Multimed Tools Appl
DOI 10.1007/s11042-017-4622-0

High performance reversible data hiding scheme through multilevel histogram modification in lifting integer wavelet transform

S. Subburam[1] · S. Selvakumar[2] · S. Geetha[3]

Received: 14 June 2016 / Revised: 15 March 2017 / Accepted: 20 March 2017

Abstract This paper proposes a digital image reversible data hiding method in integer lifting transform domain. Owing to the characteristics of the natural image statistics, the neighbor pixel values are similar mostly and hence their differences are observed to be close or equal to zero. A histogram constructed out of this difference factor is exploited for reversible data embedding. Further, data is embedded at multiple levels in the integer lifting wavelet transform domain and hence the proposed scheme facilitates higher payload capacity and exceptional perceptual quality than the conventional single level histogram based techniques. The additional information involved for restoring the cover image and the secret payload is also less compared to the conventional schemes, as the proposed method employs a single parameter called "Embedding Level" for both hiding as well as extraction. Extensive experimentation with huge database of images, five existing RDH schemes and against seven steganalysers, shows that the proposed RDH scheme outperforms other schemes and proves to be a high performance RDH scheme in terms of all the desirable features of a reversible data hiding system like high payload, imperceptible, robustness, losslessness and minimal side information.

✉ S. Geetha
geethabaalan@gmail.com

[1] Department of Computer Science and Engg, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, Tamil Nadu, India

[2] Department of Computer Science and Engg, GKM College of Engg, Chennai, Tamil Nadu, India

[3] VIT University – Chennai Campus, Vandalur-Kelambakkam Road, Chennai, Tamil Nadu 600127, India

Keywords Reversible data hiding · Reversible histogram modification · Lifting integer wavelet transform · Authentication and security

1 Introduction

The technology of information hiding through an open network is showing rapid development in recent years. Securing the information has remained to be one of the top demands in information technology and communication. In some countries, government bans on the usage of digital cryptography. Steganography is sought out as an inevitable alternative by individuals and corporates who prefer confidentiality since clubbing cryptography and steganography paradigms helps in privacy protection and covert communication. Protection of intellectual property rights by the digital content owners has become imperative especially due to the proliferation of the digital data in the Internet. Further, due to the rapid advancement in technology, steganographic technique is becoming effective in hiding information in image, audio or text files. All these factors attribute to the renaissance of steganography as an effective security component.

Steganography or data hiding is the process of embedding a secret data which carries significant information into a cover media (audio/image/video files). The media camouflaging information is referred to as the cover or host media, the secret information that is hidden and communicated covertly is called as the payload. The host image with the payload is called as the stego-media. Due to the message embedding process, the cover media suffers some distortion, at least statistically though imperceptible, irrespective of the steganographic technique used. At the receiver's end, the secret message is extracted back from the stego image by a reverse process and perhaps the cover/host image could not be restored and is ignored in most applications. Some trivial applications, beyond demanding the fidelity of cover image, stego-imperceptibility and high-payload capacity, also insist on restoring the cover image perfectly. Typical cases include diagnostic medical images, geographic maps, archival images (eg., calligraphy, painting), military maps, remote sensing images and perhaps, any type of images involving legal problems like official documents, e-signatures or legal documents etc.

In these cases the receiver is constrained to reconstruct the host image to the last intricate detail, alleviating even the minute disruption arising out of embedding process. Similarly, the medical diagnosis and further treatment, depend on the images and hence the distortions are seriously looked-upon, since they lead to fatal difference. To ensure image integrity and tamper-proof property, hash information of the image could be embedded and extracted at the communication end points. Further other information like authentication data, additional augmenting files for each image etc. can also be hidden inside the images. These cases trigger a pressing need for perfectly restoring host image after extracting the payload. Reversible or lossless data hiding is a distinct category of procedure that aims at recovering the cover image along with the embedded data from the stego image at the receiver's end. The cover media then becomes useful for legal purpose. Although the stego injection into the cover image introduces artifacts, the reversible data hiding schemes facilitate mechanism for removing the disruptions incurred and perfectly recovering the lossless host image.

A good reversible steganographic scheme is characterized by the possession of attributes like lossless/reversible, imperceptible, high payload capacity, robustness and minimal side information involved. By lossless or reversible, it is meant both the extraction of the payload as well as the restoration of host image perfectly from the stego image. Secondly, the imperceptible factor applies at two levels – the stego image resemblance against the cover/host image at the first level (this is usual even with irreversible steganographic scheme) and the extracted output image resemblance against the original cover/host image (this is specific to the reversible schemes). The payload capacity measures the maximum capacity of the payload that can be embedded into a given host image without or with minimal perceptible distortions. Robustness counts for the ability to sustain the secret payload against both intentional and inadvertent image processing operations. Finally, side information is a metric that is of high significance in a reversible stego scheme and it should be as low as possible so as to make the system practically feasible.

The main goal of this paper is to present an efficient, yet simple reversible steganographic scheme designed for digital images. The proposed scheme carries out multilevel histogram modifications in integer lifting wavelet transform domain and is assessed for the above criteria and possible applications. The paper is organized as follows: Section 2 presents a comprehensive literature survey in the RDH domain. Section 3 discusses the rationale for the choice of integer wavelet transform. Section 4 describes the proposed system while Section 5 explains the experimental setup and discusses the results obtained. Section 6 concludes the paper with the summary of the proposed scheme.

2 Literature survey

The existing reversible data hiding schemes can be categorized into six streams based on their key concerns and method adapted. They are 1) Difference Expansion based schemes; 2) Histogram Shifting based schemes; 3) Prediction based schemes; 4) Interpolation based schemes; 5) Robustness based schemes; 6) Human Visual System (HVS) based schemes. Brief descriptions of these six categories and discussions about performance assessments and corresponding limitations are summarized as follows.

2.1 Difference expansion based schemes

The difference expansion (DE) technique is one among the earliest reversible data hiding schemes [30]. The scheme adapts the idea followed in wavelet transforms, which converts the luminance values in the spatial domain into frequency components. The secret data is embedded into the frequency coefficients, with reversible feature. In the same manner, every two neighboring pixels are grouped together as a pair and are converted into frequency components. The secret message is hidden into the difference between the pixels in each pair that did not cause overflow/underflow problems. The authors demonstrated that the payload size and the picture quality of the stego images were superior among the existing works at that time. The scheme attained a payload of 0.5 bpp in a single pass embedding process. An improvement over this scheme was proposed in [2], where the author applied the DE logic on vectors instead of pixel pairs. They demonstrated their algorithm in color as well as grayscale images and reported a better payload capacity than Tian et al. [30]. Another variant of DE was proposed by Hsiao et al. [6], where data bits are hidden in two categories: user data and side/auxiliary information. The image pixels are classified as belonging to any one of the three regions namely – smooth region, normal region and complex region. Smooth and normal regions contained secret messages. The complex regions are ignored since they are incapable of withstanding any alterations and did not hold any stego bit. A disjoint, agreed upon area in the image for holding the side/auxiliary information contained the overhead bits i.e.,location map. This was used for perfect recovery of payload as well as the host image. Weng et al. [36] came out with a lossless data hiding algorithm which used the invariability of the sum of pixel pairs and pair-wise difference adjustment (PDA). The scheme reported commendable picture quality since the pixel pairs were subjected to subtle modifications. Another advantage of the scheme is that the overhead information size was reduced. A high capacity data hiding scheme was proposed by Hu et al. [7] which employed compressed location map. The authors demonstrated the high capacity of their scheme over diverse image types. Yang et al. [39] proposed a scheme that exploited the coefficient-bias for data hiding. Both spatial domain and frequency domain were employed for secret embedding. Hence the scheme exhibited good robustness property.

2.2 Histogram shifting based schemes

Histogram-based reversible data hiding has gained popularity due to its ease of implementation. The chosen luminance is forcibly made as blank in the histogram by an intentional shift in the host image histogram. This provides room for reversible data hiding. The payload capacity can be increased by cleverly selecting the appropriate luminance value and that value which is one byte in length act as the side information for decoding.

Ni et al. [17] exploited the zero or minimum points in the histogram of an image and introduced slight alterations into the pixel values to embed data bits into the images without any loss. Lin et al. [14] suggested a multilayer scheme based difference histogram modification. The system produced images with a PSNR of minimum 42.69 dB. Tai et al. [27] coupled binary tree structure with the histogram modification technique. The overflow/underflow issue was also addressed effectively. Their system exploited the difference between neighbouring pixels instead of focussing on a single pixel. Similarly by altering difference histogram between sub-sampled images, Kim et al. [10] came out with an efficient reversible data hiding algorithm. The scheme operated on the difference histogram and then embedded data bits into the modified pixel values by shifting. The algorithm did not need any side information for payload and host image recovery. By another scheme that interleaved the maximum/minimum difference histogram with the shifting technique, Yang et al. [41] realized their system with a meagre distortion in the images. Simulation results proved that the optimal embedding rate achieved was 1.120 bpp, with a PSNR value of around 30 dB.

