Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 684824, 11 pages
http://dx.doi.org/10.1155/2015/684824

Research Article

An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach

Avinash K. Gulve[1] and Madhuri S. Joshi[2]

[1]*Government College of Engineering, Aurangabad, Maharashtra 431 005, India*
[2]*Jawaharlal Nehru College of Engineering, Aurangabad, Maharashtra 431 005, India*

Correspondence should be addressed to Avinash K. Gulve; akgulve@geca.ac.in

Received 12 November 2014; Accepted 23 December 2014

Academic Editor: Gen Qi Xu

The image steganography systems use either the spatial domain or the frequency domain to hide the secret information. The proposed technique uses spatial domain technique to hide secret information in the frequency domain. The cover image is transformed using integer wavelet transform to obtain four subbands: LL, LH, HL, and HH. Then, the PVD approach is used to hide the secret information in the wavelet coefficients of all the four subbands. For improving the security of the hidden information, the proposed method first modifies the difference between two wavelet coefficients of a pair and then uses the modified difference to hide the information. This makes extraction of secret data from the stego image difficult even if the steganography method fails. The result shows that the proposed technique outperforms other PVD based techniques in terms of security of secret information and hiding capacity of cover image.

1. Introduction

Now a day, it is easy to share the information which is in the form of text, image, audio, or video using the Internet as the communication channel. Since Internet is an open channel of communication, there is always a threat of stealing the information. Therefore, it is becoming more important to adopt security measures so that the information can be protected from being stolen by malicious user. The security measures include cryptography, steganography, and coding. Steganography involves hiding secret information in a multimedia object such as image, audio, or video in such a way that its existence in these documents cannot be noticed. Digital images are preferred for hiding the secret information. It is relatively easy to place information in digital images because of the availability of sufficient redundant area where valuable information could be placed in an imperceptive way. It is possible to use images, either in the spatial domain or in the frequency domain, to hide secret information. In the spatial domain, the pixel values are used for hiding the secret information and, in the frequency domain, the wavelet coefficients are used for hiding the secret information.

The organization of the paper is as follows. A review of necessary background of IWT and PVD based steganography is presented in this section. In Section 2, the proposed method is discussed. In Section 3, the results are discussed while the paper is concluded in Section 4.

In the PVD method, as suggested by Wu et al. [1, 2], a gray-valued cover image is partitioned into nonoverlapping blocks composed with two consecutive pixels, P_i and P_{i+1}. For each block, difference value d_i is calculated by subtracting P_i from P_{i+1}. Since the pixel value ranges from 0 to 255, the difference value also ranges from −255 to 255. Therefore, $|d_i|$ ranges from 0 to 255. The block is in smooth area if the difference value $|d_i|$ is small; otherwise, it is in sharply edged area. A range table R is designed with n contiguous ranges (R_k where $k = 1, 2, 3, \ldots, n$) and the table range is from 0 to 255. The lower and upper boundaries of R_k are denoted by l_k and u_k, respectively. Hence, $R_k \in [l_k, u_k]$. The width W_k of R_k is calculated as $W_k = u_k - l_k + 1$. This width W_k is used to estimate

the number of bits t_i (where $t_i = \log_2 W_k$) of secret message that can be hidden using the difference of two consecutive pixels. After hiding t_i bits using the difference d_i, new values are assigned to P_i and P_{i+1}. The new difference d_i' is calculated by subtracting P_i from P_{i+1}. The new difference d_i' stands for the secret data hidden in the pair. During extraction, the stego image is partitioned into nonoverlapping blocks composed with two consecutive pixels, P_i and P_{i+1}. Then, the difference value d_i' for each pair of two consecutive pixels P_i and P_{i+1} is calculated. Next, $|d_i'|$ is used to locate the suitable range R_k. The decimal equivalent of the secret information hidden in the block is given by $|d_i'| - l_k$ which is then transformed into a binary sequence with t_i bits.

In order to improve the capacity of hiding secret data and to provide an imperceptible stego image quality, a novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented by Wu et al. [2]. The range table is divided into lower level (smooth area) and higher level (edged area). In the smooth area, 6 bits of the secret data is hidden by LSB method while, in the higher level, secret data is hidden using the PVD method.

To improve the hiding capacity of the cover image and quality of the stego image, another enhanced method is introduced based on the PVD method by Chang et al. [3, 5, 6]. In this method, data is hidden in vertical and diagonal edges along with the horizontal edges. The cover image is divided into the blocks of 2×2 pixels. Considering x and y to be the pixel locations, each 2×2 block includes four pixels $P_{(x,y)}$, $P_{(x+1,y)}$, $P_{(x,y+1)}$, and $P_{(x+1,y+1)}$. Pixel $P_{(x,y)}$ is grouped with the remaining three pixels in the block to form three pixel pairs. These three pairs are named PP_0, PP_1, and PP_2 where $PP_0 = (P_{(x,y)}, P_{(x+1,y)})$, $PP_1 = (P_{(x,y)}, P_{(x,y+1)})$, and $PP_2 = (P_{(x,y)}, P_{(x+1,y+1)})$, respectively. After embedding the secret information in each pair using PVD approach, values of two pixels in each pair get modified. Thus, the original difference value d_i is modified to a new difference value d_i'. The new pixel values in each pair are different from their original ones. That is, three different values are obtained for the pixel $P_{(x,y)}$. However, pixel $P_{(x,y)}$ can have only one value. Therefore, one of the PP_i' is selected as the reference pair to offset the remaining two pixel values. That is, two pixel values of the reference pair are used to adjust the pixel values of other two pairs and construct a new 2×2 block. The embedded secret data is unaffected because new difference values, d_i', are unaltered. During extraction, the difference value d_i' is used to extract the hidden information. $|d_i'|$ is used to locate the suitable range R_k. The decimal equivalent of the secret information hidden in the pair is given by $|d_i'| - l_k$ which is then transformed into a binary sequence with t_i bits.

