Tech Science Press

Reversible Data Hiding Based on Varying Radix Numeral System

J. Hemalatha[1], S. Geetha[2], R. Geetha[3], C. Balasubramanian[4], Daniela Elena Popescu[5] and D. Jude Hemanth[6,*]

[1]AAA College of Engineering and Technology, Sivakasi, India
[2]SCOPE, VIT University, Chennai, India
[3]SENSE, VIT University, Chennai, India
[4]Department of CSE, Kalasalingam Academy of Research and Education, India
[5]Faculty of Electrical Engineering and Information Technology, University of Oradea, Oradea, Romania
[6]Department of ECE, Karunya Institute of Technology and Sciences, Coimbatore, India
*Corresponding Author: D. Jude Hemanth. Email: judehemanth@karunya.edu

Abstract: A novel image reversible data-hiding scheme based on primitive and varying radix numerical model is presented in this article. Using varying radix, variable sum of data may be embedded in various pixels of images. This scheme is made adaptive using the correlation of the neighboring pixels. Messages are embedded as blocks of non-uniform length in the high-frequency regions of the rhombus mean interpolated image. A higher amount of data is embedded in the high-frequency regions and lesser data in the low-frequency regions of the image. The size of the embedded data depends on the statistics of the pixel distribution in the cover image. One of the major issues in reversible data embedding, the location map, is minimized because of the interpolation process. This technique, which is actually LSB matching, embeds only the residuals of modulo radix into the LSBs of each pixel. No attacks on this RDH technique will be able to decode the hidden content in the marked image. The proposed scheme delivers a prominent visual quality despite high embedding capacity. Experimental tests carried out on over 100 natural image data sets and medical images show an improvement in results compared to the existing schemes. Since the algorithm is based on the variable radix number system, it is more resistant to most of the steganographic attacks. The results were compared with a higher embedding capacity of up to 1.5 bpp reversible schemes for parameters like Peak Signal-to-Noise Ratio (PSNR), Embedding Capacity (EC) and Structural Similarity Index Metric (SSIM).

Keywords: Data hiding; spatial correlation; radix system; prediction error; embedding capacity

1 Introduction

In recent years of the information era, multimedia content in digital form is widely used in many applications. However, at the same time, an increasing number of security issues have been exposed. For instance, the increase of intelligent editing tools can also facilitate misuse,

illegitimate duplicating and distribution, plagiarism and misappropriation, which could bring down the interests of the creator or owner of the multimedia effort. This is creating a strong need for schemes that can efficiently cope with multimedia security and privacy, including copyright protection and integrity authentication. In the advanced digital communication era, ensuring the privacy of individuals becomes a challenging task. Various methods like encryption and steganography have been developed for the protection of personal privacy. In encryption, one can observe the communication happening. However, steganography or data hiding is not observable. For many years, with many communications having taken place over long distances, intervened by modern technology and alertness to interception related issues, there is never a guarantee for secure communication means. In an expansive mean, a covert channel for covert communication is the path for one to communicate with others and conceals the fact that the communication is taking place.

Data hiding is the art of covert communication. Secret information is embedded imperceptibly into the cover medium [1,2]. The cover medium can be any multimedia files, such as audio, images, video etc. The four prominent characteristics that any data-hiding algorithm should possess are robustness, security, capacity and quality/imperceptibility. Reversible Data Hiding (RDH), which is under research for the past two decades, has been proved with enormous improvement in the quality parameters of the image after embedding the data. The Challenge in RDH is to recover the secret data and to restore the cover medium without any degradation [3–6]. Any RDH algorithm developed should have the capacity to withstand various attacks in steganography. In general, the RDH scheme can be shown as in Eq. (1)

$$f\,(Ce,\,Em,\,Km) = Zm \tag{1}$$

The function represents the operator or the embedding scheme by which the secret information Em will be embedded into the cover image Ce, having a shared key Km as an option into the embedding scheme. The final stego image or the marked image is given as Zm. Similarly, decoding can be visualized as in Eq. (2)

$$f'\,(Zm,\,Km) = Em \tag{2}$$

An RDH scheme should generally possess four vital characteristics to facilitate a consistent and reliable covert communication channel.

Imperceptibility: Enables to embed information undetected by the Human Visual System.

Security: Provides resistance to the attack even after the realization of the existence of secret data.

Robustness: Ability of stego-object to oppose unintentional actions.

Capacity: Amount of information that can be embedded without affecting the visual quality. RDH finds its application in the medical field, law enforcement and military image processing.

In the past years, the motivation of RDH is mainly about integrity authentication. More than that, few innovative applications based on RDH, covering reversible visual transformation, reversible steganography, reversible image processing, reversible adversarial example, further support the belief that style transfer, colorization etc., can also be reversible. These applications have valuable prospects on RDH and extend it further. There are still many technical hitches to be solved in these reversible processes. As for some complex image processing methods, the secondary information for restoring the original image is too much to be included by RDH, or will greatly

degrade the quality of the processed stego image. In the future, we will try to overcome those difficulties to make these reversible operations better.

2 Structure

For more than two decades, RDH schemes have been used in the spatial domain, frequency domain or compressed domain. RDH methods are mostly derived from approaches such as Histogram Modification (HM), Difference Expansion (DE) and Interpolation in one of the domains such as frequency domain, spatial domain and encrypted domain.

2.1 Spatial Domain Techniques

Using HM techniques Lin et al. [7] presented a multilevel histogram modification reversible data hiding technique considering the difference images. They applied the peak point of a histogram into a difference image and generated an inverse transformation in the spatial domain to create free space. They also observed the characteristics of an image and found that the probability of adjacent pixels being similar is very high. Tai et al. [8] and Kim et al. [9] introduced a reversible data hiding scheme based on histogram modification. They described a binary tree structure to communicate with peak point pairs.

With the PEE technique, Thodi et al. [10] proposed an alternative technique that overcomes the undesirable distortion suffered by Tian. The histogram technique is introduced as an alternative to location map embedding. A Prediction Error Expansion Embedding method is proposed, which exploits the similarity inherent between the neighbor pixels instead of performing difference expansion. Ou et al. [11] proposed an efficient reversible data hiding using prediction error expansion for pixel pair. They exploited image redundancy and also considered the correlation between pixel errors which lead to superior performance. They proposed to pair up adjacent pixel prediction error and generated an error sequence. Based on the error sequence and the predicted error 2D histogram, single or two bits could be embedded, by shifting and expanding the bins of the 2D error histogram.