A multilevel histogram modification based reversible data hiding is proposed by Zhao et al. [43]. The embedding capacity is influenced by two factors namely – (i) the embedding level and (ii) the number of histogram bins around 0. The system was realized in spatial domain and hence is vulnerable to threats faced by any spatial domain systems.

2.3 Prediction based schemes

Another reversible data hiding method that used histogram shifting and prediction-error expansion technique, was proposed in Thodi and Rodriguez [29]. The authors demonstrated the prediction-error expansion almost increased the embedding capacity by a factor of two. The system also produced good picture quality at a moderate embedding capacity. Another variant of this scheme that used predicted encoding and histogram shifting was proposed by Tsai et al. [31]. The similarities existing between the neighbouring pixels were determined and subsequently residual histogram based on the predicted errors was constructed. The secret payload was hidden inside this histogram of predicted errors. The system provided better picture quality than the counter systems. Another scheme that exploited the difference expansion between a pixel and its predictive value was proposed by Tseng and Hsieh [32]. The system offered high payload capacity and good imperceptibility. A similar difference expansion prediction approach was proposed by Lee et al. [11]. The scheme was successful since the location map is not required during data extraction. Another scheme that used interleaving prediction was suggested by Yang et al. [40]. A histogram is constructed from all the predictive values. At the high peak values, the bits were embedded and the scheme offered high payload capacity. Even for a single-layer embedding, the average PSNR of the stego images was more than 48 dB.

Qin et al. [23] proposed a novel prediction-based reversible steganographic scheme based on image inpainting. Initially the reference pixels are chosen adaptively according to the distribution characteristics of the image content. Later, by using the two selected groups of peak points and zero points, the histogram of the prediction error is shifted to embed the secret bits reversibly. Since the same reference pixels can be exploited in the extraction procedure, the embedded secret bits is extracted from the stego image correctly, and the cover image is restored losslessly.

2.4 Interpolation based schemes

A method that scales up the neighbor mean by interpolation method was proposed by Jung and Yoo [9] as a new lossless data hiding method. The method had two advantages – high performance computing and low-time complexity. Another scheme based on interpolation was suggested by Luo et al. [16] and the scheme embedded secret with almost imperceptible modifications. Recently Xian Wang et al. [35] proposed a reversible data hiding for high quality images, where the pixels are classified as non-wall pixels and wall pixels. Then the difference values between non-wall pixels, interpolation of wall pixels and their parent pixels are calculated. Then the secret data is embedded into the wall and non-wall pixels after histogram shifting. The method demonstrated to possess higher payload capacity and better image quality than the existing multi-layer embedding schemes.

2.5 Robustness based schemes

Some systems were designed to address the robustness property, where the payload capacity and imperceptibility are treated with a less concern. One such scheme that is based on patchwork theory, permutation scheme and the distribution features of pixel groups was suggested by Ni et al. [18]. The stego images generated were robust to JPEG2000/JPEG compression and did not possess salt and pepper noise. However, the payload size was only 1034 bits and picture quality did not exceed 38 dB. Another lossless, robust data hiding scheme based on moving the mathematical difference values in a block is proposed by Zeng et al. [42]. The method was resistant to inadvertent JPEG compression since the image was separated into two zones namely (i) bit-0 zone and (ii) bit-1 zone. The resulting images exhibited increased payload capacity but at the compromise of increased bit error rate and relatively poor picture quality of the output image. In [25], the authors proposed an adaptive reversible data hiding method by extending the generalised integer transform-based RDH method. They adaptively embedded additional bits into different kinds of blocks where more data are hidden in smooth blocks. The authors of [20] describe another adaptive RDH using histogram shifting and adaptive embedding. The amount of the embedded data is adaptively determined in terms of the context of each pixel. For pixels with small prediction error, the second, third and even the fourth LSBs are modified in order to embed more than one secret bit.

Qin et al., [24] proposed a RDH scheme based on exploiting modification direction (EMD). A single cover image is employed to generate two perceptually similar steganographic images. For embedding the secret information, the pixels in the first steganographic image are altered by a maximum of one gray level using the traditional EMD method, while the pixels in the second steganographic image are altered adaptively by referring to the first steganographic image.

2.6 HVS based schemes

Another important issue of concern is the imperceptible feature measure from HVS perspective. Awrangjeb and Kankanhalli [3] came out with such a reversible data hiding algorithm that embedded the message into the host image taking into account the human visual system. The stego image contained no detectable perceptible artifacts.

2.7 RDH in encrypted domain

Recently, the research on image processing over encrypted domain, principally driven by the requirements from Cloud computing platforms and various privacy preserving applications, has become more popular. Combination of reversible data hiding and encryption has also received some of the earliest attention. Liao et al. [13] proposed a novel RDH method in encrypted images that evaluates the complexity of image blocks, which considers multiple neighboring pixels according to the locations of different pixels. Furthermore, data embedding ratio is considered. Their method offers increased correctness of data extraction/image recovery. Qin et al. [22] describe a novel reversible data hiding scheme in encrypted image that flips certain pixels and secret bits can be extracted by adaptive smoothness evaluation in isophote direction.

The majority of the above methods addressed only a few of the desired characteristics namely - lossless/reversible, imperceptible, high payload capacity, robustness and minimal side information involved and not all. Motivated by these facts, in this paper, a novel reversible data hiding scheme which operates based on multiple level embedding executed in the integer wavelet transform domain is proposed. a novel reversible data hiding technique based on the multilevel histogram shifting applied on lifting integer transform domain. The proposed method has been designed in such a way that it surpasses steganalytic detection, while preserving the perceptual quality of the images. An extensive experimental evaluation of the proposed scheme vs. other existing schemes, on a database containing thousands of natural images and security tests against different kinds of steganalytic algorithms show the superiority of the new method in capacity, picture quality and undetectability.

3 Rationale for the choice of integer lifting wavelet transform

The proposed system is designed with the following objectives:

1. Lossless/reversible property – The ability to recover the host image – it is measured as the metric Bit Error Rate (BER) between extracted output image and host image and is to be zero, indicating a perfect restoration of cover image.

2. High imperceptibility– The picture quality of the stego image should be high and is measured using Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Metric (SSIM).
3. High payload capacity – The amount of secret information to be embedded should be high and is measured in terms of maximum number of bits that can be embedded inside an image.
4. High robustness - The ability of the secret payload to withstand image processing operations and steganalysis and is measured in terms of detection accuracy of the steganalyser.
5. Minimal side information – The auxiliary information needed for recovery of payload and host image is to be minimal.

To simultaneously achieve these goals, the proposed method implements the embedding in the integer lifting wavelet transform domain through difference histogram modification. Properties like lossless, imperceptibility, robustness are realized through the usage of integer lifting wavelet transform domain. More capacity and minimal side information are attributed by the multilevel histogram shifting logic.

Among the various transform domains like DCT, DFT, DWT etc., DWT is chosen owing to the following constructive reasons. Though DCT (Discrete Cosine Transform) exhibits few merits like satisfactory performance, simplicity, and readily available special hardware for its implementation, it is not suitable for data hiding applications. The input image is divided into blocks and hence it is impossible to eliminate the correlation across the block boundaries. This factor introduces annoying and noticeable “blocking artifacts”‘issue in the image. However in wavelet-based schemes achieve superior performance than DCT, DFT etc., since the input image is not handled in blocks. Moreover, the basis functions of DWT have variable length and hence the blocking artifacts issue is completely avoided.

Another major advantage of DWT over DCT is that the high-pass DCT bands provide higher frequency resolution, but with a lower spatial resolution. Hence there are more frequency bands, while it is difficult to identify the spatial information. Alternatively, the wavelet sub-bands offer higher spatial resolution, and a lower frequency resolution. Hence the number of sub-bands is few, while the spatial resolution is commendable. The high frequency coefficients are coarsely quantized, and hence the quality of the reconstructed image at the edges will exhibit poor quality during extraction. Summarily, DWT is more suitable for data hiding applications, since

1. There is no need to divide the input coding into non-overlapping 2-D blocks and hence the transform avoids blocking artifacts.
2. DWT facilitates good localization both in time and spatial frequency domain.
3. Transformation of the whole image via sub-band decomposition, introduces inherent scaling
4. Easy and better identification of which sub-band to manipulate so as to maintain a good perceptual quality
5. Higher data hiding capacity

Wavelet transform is a significant means for multi-resolution analysis, especially in image processing applications. It obviously becomes a candidate tool for data hiding operation mainly due to its excellent modeling of the HVS, ability to easily capture the edges/textured regions in an image, and a good multi-resolution feature. The projection of the image onto a set of basis functions is obtained in the transform coding of images and the resultant transform coefficients are then encoded. Wavelet transforms are efficient in the sense that they compact the entire energy of the image into a small number of coefficients.

