S.I. Nipanikar* and V. Hima Deepthi

A Multiple Criteria-Based Cost Function Using Wavelet and Edge Transformation for Medical Image Steganography

DOI 10.1515/jisys-2016-0095
Received June 29, 2016; previously published online December 28, 2016.

Abstract: With the ever-increasing need for concealing messages within cover media like image, video, and audio, numerous attempts have been developed for steganography. Most of the steganographic techniques perform their embedding operation on the cover image without selecting a better location. The right selection of location for embedding the information can lead to high imperceptibility and robustness. Accordingly, in this paper, we develop a new cost function for estimating the cost of every pixel to identify the good location to embed the message data. The proposed cost estimation procedure utilizes multiple parameters like wavelet coefficient, edge transformation, and pixel intensity. The proposed cost matrix is then utilized to embed the message data into the cover media using an embedding integer. The proposed steganographic technique is experimented with two magnetic resonance brain images, and the results are analyzed with the peak-to-peak signal-to-noise ratio (PSNR) and mean square error. The robustness analysis ensured that the proposed steganographic technique outperforms the existing methods by reaching the maximum PSNR of 72.74 dB.

Keywords: Steganography, medical image, wavelet, edge transformation, PSNR.

1 Introduction

Recently, with the rapid improvement and evolution in biomedical systems, the importance of digital medical images has increased in the medical world. Digital hospital systems and modern clinical infrastructures are formed by using the Hospital Information System and PACS based on Digital Imaging and Communications in Medicine (DICOM) standards [12, 21, 30]. Later on, a DICOM encoding method has become the only data protection for nearly 20 years. However, it is fundamental during exchanging medical images to maintain the security and privacy of patient information. This requirement can be easily fulfilled by the technique called steganography. Steganography is the science and art of concealing a message within empirical cover media (image, audio, or video, etc.) [8].

Steganography can be done in both spatial and frequency domains [32, 38]. The least significant bit (LSB) substitution is a spatial domain steganographic technique. In LSB substitution, private data are hidden in the least significant bits (rightmost bits) so that the original pixel value is not affected by the embedding procedure. The negative part of this approach is that it is prone to minor image manipulations. Thus, this method is not safe for sending confidential data. In the frequency domain, discrete cosine transform (DCT) is a widely used method. DCT allows an image to be broken up into three frequency bands, namely the low-frequency band, high-frequency band, and mid-frequency band. In this approach, the secret data are embedded into the DCT blocks containing mid-frequency sub-band components, whereas the high-frequency sub-band components remain unused. Another approach is to do the steganography on the discrete wavelet transform (DWT) domain. Steganography using DWT has more advantages over DCT because it provides high compression

***Corresponding author: S.I. Nipanikar,** Vel Tech University, Avadi, Chennai, Tamil Nadu 600062, India,
e-mail: nipanikar.si@gmail.com
V. Hima Deepthi: Vel Tech University, Avadi, Chennai, Tamil Nadu 600062, India

ratios and also avoids interferences due to artifacts. Thus, comparatively, DWT is a better method for hiding confidential data [7].

Designing steganographic algorithms for empirical cover sources [9] is very challenging due to the fundamental lack of accurate models. The most successful approach avoids estimating (and preserving) the cover source distribution because this task is infeasible for complex and highly non-stationary sources, such as digital images. Instead, message embedding is formulated as source coding with a fidelity constraint – the sender hides the message while minimizing an embedding distortion. Practical embedding algorithms that operate near the theoretical payload-distortion bound are available for a rather general class of distortion functions [14, 15]. Generally, a good steganographic method should have acceptable statistical imperceptibility and a sufficient payload, although these two objectives are generally conflicting with each other for a given algorithm. Therefore, the purpose of the steganographer is to lower the statistical detectability, i.e. to improve the security performance for a fixed payload. In modern steganography, numerous attempts have been made to achieve this purpose. Among them, preserving a chosen cover model has been proved to be a bad idea, while the most common and effective approach is minimizing a heuristically defined embedding distortion for the empirical cover media. Such approach is also formulated as a minimal distortion embedding framework [16].

In this paper, we have developed a steganographic technique using the cost estimation process. The proposed steganographic technique is performed using three important steps. In the first step, the cost estimation process is applied to estimate the cost value of every pixel using wavelet, edge transformation, and pixel intensity. A new mathematical model is developed to find the cost of every pixel. The estimated cost matrix based on every pixel is then used to embed the message data within the cover image. The embedding operator utilizes cost, cover image, and message with the embedding integer. Finally, modular operation is used to extract the message data from the embedded image. The main contributions of the paper are given as follows:

- A new mathematical model is developed to find the cost of every pixel using wavelet coefficient, edge transformation, and pixel intensity.
- A location-aware steganographic technique is developed by giving the optimal location for embedding the message data within the cover image.

The paper is organized as follows. Section 2 presents the review of the literature, and Section 3 presents the motivation behind the approach. Section 4 presents the proposed steganographic technique, and Section 5 discusses the experimentation and results. Finally, the conclusion is given in Section 6.

2 Literature Review

The literature presents different techniques for steganography using various methods like DCT, DWT, and edge detection [4, 13, 19, 20, 36, 37]. DCT coefficients [16] and DWT coefficients [7, 18] are used commonly for steganography in most of the methods. Wavelet transform-based techniques are extensively discussed in Refs. [34, 36], and interpolation-based techniques are analyzed in Refs. [19, 37]. Meanwhile, fuzzy logic-based technique [20] and LSB-based technique [35] are also importantly used in the literature for image steganography. Also, the clustering algorithm [22] is applied to perform the embedding process. Edge transformation [3] also plays a major role in identifying the sensitive pixels for maintaining the perceptibility of the images. On the other hand, the steganography methods applicable to medical images are discussed in Refs. [5, 6, 11, 17, 19, 23–25, 28, 31, 39]. Table 1 reviews the literature of the different steganography methods.

3 Motivation Behind the Approach

This section explains the major challenges involved in steganographic techniques. Due to widespread growth of medical images, the exchange of information requires good steganography technique, where patient infor-

Table 1: Literature Review.

Authors	Methods	Advantages	Issues
Baby et al. [7]	DWT-based technique	Safe, sound, and flexible approach	Have perceptible changes
Li et al. [22]	Clustering-based method	Embedding modifications in heavily textured regions are locally heading toward the same direction	Computation of cost for every pixel should consider multiple criteria
Al-Dmour and Al-Ani [3]	Edge detection-based technique	Embedding different numbers of bits per pixel may also improve the security of the message	Right selection of edge filter
Ahani and Ghaemmaghami [1]	Sparse representation-based technique	Very effective, because it is introduced to avoid errors caused by the rounding process	Sparse process requires more computational overhead
Sedighi et al. [33]	LSB-based method	Achieves the following novel insights into both steganography design and steganalysis	The empirical detector overestimates the payload due to its lower detection power
Holub and Fridrich [18]	Wavelet-based technique	Independent of the embedding domain	This heuristics approach requires much computational time
Guo et al. [16]	DCT coefficients-based technique	Minimal distortion embedding framework	The DCT coefficients have been prohibited from embedding message in JPEG steganography for a long time

mation can be easily hidden on the medical images. The important challenge to be considered is that the embedding of information on medical images should be flexible to noisy data, as the medical images from the medical instruments are commonly affected with more noises.