Using adaptive embedding in PEE, Gui et al. [12] described a large embedding capacity RDH scheme based on adaptive embedding and generalized pixel prediction error expansion. They predicted each pixel using Gradient Adjusted Predictor (GAP) and also computed the complexity measurement partitioned into several levels according to its context. The amount of information bits that can be embedded depends upon the complexity measurement. They embedded more bits in smooth regions, and in each complexity level, the number of bits was adaptively chosen to give the best performance. Sachnev et al. [13] introduced an embedding technique that does not use a location map in most cases. The local variance magnitude is calculated and a sorting technique is used for recording the prediction error. By using sorting and prediction, information is embedded into the pixels with less distortion and the location map if required. They also introduced the concept of rhombus prediction to exploit sorting. Massive improvement in the embedding capacity and visual quality is shown in [14,15].

In interpolation RDH schemes, Jung et al. [16] introduced a reversible data hiding approach using the interpolation technique. The Neighbor mean scaling up interpolation procedure is used and they achieved high calculation speed with less time complexity. Lee et al. [17] introduced an interpolation by neighboring pixel (INP) method on maximum difference value and improved the efficiency of embedding data proposed by Jung. They also considered the pixel localization property to propose a better quality image interpolation. Zhang et al. [18] described a reversible data embedding technique based on interpolation. The cover image is revealed with a factor

of two and the interpolated image is obtained using parabolic interpolation. Seed pixels remain unchanged during the embedding process and only the interpolated pixels are scanned one by one to embed the secret data. Parah et al. [19] analyzed the importance of information security in the e-healthcare domain and introduced a RDH scheme to embed a high amount of patient clinical data imperceptibly into the medical image. They also developed a mechanism to detect tampering of embedded data using check sum calculation

2.2 Frequency Domain Techniques

Kamstra et al. [20] proposed a method with some improvement to Tian's difference expansion. They created free space for embedding the message by decorrelating the pixels using Haar Wavelet transformation and performed embedding by expanding the high-frequency Haar coefficients. They also included the LM concept introduced by Tian to identify the expandable Haar coefficients. Zou et al. [21] presented a semi-fragile RDH scheme using IWT. They used a 5/3 filter bank wavelet family for processing the cover image. Unlike the other data embedding schemes, the overflow/underflow issues are taken care of in a considerable way. The block-based coding scheme uses a special mask as the size of the block to avoid underflow/overflow. Xuan et al. [22] introduced a lossless image data embedding method using IWT and adaptive histogram modification pair. They achieved this by selecting an apt threshold to achieve a high PSNR of the stego image for a given payload. An et al. [23] described a robust reversible watermarking scheme using clustering and enhanced pixel-wise masking. They also incorporated the histogram shifting approach in the wavelet domain. This helped in improving the robustness and reduced the run time complexity.

2.3 Encrypted Domain Techniques

Qin et al. [24] introduced a separable reversible data hiding for JPEG bit stream in encrypted images. They constructed this scheme by reserving room before encryption and modified the bit stream with less distortion so that the content owner will get enough space for embedding the data. Yi et al. [25] presented a technique called binary block reversible data embedding in encrypted images. They achieved this by embedding binary bit in lower bit planes of the cover image into higher bit planes so that by reserving lower bit planes, they embed secret information. Yi [26] presented a separable reversible data hiding. They adopted the parametric binary tree labeling methodology to embed secret information in encrypted images. In order to achieve embedding, they explored the spatial redundancy present in a small block of the image. Chang et al. [27] introduced an RDH method for encrypted JPEG bitstreams in a separable form. They modified the original image with minimal distortion to provide more space for embedding data. Later, encrypting the modified bit streams. Qin et al. [28] proposed a reversible data hiding scheme for encrypted images. They developed an efficient sparse block coding scheme that makes use of the redundancy transfer. They adopted a special encryption method and bit plane disordering block scrambling followed by pixel scrambling. Wu et al. [29] and Yin et al. [30] developed a RDH algorithm in encrypted images. The authors first predicted the Most Significant Bits (MSB) adaptively and performed Huffman coding on to the original image. Later, they encrypted the image using stream cipher and introduced vacated space for embedding bits. They recorded each pixel label as auxiliary information so that to ensure reversibility of the cover image after extracting the embedded information. In all the above-mentioned strategies, the message to be communicated is represented either in decimal or binary number notation. In the proposed methodology, we aim at introducing a Prediction Error Expansion-Variable Radix Numeral System (PEE–VRNS) based RDH technique, which provides more robustness and security to the means of covert

communication. In [31], a PVO based technique using rhombus prediction and histogram shifting has been developed to improve the visual quality of the image.

3 Background of the Proposed Work

3.1 Varying Radix Numeral System

In positional terminology, an integer R may be defined by a series of digits $(d_{n-1}d_{n-2}\ldots d_2d_1d_0)$ as well as a static base or radix r. This R is taken as

$$R = \left(d_{n-1} \times r^{n-1}\right) + \left(d_{n-2} \times r^{n-2}\right) + \ldots + \left(d_2 \times r^2\right) + \left(d_1 \times r^1\right) + \left(d_0 \times r^0\right) \tag{3}$$

The decimal scheme of radix r = 10 is more occasionally found in western cultures and has been the math standard. Throughout both the machines and in optical circuitry, a discrete framework with radix r = 2 is being used. The whole radii in such devices remain unchanged. The radices with Varying Radix Numeral System (VRNS) [32] differ per each position-value of R. For VRNS the integer N is defined as shown below,

$$(d_{n-1}d_{n-2}\ldots d_2d_1d_0)_{(r_{n-1}r_{n-2}\ldots r_2r_1r_0)} \tag{4}$$

where $0 \leq d_i < r_i$.

Using $(r_{n-1}r_{n-2}\ldots r_2r_1r_0)$ reflects distinct radices. Provided N and radices, it will be possible to approximate the digits $(d_{n-1}d_{n-2}\ldots d_2d_1d_0)$ having the usual successive divisions system, except with specific radii as the divisor for every point. Consequently, that value for R could be retrieved from both the quantities d and r as

$$N = d_0 + (d_1 \times r_0) + (d_2 \times r_0 \times r_1) + \ldots + \left(d_{n-1} \times \prod_{j=0}^{n-2} r_j\right) \tag{5}$$

For e.g., if R = 59 and r = 345, for every step, we need to divide successively using each digit from r as the divisors.

Iteration 1: 59 mod 5 yields 4, throwing 11 as Quotient.

Iteration 2: 11 mod 4 yields 3, throwing 2 as Quotient.

Iteration 3: 2 mod 3 yields 2, throwing 0 as Quotient.

Finally, it is represented in VRNS as

$$59_{10} = 234_{345}$$

Well into the debugging hand we now have for

$$234_{345} = 4 + (3 \times 5) + (2 \times 5 \times 4) = 4 + 15 + 40 = 59_{10}$$

A number's radix is proportional to the sum of data that is stored in every one of the numbers. In the discrete method, for example, that digit only contains a single bit of data. When the radix factor grows it often reduces the data found in every one of the origin digits. Therefore, a variable sum of data may be ingested in various pixels of images by utilizing different bases. Fig. 1 shows the index representation of a portion of the image.