Original digital wavelet transform is not suitable for reversible data hiding scheme since it does not guarantee reversibility property. Wavelet transform operates on a floating point arithmetic basis. An image which has integer intensity values in the spatial domain is converted into decimal wavelet coefficients. The wavelet coefficients are modified appropriately during data hiding operation and inverse wavelet transform is carried out to reconstruct the stego-image back in the spatial domain. A serious note here is that practically wavelet coefficients are truncated or rounded since it is not viable to represent the coefficients to its full accuracy. Information is lost potentially during forward and reverse transforms while reconstructing the image by inverse wavelet transform. Nevertheless reversible data hiding schemes demand recovery of the host image apart from secret payload extraction. Eventually this makes the discrete wavelet transform a poor choice for reversible data hiding. To address this specific issue, an invertible integer lifting wavelet transform is used in the proposed scheme. The system operates on integer arithmetic and alleviates the loss of any information via forward and reverse transforms.

Lifting scheme is a successful execution of the naïve wavelet filtering process and it increases the speed of wavelet decomposition. The lifting scheme produces non-separable second generation wavelets. The proposed work employs the lifting scheme on the Daubechies, Cohen and Feauveau conventional bi-orthogonal wavelet both the dual and primal wavelet [4]. For ease of understanding, the lifting scheme on one dimensional signal is provided below:

Step 1. Splitting – A simple lazy wavelet that makes an original signal $S_{0,n}$ into two smaller intersection wavelet subset $s_{l,k}^{0}$ and $d_{l,k}^{0}$ is obtained according to the parity split operation given by

$$split\left(S_{0,n}\right)=\left(s_{l,k}^{0},d_{l,k}^{0}\right) \tag{1}$$

Basically the signal S is split into even $\left(s_{l,k}^{0}\right)$ and odd $\left(d_{l,k}^{0}\right)$samples, where l,k denotes the horizontal (row) and vertical (column) direction respectively and $1\le l\le M, 1\le k\le N$, where $M\times N$ is the size of the image.

Step 2. Dual Lifting – Dual lifting is achieved by predicting the odd sequence from the adjacent even number sequence based on the dependence between the data and is done by

$$d_{l,k}^{i}=d_{l,k}^{i-1}-predict\left(s_{l,k}^{i-1}\right) \tag{2}$$

Step 3. Updating – A better child data $s_{l,k}^{i}$is found which retains some of the scale character of the original subsets $s_{l,k}^{0}$and is done as per the following equation:

$$s_{l,k}^{i}=s_{l,k}^{i-1}+predict\left(d_{l,k}^{i-1}\right) \tag{3}$$

where $s_{j,n}$ and $d_{j,n}$ are the n^{th} low-frequency and high-frequency wavelet coefficients at the j^{th} level, respectively. At $j=0$, $s_{0,n}$denotes the n^{th} pixel values itself. These steps are repeated leading to a multi-resolution decomposition. The inverse process to reconstruct the image in the spatial domain is simple and just the reverse of these steps:

$$\text{Inverse updating}: \quad is^{i}_{l,k} = \mathrm{is}^{i-1}_{l,k} - predict\left(id^{i-1}_{l,k}\right) \tag{4}$$

$$\text{Inverse dual lifting}: \quad id^{i}_{l,k} = id^{i-1}_{l,k} + predict\left(is^{i-1}_{l,k}\right) \tag{5}$$

$$\text{Merging}: \quad IS_{0,n} = merge\left(is^{0}_{l,k}, id^{0}_{l,k}\right) \tag{6}$$

4 Proposed system

The proposed scheme introduces a preliminary layer of security by a small pre-processing step. The image pixels are scanned in any one of nine different ways rather than the usually adapted only one sequential order in the pattern of 'S'. Histogram shifting is done at multiple levels over the differences of the adjacent pixels. The possibility of nine different scan patterns results in multiple ways in which the pixels are paired and differences are derived. This complicates the task of a steganalyser considerably and thus offers an additional level of security. The scan pattern is taken as stego_key_1and is shared between the communicating parties by a conventional symmetric key cryptosystem.

4.1 Scan path and embedding level

In this work, nine different scan patterns are employed. They are shown in Fig. 1. Let *C* be the given gray scale image with *M*-rows and *N*-columns and each pixel is of 8-bit depth. When this image is scanned according to any one pattern, a series of pixel values $p_1, p_2, \ldots p_{MXN}$ is formed along the scan path.

Embedding Level (EL) is another integer parameter introduced into the algorithm which helps in deciding the maximum capacity of data which could be embedded inside the given image. EL is basically the representation of the number of times, the histogram is shifted so as to accommodate the secret data. Observations infer that an optimal range of EL is between 1 and 9. The lower values indicate less secret payload while higher values indicate more secret payload capacity. A value beyond 10 introduces perceptible disruptions into the cover image and makes the visual steganalysis process very simple. Hence EL value is fixed between 1 and 9. This is treated asstego_key_2, a second shared argument between the communicating parties by the symmetric key crypto systems.

4.2 Data embedding algorithm

INPUT: Clean/Host image *C* with *M*-rows and *N*-columns, Secret payload $'w'$in bits, Scan Pattern - stego_key_1, Embedding Level EL - stego_key_2.
OUTPUT: Stego image $\hat{C}$.
Procedure

Step 1. Clean image ***C*** undergoes single level integer lifting wavelet transform which results in 4 sub-bands ***(LL, LH, HL, HH)*** of size $\frac{M}{2} \times \frac{N}{2}$, each**.**

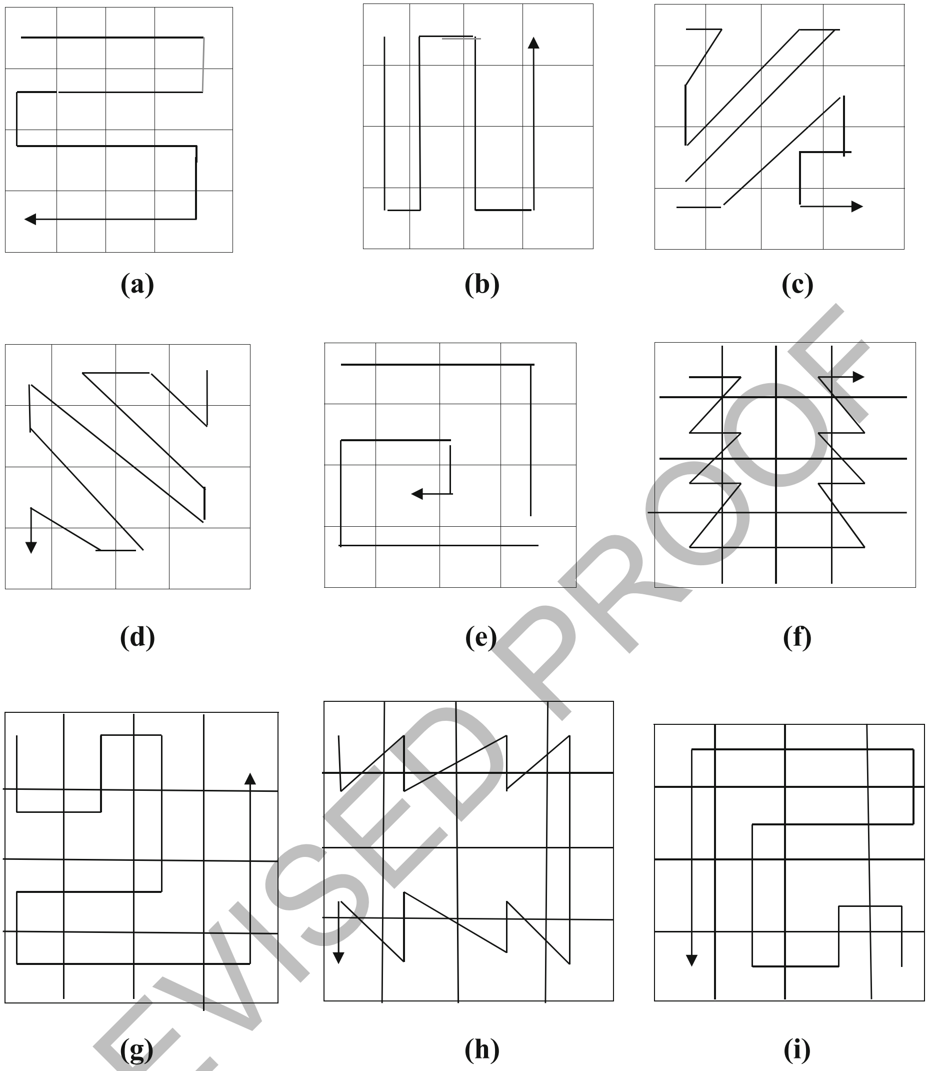


Fig. 1 Nine primitive scan patterns used for embedding (**a**) Inverse 'S' scan (**b**) Inverse 'U' scan (**c**) and (**d**) Zigzag scan (**e**) Spiral scan (**f**) – (**i**) Fractal scans

For each sub-band, do Step 2 to Step 11

Step 2. Scan the sub-band according to stego_key_1 (one of the nine patterns), ***scan*** $C\left(1\le i\le \frac{M}{2}\times\frac{N}{2}\right)$ and obtain the four, single dimensional pixel sequence p_1, p_2, . . . ,$p_{(M/2)X(N/2)}$.