Gulve and Joshi [4] have proposed a steganography method to improve the security of the secret information using five-pixel pair differencing approach. The cover image is partitioned into blocks of 2×3 pixels to form five pixel pairs. The secret data is embedded in the pairs using the difference value of pixels in that pair. Instead of hiding M bits in the pair using the difference value, bits $\leq N$ are hidden in the pair where N is the average of bits that can be hidden in each pair of the block. Thus, in case of failure of the steganography system, it becomes difficult to estimate exact number of bits hidden in each pair of the block. Another level of security for the secret information is introduced by converting the secret information in its gray code form. For each pair in the block, the method converts bits of secret information in the gray code form and then embeds these bits in that pair. Thus, the security of the secret information is improved without involving the overhead of encryption and decryption. Gulve and Joshi [7] have proposed a steganography method to improve the security of the secret data embedded in the image. The cover image is divided in the blocks of 2×3 pixels to form five pairs. The location of the common pixel is decided using the image data. For this reason, data of last few rows are used. Since the common pixel is changed randomly based on the image data, it is difficult to extract the secret data from stego image even if the steganography method fails.

Integer wavelet transform maps an integer data set into another integer data set. Calderbank et al. [8] have explained the working of integer wavelet transform. Haar wavelet transform, in its unnormalized version involving pair wise averages and differences, is written as

$$S_{1,n} = \frac{S_{0,2n} + S_{0,2n+1}}{2} \qquad d_{1,n} = S_{0,2n+1} - S_{0,2n}. \tag{1}$$

Its inverse is given by

$$S_{0,2n} = S_{1,n} + \frac{d_{1,n}}{2} \qquad S_{0,2n+1} = S_{1,n} - \frac{d_{1,n}}{2}. \tag{2}$$

Because of division by two, this is not integer transform. The integer version can be built by omitting division by two in $S_{1,n}$ and calculating the sum instead of the average. This is called S transform [8]. Consider the following example:

$$S_{1,n} = \left\lfloor \frac{(S_{0,2n} + S_{0,2n+1})}{2} \right\rfloor \qquad d_{1,n} = S_{0,2n+1} - S_{0,2n}. \tag{3}$$

It is possible to define $S_{1,n}$ as above because the sum and difference of two integers are either even or odd. Thus, it is safe to omit last bit of sum since it is similar to last bit of difference. The S transform [8] is invertible and it is given by

$$S_{0,2n} = S_{1,n} - \left\lfloor \frac{d_{1,n}}{2} \right\rfloor \qquad S_{0,2n+1} = S_{1,n} + \left\lfloor \frac{(d_{1,n} + 1)}{2} \right\rfloor. \tag{4}$$

A different way of writing Haar transform using "lifting" steps leads to natural generalizations. It is possible to write Haar and S transform using lifting schemes [8].

First, compute the difference and, then, use the difference in second step to compute the average:

$$d_{1,n} = S_{0,2n+1} - S_{0,2n} \qquad S_{1,n} = S_{0,2n} + \frac{d_{1,n}}{2}. \tag{5}$$

The inverse transform can be calculated in two steps. First, recover the even samples from the average and difference, and recover the odd samples from even and difference [8]. It is given by the following equations:

$$S_{0,2n} = S_{1,n} - \frac{d_{1,n}}{2} \qquad S_{0,2n+1} = d_{1,n} + S_{0,2n}. \tag{6}$$

It is possible to write integer transform by truncating the division:

$$d_{1,n} = S_{0,2n+1} - S_{0,2n} \qquad S_{1,n} = S_{0,2n} + \left\lfloor \frac{d_{1,n}}{2} \right\rfloor. \tag{7}$$

Lifting can be used to compute the inverse transform. The equations follow from reversing the order and changing the sign of the forward transform [8]:

$$S_{0,2n} = S_{1,n} - \left\lfloor \frac{d_{1,n}}{2} \right\rfloor \qquad S_{0,2n+1} = d_{1,n} + S_{0,2n}. \tag{8}$$

Ramalingam et al. [9] have elaborated the process of separating four subbands using Haar IWT. The first stage IWT is given by

$$\begin{aligned} \mathrm{H} &= C_o - C_e, \\ \mathrm{L} &= C_e + \left\lfloor \frac{\mathrm{H}}{2} \right\rfloor, \end{aligned} \tag{9}$$

where C_o represents pixels in odd column and C_e represents pixels in even column. In the next stage, the IWT coefficients are calculated using high pass and low pass filter banks. This process creates four subbands: low-low (LL), low-high (LH), high-low (HL), and high-high (HH). The second stage IWT is given by

$$\begin{aligned} \mathrm{LH} &= \mathrm{L}_{\mathrm{odd}} - \mathrm{L}_{\mathrm{even}}, \\ \mathrm{LL} &= \mathrm{L}_{\mathrm{even}} + \left\lfloor \frac{\mathrm{LH}}{2} \right\rfloor, \\ \mathrm{HH} &= \mathrm{H}_{\mathrm{odd}} - \mathrm{H}_{\mathrm{even}}, \\ \mathrm{HH} &= \mathrm{H}_{\mathrm{even}} + \left\lfloor \frac{\mathrm{HL}}{2} \right\rfloor, \end{aligned} \tag{10}$$

where $\mathrm{H}_{\mathrm{odd}}$ represents H band's odd row, $\mathrm{L}_{\mathrm{odd}}$ represents L band's odd row, $\mathrm{H}_{\mathrm{even}}$ represents H band's even row, and $\mathrm{L}_{\mathrm{even}}$ represents L band's even row [9].

Ghasemi et al. [10, 11] have proposed a novel steganography scheme based on integer wavelet transform and genetic algorithm. The scheme embeds data in integer wavelet transform coefficients by using a mapping function based on genetic algorithm. The methods use wavelet transform coefficients to embed secret data into the four subbands of two-dimensional wavelet transform. Genetic algorithm is used to find the mapping function. A chromosome is encoded as an array of 64 genes containing permutations 1 to 64 that point to pixel numbers in each block. OPAP is used to minimize the error between cover and stego image.

Xuan et al. [12] have suggested a lossless data hiding method for digital images using integer wavelet transform and threshold embedding technique. CDF (2.2) integer wavelet transform is used to obtain the wavelet coefficients. Histogram modification is applied to prevent possible underflow/overflow of pixel values. A predefined threshold value T is used to embed data in the wavelet coefficients.

El Safy et al. [13] have suggested an adaptive steganographic model which combines adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. Histogram modification is applied to prevent possible underflow/overflow of pixel values. The cover image is divided into 8×8 nonoverlapping blocks. Each block is transformed using 2D Haar integer wavelet transform to obtain four subbands: LLI, LHI, HLI, and HHI. Hiding capacity of each coefficient is determined and the data is embedded in the coefficients. A pseudorandom number generation function is used to select the wavelet coefficients for increasing the security of the hidden data. The OPA algorithm is applied after embedding secret message to minimize the embedding error. The extraction procedure is a blind process since it requires only the secret key from the receiver. The secret key is used to identify the wavelet coefficients. Secret message bits are extracted from each selected wavelet coefficient.