Embedding of patient information on the medical image should pose two important challenges. The detection ability for information by a third party should be low to ensure security. Also, the imperceptibility should be high, which means that the embedded images should be exactly the same as that of the cover image. An additional challenge that needs to be posed is the capacity of the cover image. When devising a new embedding algorithm, the bit of information to be embedded should be more, so that more information can be embedded on the image.

One of the recent works presented in the literature is clustering-based steganography [7]. This method utilizes the estimation of cost of every pixel to check the feasibility of the embedding strength. This cost computation does not cover the neighbor pixel coverage as well as the edge information. Additionally, wavelet coefficient can also be utilized for the cost to find the fittest of the pixels. By considering this, multiple criteria to decide the cost can improve the detection ability as well imperceptibility.

4 Proposed Methodology: Multiple Criteria-Based Cost Function for DWT-Based Medical Image Steganography

This section presents the multiple criteria-based cost function for medical image steganography to find the best location for embedding. The proposed technique is developed using three important steps: (i) identification phase, (ii) embedding phase, and (iii) extraction phase. In the identification phase, a novel cost function is devised to identify the relevant pixels by considering multiple criteria like wavelet energy, pixel coverage, and edge information. Once the relevant pixels are identified, embedding of patient information to the original medical image is done using the proposed embedding mechanism. The proposed embedding mechanism

utilizes the cost function for embedding the patient information into the magnetic resonance images along with embedding the integer. In the extraction step, the patient information is extracted from the original medical image using the proposed extraction scheme. Figure 1 shows the block diagram of the proposed steganographic technique.

4.1 Cost Estimation of Pixels for Embedding

The first step of the proposed steganographic technique is the estimation of the cost of the pixels for embedding. The estimation of the cost value should handle the two objectives like visual quality in the embedded image and message quality in the extracted message. Thus, the identification of parametric measure to preserve the visual quality of embedded image and extracted image is important. Here, we have taken three levels of informatics measure, like wavelet coefficients, pixel intensity, and edge transformation, to find the cost value of pixels. The wavelet coefficients are capable of isolating fine details and identifying coarse details. Also, it is able to reveal aspects like trends, breakdown points, and discontinuities in higher derivatives and self-similarity. The pixel intensity is also an important parameter, as intensity is directly correlated with the human visual system. The third parameter we considered is the edge transformation, which can identify vital information of images, like boundary, corners, and curves, easily.

Let us assume that the input medical image is represented as A, which has the size of $m \times n$. Every pixel within this image is denoted as a_{ij}. The intensity of the pixel a_{ij} is varied from 0 to 255, $a_{ij} \in (0.255)$.

$$A = \left\{ a_{ij};\ 1 \le i \le m\ ;\ 1 \le j \le n \right\}. \tag{1}$$

The intensity-based cost vector is computed based on the variance among the neighbor pixels. The original image A is processed with neighbor pixels, and every pixel value is replaced by the variance among the neighbor's pixels. The formula used to compute the variance of the pixel intensity is given as follows:

$$a_{ij}^{v} = \frac{1}{p} \sum_{k=1}^{p} (a_{ij}^{k} - \mu_{ij}), \tag{2}$$

where p is the number of neighbor pixels considered and μ_{ij} is the mean of the neighbor pixels, which is computed as follows:

$$\mu_{ij} = \frac{1}{p} \sum_{k=1}^{p} a_{ij}. \tag{3}$$

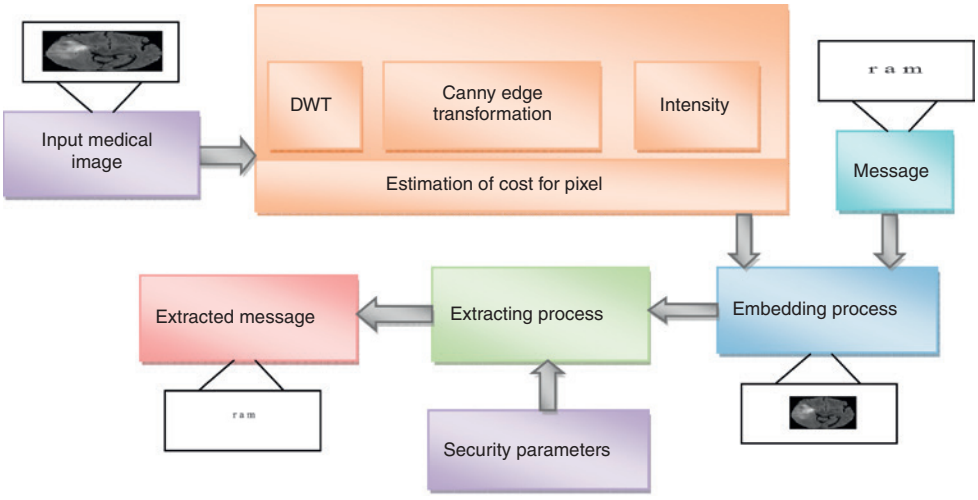

Figure 1: Block Diagram of the Proposed Method.

Once the variance of the pixels based on neighbors are computed, the binary cost is then found by applying a threshold T_r. Here, if the variance of the pixel is less than the threshold T_r, then we assign the binary cost as 1. Otherwise, the binary cost is assigned as 0. The idea behind this computation is that if the variance obtains minimum among the neighbor pixels, then this region is more like a texture part, so these pixels can be modified to embed the original message within the data.

$$g_{ij} = \begin{cases} 1 \text{ if } a_{ij}^{v} < T_r \\ 0 \text{ if } a_{ij}^{v} \geq T_r \end{cases}. \tag{4}$$

The next parameter is the utilization of DWT coefficients to identify the cost of the pixels a_{ij}. The input image A is directly given to DWT computation [2] to find the wavelet coefficients.

$$B = \text{DWT}(A), \tag{5}$$

where B is wavelet-transformed approximation image. Here, every wavelet coefficient is represented as b_{ij}, as follows:

$$B = \left\{ b_{ij};\ 1 \leq i \leq m;\ 1 \leq j \leq n \right\}. \tag{6}$$

The wavelet-approximated image is given for the neighborhood-based variance computation to find the cost of the pixels for identifying the better location. Every wavelet coefficient is subtracted from the mean of the neighbor pixels to find the variance. The formula used to find the variance based on wavelet coefficients is given as follows:

$$b_{ij}^{v} = \frac{1}{p} \sum_{k=1}^{p} (b_{ij}^{k} - \mu_{ij}), \tag{7}$$

where p is the number of neighbor pixels and μ_{ij} is the mean of the neighbor pixels. The mean of every wavelet coefficient based on the neighbor pixels is computed as follows:

$$\mu_{ij} = \frac{1}{p} \sum_{k=1}^{p} b_{ij}. \tag{8}$$

Then, the variance of the wavelet approximation b_{ij}^{v} is used to find the cost vector h_{ij}, which is a binary matrix, containing the cost value of either 0 or 1. If the variance is less than threshold T_D, then the binary cost is assigned as 1. Otherwise, it is assigned as 0.

$$h_{ij} = \begin{cases} 1 \text{ if } b_{ij}^{v} < T_D \\ 0 \text{ if } b_{ij}^{v} \geq T_D \end{cases}. \tag{9}$$

