1118, 2013.

[14] W. Hong, T. S. Chen, and C. W. Shiu, "**Reversible data hiding for high quality images using modification of prediction errors,**" *J. Syst. Softw.*, vol. 82, no. 11, pp. 1833–1842, 2009.

[15] A. K. Gulve and M. S. Joshi, "**An image steganography method hiding secret data into coefficients of integer wavelet transform using pixel value differencing approach,**" *Math. Probl. Eng.*, vol. 2015, 2015.

[16] S. A. Khayam, "**The Discrete Cosine Transform (DCT): Theory and Application,**" *Components*, 2003.

[17] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "**Image steganographic scheme based on pixel-value differencing and LSB replacement methods,**" *IEE Proc. Vision, Image Signal Process.*, vol. 152, no. 5, pp. 611–615, 2005.

[18] C. H. Yang, S. J. Wang, and C. Y. Weng, "**Analyses of pixel-value-differencing schemes with LSB replacement in stegonagraphy,**" *Proc. - 3rd Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2007.*, vol. 1, pp. 445–448, 2007.

[19] J. Fridrich, M. Goljan, and R. Du, "**Detecting LSB steganography in color and gray-scale images,**" *IEEE Multimed.*, vol. 8, no. 4, pp. 22–28, 2001.

[20] M. Khodaei and K. Faez, "**New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing,**" *IET Image Process.*, vol. 6, no. 6, pp. 677–686, 2012.

[21] A. K. Sahu and G. Swain, "**An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function,**" *Wirel. Pers. Commun.*, no. 0123456789, 2019.

[22] D. Rawat and V. Bhandari, "**A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image,**" *Int. J.*

Comput. Appl., vol. 64, no. 20, pp. 15–19, 2013.

[23] A. Haar, "**Zur Theorie der orthogonalen Funktionensysteme - Erste Mitteilung,**" *Math. Ann.*, vol. 69, no. 3, pp. 331–371, 1910.

[24] A. Fournier, "**Wavelets and their applications in computer graphics,**" p. 239, 1995.

[25] S. K. Mahendran *et al.*, "**Chapter 4 Proposed Methodology for Fracture Detection,**" *IEEE Trans. Biomed. Eng.*, vol. 59, no. 14, pp. 22–24, 2012.

[26] T. Sharp, "**An implementation of key-based digital signal steganography,**" *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2137, pp. 13–26, 2001.

[27] "**misc.**" .

[28] M. Hussain, A. W. A. Wahab, N. Javed, and K. H. Jung, "**Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE,**" *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 35, no. 1, pp. 53–63, 2018.

[29] K. Jung, "**Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane,**" *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 127–136, 2018.

[30] S. Singh, "**Adaptive PVD and LSB based high capacity data hiding scheme,**" 2020.

[31] A. Kumar and S. Gandharba, "**A Novel n-Rightmost Bit Replacement Image Steganography Technique,**" *3D Res.*, vol. 10, no. 1, pp. 1–18, 2019.

[32] E. G. Turitsyna and S. Webb, "**Simple design of FBG-based VSB filters for ultra-dense WDM transmission ELECTRONICS LETTERS 20th January 2005,**" *Electron. Lett.*, vol. 41, no. 2, pp. 40–41, 2005.

[33] J. K. Yan *et al.*, "**Subjective MSE Measures,**" vol. 00, pp. 486–489, 1986.

[34] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "**Image quality assessment: From error visibility to structural similarity,**" *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, 2004.

[35] A. G. Barnston, "**Correspondence among the correlation, RMSE, and Meidke Foresast verification measures; Refinement of the Neidke Score,**" *Weather and Forecasting*, vol. 7, no. 4. pp. 699–709, 1992.

[36] J. Fridrich, M. Goljan, and R. Du, "**Reliable detection of LSB steganography in color and grayscale images,**" *Proc. ACM Int. Multimed. Conf. Exhib.*, no. II, pp. 27–30, 2001.