Archana et al. [14] have proposed a method for hiding secret information in the discrete wavelet transform coefficients using GA and OPAP algorithm to provide optimum hiding capacity. The four subbands LL, HL, LH, and HH are used for hiding the data. Hiding capacity function is modified by using different ranges for k for the LH, HL, and HH subbands where its values range from 1 to 4. The length L of message bits to be hidden in wavelet coefficient is determined by using hiding capacity function.

Al-Asmari et al. [15] have proposed a method using discrete wavelet transform and pixel value differencing approach to hide the information. Using the discrete wavelet transform, the cover image is decomposed to obtain the four subbands (LL, HL, LH, and HH). Then, the LSB method is used to hide secret information in the LL subband by hiding two bits of secret information in each coefficient. The PVD approach is used to hide the information in the remaining three subbands. For hiding the information, two consecutive pixels in the vertical direction are grouped to form a pair. The method gives high performance in terms of capacity, human visual quality, and PSNR.

2. Proposed Method

The proposed method hides secret information in the gray scale images. It uses spatial domain technique to hide secret information in the frequency domain. In the frequency domain, the image is decomposed into four subbands using integer wavelet transform and then the spatial domain technique is used to hide secret information in the wavelet coefficients of the four subbands.

The cover image is transformed using 2D Haar integer wavelet transform to obtain four subbands: LL, LH, HL, and HH. The proposed method embeds data in the coefficients of four subbands by using the pixel value differencing approach.

2.1. Preprocessing. The gray scale image is read as a 2D array of size $[M, N]$. Histogram modification [12–15] is applied to prevent the possible overflow/underflow of pixel values. This problem occurs when the pixel values of the cover image are close to 255 or 0, because they may exceed 255 or fall below 0

LL	HL
LH	HH

Figure 1: Arrangements of wavelet coefficients.

Figure 2: The image lena.tiff after performing Harr transform.

during inverse integer wavelet transform. The problem can be solved by mapping the lowest 15 gray scale levels to the value 15 and the highest 15 gray scale levels to the value 240. If the pixel values exceed the boundaries during the inverse wavelet transform, the image is not suitable for hiding secret data. The image is transformed using 2D Haar wavelet transform to obtain four subbands: LL, LH, HL, and HH of size $[M/2, N/2]$ each. All the four subbands are used to hide the secret information. The 2D array of size $[M, N]$ is again constructed by arranging the four subbands as shown in Figure 1.

Figure 2 shows the arrangement of four subbands of the image lena.tiff after transforming it using 2D Harr integer wavelet transform.

A 2D array obtained by arranging the wavelet coefficients of four subbands is shown as follows:

$$\begin{pmatrix} 112 & 230 & 150 & \cdots & -45 & -120 & 80 \\ 130 & 159 & 172 & \cdots & -37 & -89 & -72 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ -30 & -59 & -72 & \cdots & -37 & -89 & -72 \end{pmatrix}. \quad (11)$$

The difference operation in Haar transform may cause some of the wavelet coefficients in HL, LH, and HH subbands to have negative values.

Since some of the wavelet coefficients have negative values, the 2D array shown in (11) cannot be used for hiding secret information using the pixel value differencing approach. Hence, absolute values are used for the coefficient with negative values to create a new 2D array with positive elements as follows:

$$\begin{pmatrix} 112 & 230 & 150 & \cdots & 45 & 120 & 80 \\ 130 & 159 & 172 & \cdots & 37 & 89 & 72 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ 30 & 59 & 72 & \cdots & 37 & 89 & 72 \end{pmatrix}. \quad (12)$$

After hiding the secret information in the 2D array shown in (12), inverse wavelet transform is performed to obtain the stego image. To obtain good quality of stego image, the original sign of each wavelet coefficient, as shown in (11), is required. Hence, the 2D array shown in (11) is used to create a sign matrix of the size $[M, N]$ having elements with values 1 or −1. The sign matrix so created is shown as follows:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & -1 & -1 & 1 \\ 1 & 1 & 1 & \cdots & -1 & -1 & -1 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ -1 & -1 & -1 & \cdots & -1 & -1 & -1 \end{pmatrix}. \quad (13)$$

The wavelet coefficients having positive values are represented by 1 whereas wavelet coefficients having negative values are represented by −1 in the sign matrix.

2.2. Embedding Process. For hiding the data in the 2D array, the method suggested by Gulve [4, 7] is used. In the method proposed by Chang [3], a block of 2×2 pixels is used to form 3 pairs which are then used to hide the secret information. The proposed method uses the block of 2×3 wavelet coefficients. The introduction of 2 wavelet coefficients in the 2×2 block forms two extra pairs. For a 512×512 image, it is possible to form 196608 pairs using the approach suggested by Chang [3] whereas, using the proposed approach, 217600 pairs can be formed. A greater number of pairs provide extra space for hiding the secret information. Thus, the proposed method improves the hiding capacity of the cover image.

The difference between two wavelet coefficients in the pair is used to hide the secret information. If the difference value is directly used to hide the information, it is easy to retrieve the embedded information in case the steganography system fails. To enhance the security of the secret information, the proposed algorithm modifies the difference between the two wavelet coefficients in the pair and this modified difference is used to hide the secret information. This imposes extra layer of security making harder extraction of original secret information from stego image using the difference values directly [4, 7].

The arrangement of wavelet coefficients into nonoverlapping blocks of 2×3 wavelet coefficients is shown in Figure 3. As shown in Figure 3, each 2×3 block includes six wavelet coefficients $P_{(x,y)}$, $P_{(x,y+1)}$, $P_{(x,y+2)}$, $P_{(x+1,y)}$, $P_{(x+1,y+1)}$, and $P_{(x+1,y+2)}$, where x and y are the locations of wavelet coefficients. Five pairs are formed by grouping the common wavelet coefficient PX_1 with the remaining five wavelet

PX_0 $P_{(x,y)}$	PX_1 $P_{(x,y+1)}$	PX_2 $P_{(x,y+2)}$
PX_3 $P_{(x+1,y)}$	PX_4 $P_{(x+1,y+1)}$	PX_5 $P_{(x+1,y+2)}$

Figure 3: Pixel block.