The third parameter considered here is the edge transformation, which can be found using the canny edge detection algorithm [10]. The process of canny edge detection algorithm contains five different steps. Initially, Gaussian filter is applied to smooth the image in order to remove the noise, and the intensity gradients of the image are computed. Then, non-maximum suppression is found out to get rid of spurious response to edge detection and, finally, double threshold is applied to determine potential edges. The edge-detected output from the input image is given as follows:

$$C = \text{edge}(A). \tag{10}$$

This edge detection process marks the edge pixels as 0 and the non-edge pixels as 1. Thus, the cost vector belonging to the edge transformation is represented as C. Every value in c_{ij} belongs to either 0 or 1, $c_{ij} \in 0$ & 1:

$$C = \left\{ c_{ij};\ 1 \leq i \leq m;\ 1 \leq j \leq n \right\}. \tag{11}$$

After finding the cost values of pixels based on intensity, wavelet, and edge, the aggregated cost of every pixel is computed by taking average of the cost value:

$$r_{ij} = \frac{1}{3}(g_{ij} + h_{ij} + c_{ij}), \tag{12}$$

where g_{ij} is cost vector related to intensity, h_{ij} is cost related to wavelet, and c_{ij} is cost related to edge. Finally, the cost value that is greater than the threshold R_T is taken as the final cost of the pixels, l_{ij}, and those pixels are taken for embedding the message data:

$$l_{ij} = \begin{cases} 1 \text{ if } r_{ij} > R_T \\ 0 \text{ if } r_{ij} \le R_T \end{cases}. \tag{13}$$

4.2 Embedding of Message into Cover Image

The second step is to perform the embedding process, where the message will be hidden within the cover image A. The message information is taken here as binary image m, which is in the size of $u \times v$.

$$m = \left\{ m_{kl};\ \ 1 \le k < u :\ 1 \le l \le v \right\}. \tag{14}$$

The embedding of the message m within the cover image A is performed using cost matrix L and embedding integer X. At first, the input message is sequentially scanned to embed into the original image, and the order of embedding within the original image is performed based on the cost matrix L, which contains the elements either 0 or 1. The pixel elements that have the cost value of 1 are the right location in the cover image for embedding. Thus, we consider only the location having a cost value of 1 of the original image for the embedding process. The changing of every pixel within the embedding image S is as follows. If the cost vector is not equal to 1, then there will not be any change in the pixel of the original image. The same pixel intensity of the original image is assigned to the embedded image S. If the cost vector is equal to 1, then the intensity of the original pixel value will be changed based on the message information.

$$s_{ij} = \begin{cases} a_{ij} * (1 - l_{ij}); \text{ if } l_{ij} \ne 1 \\ y_{ij} * l_{ij}; \quad \text{if } l_{ij} == 1 \end{cases}. \tag{15}$$

The changing of pixel value based on message is denoted as y_{ij}. If the message bit is equal to 1, bitwise AND operation is performed in between the pixel value of the original image and embedding integer X. If the message bit is equal to 0, bitwise OR operation is performed in between the pixel value of the original image and complement of embedding integer:

$$y_{ij} = \begin{cases} a_{ij} \,\&\, X \text{ if}; m_{kl} == 1 \\ a_{ij} \,|\, \sim X; \text{ if } m_{kl} == 0 \end{cases}, \tag{16}$$

where X is initialized as 254. This process is repeated for every bit value of message data until it embeds on the cover image.

4.3 Extraction of Message from Embedded Image Using Security Parameters

The extraction step is to retrieve back the hidden message within the embedded image using the extraction step. Once the sender embeds the message into the cover image, the receiver receives the embedded image and the message information should be extracted back from the embedded image. If any intruder receives the embedded image and the extraction algorithm, they can easily identify the message information. Thus, in order to improve the security concern, the receiver requires three additional parameters here to find the

original message from the embedded image. As we perform the embedding process based on the cost vector, the cost vector is required at the receiver, but we can compute the cost vector at the receiver end through the proposed procedure if the input image is known at the receiver. Also, the size of message bit is also important for extracting the message from the cover image. Accordingly, the input image A and size of the message data, u and v, should be known at the receiver end.

In the receiver side, the original image is used to find the cost matrix L. The modular 2 operation is performed on the embedded image S if the cost matrix of the location is 1. The modular 2 operation provides either 0 or 1 based on the embedded data:

$$m^{*}_{kl} = \mathrm{mod}(s_{ij}, 2); \quad l_{ij} == 1. \tag{17}$$

This process of extracting the message is performed sequentially until the size of the extracted message is equal to uxv.

4.4 Running Example of Embedding and Extraction Procedure

Figure 2 shows the example of embedding and extraction procedure for steganography. Let us assume that the input image R contains 3×3 pixels, which is directly given to the procedure of the proposed cost estimation that utilizes the DWT and canny edge detection. The binary cost is assigned to every pixel. The first pixel 25 obtains the cost value of 1 and the second pixel 30 obtains the value of 0. Then, the DWT-dependent cost matrix L and the input image R are utilized to find the embedded image. In order to select the embedding location, the cost matrix is utilized. The location that does not have the cost value of 0 is taken for embedding. The selected location for embedding is marked with different colors in Figure 2. Pixels 25, 46, 120, 86, 32, and 32 are selected to embed the message data. Then, message data are sequentially scanned and embedded into the original image sequentially within the selected pixels. The first message bit is 1, which should be embedded into the pixel value 24. Thus, bitwise AND operation is performed in between 25 and 254, which gives the value of the 24, which is then placed in the first location instead of 25. The second bit of the message data is

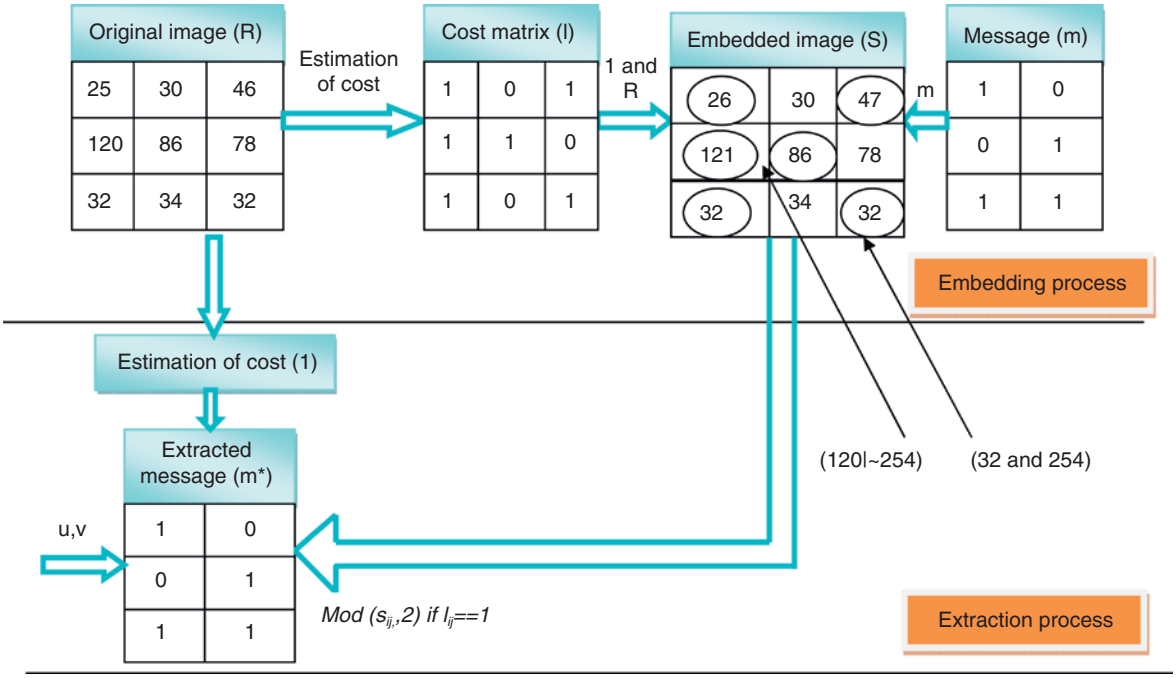

Figure 2: Example of Embedding and Extraction Procedures.