	1	2	3	4	5
1	$<i_o,j_o>$	$<i_o,j_e>$	$<i_o,j_o>$	$<i_o,j_e>$	$<i_o,j_o>$
2	$<i_e,j_o>$	$<i_e,j_e>$	$<i_e,j_o>$	$<i_e,j_e>$	$<i_e,j_o>$
3	$<i_o,j_o>$	$<i_o,j_e>$	$<i_o,j_o>$	$<i_o,j_e>$	$<i_o,j_o>$
4	$<i_e,j_o>$	$<i_e,j_e>$	$<i_e,j_o>$	$<i_e,j_e>$	$<i_e,j_o>$
5	$<i_o,j_o>$	$<i_o,j_e>$	$<i_o,j_o>$	$<i_o,j_e>$	$<i_o,j_o>$

Figure 1: Matrix arrangement of pixels showing the pixel group

3.2 Rhombus Mean Computation

To achieve reversibility in the proposed method, the original image is up-sampled to get the cover image. The interpolated image comprises of two different pixels, the seed pixels or the pivot pixels being the actual points present in the image and the additionally added interpolated pixels which are approximated by computation. In all the RDH schemes based on interpolation, the message to be hidden is embedded into the interpolated points and the seed pixels remain unchanged to obtain reversibility. The proposed approach to estimate the interpolated point is by the means of rhombus mean computation, which is considered the best approximation procedure. Instead of duplicating the pixels to form a block, the Rhombus Mean Interpolation (RMI) technique measures the average of four pixels of the nearest neighbor. In equation form, RMI is expressed as

$$
CI(w,h) = \begin{cases}
\dfrac{CI(w-1,h-1)+CI(w-1,h+1)+CI(w+1,h-1)+CI(w+1,h+1)}{4}, \\
\qquad\qquad\qquad if \ \mod(w,2)=\mod(h,2)=0 \\[4pt]
\dfrac{CI(w,h-1)+CI(w-1,h)+CI(w,h+1)+CI(w+1,h)}{4}), \\
\qquad\qquad\qquad if \ \mod(w,2)=0 \ and \ \mod(h,2)=1 \\[4pt]
\dfrac{CI(w,h-1)+CI(w-1,h)+CI(w,h+1)+CI(w+1,h)}{4}, \\
\qquad\qquad\qquad if \ \mod(w,2)=1 \ and \ \mod(h,2)=0 \\[4pt]
CI(w,h), \quad if \ \mod(w,2)=\mod(h,2)=1.
\end{cases}
$$

(6)

The cover image *CI* for the proposed scheme is computed using Eq. (6) of size $w*h$, and the secret *j* bit message data to be embedded is M, expressed in Eqs. (7) and (8) respectively.

$$CI = \{y_{mn} \mid 0 \le m \le w, \ 0 \le n \le h, \ y_{mn} \in (0, 1, \ldots, 255)\}. \tag{7}$$

$$M = \{m_j \mid 0 \le j \le k, \ m_j \in \{0, 1\}\} \tag{8}$$

where, M represents the set of j bit secret data. The resultant stego image after embedding the secret message is given by Eq. (9)

$$CI' = CI + \lambda M \tag{9}$$

where, the resistance factor λ controls the payload for embedding.

Fig. 2 explains a part of image size 2×3 being interpolated to form an image size 4×6. For all index values w, h where $mod\,(w, 2) = 1$ & $mod\,(h, 2) = 1$, the seed points are preserved. The pixels present at the index valued $mod\,(i, 2) = 0$ and $mod\,(j, 2) = 0$ are calculated initially by taking the average of the available neighbors $\dfrac{x1 + x2 + x4 + x5}{4}$ & $\dfrac{x2 + x3 + x5 + x6}{4}$. Then, the left over points are estimated by calculating the average of the available vertical and horizontal neighbors e.g., $\dfrac{x2 + x5 + \text{'O'} + \text{'O'}}{4}$ & $\dfrac{x3 + x6 + \text{'O'} + \text{'O'}}{4}$. In the scaled up cover image CI which is shown in Fig. 2, the points indicated as 'O' are calculated with the help of pivot pixels present in the image. Set of points indicated as '@' are estimated considering the pivot pixels as well as the 'O' set points in the image. Finally, the set of points due to interpolation are estimated to get the approximated cover image CI that can be used for hiding the message. The seed pixels P1, P2, P3... remain unchanged during the embedding process. We modify only the interpolated points for embedding. So the problem of location map could be eliminated using interpolation methods.

	1	2	3	4	5	6
1	P1	@	P2	@	P3	@
2	@	O	@	O	@	O
3	P4	@	P5	@	P6	@
4	@	O	@	O	@	O

Figure 2: Computation of interpolated points using RMI

4 Proposed Methodology

The correlation between the image pixel intensity is used for adaptively embedding the information into the cover. In general, smooth regions of the image constitutes the low-frequency area, the edges and sharp intensity variations indicate high-frequency regions. A considerable change in the smooth region will be perceptible to the human virtual system. Hence, uniform embedding of information will result in the poor quality of marked images. In the proposed system, we adopt an adaptive embedding scheme, which embeds more information in high-frequency points and less amount of data in low-frequency points. The pixel value in the low-frequency region is closely correlated to its neighbor when compared to the high-frequency region, which is much more deviated from its neighbors. This characteristic of pixel distribution in the image is used to adaptively embed the data. The information to be hidden is modified into a series of numbers with varying information, carrying capacity by means of different radices. A larger variance in the predicted pixel value and the neighborhood will result in a larger radix.

4.1 Embedding Procedure

The pixel coordinates in an image can be represented using any one of the following combinations: $\langle i_0, j_0 \rangle$, $\langle i_0, j_e \rangle$, $\langle i_e, j_0 \rangle$, $\langle i_e, j_e \rangle$ where i, j represents the row and column respectively and o, e represents odd and even respectively as given in Fig. 2. In the cover image, the pixels $\langle i_e, j_e \rangle$ carry the hidden information while the remaining pixels $\langle i_0, j_0 \rangle$, $\langle i_0, j_e \rangle$, $\langle i_e, j_0 \rangle$ decide the amount of information that $\langle i_e, j_e \rangle$ can carry without causing perceptual distortion to the image.

The information to be hidden is divided into a fixed length sequence of α bits (say $\alpha = 8$). The integer version of the sequence can be embedded sequentially into the pixels in a specific traversal sequence 'T_s' that can be used as a key.

The following steps are used for embedding an integer m of range [0 to $2^\alpha - 1$] into a cover image CI :

(1) Assume g = 1, the variable that is used to find whether the message to be embedded, 'm', had been embedded completely into cover image pixels.

(2) Let the marked value of the pixel be $I'(x, y)$.