coefficients PX_0, PX_2, PX_3, PX_4, and PX_5. The five pairs PP_i where $i = 0, 1, 2, 3, 4$ are as shown below:

$$\begin{aligned} PP_0 &= \left(P_{(x,y+1)}, P_{(x,y)}\right), \\ PP_1 &= \left(P_{(x,y+1)}, P_{(x,y+2)}\right), \\ PP_2 &= \left(P_{(x,y+1)}, P_{(x+1,y)}\right), \\ PP_3 &= \left(P_{(x,y+1)}, P_{(x+1,y+1)}\right), \\ PP_4 &= \left(P_{(x,y+1)}, P_{(x+1,y+2)}\right). \end{aligned} \tag{14}$$

The difference value d_i is calculated for each pair PP_i by subtracting the common wavelet coefficient PX_1 from the other wavelet coefficient in that pair. This difference value is used to identify the corresponding range $R_{k,i}$ from the range table R. The range table is designed with ranges [0–7], [8–15], [16–31], [32–63], [64–127], and [128–255]. The width $W_{k,i}$ of range $R_{k,i}$ is used to determine the number of bits t_i ($t_i = \log_2 W_{k,i}$) that can be hidden in each pair where $i = 0, 1, 2, 3, 4$. This t_i is then used to calculate the average value (N) of number of bits possible to be hidden in each pair of the block. The average value N is used to calculate the revised difference Rd_i as Rd_i is remainder $(d_i/2^N)$ so that $Rd_i \leq 2^N$ where d_i is the original difference. The offset difference OD_i is calculated as $|d_i| - |Rd_i|$ for each pair in the block. The revised difference $|Rd_i|$ is then used to determine the number of bits t_i for each pair in the block. Thus, if the original difference value $|d_i|$ allows M bits to be hidden in the pair; then the proposed approach hides bits $\leq N$ in that pair [4, 7].

After embedding t_i bits of the message in the pair, new difference d_i' is calculated as $OD_i + l_{k,i} + b$ where $l_{k,i}$ represents lower boundary of the range $R_{k,i}$ in the range table R and b represents the decimal equivalent of t_i message bits hidden in that pair.

Embedding t_i bits in the pair modifies the values of both the wavelet coefficients in the pair. The new values of wavelet coefficients in each pair are different from their original values. Since new value is assigned to common wavelet coefficient PX_1 in each pair, five different values are obtained for the common wavelet coefficient PX_1. However, the common wavelet coefficient PX_1 can have only one value in each bock. This requires values of other five wavelet coefficients PX_0, PX_2, PX_3, PX_4, and PX_5 to be adjusted such that the new difference d_i' remains unchanged. Therefore, the pair, having new values of wavelet coefficients close to their original values, is selected as the reference pair. To find the reference pair, the difference m between d_i and d_i' is calculated. Small value of $|m|$ indicates that the new difference value d_i' is close to the original difference value d_i. Thus, for the pair with minimum $|m|$, the new values of wavelet coefficients are close to their original values. So the pair with minimum $|m|$ is selected as the reference pair. The values of the two wavelet coefficients in the reference pair are used to adjust the values of wavelet coefficients in other pairs and construct a new 2×3 block. The embedded secret information in newly constructed block is unaffected because difference values for the pairs are unaltered [4, 7].

During the extraction process, average value (N) is calculated using the same process adopted during embedding of the secret message. The average value N is used to calculate the revised difference Rd_i' as Rd_i' is remainder $(d_i/2^N)$. Suitable range $R^{k,i}$ is identified using this revised difference. The secret message is extracted in the decimal form by subtracting l_k from $|Rd_i'|$. Secret message is then converted into a binary stream with t_i ($t_i = \log_2 W_{k,i}$) bits [4, 7].

The process of hiding secret information in the cover image is described below [4, 7].

(1) Create the 2D array as shown in (12) by preprocessing the gray scale cover image.

(2) Partition the array into nonoverlapping blocks of 2×3 wavelet coefficients and group wavelet coefficient PX_1 with the remaining wavelet coefficients in the block to form five pairs.

(3) Calculate the difference values d_i for the five pairs in each block:

$$\begin{aligned} d_0 &= P_{(x,y)} - P_{(x,y+1)}, \\ d_1 &= P_{(x,y+2)} - P_{(x,y+1)}, \\ d_2 &= P_{(x+1,y)} - P_{(x,y+1)}, \\ d_3 &= P_{(x+1,y+1)} - P_{(x,y+1)}, \\ d_4 &= P_{(x+1,y+2)} - P_{(x,y+1)}. \end{aligned} \tag{15}$$

(4) Use $|d_i|$ where $i = 0, 1, 2, 3, 4$ to locate suitable range R_k in the designed range table. Use this range to calculate number of bits t_i that can be hidden in each pair PP_i. Then, calculate the average bits using

$$\text{avg} = \left\lfloor \left(\frac{\sum_{i=0}^{4} t_i}{5} \right) \right\rfloor. \tag{16}$$

(5) Calculate the revised difference $|Rd_i|$ where $i = 0, 1, 2, 3, 4$ as Rd_i is remainder $(d_i/2^{\text{avg}})$ so that $Rd_i <= 2^{\text{avg}}$.

(6) Calculate the difference OD_i as $OD_i = |d_i| - |Rd_i|$ for each pair.

(7) Use $|Rd_i|$ where $i = 0, 1, 2, 3, 4$ to locate suitable range R_k in the designed range table.

(8) Compute the number of bits t_i that can be embedded in each pair using the corresponding range given by R_k. The value t_i can be estimated from the width w_k of R_k, which is given by $t_i = \log_2 w_k$ where width $w_k = u_k - l_k + 1$ and u_k and l_k are upper and lower boundaries of the range R_k.

(9) Read t_i bits from the binary secret data.

(10) Calculate the new difference value d_i' given by

$$\begin{aligned} d_i' &= \mathrm{OD}_i + l_{k,i} + b_i, \quad \text{if } d_i \geq 0, \\ d_i' &= -\left(\mathrm{OD}_i + l_{k,i} + b_i\right), \quad \text{if } d_i < 0. \end{aligned} \tag{17}$$

(11) Modify the values of wavelet coefficients in the pair PP_i using

$$\left(P_n', P_{n+1}'\right) = \left(P_n - \left\lceil \frac{m}{2} \right\rceil, P_{n+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), \tag{18}$$

where P_n and P_{n+1} represent two wavelet coefficients in the pair PP_i and m is obtained by subtracting d_i from d_i'.