0, which should be embedded within 47. While performing bitwise OR operation between 46 and negation of 254, we obtain the value of 47, which is filled instead of 46. This process is repeated for all the pixels, and the embedded image is obtained. After embedding, the pixels are 24, 30, 47, 121, 86, 79, 32, 34, and 32. In the extraction process, security attributes like original image or size of message data should be known at the receiver. The cost matrix can be computed from the original image, so the location of embedded pixels can be identified. Then, modular 2 operation is applied to retrieve the message data.

5 Results and Discussion

This section presents the experimental results of the proposed steganographic technique and the detailed evaluation of the proposed techniques.

5.1 Experimental Setup

5.1.1 Images considered

The experimentation is performed using the medical images available in the BRATS database [26]. Two magnetic resonance medical images are taken here for experimental purpose. Also, two mammogram images are taken from the MIAS database [27]. The message data are the synthetically generated image. The size of the medical image is 255×255, and the size of the message data is 90×90.

5.1.2 Evaluation metrics

The evaluation of the proposed technique is done using two metrics, called peak-to-peak signal-to-noise ratio (PSNR) and mean square error (MSE), which are taken to evaluate the two objectives of steganography. PSNR is computed between the original image and the embedded image to ensure that the embedded image is visually balanced with respect to the original images. MSE is computed in between the original message and the extracted message to ensure that the extracted message preserves the original message.

$$\mathrm{PSNR} = 20\log_{10} \frac{E_{\max} \times m \times n}{\sum\sum (A_{xy} - S^{*}_{xy})^{2}}, \tag{18}$$

where m and n are the width and height of the image, A_{xy} is the pixel value of the original image at coordinates (x, y), S^{*}_{xy} is the embedded pixel value at coordinates (x, y), and $E_{\max}$ is the largest energy of the pixels (i.e. $E_{\max} = 255$ for 256 gray-level images).

$$\mathrm{MSE} = \frac{1}{u \times v} 2 \sum_{k=1}^{u} \sum_{l=1}^{v} (m_{kl} - m^{*}_{kl})^{2}, \tag{19}$$

where u and v are the width and height of the message, m_{kl} is the pixel value of message at coordinates (k, l), and m^{*}_{kl} is the pixel value of the extracted message at coordinates (k, l).

5.1.3 Parameters considered

The implementation is done using MATLAB 2014, and the performance of the proposed technique is compared with the existing methods, such as random order-based embedding, sequential order-based embedding, and the existing work given in Ref. [22]. In random order-based embedding, embedding locations are

randomly selected and the sequential order-based method embeds the message by scanning the cover image sequentially.

5.2 Experimental Results

The experimental results of the proposed steganographic technique are presented in this section. Figure 3A shows the first cover image taken for embedding, and Figure 3B shows the message data. Then, the original image is given for the embedding process. The embedded image is shown in Figure 3C, and the extracted message is given in Figure 3D. Figure 4A shows the second cover image taken for embedding, and Figure 4B shows the message data of the second image. The embedded image of the second one is shown in Figure 4C, and the extracted message is given in Figure 4D. Figure 5 shows the intermediate results of mammogram image 3. Here, Figure 5A shows the original cover image and Figure 5B shows the message. The embedded image is given in Figure 5C, and the extracted message is given in Figure 5D. Similarly, Figure 6A shows the original cover image 4, and Figure 6B shows the message. Figure 6C shows the embedded image, and the extracted message is given in Figure 6D.

Figure 7 shows the quantitative results of the four methods for the two images. From Figure 7A, we understand that the random order-based technique obtains the PSNR value of 59.4 dB and the sequential order-based technique obtains the PSNR value of 59.6 dB. The proposed method obtains 61.1 dB as PSNR for image 1. This shows that the proposed technique obtains the maximum PSNR as compared with the existing technique. When image 2 is given as input, the clustering modification directions (CMD) technique obtains the value of 59.2 dB and the random order-based technique obtains the value of 59.4 dB, but the proposed technique obtains the value of 59.6 dB. When image 3 is given as input, the proposed method obtains the PSNR value of 72.5 dB and the existing random order-based technique obtains the PSNR value of 62.5 dB. Similarly,

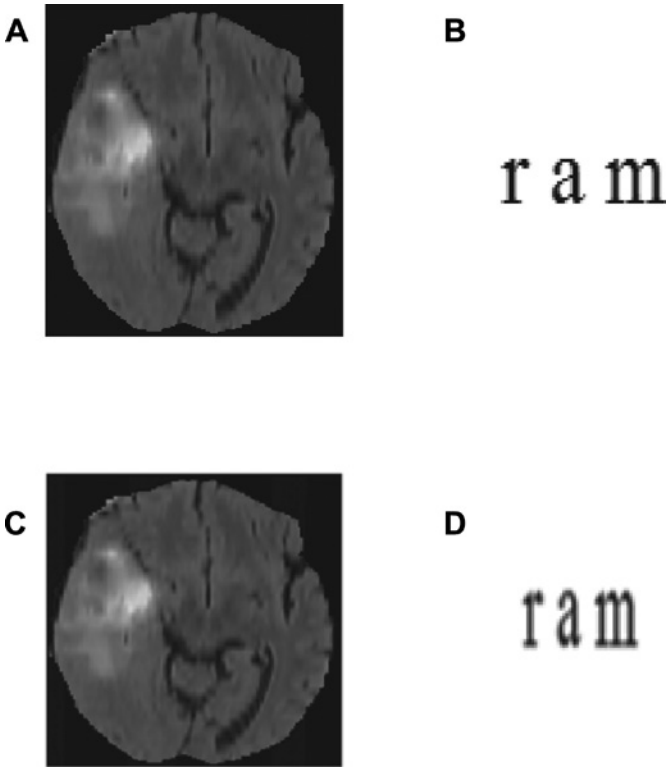

Figure 3: Intermediate Results of Image 1.
(A) Original cover image. (B) Message. (C) Embedded image. (D) Extracted message.

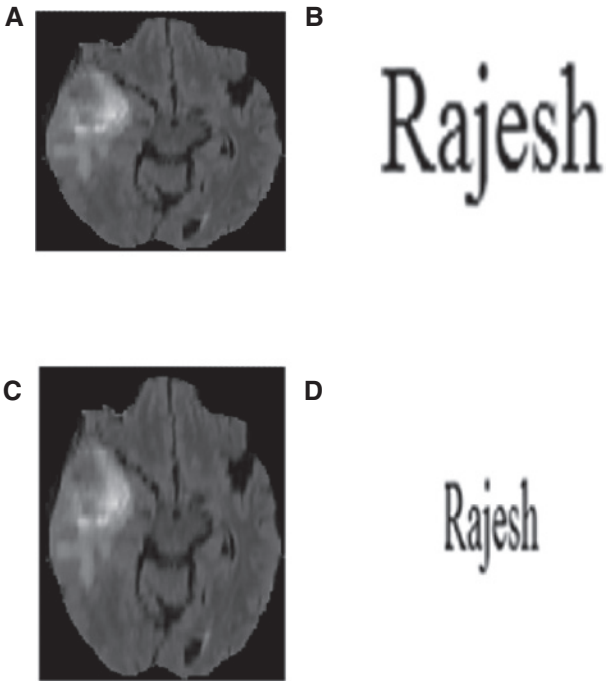

Figure 4: Intermediate Results of Image 2.
(A) Original cover image. (B) Message. (C) Embedded image. (D) Extracted message.