(3) Neighbour of $I(x, y)$ are given by the set S i.e.,

$$S = \{I(x, y-1), I(x-1, y-1), I(x-1, y)\} \tag{10}$$

(4) The radix r for pixel into which the information is embedded is calculated based on the prediction of the pixel $I(x, y)$

$$r(x, y) = |\max[I(x, y-1), I(x-1, y-1), I(x-1, y)] - [I(x, y-1) + I(x-1, y) - I(x-1, y-1)]| \tag{11}$$

where, $1 < r \leq 16$.

For $r \leq 1$ means that the pixel is very sensitive to small changes, hence ignores the pixel and proceed to the next pixel. If $r > 16$, then fix the radix value as 16.

(5) Compute the digit to be embedded in VRNS

$$b(x, y) = mod[m, r(x, y)] \tag{12}$$

(6) Find the binary equivalent of $b(x, y)$ and code it as: b_3, b_2, b_1, b_0. This is embedded into $\langle i_e, j_e \rangle$, $\langle i_e, j_o \rangle$, $\langle i_0, j_e \rangle$, $\langle i_0, j_0 \rangle$ respectively by PEE based embedding technique and then compute $I'(x, y)$

(7) Update the value of w

$$w = w \times r(x, y) \tag{13}$$

If $w < 2^b$ then 'm' is not embedded completely. Detect the value 'm' that has been embedded and update 'm' and start again from Step (2)

$$m = \frac{m - b(x, y)}{r(x, y)} \tag{14}$$

If $w > 2^b$, then message 'm' is successfully embedded.

This procedure is followed for the remaining bits in the message stream and the final marked image is generated.

4.2 Extraction Procedure

The extraction procedure involves the recovery of the cover pixel and extraction of the symbols hidden using variable radices. Later, the symbols and the order of extraction of bits for radices should be the same as mentioned in Step (6). The following steps are followed to extract the message and recover the original pixels from the marked image

(1) Set w = 1 and k = 0, to have a check whether 'm' has been completely extracted.

(2) Sequentially extract the bits b_0, b_1, b_2, b_3 from the LSB of $I'(i_e j_e)$, $I'(i_e j_o)$, $I'(i_o j_e)$, $I'(i_o j_o)$ respectively and the original pixel can be restored as $x = \hat{x} + \left(\dfrac{P_e}{2}\right)$

(3) Calculate $r(x, y)$ using Eq. (3)

If $r \le 1$; go to Step (2), if $r > 1$; proceed with Step (4), else set r = 16.

(4) Convert the extracted bits b_3, b_2, b_1, b_0 into its equivalent decimal which is nothing but $b(x, y)$

(5) Revise the value of 'w' using

$$w = w \times r(x, y) \tag{15}$$

(6) Set $B_k = b(x, y)$ and $R_k = r(x, y)$

(7) If $w < 2^\alpha$: then k = k + 1 and go to Step (2)

Else: Reconstruct 'm' from digits

$(A_{k-1} A_{k-2} \dots A_2 A_1 A_0)$ and

radix$(R_{k-1} R_{k-2} \dots R_2 R_1 R_0)$

The embedding and the extraction procedure is represented as a flow chart in Fig. 3.

This procedure is followed for all the non-overlapping blocks in the entire image. Finally, we get the recovered cover image and the secret bits separated from the marked image. The basic embedding and extraction procedure has been explained in the above sections. The embedding rate can be improved by implementing the adaptive pixel selection procedure which will be explained in the further section. The proposed algorithm is illustrated using a portion of the 512 × 512 Lena as image shown in Fig. 3. The advantage of imposing adaptive embedding in the proposed scheme can be analyzed using the average distortion Eqs. (19) and (20) which holds for conventional PEE and double embedding adaptive. For conventional PEE, the expansion is only once and the average distortion is given

$$D_{PEE} \underline{\Delta} E[(x^m - x)^2] = E[(e^m - e)^2] \tag{16}$$

$$D_{Ap} \underline{\Delta} \frac{1}{4} \sum_{b=0}^{3} (3e + b)^2 = 9e^2 + 9e + 3.5 \tag{17}$$

When we compare the above two equations for arbitrary prediction errors e_1 *and* e_2, it can be derived that $D_{Ap} < D_{PEE}$ provided that $0 \le e_1 \le e_2/(3 - 1)$. It shows that instead of embedding a single bit into a pixel having a larger prediction error, it is better to embed one more bit into a pixel having a lesser prediction error and embedded once. Instead of having only two regions in the image as smooth and rough surfaces, it is advisable to partition the image into regions based on the complexity, and a capacity parameter can be used to optimize the capacity in each region of the image. So that the redundancy of the image could be better utilized.

We define a parameter P for optimizing the embedding capacity in each region of the image. The data embedding procedure is implemented for various values of P being 1–4. Fig. 4 shows the plot for various embedding capacities and the corresponding PSNR values for randomly selected parameter values in each region and the optimized parameter values on a 512 × 512 Lena image. To demonstrate the features for the parameter determination procedure, we will examine the graph plot shown in Fig. 5. One can see that the performance evaluation for optimization parameter P = 3 which is shown as a solid blue line, out performs the randomly selected parameter sets. This also proves the effectiveness of the algorithm. When the parameter is increased from 1–3, the performance increased with an improvement in the maximum EC and with the performance gain. There was a slight increase in gain as P changes from 3 to 4. This observation was also validated for the remaining test images. Running time for the given image to determine the parameter implemented in Matlab is about 1 s for P = 1, 15 s for P = 2, 2 min for P = 3 and 45 min for P = 4.
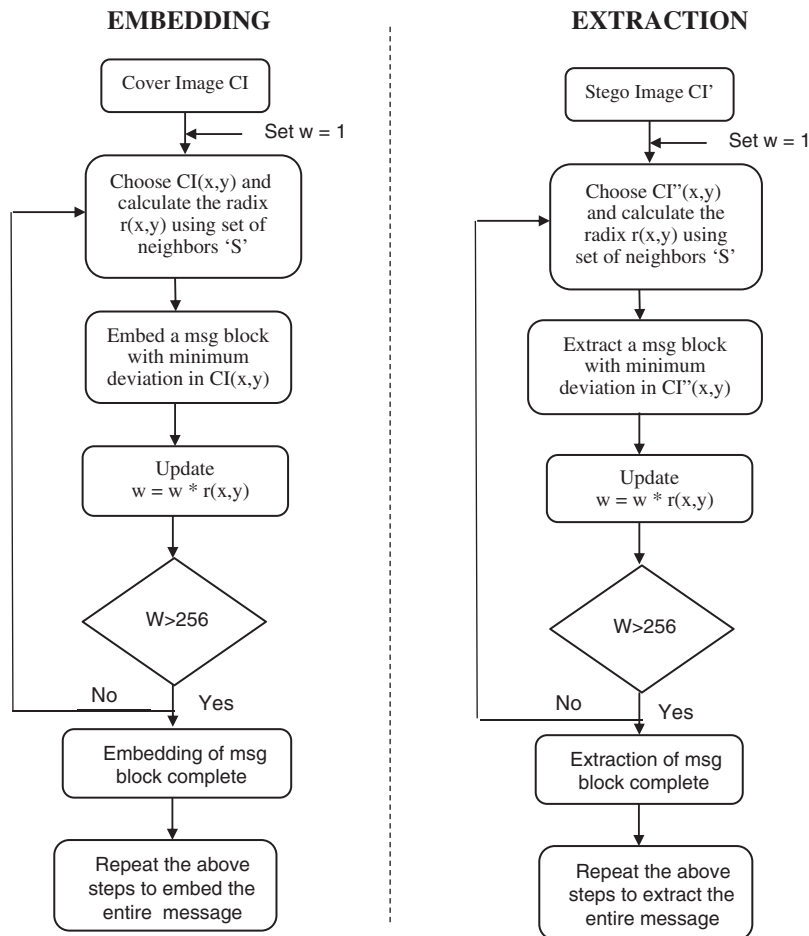
EMBEDDING