(12) Select the pair with minimum $|m|$ as the optimal reference pair and use this pair to adjust the values of wavelet coefficients of the other four pairs. The value of the common wavelet coefficient is given by P_n' of the reference pair. Modify value of another wavelet coefficient P_{n+1}' of remaining four pairs such that the new difference d_i' will remain unchanged. Thus, new values are assigned to remaining four wavelet coefficients in the block.

(13) Check the new values of wavelet coefficients for fall-off boundaries; that is, check whether all the values are within the range from 0 to 255. If not, modify the values preserving the difference between the values of two wavelet coefficients of each pair in the block.

(a) Find out the smallest of all the wavelet coefficients. If the smallest is less than 0 then add |smallest| in all the wavelet coefficients in that block.

(b) Find out the largest of all the wavelet coefficients. If the largest is greater than 255, subtract largest − 255 from all the wavelet coefficients in that block.

(c) If fall-off boundary problems still exist, the cover image is not suitable for hiding secret information.

(14) Now, reconstruct the block from all pairs with modified values of wavelet coefficients.

(15) Repeat steps (2) through (14) until the secret information is embedded in the cover image.

2.3. Postprocessing. After the embedding process is over, original signs are assigned to the elements of 2D array using the sign matrix created during preprocessing phase. This is accomplished by one to one comparison of elements of 2D array with the elements of 2D sign matrix. The 2D array is then split to obtain the four subbands. Using inverse 2D Haar integer wavelet transform, the four subbands are combined to obtain the stego image of size $[M, N]$. All the pixel values of the stego image in the range from 0 to 255 indicate that secret data is safely hidden and can be extracted accurately.

2.4. Extraction Process. The extraction process is blind. It does not require the existence of cover image for extracting hidden secret data from the stego image. The stego image is preprocessed to obtain the 2D array as shown in (12). The process of extraction of secret information from the stego image is described below [4, 7].

(1) Create the 2D array as shown in (12) by preprocessing the gray scale stego image.

(2) Partition the array into nonoverlapping blocks of 2×3 wavelet coefficients and group wavelet coefficient PX_1 with the remaining wavelet coefficients in the block to form five pairs. Keep the partition order the same as that of the embedding.

(3) Calculate the difference values d_i for the five pairs in each block:

$$\begin{aligned} d_0 &= P_{(x,y)} - P_{(x,y+1)}, \\ d_1 &= P_{(x,y+2)} - P_{(x,y+1)}, \\ d_2 &= P_{(x+1,y)} - P_{(x,y+1)}, \\ d_3 &= P_{(x+1,y+1)} - P_{(x,y+1)}, \\ d_4 &= P_{(x+1,y+2)} - P_{(x,y+1)}. \end{aligned} \tag{19}$$

(4) Use $|d_i|$ where $i = 0, 1, 2, 3, 4$ to locate suitable range R_k in the designed range table. Use this range to calculate number of bits, t_i, which is hidden in each pair PP_i. Then, calculate the average bits using (16).

(5) Calculate revised difference $|Rd_i'|$ where $i = 0, 1, 2, 3, 4$ as Rd_i' is remainder $(d_i/2^{\mathrm{avg}})$

(6) Use $|Rd_i'|$ where $i = 0, 1, 2, 3, 4$ to locate suitable R_k in the designed range table.

(7) After R_k is located, l_k is subtracted from $|Rd_i'|$ and b_i' is obtained in decimal form. A binary sequence is generated from b_i' with t_i bits where $t_i = \log_2 w_k$.

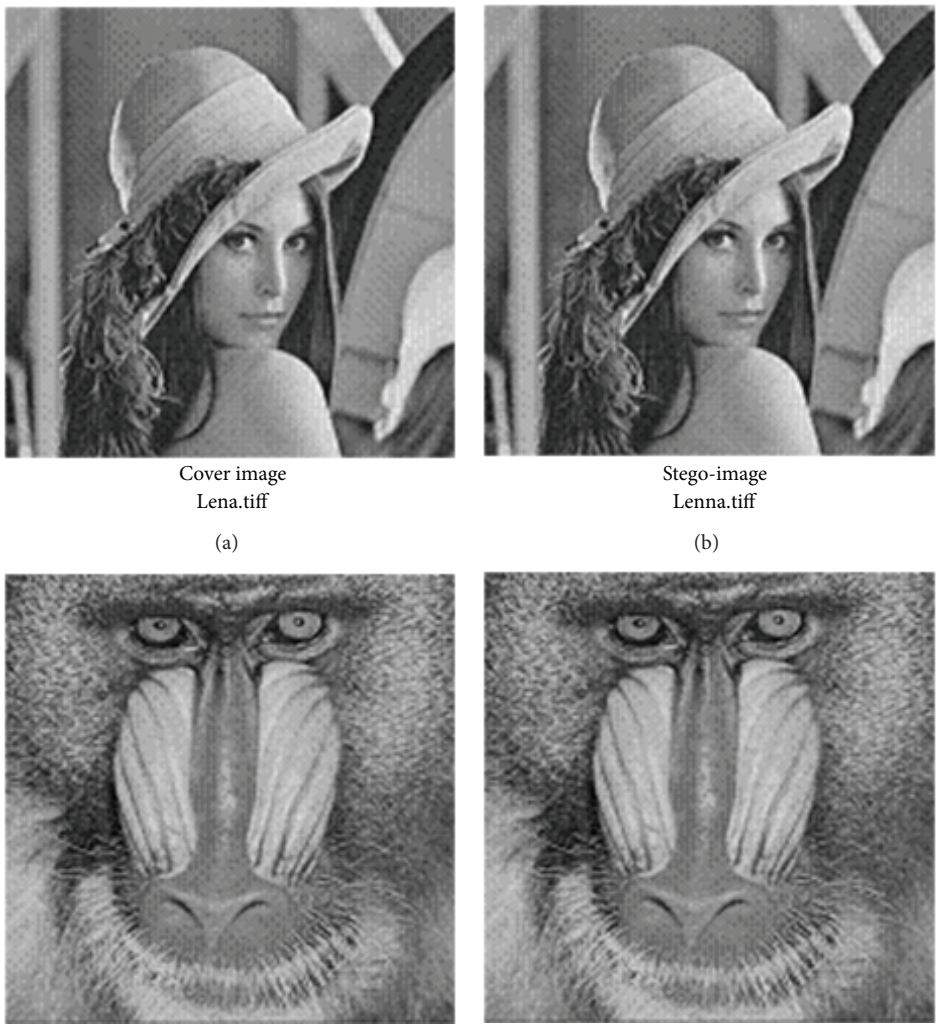
Repeat steps (2) through (7) until embedded message is extracted.