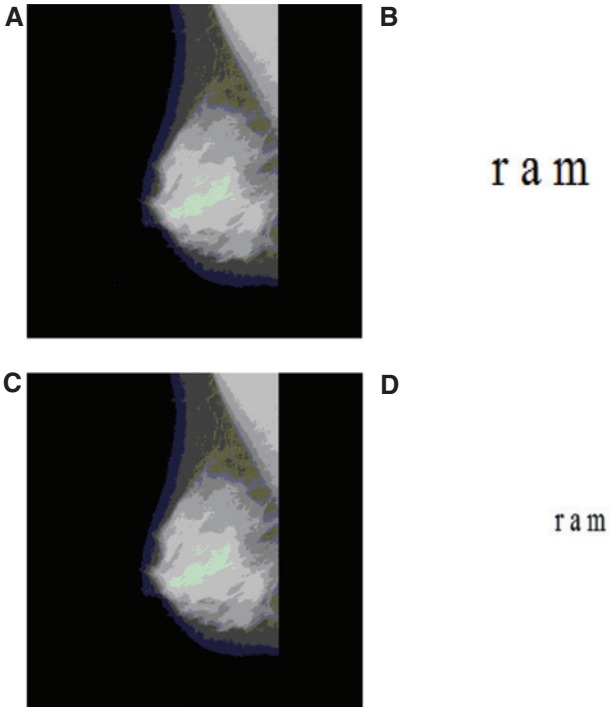

Figure 5: Intermediate Results of Image 3.
(A) Original cover image. (B) Message. (C) Embedded image. (D) Extracted message.

a PSNR value of 72.74 dB is obtained for the proposed algorithm in image 4. Figure 7B shows the performance of the methods using MSE in four images considered for the experimentation. From the graph, we understand that the MSE of four methods is 0, which ensures that all the methods are correctly extracting the message

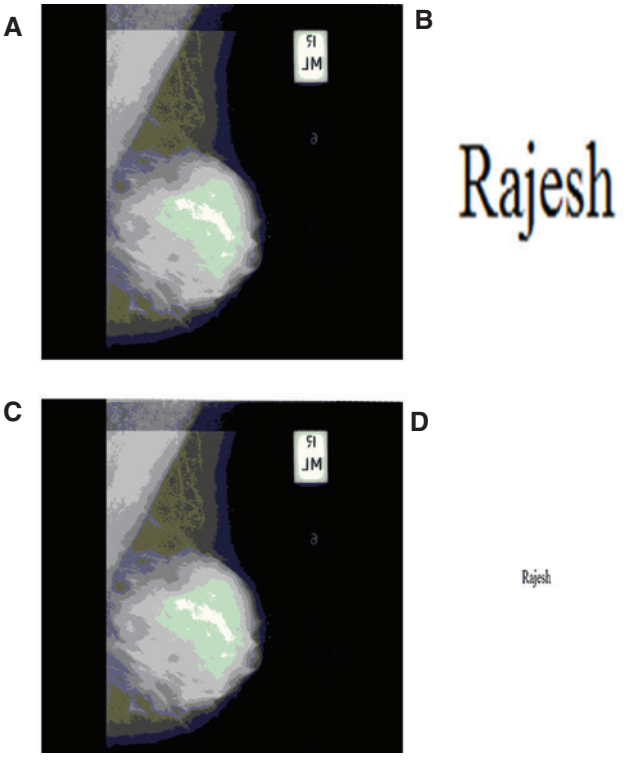

Figure 6: Intermediate Results of Image 4.
(A) Original cover image. (B) Message. (C) Embedded image. (D) Extracted message.

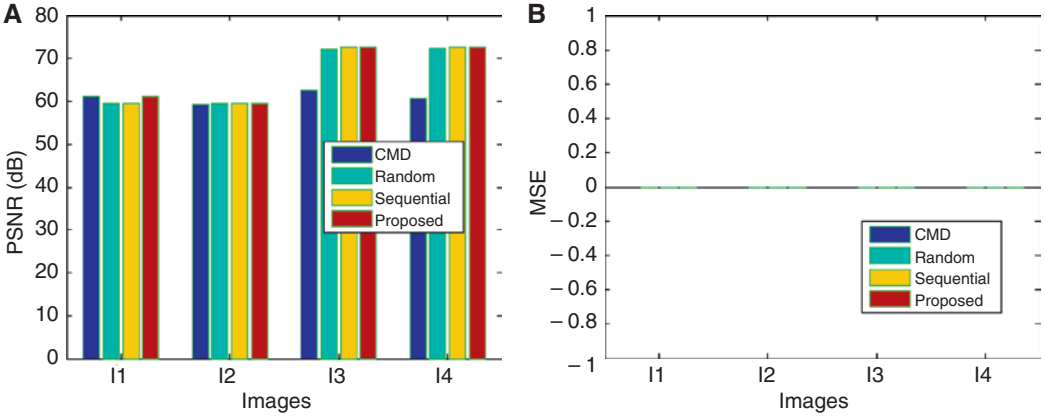

Figure 7: Quantitative Results.
(A) PSNR. (B) MSE.

information. Overall, even though all the methods show similar performance in terms of MSE, the proposed technique outperforms the other methods in showing the better visual quality for the embedded image.

5.3 Attack Analysis

This section shows the attack analysis of the four methods to ensure the robustness of the methods. In order to analyze the robustness of the methods, the embedded image is applied with different attacks, like filtering, noise, and contrast enhancement, and then the message is extracted from the attacked images.

– Filtering attack
  Figure 8 shows the performance of the methods after applying a filtering attack. Here, Gaussian filtering is used for the filtering attack. Figure 8A shows the performance of the extraction process. Here, filter size is varied from 2 to 6, and the results are analyzed. For the filter size of 2, the CMD, random order, sequential order, and proposed technique obtain the MSE of 5.9E4, 0.65E4, 1.4E4, and 0.42E4, respectively. Also, for the filter size of 6, the proposed technique obtains MSE of 0.47E4, which is lesser than that of the existing methods. Figure 8B shows the performance of the methods for image 2. When the size of the filter is increased, MSE is also increased. For the filter size of 6, the proposed technique obtains 0.65E4, which is lesser than that of the existing methods.
– Noisy attack
  Figure 9 shows the attack analysis of the methods using noisy information. Here, we utilized salt and pepper noise for the robustness analysis. The graph given in Figure 9A is plotted by varying the density of the noise from 0.05 to 0.09 for image 1. For the density of noise of 0.05, the proposed technique obtains the value of 0.05E4, which is lesser than that of the CMD technique. The CMD technique obtains the value of 5.9E4. For the density of 0.09, the CMD technique, random order, sequential order, and proposed