Step 3. Find the pixel difference over the pixel sequence obtained in Step 2 by the formula

$$\boldsymbol{pixdiff}(\boldsymbol{i}) = \begin{cases} P_1 \ \ \boldsymbol{if} \ \boldsymbol{i} = \mathbf{1} \\ Pi{-}1 \ \ -Pi \text{ if } \ \mathbf{2} \le \boldsymbol{i} \le \dfrac{\boldsymbol{M}}{\mathbf{2}} \, \boldsymbol{X} \dfrac{\boldsymbol{N}}{\mathbf{2}} \end{cases} \tag{7}$$

Construct a histogram for the ***pixdiff*** values.

Step 4. Select embedding level (EL) which is the stego_key_2. EL should be less than 9 to avoid distortion. If EL = 0 implement the Steps 5, 6, 7 and 8, else implement from Step 6,7 and 8, skipping Step 5.

Step 5. Data embedding for EL = 0.

Step 5.1. Shift the right bins of b(0) one level rightward as:

$$pixdiff'_i = \begin{cases} p_1 & if \quad i = 1 \\ pixdiff_i & if \quad pixdiff_i \le 0, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ pixdiff_i + 1 & if \quad pixdiff_i > 0, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{8}$$

Step 5.2. Examine $pixdiff_i$=0 ($2 \le i \le \frac{M}{2} \times \frac{N}{2}$). Each difference that is 0 can be used to hold one secret bit. If the current processing secret bit w = 0, it is not altered. If w = 1, it is increased by 1. The operation is like:

$$pixdiff''_i = \begin{cases} p_{1,} & if \quad i = 1 \\ pixdiff'_i + w & if \quad pixdiff'_i = 0, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ pixdiff'_i & if \quad pixdiff'_i \ne 0, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{9}$$

Step 6. Data embedding for EL > 0.

Step 6.1. Shift the right bins of b(EL) EL + 1 levels rightward, and shift the left bins of b(−EL) EL levels leftward as:

$$pixdiff'_i = \begin{cases} p_1 & if \quad i = 1 \\ pixdiff_i & \text{if} \quad -EL \le pixdiff_i \le EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ pixdiff_i + EL + 1 & if \quad pixdiff_i > EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ pixdiff_i - EL & if \quad pixdiff_i < -EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{10}$$

Step 6.2. Examine $pixdiff'_i$=0 ($2 \le i \le \frac{M}{2} \times \frac{N}{2}$) in the range of [$-EL$, EL]. The multilevel data embedding strategy in the integer wavelet transform is described as follows.

Step 6.2.1. Embed the secret data as:

$$pixdiff''_i = \begin{cases} p^1 & if \quad i = 1 \\ pixdiff'_i & if \quad -EL < pixdiff'_i < EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ 2 \times EL + w & if \quad pixdiff'_i = EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ -2 \times EL - w + 1 & if \quad pixdiff'_i = -EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{11}$$

Step 6.2.2. EL is deducted by 1.

Step 6.2.3. If $EL \neq 0$, execute Step 5.2.1 and Step 5.2.2 repeatedly. If $EL = 0$, execute Eq. (6) and then go to Step 6:

$$pixdiff_i^{''} = \begin{cases} p_1 & if \quad i = 1 \\ pixdiff_i^{'} + w & if \quad pixdiff_i^{'} = 0, 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \\ pixdiff_i^{'} & if \quad pixdiff_i^{'} \neq 0, 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{12}$$

Step 7. Generate the marked pixels sequence $p_1^{'}, p_2^{'}, ...p_{\frac{M}{2}X\frac{N}{2}}^{'}$ as:

$$p_i^{'} = \begin{cases} p_1 & if \quad i = 1 \\ p_{i-1} - pixdiff_i^{''} & if \quad 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{13}$$

Step 8. Rearrange the pixels $p_1^{'}, p_2^{'}, ...p_{\frac{M}{2}X\frac{N}{2}}^{'}$ in the reverse order of the scan pattern decided bystego_key_1. Apply inverse integer lifting wavelet transform with the four sub-bands as input and construct the output the image $\hat{C}$ with M-rows and N-columns (Stego version of C)

4.3 Data extraction algorithm

INPUT: Stego image $\hat{C}$ with M-rows and N-columns, Scan Pattern - stego_key_1, Embedding Level EL - stego_key_2.
OUTPUT: Secret payload $'w'$in bits, Extracted version E of the host image C with M-rows and N-columns.
Procedure

Step 1. Stego image $\hat{C}$ undergoes single level integer lifting wavelet transform which results in 4 sub-bands ***(LL, LH, HL, HH)*** of size $\frac{M}{2} \times \frac{N}{2}$, each**.**

For each sub-band, do Step 2 to Step 7

Step 2. Scan the sub-band according to stego_key_1 (one of the nine patterns), ***scan*** $\left(1 \leq i \leq \frac{M}{2} \times \frac{N}{2}\right)$ and obtain the four, single dimensional pixel sequences $p^{'}_1$, $p^{'}_2$, . . . , $p^{'}_{(M/2)X(N/2)}$.

Step 3. Select embedding level (EL) - stego_key_2. If $EL = 0$ implement from Step 4 and 5 else implement Step 6 and 7.

Step 4. For $EL = 0$, the host image pixels are recovered as:

$$p_i = \begin{cases} p_1^{'} & if \quad i = 1 \\ p_i & if \quad p_{i-1} - p_i^{'} \leq 0, 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \\ p_i^{'} + 1 & if \quad p_{i-1} - p_i^{'} \geq 0, 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{14}$$

Step 5. For $EL = 0$, the secret data is extracted as:

$$w = \begin{cases} 0 & if \ \ p_{i-1} - p_i^{'} = 0, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ 1 & if \ \ p_{i-1} - p_i^{'} = 1, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{15}$$

That is, if coming across $p_{i-1} - p_i^{'} = 0$ $(2 \le i \le \frac{M}{2} \times \frac{N}{2})$, a secret bit "0" is extracted. If $p_{i-1} - p_i^{'} = 1$ $(2 \le i \le \frac{M}{2} \times \frac{N}{2})$, a "1" is extracted.

Rearrange these extracted bits to obtain the original secret sequence. After that, go to Step 8.

Step 6. For $EL > 0$, obtain the first host pixel as $p_1 = p_{1'}$

Step 6.1. The marked differences are calculated as:

$$pixdiff_i^{''} = \begin{cases} p_1^{'} & if \quad i = 1 \\ p_{i-1} - p_{\ i}^{'} & if \quad 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{16}$$

Later the original differences are computed as:

$$pixdiff_{_i}^{\ i} = \begin{cases} pixdiff_i^{''} - EL - 1 & if \quad pixdiff_i^{''} > 2 \times EL + 1, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ pixdiff_i^{''} + EL & if \quad pixdiff_i^{''} < -2 \times EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ q & if \quad pixdiff_i^{''} \in \{2 \times q, 2 \times q + 1\}, q = 0, 1, ...EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ -q & if \quad pixdiff_i^{''} \in \{-2 \times q, -2 \times q + 1\}, q = 1, ...EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{17}$$

Next the host pixel sequence is recovered as:

$$p_i = \begin{cases} p_1^{'} & \text{if} \quad i = 1 \\ p_{\ i-1}^{'} - pixdiff_i & \text{if} \quad 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{18}$$

Note Eqs. (10)–(12) are executed repeatedly, i.e., $p_i(2 \le i \le \frac{M}{2} \times \frac{N}{2})$ is recovered in advance, and then $p_i + 1$ is recovered with the aid of p_i. In other words, a sequential recovery strategy is utilized.

Step 7. For $EL > 0$, the secret data extraction is associated with $EL + 1$ rounds. First set the round index $RI = 0$.

Step 7.1. Extract the data as:

$$w_{RI} = \begin{cases} 0 \ if & pixdiff_i^{''} = 2 \times EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ 0 \ if & pixdiff_i^{''} = -2 \times EL + 1, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ 1 \ if & pixdiff_i^{''} = 2 \times EL + 1, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \\ 1 \ if & pixdiff_i^{''} = -2 \times EL, 2 \le i \le \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{19}$$

Step 7.2. *EL*is decreased by 1 and *RI* is increased by 1.

Step 7.3. If $EL \neq 0$, execute Steps 6.1 and 6.2 repeatedly. If $EL = 0$, execute:

$$w_{RI} = \begin{cases} 0 & if \quad pixdiff_i^{''} = 0, 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \\ 1 & if \quad pixdiff_i^{''} = 1, 2 \leq i \leq \frac{M}{2} \times \frac{N}{2} \end{cases} \tag{20}$$

RI is increased as $EL + 1$.