3. Results

A set of gray scale TIFF images is used for the experimentation. This set consists of standard images as well as images taken from the camera. The standard images are obtained from the "the USC-SIPI image database (http://sipi.usc.edu/database/)". The images taken from Canon A45 camera

Table 1: Comparison of hiding capacity (in bytes).

Cover image	PVD method [1]		TPVD method [3]		Gulve's method [4]		Proposed method	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	50960	41.79	75836	38.89	81305	42.86	81326	39.84
Baboon	56291	37.90	82407	33.93	81766	41.99	82933	39.62
Peppers	50685	41.73	75579	38.50	81326	42.80	81387	40.29



Cover image
Lena.tiff
(a)

Stego-image
Lenna.tiff
(b)

Cover image
Baboon.tiff
(c)

Stego-image
Baboon.tiff
(d)

Figure 4: Cover and stego images.

in JPG format are converted into gray scale tiff format. The text files are used as secret data. Since the proposed algorithm use PVD approach to hide information in wavelet coefficients, the data hiding capacity and PSNR values of the proposed method are compared with PVD method [1], TPVD [3] method, and Gulve's method [4]. The comparison is shown in Table 1. The proposed method provides increased hiding capacity and improved PSNR values as compared to PVD and TPVD method. Although the PSNR is less as compared to Gulve's [4] method, there is an improvement in the security of secret data.

The average payload of the proposed system is ~2.48 bpp. The performance of the proposed method is analyzed using PSNR, Universal Quality Index (Q), and Structural Similarity Index Measure (SSIM). Q and SSIM are full reference image quality assessment models and require the cover image to be available [16, 17]. Table 2 shows the PSNR values, MSE, Universal Quality Index (Q), and Structural Similarity Index

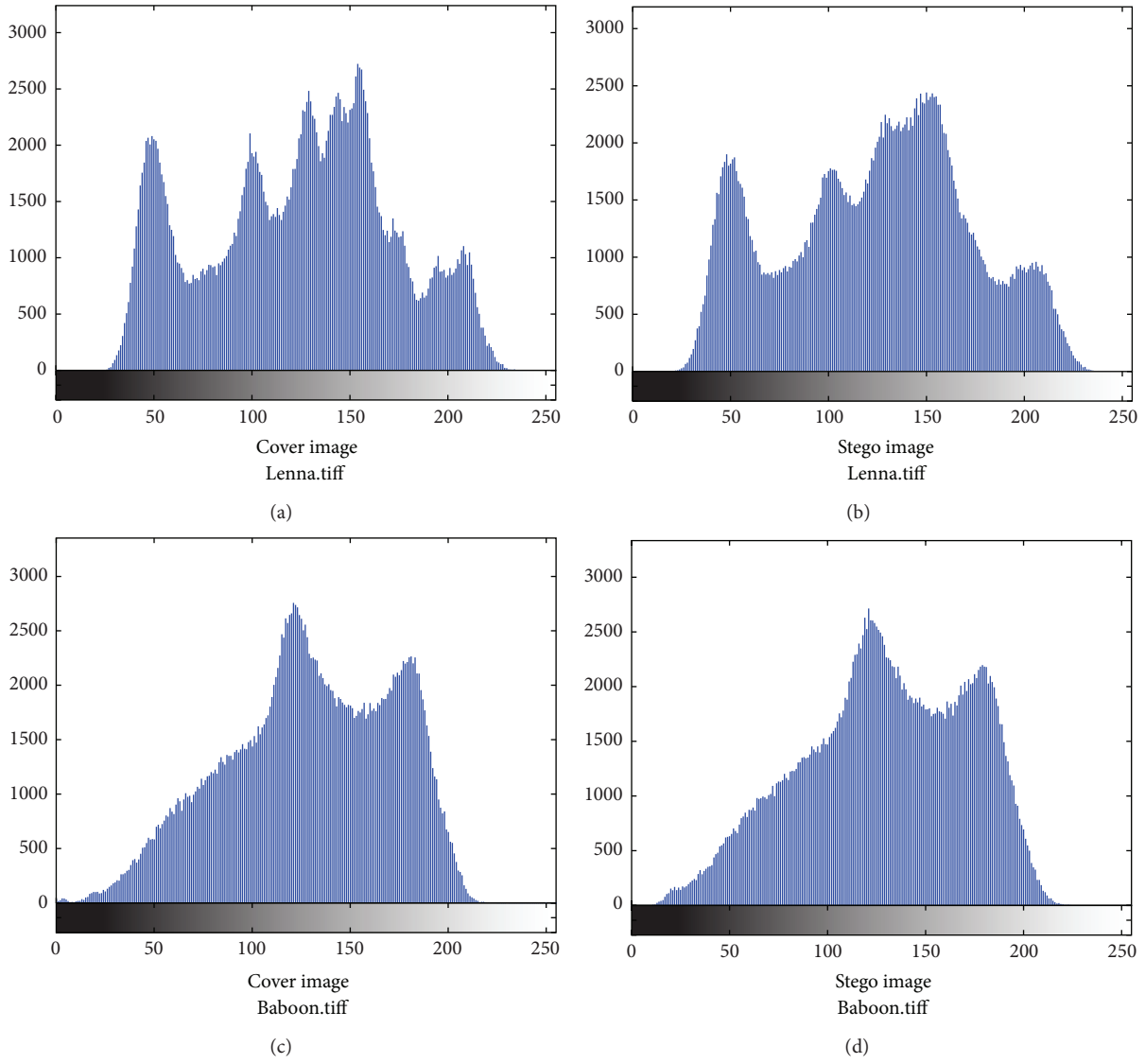


Figure 5: Histograms of cover and stego images.

Measure (SSIM) for different images obtained using proposed method. The PSNR values are above the threshold of 36 dB [18] even after using more than 95% of the hiding capacity of the cover image. Also Universal Quality Index (Q) values [16] and Structural Similarity Index Measure (SSIM) values [17] are close to 1, which proves that the stego images are visually indistinguishable from original cover images.

Figure 4 shows the cover image and the corresponding stego images obtained using the proposed method. As the figures show, distortions resulted from embedding are imperceptible to human vision.

Figure 5 shows the histogram of the cover and stego image obtained using the proposed method. From the figure, it can be observed that the shape of the histogram is preserved.