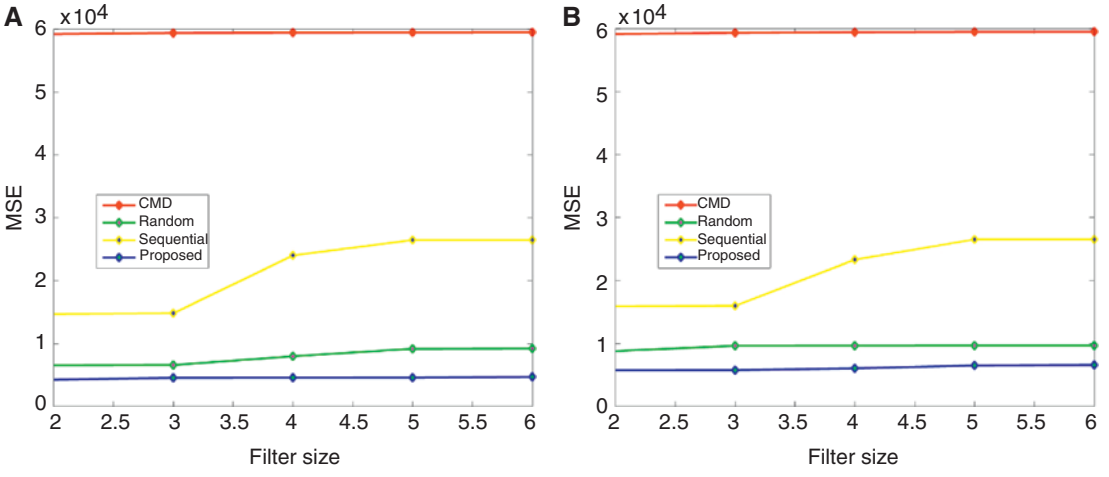

Figure 8: MSE after Filtering Attack.
(A) Image 1. (B) Image 2.

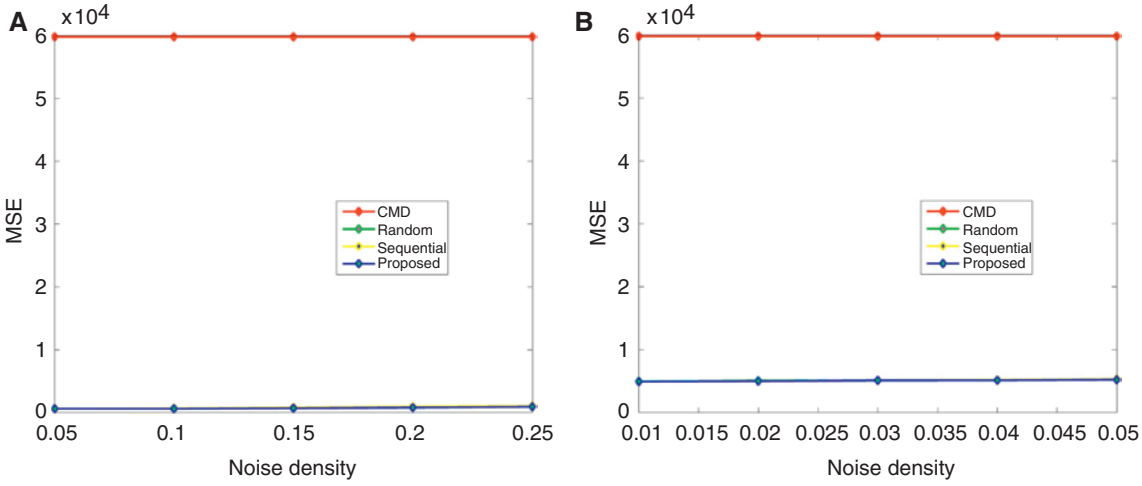

Figure 9: MSE after Noise Attack.
(A) Image 1. (B) Image 2.

technique obtain the value of 5.98E4, 0.08E4, 0.1E4, and 0.08E4, respectively. Here, random order, sequential order, and proposed technique almost behave similarly. Figure 9B shows the MSE of the four methods for image 2. From Figure 9B, we ensured that the random order, sequential order, and proposed technique show almost similar performance. For example, they obtain the MSE value of 5.9E4, 0.51E4, 0.53E4, and 0.52E4, respectively.

- Histogram attack

  Figure 10 shows the performance of the extraction process using MSE after performing histogram equalization. Here, the embedded image is directly applied to the histogram equalization procedure and the resultant is used to extract the message. Here, hgram is varied from 250 to 254. When we increase the hgram from lowest to highest, the MSE of all the methods is also increased. For the hgram of 250, the proposed technique obtains the value of 0.43E4, which is lesser than that of the CMD technique. The CMD technique obtains the value of 3.4E4. For the hgram of 254, the CMD technique, random order, sequential order, and proposed technique obtain the value of 3.68E4, 4.7E4, 2.4E4, and 0.46E4, respectively. This shows that the proposed techniques obtain the maximum PSNR as compared with the existing technique. When image 2 is given as input, the CMD technique obtains the value of 3.7E4 and the random order-based technique obtains the value of 3.3E4, but the proposed technique obtains the value of 0.62E4. This ensures that the proposed technique obtains the better performance in both the images than the existing methods.
- Motion attack

  Figure 11 shows the robustness analysis of the four methods against the motion attack. Here, motion blurring is applied on embedded image and the extraction is performed from the attacked embedded image for extracting the secret message. Here, the performance is varied for various lengths of blurring parameters. Figure 11A shows the MSE of image 1 after applying blurring attack. From the results, we proved that the proposed method obtained the MSE of 4.8E4, which is less than that of the existing random order-based technique, which obtained the MSE value of 1.6E5. For the higher blurring length, the proposed method obtained the MSE value of 6.8E4, which is also less than that of the existing method. Similarly, the performance analysis of the proposed method with the existing method for image 2 is given in Figure 11B. From Figure 11B, we ensure that the proposed method obtained the MSE value of 7.1E4 for higher blurring length. This is far better than the existing random order-based technique, which obtained the MSE value of 1.61E5. The same kind of performance analysis for image 3 and image 4 is given in Figure 11C and D. These graphs also clearly prove that the performance is better for the proposed technique than for the existing methods.

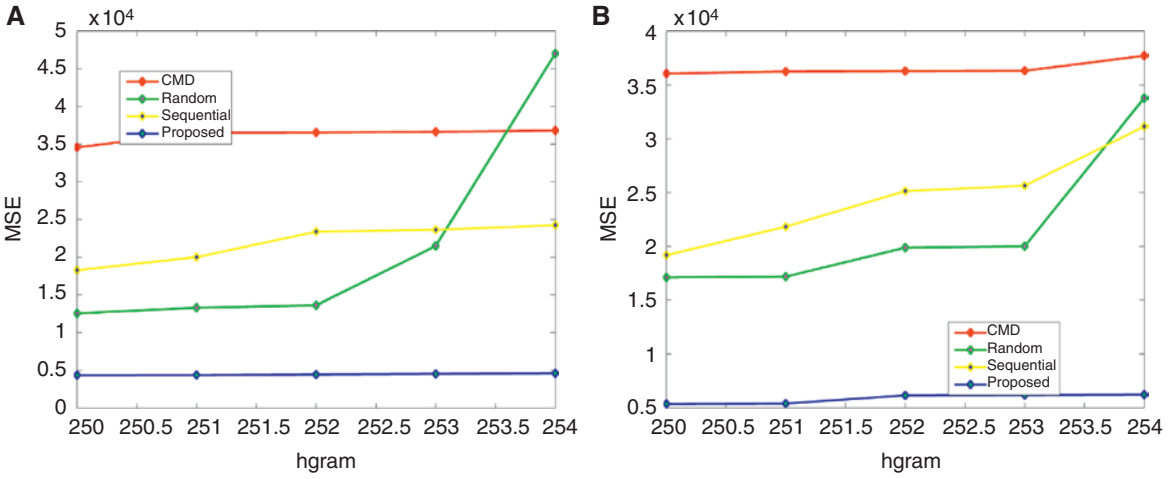

Figure 10: MSE after Equalization Attack.
(A) Image 1. (B) Image 2.