Step 7.4. Rearrange and concatenate the extracted data w_{RI} $(1 \leq RI \leq EL + 1)$ as:

$$w = cat(w_1, w_2, ...w_{EL+1}) \tag{21}$$

Thus, the hidden secret bits are extracted, and then go to Step7.

Step 8. Rearrange the pixels $p_1, p_2, ...p_{\frac{M}{2}X\frac{N}{2}}$ in the reverse order of the scan pattern decided bystego_key_1. Apply inverse integer lifting wavelet transform with the four sub-bands as input and construct the output the image E with M-rows and N-columns (Extracted version of the original cover image C)

END

4.4 Overflow and underflow prevention

The proposed scheme requires mainly three side information for extraction – (i) Scan Pattern - stego_key_1; (ii) Embedding Level EL - stego_key_2 and (iii) Location map. Since the scan pattern can be one among the nine different patterns, 4 bits are sufficient to store this value. Further, the embedding level can also be stored in 4 bits, since we do not set it beyond a value of 10. For a given large EL value, the processes of emptying the histogram bins and shifting them leads to overflow (i.e., $p_i^{'} > 255$) or underflow (i.e., $p_i^{'} < 0$). However, these extreme conditions are predictable. They are possible on the pixels with values close to 255 or 0. Consider $p_{\max}$and $p_{\min}$denote the maximum and minimum pixel values in the image Crespectively. The extreme worst case distortions that can be occurring at $p_{\max}$and $p_{\min}$can be calculated by:

$$\begin{cases} p'_{\max,} = p_{\max} + EL + 1 \\ p_{\min} = p_{\min} - EL \end{cases} \tag{22}$$

where $p^{'}_{\max}$and $p^{'}_{\min}$denote the modified pixels. There is no overflow or underflow, when $p_{\max} < 255$and $p_{\min} > 0$. In turn, EL must be assigned as:

$$EL \leq \min((254 - p_{\max}), (p_{\min})) \tag{23}$$

The EL value must not be exceeding the minimum of $(254 - p_{\max})$ and $p_{\min}$. In short, when the cover image pixel has a value in $[0, EL - 1]$, it leads to the occurrence of underflow. Similarly, if it is in the range of $[255 - EL, 255]$, it may result in overflow. In the proposed work, the EL is contained as an integer with a value of less than 10. This is primarily because when we increase EL, it triggers more overflow/underflow conditions. Then, huge number of pixels with boundary values like close to 255 or 0, becomes unfit for data embedding operation. This hinders the embedding payload capacity. Further, the size of the compressed location map also increases. Since this compressed location map is also hidden inside the cover image, its size increase reduces the room for the actual data. Though the EL value is influenced by the content of the cover image, our experimental results prove that a value less than 10 is good on the grounds of capacity, preventing overflow/underflow problem etc. We employ a location map $LM$of size same as that of the cover image i.e., $M \times N$. Before the embedding procedure, the cover image $C$is preprocessed. All the pixels that are in the range of $[0, EL-1]$ or $[255-EL, 255]$are not included for embedding. A value of '1' is recorded at these locations in the location map LMindicating the data embedding procedure to exclude them and a value of '0' is recorded, otherwise. We have a $LM$with all binary values only. Apparently, a bigger value of ELresults in more '1's and fewer 0's in it. Later, LM is subjected to lossless compression. We employed arithmetic coding for higher efficiency. The compressed location map LM_C is also hidden inside the cover image C. It is executed in a way where the cover image $C$is divided into two portions, C_1 and C_2, for embedding w and (LM_C,stego_key_1,stego_key_2), respectively. In the C_2 region, (LM_C,stego_key_1,stego_key_2) is hidden using LSB replacement strategy and these original LSBs at the embedded pixels are concatenated with w and the complete data is embedded in the C_1 region. During extraction, the reverse procedure is adapted. Based on the secret key, from the C_2 region, (LM_C,stego_key_1,stego_key_2) is extracted first. After lossless decompression of LM_c, LM is obtained. Later w is extracted using stego_key_1 and stego_key_2. The original LSB bits are recovered by removing $w$from C_1. The selected pixels in C_2 are replaced with these original LSBs, which form the latter portion of the data extracted from C_1.

5 Experimental results

Five test goals are defined for this work. The primary goal is to demonstrate that the proposed system exhibits reversible property while offering excellent payload hiding capacity. The secondary goals are to prove the efficiency of this system by exhibiting the commendable perceptual quality, good statistical un-detectability of the generated stego images and realisation of cover image reversibility with minimal side information. The following section describes the test scenario, test data sets, set-up and procedure adapted for the evaluation of these goals:

5.1 Test sets and test set-up

This section describes the set of algorithms$A$, set of test files *Test Files* and the set of experiments conducted for each of the defined test objectives focused for the evaluations.

For the evaluation of the proposed method, our cover image dataset consists of 1338 uncompressed color images with a size of 384 ×512 or 512 × 384, from UCID [26], 2000 images from [8] and NRCS image database [19] with categories like Portraits, Gardens, Architecture, Interiors, Macro, Studio, Underwater, Street photography, Aerial photography and Tourists, having a wide range of image samples. These images portrayed sufficiently diverse nature for fair evaluation with good degrees of variation in texture, color, brightness and intensity. The RGB color images are converted to grayscale before data embedding. The proposed algorithm is implemented in MATLAB version 13.b on an Intel i7 system with 4GB RAM and 1 TB hard disk.

5.2 Other RDH schemes used for comparison

Our scheme is compared with five state-of-the-art methods proposed by Kim et al.'s scheme [10], Luo et al.'s scheme [16], Tsai et al.'s scheme [31], Li et al.'s scheme [12], and Zhao et al.'s scheme [43].

From the goals stated earlier (first: perfect restoration of the cover image, second: enhanced visual quality of the stego images generated by the presented approach through assessment of appropriate image quality metrics, third: increased payload hiding capacity than other existing stego schemes by hiding more number of bits in less number of pixels, fourth: statistical undetectability of the stego images when tested against some successful steganalysers in the field and fifth: minimal side information for recovery of secret information and cover image) the following experimentations are conducted:

In our experiments, the pseudo-random bit generator function is employed to produce the secret message bits, and the peak signal to noise ratio (PSNR) according to Eqs. (24) and (25), and structural similarity (SSIM) [33, 34] has been adopted as measurements of image quality. The payload capacity is measured in terms of maximum number of bits that can be hidden.

$$\mathrm{PSNR} = 10 \text{ x } \log_{10} \frac{255^2}{\mathrm{MSE}} (\mathrm{dB}) \tag{24}$$

where the MSE is the mean squared error and is measured between the cover image C and the stego image $\hat{C}$, of size M × Nas

$$MSE = \frac{1}{M \times N} \text{ x } \sum_{i=1}^{M} \sum_{j=1}^{N} \left(C(i,j) - \hat{C}(i,j) \right)^2 \tag{25}$$

5.3 Objective 1, 2, 3 - restoration of the cover image, perceptual quality analysis and payload capacity

One of the salient characteristics of the proposed RDH scheme is that it first chooses the lifting integer wavelet transform for embedding. Since the digital image consists of integer samples as gray values, the lifting scheme maps integers to integers and that is still reversible. Hence the extraction process perfectly restores the cover image. Table 1 shows the experimental results on 15 test images comparing the maximum capacity (maximum number of bits embedded), PSNR-Peak Signal to Noise Ratio and 2 SSIM – Structural Similarity Index Measures (SSIM1 - between Cover image *C*and Stego Image C and SSIM2 - between Restored image *E*and Cover image *C*). The reported results of capacities, PSNRs and SSIMs are the averages of results of 50 executions with different random bit streams as secrets payloads.

All these results illustrate that the proposed method not only provides higher payload capacity but also an improved PSNR. In other words, the quality of stego images is still superior to those in [43] and hence could be effectively used for hiding large size files in a single image itself efficiently.