The cover image data is subtracted from stego image and plotted as histogram. Figure 6 shows the pixel difference histogram. From the figure, it can be observed that there are more numbers of bins which are close to 0 as compared to bins which are away from 0. Also the step pattern is not observed in the figure. This confirms that the method is robust against histogram analysis attack.

Histogram of cover image is represented as $[h_0, h_1, \ldots, h_{255}]$ whereas histogram of stego image is represented as $[h'_0, h'_1, \ldots, h'_{255}]$. The change in histogram [19] is measured by

$$D_h = \sum_{m=1}^{255} \left| h'_m - h_m \right|. \tag{20}$$

The proposed method can hide at least 3 bits in each pair considering the smallest width of the subrange to be 8. Figure 7 shows the comparison of the value of D_h of the 3 bit LSB replacement method and the proposed method with different size of secret data embedded in the cover image, Lena.tiff. It can be observed that difference in histogram for the proposed method is less than that of 3 bit LSB method.

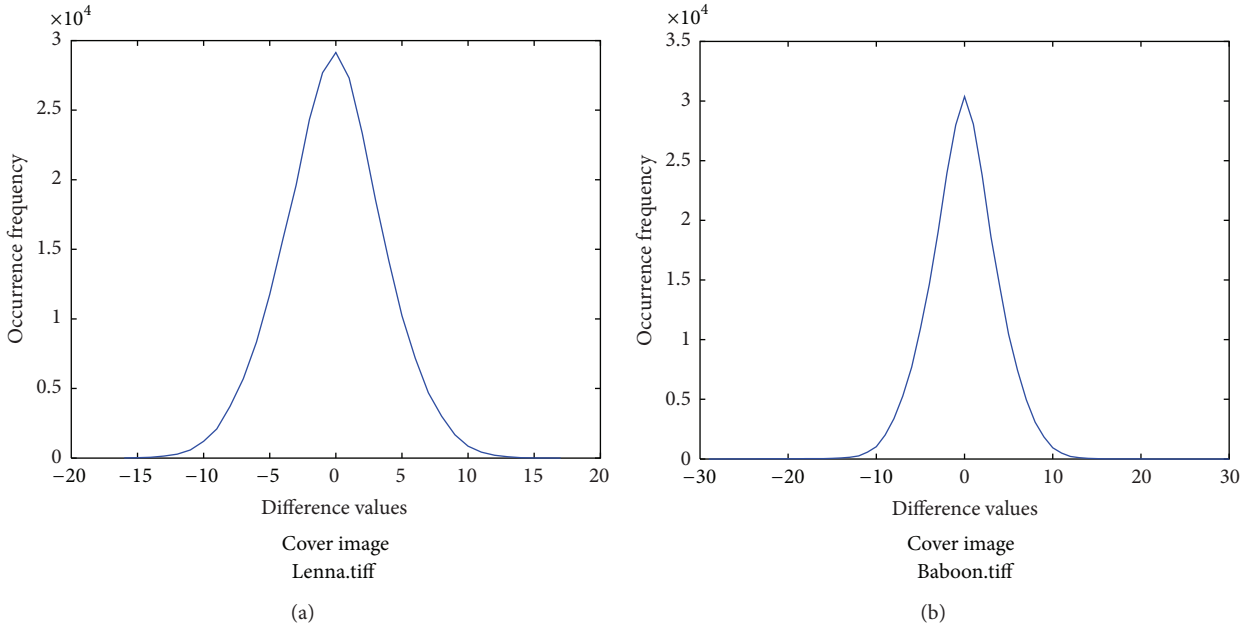


Figure 6: Difference histogram.

Table 2: Hiding capacity, PSNR, MSE, and Q index.

Cover image	Resolution of cover image	Hiding capacity (Kb)	% of hiding capacity	Message file size (Kb)	PSNR	MSE	Q	SSIM
Baboon	256 × 256	19.92	30.65	19.5	39.87	6.684	0.959	0.965
Lena	256 × 256	19.94	30.68	19.5	39.91	6.633	0.899	0.937
Elaine	512 × 512	79.42	30.9	78.7	40.01	6.482	0.890	0.956
Baboon	512 × 512	80.99	30.68	78.7	39.62	7.089	0.961	0.979
Lena	512 × 512	79.47	30.68	78.7	39.84	6.740	0.806	0.953
Tank	512 × 512	79.41	30.9	78.7	39.86	6.700	0.896	0.954
Peppers	512 × 512	79.48	30.22	78.7	40.29	6.074	0.800	0.932
Barbara	512 × 512	80.35	30.55	78.7	39.70	6.961	0.857	0.964
Boat	512 × 512	79.64	30.75	78.7	39.90	6.652	0.883	0.962
Grass	1024 × 1024	319.32	31.15	317	39.51	7.274	0.979	0.998

The output images are tested under the *RS* steganalysis [20]. It is observed from Figure 8 that the difference between R_M and R_{-M} and S_M and S_{-M} is very small. The rules $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$ are satisfied for the output images. This proves that the proposed method is secure against *RS* attack.

4. Conclusion

In steganography, hiding capacity of cover image, quality of stego image, and security of secret data are three important factors. There is always a trade-off between data hiding capacity of cover image and security of secret data. The proposed algorithm provides improvements in the data hiding capacity as well as security of the secret data as compared to PVD [1] and TPVD [3] methods. Although Gulve's [4] method provides better PSNR values as compared to proposed method, the proposed method improves security of secret information. The secret information is securely hidden in the coefficients of integer wavelet transform. For the implementation purpose, the four subbands obtained after decomposing the cover image by integer wavelet transform are arranged as shown in Figure 1. But it is possible to arrange the four subbands in 4! = 24 different ways thereby improving the security of the steganography system since the exact arrangement of four subbands will be known to sender and receiver only. The algorithm revises the original difference between two wavelet coefficients in the pair and this revised difference is used for hiding the data in that pair. This makes estimation of exact number of bits hidden in the pair difficult. Image steganography techniques hiding textual information require 100% accuracy for successful retrieval of hidden information from stego image. If the steganography method fails, correct estimation of number of bits hidden for some of the pairs will be a challenge for the invader. Thus,