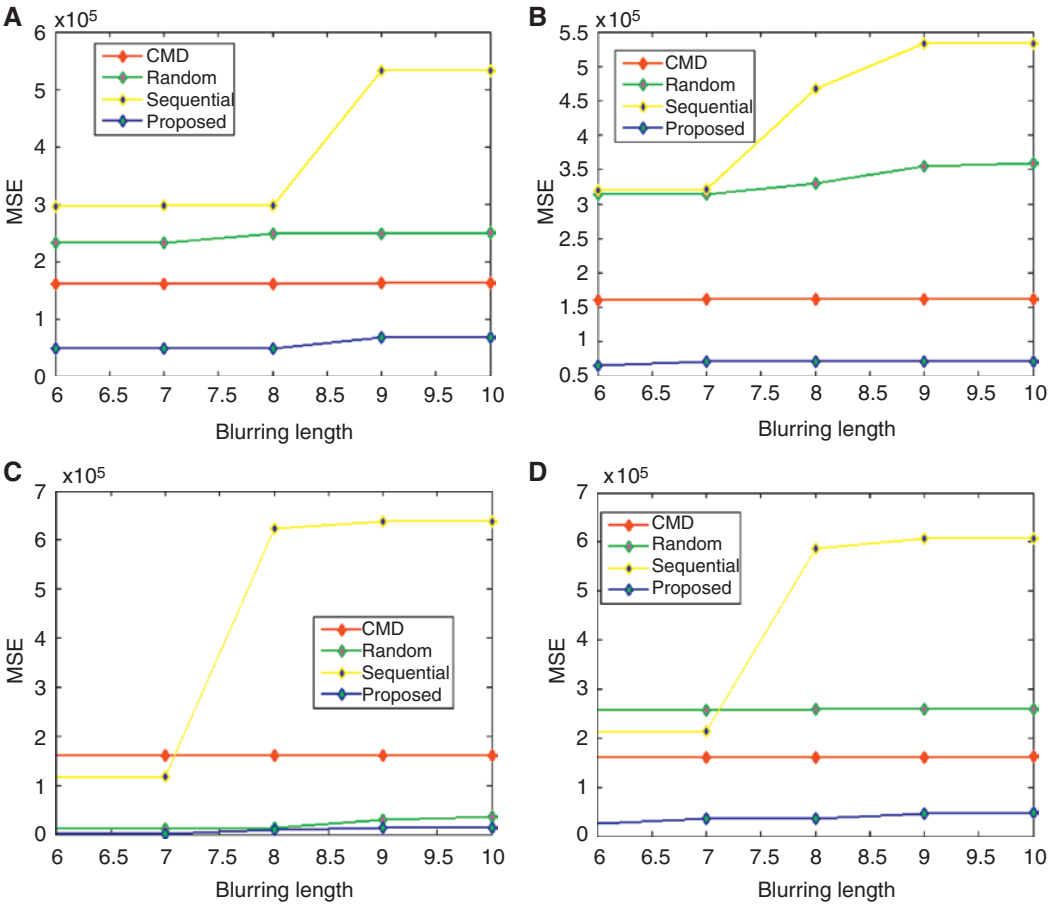

Figure 11: MSE after Motion Attack.
(A) Image 1. (B) Image 2. (C) Image 3. (D) Image 4.

5.4 Comparative Analysis

Table 2 shows the comparative analysis of the proposed method with the reported results available in Ref. [5]. This table discusses the performance in terms of comparative parameters like image modality, embedding domain, embedding technique, secret data, embedding rate, and image quality. From the table, the embedding rate is analyzed with various parameters. Through the bit rate comparison, the proposed method ensures that the maximum capability of the proposed method is 32,512 bits, which is higher than that by Memon and Gilani [24], who obtained the maximum capacity of 23,184 bits. In terms of image quality, the proposed method outperformed all the existing methods by reaching the maximum PSNR of 72.7 dB.

6 Conclusion

In this paper, we have developed a steganographic technique using three important steps, such as cost estimation, embedding, and extraction. In the proposed cost estimation process, a new mathematical model was developed to find the cost of every pixel. This new cost function utilized multiple parameters like wavelet coefficient, edge transformation, and pixel intensity to identify the good location to embed the message data. Then, estimated cost matrix based on every pixel is used to embed the message data within the cover image. Finally, modular operation is utilized to extract the message data from the embedded image. For the experimentation, two magnetic resonance brain images are taken and the results are analyzed using PSNR and

Table 2: Comparative Analysis.

Method	Image modality	Embedding domain	Embedding technique	Secret data	Embedding rate	Image quality
Zhou et al. [39]	Mammography image (IM)	Spatial	LSB of random pixels	Patient's data, digital signature	6720 bits	–
Chao et al. [11]	Hospital mark image	DCT	LSB	EPR, ECG, digital signature	–	33.47–42.62 dB
Navas et al. [29]	MRI	IWT	LSB	EPR	3400 characters	44 dB
Hajjaji et al. [17]	IRM echo graphics	Spatial	LSB	Patient's data, medical diagnostic	1700 bits	35–60 dB
Nagaraju and ParthaSarathy [28]	CT, MRI, US	Spatial	2-LSB	ECG, patient's information	0.04–0.97%	70–40 dB
Rahimi and Rabbani [31]	CT, MRI	SVD, contourlet transform	New method	Patient's data, signature, watermark	2010 bits	52.2 dB
Lou et al. [23]	–	Spatial	Difference expansion	–	Up to 134,898 bits	21.59–48.86 dB
Memon et al. [25]	CT, MRI, X-ray, US	IWT	New hybrid	Patient's data, doctor's code, LSB of ROI	32 char doctor's code, 96 char patient's info, 1st LSB plane ROI	58.44–60.94 dB
Memon and Gilani [24]	CT	Spatial	LSB	Patient's data, message, hospital logo, authentication code	3528–23,184 bits	63.98–55.6 dB
Qershi and Khoo [6]	US	DWT	Difference expansion	Patient's data, hash ROI, ROI embedding, map	10 KB	41.25 dB
Proposed method	MRI and mammogram	Spatial	Multiple criteria-based cost function	Patient's data	8100 bits	61.1–72.7 dB

MSE. The robustness analysis ensured that the proposed steganographic technique outperforms the existing methods by reaching the maximum PSNR of 61.16 dB. In the future, the proposed cost estimation procedure can be improved with the recent optimization algorithms.

Bibliography

[1] S. Ahani and S. Ghaemmaghami, Colour image steganography method based on sparse representation, *IET Image Process.* **9** (2015), 496–505.

[2] A. N. Akansu, W. A. Serdijn and I. W. Selesnick, Wavelet transforms in signal processing: a review of emerging applications, *Phys. Commun.* **3** (2010), 1–18.

[3] H. Al-Dmour and A. Al-Ani, Quality optimized medical image steganography based on edge detection and Hamming code, in: *Proceedings of 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI)*, pp. 1486–1489, 2015.

[4] H. Al-Dmour and A. Al-Ani, A steganography embedding method based on edge identification and XOR coding, *Expert Syst. Appl.* **46** (2016), 293–306.

[5] H. Al-Dmour and A. Al-Ani, Quality optimized medical image information hiding algorithm that employs edge detection and data coding, *Comput. Methods Progr. Biomed.* **127** (2016), 24–43.

[6] O. M. Al-Qershi and B. E. Khoo, High capacity data hiding schemes for medical images based on difference expansion, *J. Syst. Softw.* **84** (2011), 105–112.