Table 1 Comparison of the maximum embedding capacities, PSNRs and SSIMs (Cover vs. Stego and Restored Cover vs. Original Cover) produced by various RDH algorithms

Cover-images (512 × 512)	Maximum Capacity (Bits)	PSNR (dB)	SSIM1 (Cover vs. Stego)	SSIM2 (Restored Cover vs Original Cover)	Maximum Capacity (Bits)	PSNR (dB)	SSIM1 (Cover vs. Stego)	SSIM2 (Restored Cover vs Original Cover)	Maximum Capacity (Bits)	PSNR (dB)	SSIM1 (Cover vs. Stego)	SSIM2 (Restored Cover vs Original Cover)
	Kim et al.'s scheme [10]				Luo et al.'s scheme [16]				Tsai et al.'s scheme [31]			
Lena	529,842	44.21	0.94	0.92	403,450	36.39	0.9	0.92	505,141	42.20	0.91	0.92
Baboon	570,299	39.91	0.73	0.93	483,516	33.37	0.75	0.92	592,362	38.56	0.75	0.93
Airplane	526,688	44.10	0.84	0.94	411,398	35.85	0.86	0.95	514,654	41.90	0.86	0.94
Clown	523,295	43.25	0.84	0.91	414,230	35.78	0.85	0.94	511,087	41.15	0.86	0.94
Peppers	522,985	43.58	0.85	0.93	405,893	36.46	0.87	0.94	510,056	42.04	0.88	0.94
Barb	537,163	41.71	0.9	0.91	444,967	34.5	0.83	0.94	557,096	39.99	0.83	0.95
Zelda	515,795	44.80	0.91	0.95	494,750	36.96	0.91	0.94	595,546	42.79	0.92	0.94
House	526,535	43.16	0.83	0.94	417,195	35.65	0.84	0.95	522,572	41.23	0.84	0.94
Lighthouse	541,633	41.61	0.82	0.94	443,291	34.61	0.8	0.94	543,881	39.82	0.81	0.91
Pent	537,056	42.08	0.8	0.94	427,290	35.25	0.81	0.94	529,245	40.43	0.81	0.91
Boats	533,566	43.33	0.83	0.94	419,282	35.40	0.84	0.94	519,720	41.23	0.85	0.94
Truck	528,632	43.41	0.84	0.96	407,352	36.26	0.86	0.93	508,352	41.58	0.86	0.94
Kiel	557,078	41.89	0.8	0.96	450,078	34.48	0.83	0.93	551,189	39.99	0.83	0.93
Houses	561,310	41.03	0.81	0.95	473,241	33.63	0.8	0.91	583,481	38.80	0.8	0.9
	Li et al.'s scheme [12]				Zhao et al.'s scheme [43]				Proposed scheme			
Lena	413,625	40.39	0.93	0.96	403,450	36.37	0.9	0.92	605,141	46.24	0.94	0.96
Baboon	409,029	36.38	0.71	0.96	483,516	33.36	0.71	0.92	692,362	44.39	0.85	0.97
Airplane	417,441	40.26	0.87	0.95	411,398	35.82	0.86	0.95	614,654	47.03	0.88	0.96
Clown	429,947	39.46	0.85	0.95	414,230	35.72	0.85	0.94	611,087	47.04	0.86	0.97
Peppers	413,213	40.71	0.83	0.94	405,893	36.40	0.87	0.94	610,056	48.65	0.88	0.96
Barb	494,601	36.92	0.86	0.94	444,967	34.55	0.83	0.94	657,096	46.67	0.93	0.98
Zelda	499,829	41.50	0.91	0.95	494,750	36.94	0.91	0.94	595,546	48.19	0.92	0.97
House	431,313	39.40	0.82	0.94	417,195	35.68	0.83	0.95	527,572	47.02	0.84	0.96
Lighthouse	464,825	38.00	0.82	0.93	443,291	34.61	0.8	0.94	543,881	46.8	0.83	0.95
Pent	443,137	38.73	0.77	0.93	427,290	35.25	0.82	0.94	539,245	46.44	0.82	0.95
Boats	424,031	39.74	0.89	0.94	419,282	35.40	0.84	0.94	619,720	47.29	0.89	0.94
Truck	409,001	41.33	0.84	0.96	407,352	36.26	0.86	0.91	608,352	47.57	0.89	0.97
Kiel	452,021	38.548	0.88	0.95	450,078	34.48	0.83	0.93	651,189	46.92	0.88	0.97
Houses	492,081	36.54	0.81	0.95	473,241	33.6253	0.8	0.91	683,481	44.833	0.82	0.96

5.4 Objective 4 - security under steganalysis systems

RS analysis The security of the proposed method against the famous RS-analysis technique [5] is evaluated. RS-analysis describes a differentiating function *DF*and a corresponding flipping mask *M*. R_M denotes the proportion of blocks where the magnitude of *DF* increases while applying DF_1 to a part of each block, and S_M denotes the proportion of blocks where the magnitude of *DF*decreases. Similarly, there are two other parameters namely$R_{-M}$and S_{-M}which are defined when $DF_{-1}$is executed to a part of each block. If the test image has no embedded secret data, then the state $R_M \approx R_{-M} > S_M \approx S_{-M}$ is true. Statistically, if the image has no embedded secret data, then F_1 and F_{-1}equally increase the magnitudes of fluctuation, thereby leading to the state of $R_M \approx R_{-M} > S_M \approx S_{-M}$. When the test image is a stego image, the difference between $R_M$and $S_M$declines whereas the difference between $R_{-M}$and S_{-M}rises because the data embedding and the DF_1operation neutralize each other. Hence these four parameters can be compared to detect the presence of embedded data. The RS analysis was observed to be ineffective over the proposed RDH stego images.

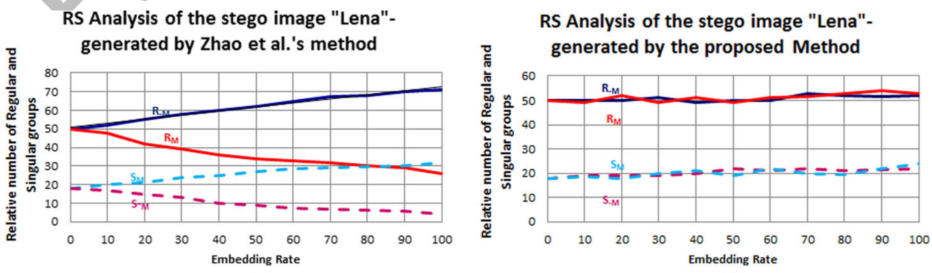
This could be verified from the Fig. 2 which shows the RS analysis results for two stego-images generated using the Zhao et al.'s method and the proposed method respectively with $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ as M and −M . Since the Zhao et al.'s method operates in the spatial domain, the visual artifacts introduced by embedding process are reflected in the corresponding RS diagram. It is observed that the Zhao et al.'s method of embedding causes R_M and R_{-M} as well as S_M and S_{-M} to separate with an increasing payload, providing a clear signature of the hidden information, whereas the proposed technique is shown to be secure under the RS analysis.

Moreover, the RS detection values $((|R_M - R_{-M}| + |S_M - S_{-M}|)/(R_M + S_M))$ for a randomly chosen 500 cover images and the respective stego images generated by the proposed RDH method are shown in Fig. 3. The RS difference values appear to be close to 0 for the cover and the stego images of the proposed system, whereas those of other methods were very much higher than 0. The proposed method is therefore well secure against RS-analysis, in common with other RDH methods.

5.4.1 Specific steganalysis- histogram based steganalysis schemes

1) *Zhihua Xia et al. [38]:*

The 20 features that characterize the difference histogram characteristic function's center of mass (DHCF COM) of the test images are extracted which can effectively



(a) (b)

Fig. 2 RS analysis for the stego image -"Lena" at various embedding rates. **a** RS analysis curve of Zhao et al.'s stego image. **b** RS analysis curve of the proposed method stego image

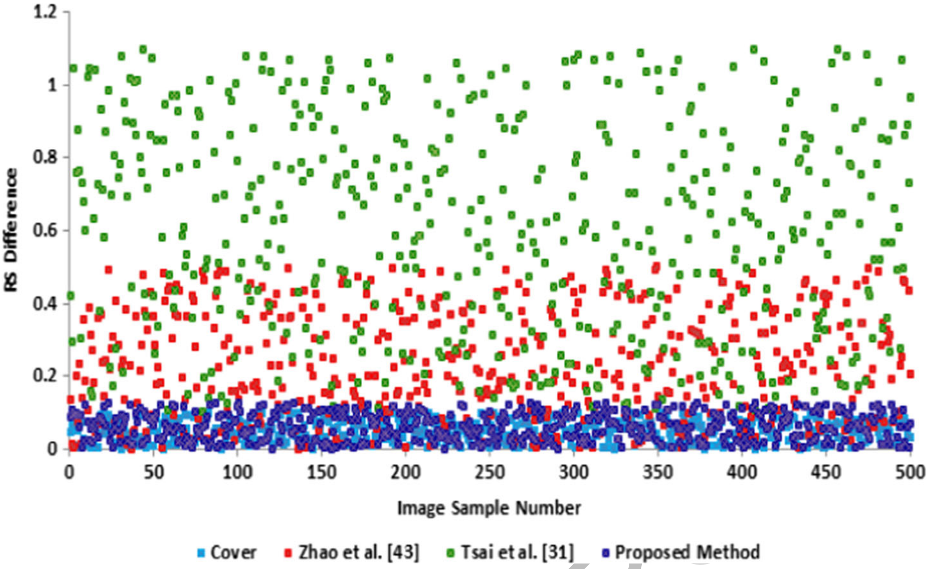


Fig. 3 RS detection values of the cover images, stego images using the Zhao et al. method [43], Tsai et al. method [31] and the proposed method for 500 randomly chosen images

reveal the presence of pixel pairs with different distances leading to stego anomalies. The calibrated features after averaging operation are given to SVM classifier model for effective steganalysis.