Cover Image CI

Set w = 1

Choose CI(x,y) and calculate the radix r(x,y) using set of neighbors 'S'

Embed a msg block with minimum deviation in CI(x,y)

Update w = w * r(x,y)

W>256

No   Yes

Embedding of msg block complete

Repeat the above steps to embed the entire message

EXTRACTION

Stego Image CI'

Set w = 1

Choose CI''(x,y) and calculate the radix r(x,y) using set of neighbors 'S'

Extract a msg block with minimum deviation in CI''(x,y)

Update w = w * r(x,y)

W>256

No   Yes

Extraction of msg block complete

Repeat the above steps to extract the entire message

Figure 3: Flow chart of the proposed embedding and extraction procedure
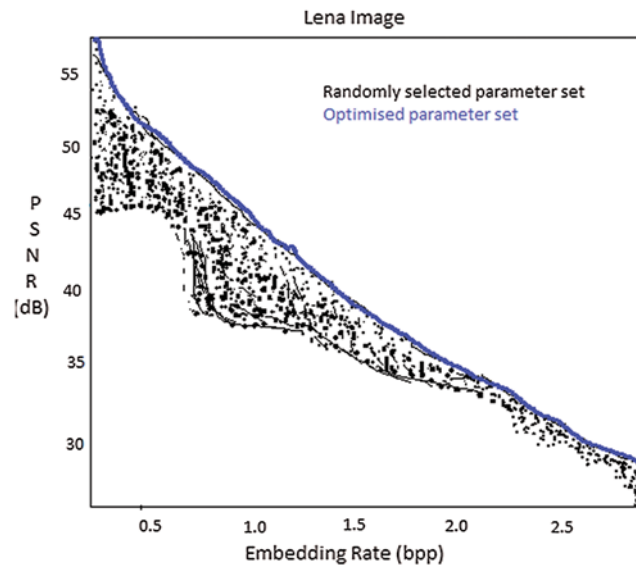
Figure 4: Performance comparison of the proposed scheme with randomly selected parameters
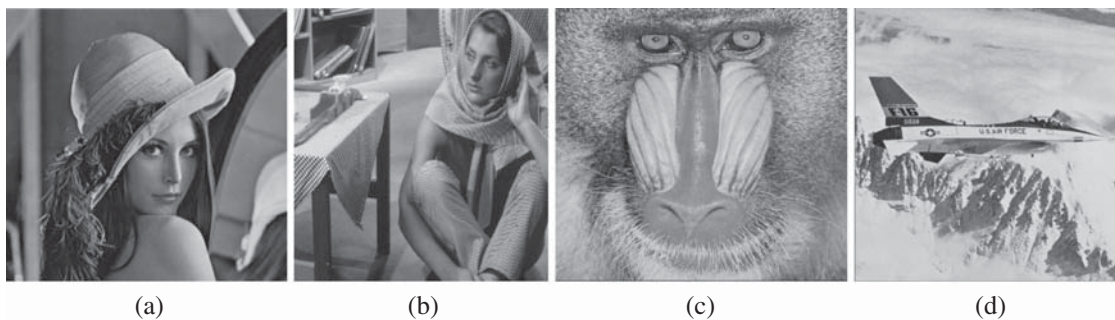

| (a) | (b) | (c) | (d) |

Figure 5: Standard test images. (a) Lena (b) Barbara (c) Baboon (d) Airplane

5 Experimental Results and Discussions

The proposed algorithm has been experimented with different medical images and natural images like Lena, Barbara, Baboon, Airplane as shown in Fig. 5, using the MATLAB R2014a platform. The input image size of 512×512 was considered for the cover image. Fig. 6 shows the 512×512 medical images considered for experimentation. The iteration steps for the embedding and extraction procedures are given in Tab. 1. The proposed scheme has been experimented upon 100 uncompressed, standard and clinical 512×512 text images. No other auxiliary information is required for decoding the embedded information.

Fig. 6 shows some of the medical images for which the results have been tabulated and is shown in Tab. 2. The average objective quality parameters for a payload of 0.75 bpp came to be 52.75 dB PSNR, 0.983 for SSIM and for 1.5 bpp, it turned out to be 48.36 dB PSNR and 0.9811 SSIM.
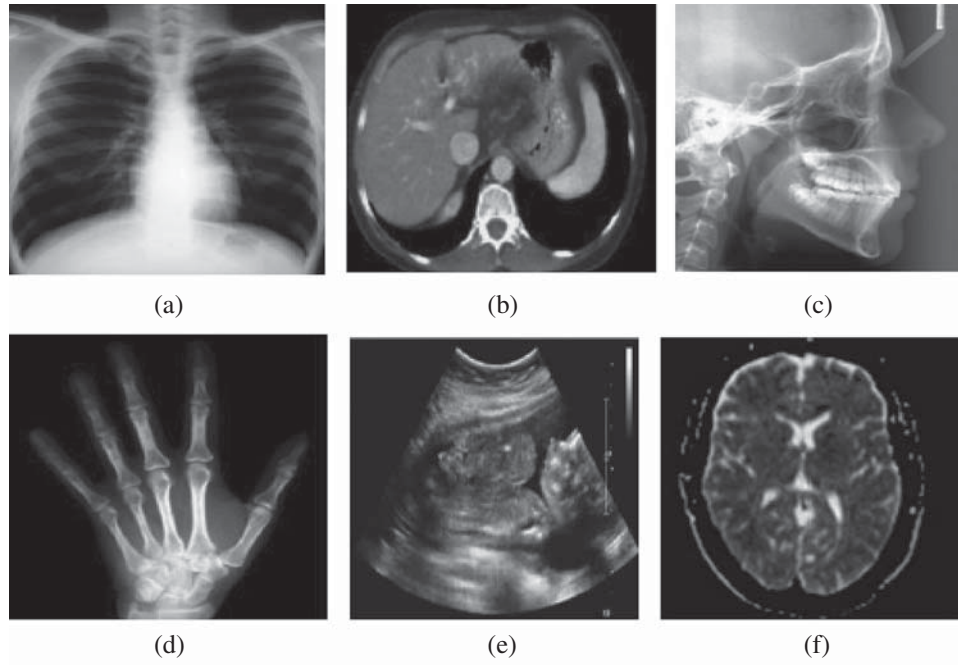
Figure 6: (a) Thorax X-ray image (b) Brain CT scan image (c) Cephalogram dental image (d) Palm X-ray image (e) Ultra scan fetus image (f) Brain MRI scan image