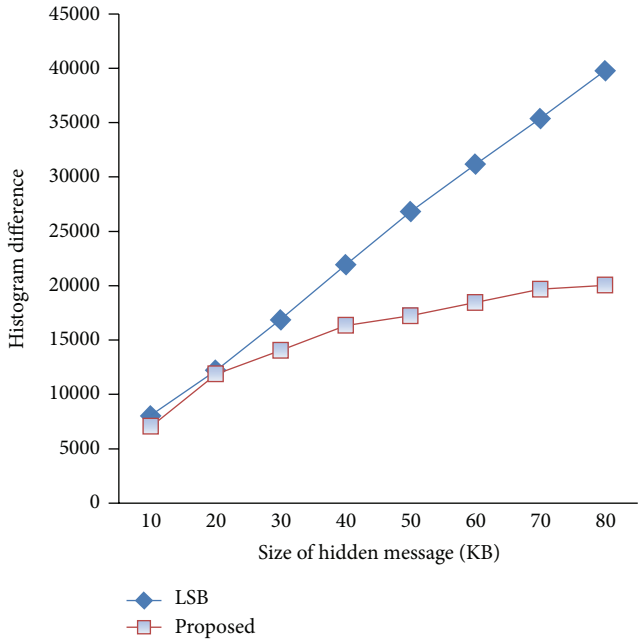


Figure 7: Histograms comparison of 3 bit LSB substitution and proposed method (Lena.tiff).

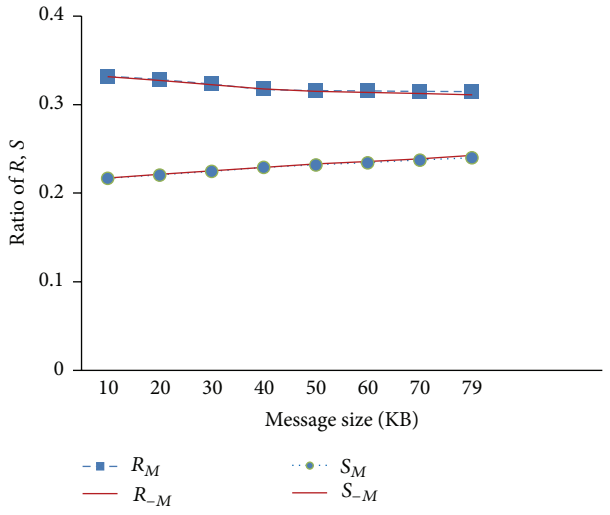


Figure 8: *RS* diagram.

one more level of security is imposed to secure the secret information.

The PSNR values produced by the algorithm are close to 39.5 which are well above the threshold of 36 dB after using full hiding capacity of the cover image. This proves that the stego images are of good quality. Results also show that the difference between cover image and stego image cannot be noticed by human visual system (HVS).

Considering the fact that there is currently no steganography system that can resist all the steganalysis attacks, the best way to provide security to the secret data and to eliminate the attack of comparing the original image with the stego image is to freshly create an image and destroy it after generating the stego image.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

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

[3] K.-C. Chang, P. S. Huang, T.-M. Tu, and C.-P. Chang, "Adaptive image steganographic scheme based on tri-way pixel-value differencing," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC '07)*, pp. 1165–1170, Montreal, Canada, October 2007.

[4] A. K. Gulve and M. S. Joshi, "An image steganography algorithm with five pixel pair differencing and gray code conversion," *International Journal of Image, Graphics and Signal Processing*, vol. 6, no. 3, pp. 12–20, 2014.

[5] K.-C. Chang, C.-P. Chang, P. S. Huang, and T.-M. Tu, "A novel image steganographic method using tri-way pixel-value differencing," *Journal of Multimedia*, vol. 3, no. 2, pp. 37–44, 2008.

[6] K. C. Chang, P. S. Huang, T. M. Tu, and C. P. Chang, "Image steganographic scheme using tri-way pixel-value differencing and adaptive rules," in *Proceedings of the IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 449–452, Kaohsiung, Taiwan, 2007.

[7] A. K. Gulve and M. S. Joshi, "A secured image steganography algorithm with five pixel pair differencing by selecting the common pixel randomly," in *Proceedings of the 3rd International Conference on Computational Intelligence and Information Technology (CIIT '13)*, pp. 55–61, Elseveir, Mumbai, India, 2013.

[8] A. R. Calderbank, I. Daubechies, W. Sweldens, and B.-L. Yeo, "Wavelet transforms that map integers to integers," *Applied and Computational Harmonic Analysis*, vol. 5, no. 3, pp. 332–369, 1998.

[9] B. Ramalingam, R. Amirtharajan, and J. B. B. Rayappan, "Stego on FPGA: an IWT approach," *The Scientific World Journal*, vol. 2014, Article ID 192512, 9 pages, 2014.

[10] E. Ghasemi, J. Shanbehzadeh, and B. ZahirAzami, "A steganographic method based on Integer Wavelet Transform and Genetic Algorithm," in *Proceedings of the International Conference on Communications and Signal Processing (ICCSP '11)*, pp. 42–45, Calicut, India, February 2011.

[11] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, "High capacity image steganography using wavelet transform and genetic algorithm," in *Proceedings of the International Multi Conference of Engineers and Computer Scientists (IMECS '11)*, pp. 495–498, Hong Kong, March 2011.

[12] G. Xuan, Y. Q. Shi, C. Yang, Y. Zheng, D. Zou, and P. Chai, "Lossless data hiding using integer wavelet transform and threshold embedding technique," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '05)*, pp. 1520–1523, IEEE, Amsterdam, The Netherlands, July 2005.

[13] R. O. El Safy, H. H. Zayed, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," in *Proceedings of the International Conference on Networking and Media Convergence (ICNM '09)*, pp. 111–117, Cairo, Egypt, March 2009.

[14] S. Archana, A. Judice, and K. P. Kaliyamurthie, "A novel approach on image steganographic methods for optimum hiding capacity," *International Journal of Engineering and Computer Science*, vol. 2, no. 2, pp. 378–385, 2013.

[15] A. K. Al-Asmari, M. A. Al-Qodah, and A. S. Salama, "Wavelet-pixel value differencing technique for digital images data hiding," in *Proceedings of the IEEE International Conference on System Engineering and Technology (ICSET '11)*, pp. 15–18, June 2011.

[16] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81–84, 2002.

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

[18] N. I. Wu and M. S. Hwang, "Data hiding: current status and key issues," *International Journal of Network Security*, vol. 4, no. 1, pp. 1–9, 2007.

[19] X. Zhang and S. Wang, "Efficient data hiding with histogram-preserving property," *Telecommunication Systems*, vol. 49, no. 2, pp. 179–185, 2012.

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