2) *Zhihua Xia et al. [37]:*

The low-order differences of image pixels are calculated which reflect the smoothness caused by reversible data hiding operation at the peak of the difference histograms. Features from the respective co-occurrence matrix are extracted from the test image to reveal the differences in the small absolute value. The features are extracted from the image and the pixel difference histograms. SVM classifier is employed for classification.

The detection accuracy curves are shown in Fig. 4. It can be noted that both of these specific steganalytic systems are ineffective in detecting the stego images generated by the proposed system (still getting closer only to random guessing) even though the embedding rate

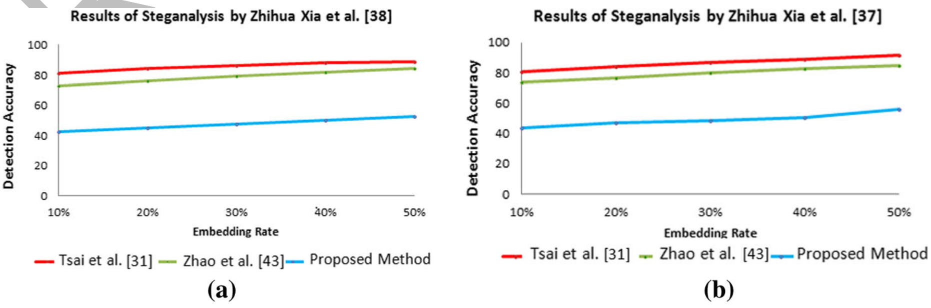


Fig. 4 Detection accuracy curves of Zhao et al. method [43], Tsai et al. method [31] and the proposed method, by the specific steganalysis systems at various embedding rates by Zhihua Xia et al. (**a**) DHCF COM features [38] (**b**) low order difference co-occurrence matrix features [37]

is 50%. However the other RDH schemes are detected by these systems effectively. Existing RDH methods introduced modifications which resulted in stepping artifacts, fluctuations, and uncharacteristic rises. Nevertheless, the proposed method possessed the smallest value in statistical terms among all the RDH steganographic methods of this nature.

5.4.2 Universal steganalysis

In this subsection, the proposed reversible data hiding method is subjected to undetectability using the four successful universal steganalytic methods. The results are compared with the other six RDH schemes, including two typical LSB based and four transform-based schemes.

1) **Tang et al.** [28] The system assigns different weights to different pixels in feature extraction process with the basic knowledge that all the pixels do not contribute equally to the steganalysis process. The pixels with high embedding probabilities are assigned larger weights since they contribute more to steganalysis and vice versa. Residual images are obtained by applying various filters and for each residual image horizontal and vertical co-occurrence matrix is calculated by assigning varying weights to each pixel according to the embedding probabilities. Finally all the features are combined to form the 34,671-D feature vector, which basically represents the spatial rich model for steganalysis.
2) **Abdul Rahman et al.** [1]**:** The approach applies steerable Gaussian filters angled in various directions to accurately calculate the tangent of the gradient vector and estimates the 2808 features from gradient magnitude and 1598 features from the derivative of this tangent direction. Later it computes the co-occurrence of pixel pairs in all the eight directions. All features are collectively put together to form the 22,563-D feature vector.
3) **Liu et al.** [15]**:** The method forms a 63-D feature vector derived from the neighboring joint density of the DCT coefficients by exploring the self-calibration under various shift recompressions, so as to reveal the difference between untouched image and the stego image.
4) **Pevný et al.** [21]**:** This approach models the differences between adjacent pixels using first-order and second-order Markov chains. Since more clues are obtained from higher order statistics, we used 686 s-order features for steganalysis process, ignoring the first-order features.

To evaluate the security of the proposed RDH method, 300 images are randomly selected from the entire image dataset. To this dataset, stego images generated using the proposed RDH method and six other RDH schemes, with different payloads ranging from 10% to 50%, are added. Steganalysis by each approach is executed on the image database. SVM classifier is used for classification, since it is reported in all the steganalysis works. Table 2 summarises the detection accuracy obtained by averaging the results of ten-fold cross-validation experimentation. It can be noted that the proposed RDH scheme is able to survive/bypass many steganalytic systems better than the other RDH schemes nearly at all the payload capacities. The results are remarkably good at payload capacity less than 30%. For instance, at 20% payload capacity, the maximum detection rate obtained was only 57.33%, which is more like a random guessing. At high payload capacities like 50%, the detection rate is 74.01%. This may be due to the fact that the pixel differences is subtle in these levels and hence they are unable to carry more payload in these levels and naturally the EL drops to a lower value thus revealing more clues to the steganalysers.

However, by a clever choice of the cover image, this issue can be solved. The steganographer can intelligently choose an image with more variations, since they offer good adjacent pixel differences, as the cover image.

Table 2 Comparison of the average detection accuracy (%) of each feature set with SVM at different payload capacities

Payload capacity	Steganographic algorithms	Weixuan Tang - 34,671-D	Hasan Abdul Rahman 22,563-D	Qingzhong Liu 63-D	Tomáš Pevný 686-D	Max. accuracy
10%	Kim et al. [10]	70.2	68.1	54.71	66.71	70.2
	Luo et al. [16]	69.6	57.88	52.33	58.1	69.6
	Tsai et al. [31]	83.97	80.61	71.66	78.22	83.97
	Li et al. [12]	64.46	63.22	53.4	58.3	64.46
	Zhao et al. [43]	81.25	76.11	61.11	69.88	81.25
	Proposed Method	54.8	52.35	44.75	50.9	54.8
20%	Kim et al. [10]	72.2	71.55	58.9	68.5	72.2
	Luo et al. [16]	71.1	60.35	56.5	60.33	71.1
	Tsai et al. [31]	85.66	82.33	74.01	79.25	85.66
	Li et al. [12]	67.33	66.6	57.5	61.33	67.33
	Zhao et al. [43]	83.45	77.2	64.21	71.5	83.45
	Proposed Method	57.33	55.6	49.5	52.25	57.33
30%	Kim et al. [10]	78.66	77.81	66.2	69.5	78.66
	Luo et al. [16]	77.35	67.66	80.8	60.1	80.8
	Tsai et al. [31]	90.6	86.65	78.2	83.33	90.6
	Li et al. [12]	87.66	85.11	77.33	82.5	87.66
	Zhao et al. [43]	87.26	80.03	69.5	74.12	87.26
	Proposed Method	60.33	58.48	55.33	57.5	60.33
40%	Kim et al. [10]	81.68	79.33	69.2	74.66	81.68
	Luo et al. [16]	80.66	73.01	82.1	63.22	82.1
	Tsai et al. [31]	91.45	88.9	79.01	85.76	91.45
	Li et al. [12]	89.33	87.22	79.22	84.33	89.33
	Zhao et al. [43]	90.5	83.35	71.1	79.5	90.5
	Proposed Method	62.6	60.88	57.31	59.33	62.6
50%	Kim et al. [10]	84.33	81.33	71.2	77.5	84.33
	Luo et al. [16]	84.9	75.25	86.33	66.22	86.33
	Tsai et al. [31]	92.5	90.13	83.6	88.5	92.5
	Li et al. [12]	91.97	89.33	80.2	86.26	91.97
	Zhao et al. [43]	92.7	85.12	76.02	81.33	92.7
	Proposed Method	74.01	72.26	70.2	72.55	74.01

5.5 Objective 5 – minimal side information

The proposed scheme requires space for (i) Scan Pattern - stego_key_1 (4-bits); (ii) Embedding Level EL - stego_key_2, (4-bits) (iii) Compressed location map LM_C. This is a minimal information when compared to the picture quality, embedding capacity and robustness offered by the proposed method. The size of the $LM_C$is greatly influenced by the cover image, EL value and compression algorithm chosen.

6 Conclusion

There has been a rapid growth of interest in reversible data hiding schemes recently because of its wide range of applications. RDH finds its applications in, but not limited to, the following areas: hiding huge data like Electronic Patient Records (EPR), authentication information, annotation or tag information of the patients inside the respective medical image. The system can be well utilised to store the images securely on a semi trusted cloud server, secret communication, and media database systems. In this paper a novel, RDH method is proposed that is based on lifting integer wavelet transform scheme for embedding. Extensive empirical study is carried out to investigate the efficiency and reliability of the proposed system.

The major findings evolved are summarized as follows:

1) The payload capacity offered by the proposed system is exceptionally enhanced, with minimum distortion in the perceptual quality of the stego images. Multi-level embedding possible with the proposed system offers this high payload capacity.
2) The stego images possessed competent visual quality even at considerably high embedding rates. The stego images sustained a very close pattern as that of the cover image. Embedding operation done in the integer wavelet domain facilitated the remarkable picture quality of the stego images. An adaptive embedding level also minimized, the stepping effects and other artifacts arising out of stego noise injection, profoundly.
3) The proposed method proved to be statistically undetectable by many promising steganalytic systems like RS steganalysis, histogram based steganalysers, and universal steganalysers. Choice of the scan pattern that produced the least distortion and maximum security, along with the prevention of overflow/underflow problem provided the robustness property as well as restoration of cover image.
4) The proposed system is tested on a massive image database comprised of diverse natural image samples. Stego images are generated at varying embedding rates ranging from 10% - 50%. The performance of the proposed system proved to be superior when compared against five other state-of-the-art RDH schemes for payload capacity, visual quality and statistical undetectability. This diversity makes our system more appropriate to real applications.