PSNR (Eq. (18)) gives the similarity between the cover data and the stego data. The higher the value of PSNR, the better is the imperceptibility of the stego image.

$$PSNR = 10 \, log_{10} \, (255^2/MSE) dB \tag{18}$$

where MSE (Eq. (19)) is nothing but the Mean Square Error which is computed between the cover image CI and stego image CI', both of size $M \times N$.

$$MSE = \frac{1}{M \times N} X \sum_{i=1}^{a} \sum_{j=1}^{b} (CI\,(i,j) - CI'\,(i,j))^2 \tag{19}$$

The computation of SSIM (Eqs. (20)–(23)) is centered on the estimates of three terms, namely the contrast, luminance, and structure. The complete index is presented by:

$$SSIM\,(x,y) = [I\,(x,y)]^{\propto}, \, [C\,(x,y)]^{\beta} [S\,(x,y)]^{\gamma} \tag{20}$$

where,

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \tag{21}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \tag{22}$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \tag{23}$$

where, σ_x, σ_y, μ_x, μ_y and σ_{xy} are the standard deviations, local means, and cross-covariance for images x, y respectively. The term $l(x, y)$ gives the luminance assessment between the two images, the next term $c(x, y)$ gives the contrast assessment and the final term $s(x, y)$ gives the structure assessment of the two images x, y.

Table 1: Embedding and extraction procedure

Embedding procedure	Extraction procedure
ITERATION 1	*ITERATION 1*
(2) Set w = 1	(1) Set k = 0 and w = 1
(3) Pixel to be considered is $I(2, 2)$	(2) Framing set S = {$CI'(1, 1)$, $CI'(1, 2)$
(4) Set that should be taken S = {$CI(1, 1)$, $CI(1, 2)$	$CI'(1, 3)$, $CI'(2, 3)$, $CI'(3, 1)$, $CI'(3, 2)$, $CI'(3, 3)CI'(2, 1)$}
$CI(1, 3)$, $CI(2, 3)$, $CI(3, 1)$, $CI(3, 2)$, $CI(3, 3)CI(2, 1)$}	(3) r(2, 2) = 16
(5) r(2, 2) = 16	(4) $b(2, 2)$ = mod (139, 16) = 11
(6) Then b(2, 2) = mod (59, 16) = 11	(5) Revise w as w = 16
(7) The possible choices for $CI'(2, 2)$ are $CI'^1(2, 2) = 123$	(6) $A_0 = 11$, $R_0 = 16$
and $CI'^2(2, 2) = 139$. Since both values have a difference	(7) Since g < 256
of 8 from $CI(2, 2)$, assign any value. Let us consider the	(8) K = k + 1
value 139 for further calculation	(9) Go to Step (2)
(8) Update w = 16. Since w ≤ 256, the new value for m =	(10) Pixels to be considered is $CI'(2, 4)$
3 and go to Step (2)	
ITERATION 2	*ITERATION 2*
(9) Go to next pixel in T.$I(2, 4)$	(11) S = {$CI'(1, 3)$, $CI'(2, 3)$
(10) Set that should be taken S = {$CI(1, 3)$, $CI(2, 3)$	$CI'(3, 3)$, $CI(1, 4)$, $CI'(3, 4)$, $CI'(1, 5)$, $CI'(2, 5)CI'(3, 5)$}
$CI(3, 3)$, $CI(1, 4)$, $CI(3, 4)$, $CI(1, 5)$, $CI(2, 5)CI(3, 5)$}	(12) r (2, 4) = 16
(11) r(2, 4) = 16	$b(2, 4) = mod(195, 16) = 3$
(12) Calculating b (2, 4) = mod (3, 16) = 3	(13) Revise w as 16 × 16 = 256
(13) The possible choices for $CI'(2, 4)$ are	(14) $A_1 = 3$, $R_1 = 16$
$CI'^1(2, 4) = 179$ and $CI'^2(2, 4) = 195$. Let us consider the	(15) Since w ≥ 256, we can start to reconstruct message m
value 195 since it is close to 188	from $(11, 3)_{(16.16)} = 11 + (3 × 16) = 59$
(14) Update w = 256. Since w ≥ 256, the entire message	
has been encoded completely.	