[7] D. Baby, J. Thomas, G. Augustine, E. George and N. R. Michael, A novel DWT based image securing method using steganography, in: *International Conference on Information and Communication Technologies, Procedia Computer Science*, pp. 612–618, 2015.

[8] R. Böhme, *Improved statistical steganalysis using models of heterogeneous cover signals*, PhD dissertation, Faculty Comput. Sci., Tech. Univ. Dresden, Dresden, Germany, 2008.

[9] R. Böhme, *Advanced statistical steganalysis*, Springer-Verlag, Berlin, 2010.

[10] J. Canny, A computational approach to edge detection, *IEEE Trans. Pattern Anal. Mach. Intell.* **8** (1986), 679–698.

[11] H. M. Chao, C. M. Hsu and S. G. Miaou, A data-hiding technique with authentication, integration, and confidentiality for electronic patient records, *IEEE Trans. Inform. Technol. Biomed.* **6** (2002), 46–53.

[12] S. Das and M. K. Kundu, Effective management of medical information through ROI-lossless fragile image watermarking technique, *Comput. Methods Progr. Biomed.* **111** (2013), 662–675.

[13] N. N. El-Emam and M. Al-Diabat, A novel algorithm for colour image steganography using a new intelligent technique based on three phases, *Appl. Soft Comput.* **37** (2015), 830–846.

[14] T. Filler and J. Fridrich, Gibbs construction in steganography, *IEEE Trans. Inform. Forensics Security* **5** (2010), 705–720.

[15] T. Filler, J. Judas and J. Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, *IEEE Trans. Inform. Forensics Security* **6** (2011), 920–935.

[16] L. Guo, J. Ni, W. Su, C. Tang and Y. Q. Shi, Using statistical image model for JPEG steganography: uniform embedding revisited, *IEEE Trans. Inform. Forensics Security* **10** (2015), 2669–2680.

[17] M. A. Hajjaji, A. Mtibaa and E. B. Bourennane, A watermarking of medical image: method based 'LSB', *J. Emerging Trends Comput. Inform. Sci.* **2** (2011), 714–721.

[18] V. Holub and J. Fridrich, Universal distortion function for steganography in an arbitrary domain, *EURASIP J. Inform. Security*, December 2014.

[19] J. Hu and T. Li, Reversible steganography using extended image interpolation technique, *Comput. Elect. Eng.* **46** (2015), 447–455.

[20] R. Karakış, İ. Güler, İ. Çapraz and E. Bilir, A novel fuzzy logic-based image steganography method to ensure medical data security, *Comput. Biol. Med.* **67** (2015), 172–183.

[21] H. K. Lee, H. J. Kim, S. G. Kwon and J. K. Lee, ROI medical image watermarking using DWT and bit-plane, in: *2005 Asia Pacific Conference on Communications*, IEEE, pp. 512–515, 2005.

[22] B. Li, M. Wang, X. Li, S. Tan and J. Huang, A strategy of clustering modification directions in spatial image steganography, *IEEE Trans. Inform. Forensics Security* **10** (2015), 1905–1917.

[23] D. C. Lou, M. C. Hu and J. L. Liu, Multiple layer data hiding scheme for medical images, *Comput. Standards Interfaces* **31** (2009), 329–335.

[24] N. A. Memon and S. A. M. Gilani, Watermarking of chest CT scan medical images for content authentication, *Int. J. Comput. Math.* **88** (2011), 265–280.

[25] N. A. Memon, A. Chaudhry, M. Ahmad and Z. A. Keerio, Hybrid watermarking of medical images for ROI authentication and recovery, *Int. J. Comput. Math.* **88** (2011), 2057–2071.

[26] B. H. Menze, A. Jakab, S. Bauer, J. Kalpathy-Cramer, K. Farahani, J. Kirby, Y. Burren, N. Porz, J. Slotboom, R. Wiest, L. Lanczi, E. Gerstner, M. A. Weber, T. Arbel, B. B. Avants, N. Ayache, P. Buendia, D. L. Collins, N. Cordier, J. J. Corso, A. Criminisi, T.

Das, H. Delingette, Ç. Demiralp, C. R. Durst, M. Dojat, S. Doyle, J. Festa, F. Forbes, E. Geremia, B. Glocker, P. Golland, X. Guo, A. Hamamci, K. M. Iftekharuddin, R. Jena, N. M. John, E. Konukoglu, D. Lashkari, J. A. Mariz, R. Meier, S. Pereira, D. Precup, S. J. Price, T. R. Raviv, S. M. Reza, M. Ryan, D. Sarikaya, L. Schwartz, H. C. Shin, J. Shotton, C. A. Silva, N. Sousa, N. K. Subbanna, G. Szekely, T. J. Taylor, O. M. Thomas, N. J. Tustison, G. Unal, F. Vasseur, M. Wintermark, D. H. Ye, L. Zhao, B. Zhao, D. Zikic, M. Prastawa, M. Reyes and K. Van Leemput, The multimodal brain tumor image segmentation benchmark (BRATS), *IEEE Trans. Med. Imaging* **34** (2015), 1993–2024.

[27] MIAS database, Available from http://atc.udg.edu/~aoliver/publications/tesi/node64.html, Accessed 5 Month, 2015.

[28] C. Nagaraju and S. ParthaSarathy, Embedding ECG and patient information in medical image, in: *Recent Advances and Innovations in Engineering (ICRAIE) 2014*, IEEE, pp. 1–6, 2014.

[29] K. Navas, S. A. Thampy and M. Sasikumar, EPR hiding in medical images for telemedicine, *Proc. World Acad. Sci. Eng. Technol.* **2** (2008), 292–295.

[30] H. Nyeem, W. Boles and C. Boyd, A review of medical image watermarking requirements for teleradiology, *J. Digital Imaging* **26** (2013), 326–343.

[31] F. Rahimi and H. Rabbani, A dual adaptive watermarking scheme in contourlet domain for DICOM images, *Biomed. Eng. Online* **10** (2011), 53.

[32] H. Sajedi and M. Jamzad, ContSteg: contourlet-based steganography method, *J. Wirel. Sens. Netw.* **1** (2009), 163–170.

[33] V. Sedighi, R. Cogranne and J. Fridrich, Content-adaptive steganography by minimizing statistical detectability, *IEEE Trans. Inform. Forensics Security* **11** (2016), 221–234.

[34] K. S. Shet, Nagaveni and A. R. Aswath. Image steganography using integer wavelet transform based on color space approach, in: *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, Springer International Publishing, 2015.

[35] K. S. Shet, A. R. Aswath, M. C. Hanumantharaju and X. Z. Gao, Design and development of new reconfigurable architectures for LSB/multi-bit image steganography system, *Multimed. Tools Appl.* (2016), 1–23.

[36] S. Sidhik, S. K. Sudheer and V. P. Mahadhevan Pillai, Performance and analysis of high capacity steganography of color images involving wavelet transform, *Optik – Int. J. Light Electron. Optics* **126** (2015), 3755–3760.

[37] M. Tang, S. Zeng, X. Chen, J. Hu and Y. Du, An adaptive image steganography using AMBTC compression and interpolation technique, *Optik – Int. J. Light Electron Optics* **127** (2016), 471–477.

[38] P. Tsai, Histogram-based reversible data hiding for vector quantisation-compressed images, *IET Image Process.* **3** (2009), 100–114.

[39] X. Zhou, H. Huang and S. L. Lou, Authenticity and integrity of digital mammography images, *IEEE Trans. Medical Imaging* **20** (2001), 784–791.