Acknowledgements This paper is based upon work supported by the All India Council for Technical Education - Research Promotion Scheme under Grant No. 20/AICTE/RIFD/RPS(POLICY-II)65/2012-13.

References

1. Abdulrahman H, Chaumont M, Montesinos P, and Magnier B (2016) "Color image Steganalysis based on Steerable Gaussian filters bank," Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security - IH&MMSec ‘16, 109–114
2. Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156
3. Awrangjeb M (2005) Reversible watermarking using a perceptual model. Journal of Electronic Imaging 14(1):013014
4. Cohen A, Daubechies I, Feauveau J-C (1992) Biorthogonal bases of compactly supported wavelets. Communications of Pure Applied Mathematics 45(1):485–560
5. Fridrich J, Goljan M, Du R (2001) Detecting LSB steganography in color, and gray-scale images. IEEE Multimedia 8(4):22–28
6. Hsiao J-Y, Chan K-F, Morris Chang J (2009) Block-based reversible data embedding. Signal Process 89(4): 556–569
7. Hu Y, Lee H-K, Li J (2009) DE-based reversible data hiding with improved overflow location map. IEEE Transactions on Circuits and Systems for Video Technology 19(2):250–260
8. Images were obtained from: http://philip.greenspun.com/
9. Jung K-H, Yoo K-Y (2009) Data hiding method using image interpolation. Computer Standards & Interfaces 31(2):465–470
10. Kim K-S, Lee M-J, Lee H-Y (2009) Reversible data hiding exploiting spatial correlation between sub-sampled images. Pattern Recogn 42(11):3083–3096

11. Lee S, Yoo CD, Kalker T (2007) Reversible image Watermarking based on integer-to-integer Wavelet transform. IEEE Transactions on Information Forensics and Security 2(3):321–330
12. Li X, Zhang W, Gui X, Yang B (2015) Efficient reversible data hiding based on multiple histograms modification. IEEE Transactions on Information Forensics and Security 10(9):2016–2027
13. Liao X, Shu C (2015) Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J Vis Commun Image Represent 28:21–27
14. Lin C-C, Tai W-L, Chang C-C (2008) Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn 41(12):3582–3591
15. Liu Q, Chen Z (2014) Improved approaches with calibrated neighboring joint density to Steganalysis and seam-carved forgery detection in JPEG images. ACM Trans Intell Syst Technol 5(4):1–30
16. Luo L, Chen Z, Chen M, Zeng X, Xiong Z (2010) Reversible image watermarking using interpolation technique. IEEE Transactions on Information Forensics and Security 5(1):187–193
17. Ni Z, Shi Y-Q, Ansari N, Su W (2006) Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology 16(3):354–362
18. Ni Z, Shi YQ, Ansari N, Su W, Sun Q, Lin X (2008) Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Transactions on Circuits and Systems for Video Technology 18(4):497–509
19. NRCS Photo Gallery Home, http://photogallery.nrcs.usda/ .gov/
20. Pei Q, Wang X, Li Y, Li H (2013) Adaptive reversible watermarking with improved embedding capacity. J Syst Softw 86(11):2841–2848
21. Pevny T, Bas P, Fridrich J (2010) Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on Information Forensics and Security 5(2):215–224
22. Qin C, Zhang X (2015) Effective reversible data hiding in encrypted image with privacy protection for image content. J Vis Commun Image Represent 31:154–164
23. Qin C, Chang C-C, Huang Y-H, Liao L-T (2013) An Inpainting-assisted reversible Steganographic scheme using a histogram shifting mechanism. IEEE Transactions on Circuits and Systems for Video Technology 23(7):1109–1118
24. Qin C, Chang C-C, Hsu T-J (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimedia Tools and Applications 74(15):5861–5872
25. Qiu Y, Qian Z, Yu L (2016) Adaptive reversible data hiding by extending the generalized integer transformation. IEEE Signal Processing Letters 23(1):130–134
26. Schaefer G, Stich M (2003) UCID: An uncompressed color image database. Proc SPIE Electronic Imaging, Storage and Retrieval Methods and Applications for Multimedia 5307:472–480
27. Tai W-L, Yeh C-M, Chang C-C (2009) Reversible data hiding based on histogram modification of pixel differences. IEEE Transactions on Circuits and Systems for Video Technology 19(6):906–910
28. Tang W, Li H, Luo W, Huang J (2015) Adaptive Steganalysis based on embedding probabilities of pixels. IEEE Transactions on Information Forensics and Security 11(4):734–745
29. Thodi DM, and Rodríguez JJ (2004) "Prediction-error based reversible watermarking", Proceedings of International Conference on Image Processing (ICIP '04), vol. 3, 1549–1552
30. Tian J (2003) Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology 13(8):890–896
31. Tsai P, Hu Y-C, Yeh H-L (2009) Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process 89(6):1129–1143
32. Tseng H-W, Hsieh C-P (2009) Prediction-based reversible data hiding. Inf Sci 179(14):2460–2469
33. Wang Z, Bovik AC (2002) A universal image quality index. IEEE Signal Processing Letters 9(3):81–84
34. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
35. Wang X, Pei Q, Li Y, Li H (2013) Adaptive reversible watermarking with improved embedding capacity. J Syst Softw 86(11):2841–2848
36. Weng S, Zhao Y, Pan J-S, Ni R (2007) A novel high-capacity reversible water-marking scheme. In: IEEE International conference on multimedia and expo (ICME '07). IEEE, Beijing, pp 631–634
37. Xia Z, Wang X, Sun X, Wang B (2014) Steganalysis of least significant bit matching using multi-order differences. Security and Communication Networks 7(8):1283–1291
38. Xia Z, Wang X, Sun X, Liu Q, Xiong N (2016) Steganalysis of LSB matching using differences between nonadjacent pixels. Multimedia Tools and Applications 75(4):1947–1962
39. Yang C-Y, Lin C-H (2012) High-quality and robust reversible data hiding by coefficient shifting algorithm. ETRI J 34(3):429–438
40. Yang C, Tsai M (2010) Improving histogram-based reversible data hiding by interleaving predictions. IET Image Process 4(4):223
41. Yang B, Schmucker M, Niu X, Busch C, and S. Sun (2004) "Reversible image watermarking by histogram modification for integer DCT coefficients", Proceedings of the 6th Workshop on Multimedia Signal Processing (MMSP '04), 143–146

42. Zeng X-T, Ping L-D, Pan X-Z (2010) A lossless robust data hiding scheme. Pattern Recogn 43(4):1656–1667
43. Zhao Z, Luo H, Lu Z-M, Pan J-S (2011) Reversible data hiding based on multilevel histogram modification and sequential recovery. AEU - International Journal of Electronics and Communications 65(10):814–826

Dr. S. Subburam received Ph.D. in Computer Science and Engineering from the Satyabama University. He received the Master Degree in Computer Science & Engineering from the Madurai Kamaraj University. He has over 20 years' of experience in various institutions and Industry. Currently working as Professor in Department of Computer Science & Engineering at Prince Shri Venkateshwara Padmavathy Engineering College. His teaching and research interests includes Software Engineering, Wireless Networks, Data Base Systems, Multicore Architecture and Programming & Cloud Computing. He has organized various seminars, conferences and workshops. He is a Member of ISTE.

Dr. S. Selvakumar received Doctor of Philosophy in Computer Science and Engineering from the Anna University, Chennai. He received the Master Degree in Computer Science & Engineering from the Madurai Kamaraj University. He has over 20 years experience in various institutions. Currently he is a Professor in Department of Computer Science & Engineering, GKM College of Engineering & Technology. His teaching and research interests includes Software Engineering, Software Testing, Data Mining and Data Analytics. He has carried out various AICTE sponsored Short Term Programs and worked on various Projects. He is a Senior Member in the Computer Society of India, Member in IEEE, ACM, the Institution of Engineers and the ISTE. He has published over 50 papers in various International Journals and Conferences.

Dr. S. Geetha received the B.E., and M.E., degrees in Computer Science and Engineering in 2000 and 2004, respectively, from the Madurai Kamaraj University and Anna University of Chennai, India. She obtained her Ph.D. Degree from Anna University in 2011. She has rich teaching and research experience of 15+ years. She has published more than 60 papers in reputed International Conferences and refereed Journals. She joins the review committee for IEEE Transactions on Information Forensics and Security and IEEE Transactions on Image Processing. Her research interests include steganography, steganalysis, multimedia security, intrusion detection systems, machine learning paradigms and information forensics. She is a recipient of University Rank and Academic Topper Award in B.E. and M.E. in 2000 and 2004 respectively. She is also the proud recipient of ASDF Best Academic Researcher Award 2013 and ASDF Best Professor Awards 2014.