The proposed approach for embedding into the rhombus mean interpolated image by adaptive means of pixels selection is carried out to avoid uniform embedding throughout the image. The embedding procedure is carried out by dividing the image into blocks of 3×3, overlapping blocks on the rows and columns. The generated stego image can withstand a moderate embedding capacity maintaining the perceptual quality of the image. Moreover, it can overcome the LSB attack on the marked image. Experimental results and comparison over other existing techniques show that the proposed scheme delivers the quantity as well as the quality requirement for the RDH scheme. This approach could be extended for other multimedia files such as audio/video, to enable correct communication. The proposed method can be improved to overcome other active attacks like RS steganalysis. By employing a suitable image pre-processing technique, the proposed method can be used to improve the contrast of low-quality medical images. This can also help in the proper diagnosis of the clinical images.
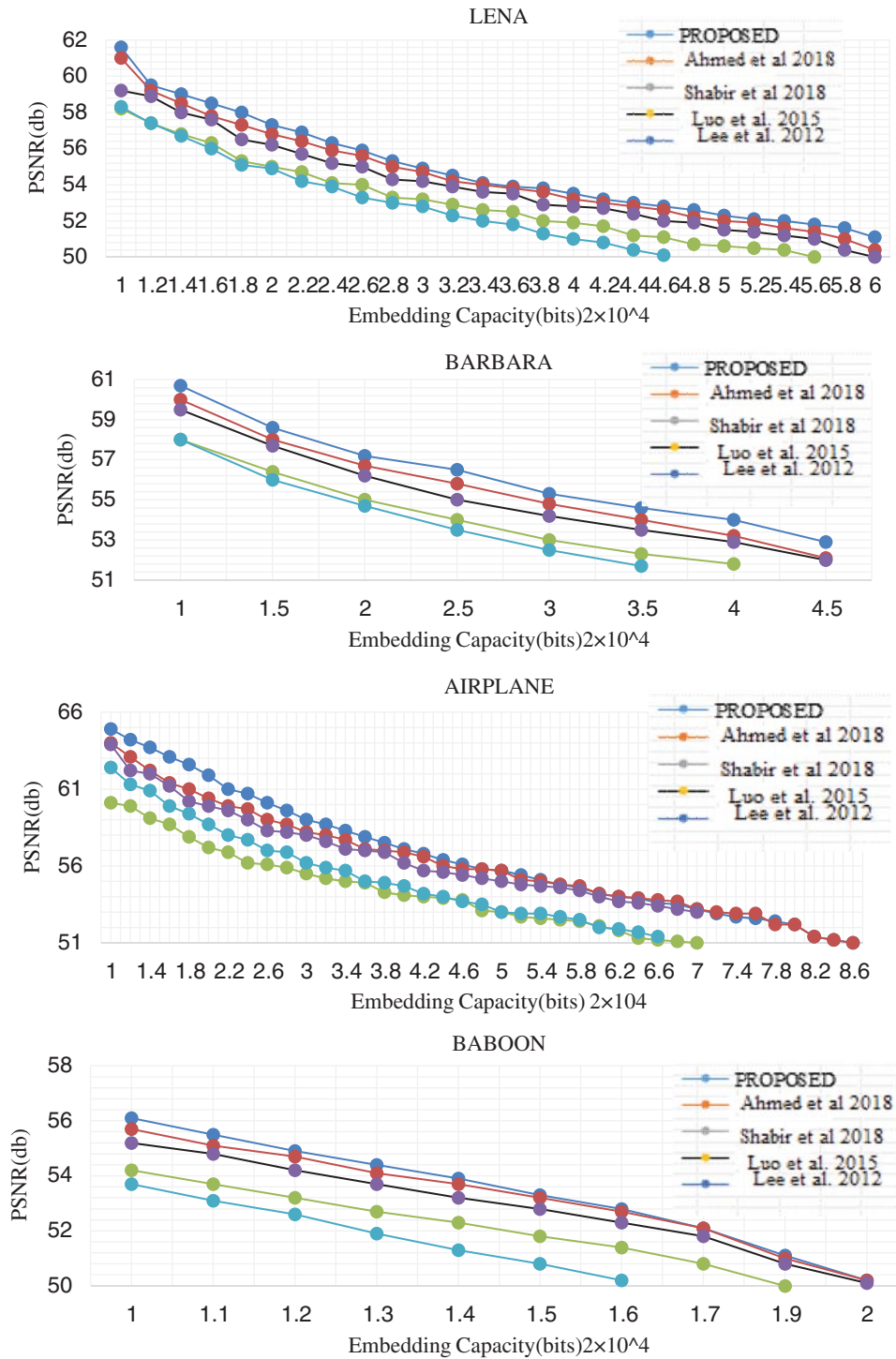
Figure 7: Performance evaluation curve showing the comparison of various schemes

Performance analysis of the proposed scheme is compared with various existing schemes. The performance comparison curve is shown in Fig. 7. The VRNS based embedding into the interpolated image performance at a lower embedding rate is almost similar to the existing schemes. But the proposed scheme performs better at higher embedding rates. This is because, in histogram shifting or expansion schemes, as the embedding rate increase, more bins need to be shifted or expanded. Here, we adopted an adaptive embedding in the interpolated image. Pixel modification happens in higher frequency points and low-frequency points undergo fewer modifications. The graph is plotted for Lena, Barbara, Airplane and Baboon images up to an embedding rate of 1.0 bpp. Tab. 2 shows the performance comparison of the proposed method with recent existing schemes that had shown better performance in medical images. The performance metric capacity, PSNR and SSIM is also computed and tabulated.

Table 2: Comparison of proposed method with other schemes

Clinical image	Schemes	Capacity (bpp)	Capacity (bits)	PSNR (dB)	SSIM
Thorax X-Ray	**Proposed method**	**1.5**	**3,93,216**	**48.36**	**0.9812**
	Kumar R 2020	1.0	2,62,144	46.15	0.9810
	Yin et al. 2019	1.5	3,93,216	46.676	0.9922
	Ahmed A et al. 2018	1.5	3,93,216	46.15	0.9810
	Shabir et al. 2017	1.0	2,62,144	48.43	0.998943
Palm X-Ray	**Proposed method**	**1.5**	**3,93,216**	**48.36**	**0.9801**
	Kumar R 2020	1.0	2,62,144	48.12	0.9809
	Yin et al. 2019	1.5	3,93,216	45.685	0.9909
	Ahmed A et al. 2018	1.5	3,93,216	46.946	0.99958
	Shabir et al. 2017	1.0	2,62,144	48.42	0.998943
Ultra Scan Fetus	**Proposed method**	**1.5**	**3,93,216**	**48.36**	**0.9801**
	Kumar R 2020	1.0	2,62,144	47.95	0.9810
	Yin et al. 2019	1.5	3,93,216	46.6873	0.9932
	Ahmed A et al. 2018	1.5	3,93,216	45.94	0.99958
	Shabir et al. 2017	1.0	2,62,144	48.42	0.998943
Brain MRI Scan	**Proposed method**	**1.5**	**3,93,216**	**48.36**	**0.9821**
	Kumar R 2020	1.0	2,62,144	47.95	0.9819
	Yin et al. 2019	1.5	3,93,216	45.683	0.9928
	Ahmed A et al. 2018	1.5	3,93,216	45.947	0.99958
	Shabir et al. 2017	1.0	2,62,144	48.421	0.998943
Cephalogram Dental	Proposed method	**1.5**	**3,93,216**	**48.36**	**0.9821**
	Kumar R 2020	1.0	2,62,144	48.15	0.9817
	Yin et al. 2019	1.5	3,93,216	46.68	0.9958
	Ahmed A et al. 2018	1.5	3,93,216	46.946	0.99958
	Shabir et al. 2017	1.0	2,62,144	48.42	0.998943
Brain CT Scan	Proposed method	**1.5**	**3,93,216**	**48.36**	**0.9802**
	Kumar R 2020	1.0	2,62,144	45.65	0.9810
	Yin et al. 2019	1.5	3,93,216	45.682	0.9938
	Ahmed A et al. 2018	1.5	3,93,216	46.946	0.99958
	Shabir et al. 2017	1.0	2,62,144	48.42	0.998943

Message m = 59 is embedded into the cover image $I(x, y)$ and the resultant marked image is denoted as $I'(x, y)$. Steps involved in extracting the message from $I'(x, y)$ is also summarized in Tab. 1.

The proposed method can also be considered for color images. Color images consists of three color components namely R G B. Using the relationship $v = \lfloor 0{:}299r + 0{:}587g + 0{:}114b \rceil$ and fv(r; g; b) = $\lfloor 0{:}299r + 0{:}587g + 0{:}114b \rceil$, convert the color components into the corresponding grey version of color image. Later, embedding can be performed using the proposed method in each of the color components. But, the major challenge is to explore the correlation between each of the color channel in RGB. Another approach would be to perform color plane separation and hide data in either red or blue color channels. Since the green channel is highly sensitive to any stego noise injection, it has to be spared. After the data hiding process, the three color channels can be combined and the stego color image is constructed back. The extraction is a reverse process of the same, with one additional information needed about the color plane in which data is hidden.

Perceptual Quality Analysis: A moderate amount of payload capacity up to 1.5 bpp were experimented on various test images using the proposed schemes. The PSNR for various embedding capacity of the proposed algorithm is compared with the latest scheme that works on low embedding capacity and shown in Fig. 7. It is evident that the proposed scheme gives a better perceptual quality.

Attacks on RDH: Most of the RDH techniques are LSB embedding and of radix 10. Collection of LSB's of various pixels and reordering will result in the secret information. The proposed technique, which is actually LSB matching, embeds only the residuals of the radix into the LSB's of each pixel. No attacks on this RDH technique will be able to decode the hidden content in the marked image.

6 Conclusion

In this paper, we proposed a novel VRNS based RDH using the rhombus mean interpolation technique. Wherein embedding is carried out by dividing the image into blocks of 3×3, non-overlapping on the rows and overlapping on the columns. The generated marked image can withstand higher embedding capacity, maintaining the perceptual quality of the image. Moreover, it can overcome the LSB attack on the marked image. Experimental results and comparison over other existing techniques show that the proposed scheme delivers the quantity as well as the quality requirement for the RDH scheme. This approach could be extended for other multimedia files such as audio/video, to enable correct communication. Since all RDH schemes are fragile in nature, the same can be applied on the receiving end to verify the integrity of the received message. Our method can be improved to overcome other active attacks. By employing a suitable image pre-processing technique, the proposed method can be used to improve the contrast of low quality medical images. This can be achieved by applying histogram shifting to the rhombus predicted image and selecting suitable bins on both sides of the prediction error histogram so as to enhance the contrast of the texture area. This can also help in the proper diagnosis of the clinical images. Other than data hiding for content retrieval, more functions such as content enhancement, authentication and content annotation can be achieved. The future scope of the paper is to develop a scheme that could be suitable for images in the encrypted domain.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann, 2007.

[2] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K: Cambridge Univ. Press, 2009.

[3] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[4] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, 2004.

[5] Z. Ni, Y. Shi, N. Ansari and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–361, 2006.

[6] Z. Ni, Y. Shi, N. Ansari, W. Su, Q. Sun *et al.,* "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 4, pp. 497–509, 2008.

[7] C. C. Lin, W. L. Tai and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Journal of Pattern Recognition*, vol. 41, no. 1, pp. 3582–3591, 2008.

[8] W. L. Tai, C. M. Yeh and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906–910, 2009.

[9] K. S. Kim, M. J. Lee, H. Y. Lee and H. K. Lee, "Reversible data hiding exploiting spatial correlation between sub-sampled images," *Journal of Pattern Recognition*, vol. 42, no. 1, pp. 3083–3096, 2009.

[10] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, 2007.

[11] B. Ou, X. Li, Y. Zhao, R. Ni and Y. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 5010–5021, 2013.

[12] X. Gui, X. Li and B. Yang, "A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding," *Signal Processing*, vol. 98, no. 2, pp. 370–380, 2014.

[13] V. Sachnev, H. J. Kim, J. Nam, S. Suresh and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 7, pp. 989–999, 2009.

[14] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri *et al.,* "Efficient quantum infohrmation iding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[15] B. Ou, X. Li, J. Wang and F. Peng, "High-fidelity reversible data hiding based on geodesic path and pairwise prediction-error expansion," *Neurocomputing*, vol. 226, no. 2, pp. 23–34, 2017.

[16] K-H. Jung and K-Y. Yoo, "Data hiding method using image interpolation," *Computer Standards Interfaces*, vol. 31, no. 2, pp. 465–470, 2009.

[17] C-F. Lee and Y-L. Huang, "An efficient image interpolation increasing payload in reversible data hiding," *Expert Systems with Applications*, vol. 39, no. 8, pp. 6712–6719, 2012.

[18] X. Zhang, Z. Sun, Z. Tang, C. Yu and X. Wang, "High capacity data hiding based on interpolated image," *Multimedia Tools and Applications*, vol. 6, no. 7, pp. 9195–9218, 2017.

[19] S. A. Parah, F. Ahad, J. A. Sheikh and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and rever-sible data hiding technique," *Journal of Biomedical Informatics*, vol. 66, no. 1, pp. 214–230, 2018.

[20] L. H. J. Kamstra and A. M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2082–2090, 2005.

[21] D. Zou, Y. Q. Shi, Z. Ni and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 10, pp. 1294–1300, 2006.

[22] G. Xuan, Guorong, Y. Q. Shi, J. Chen, C. Yang *et al.,* "High capacity lossless data hiding based on integer wavelet transform," in *Proc. IEEE*, Vancouver, Canada, pp. 29–32, 2004.

[23] L. An, X. Gao, X. Li, D. Tao, C. Deng *et al.,* "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 21, no. 8, pp. 3598–3611, 2012.

[24] C. Qin, C. C. Chang and Y. P. Chiu, "A novel joint data-hiding and compression scheme based on SMVQ and image inpainting," *IEEE Transactions on Image Processing*, vol. 23, no. 3, pp. 969–978, 2014.

[25] S. Yi and Y. C. Zhou, "Binary-block embedding for reversible data hiding in encrypted images," *Signal Processing*, vol. 133, no. 3, pp. 40–51, 2017.

[26] S. Yi, Y. Zhou and Z. Hua, "Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion," *Signal Processing: Image Communication*, vol. 64, no. 8, pp. 78–88, 2018.

[27] J. C. Chang, Y. Lu and H. L. Wu, "A separable reversible data hiding scheme for encrypted JPEG bitstreams," *Signal Processing*, vol. 133, no. 5, pp. 135–143, 2017.

[28] C. Qin, X. Qian, W. Hong and X. Zhang, "An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer," *Information Sciences*, vol. 487, no. 8, pp. 176–192, 2019.

[29] H. Wu, W. Mai, S. Meng, Y. Cheung and S. Tang, "Reversible data hiding with image contrast enhancement based on two-dimensional histogram modification," *IEEE Access*, vol. 7, pp. 83332–83342, 2019.

[30] Z. Yin, Y. Xiang and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and huffman coding," *IEEE Trans Multimedia*, vol. 22, no. 4, pp. 874–884, 2020.

[31] R. Kumar and K. H. Jung, "Enhanced pairwise IPVO-based reversible data hiding scheme using rhombus context," *Inf. Sci. (Ny)*, vol. 536, no. 2, pp. 101–119, 2020.

[32] S. Geetha, V. Kabilan, S. P. Chockalingam and N. Kamaraj, "Varying radix numeral system based adaptive image steganography," *Information Processing Letters*, vol. 111, no. 16, pp. 792–797, 2011.