



An improved separable reversible patient data hiding algorithm for E-healthcare

Rupali Bhardwaj¹

Received: 2 June 2020 / Revised: 7 August 2020 / Accepted: 22 December 2020 /

Published online: 4 May 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC part of Springer Nature 2021

Abstract

In the telemedicine industry, a standout among the most significant issue is the exchange of Electronic Patient Information (EPI) between patient and a doctor that are remotely connected. A minute change to EPI may result in a wrong diagnosis for the patient. To ensure secure and safe communication for telemedicine applications, a dual-image separable block-based reversible data hiding algorithm in encrypted domain for embedding secret message in *base5* numeral framework is proposed here. The proposed scheme has not been suffering from underflow and overflow problem so that empowering it to embed and recover information precisely from low-intensity pixels too. This property makes our proposed methodology truly reasonable for its utilization on medical images. To prove the effectiveness of our proposed approach, experiments have been performed on different test images. The average PSNR value is 54.10 dB for an embedding capacity of 327,680 bits for all test images which demonstrates that the method is capable of giving good quality stego images even at high payload also. The experimental study revealed that for all types of test images, the proposed methodology altogether beaten all the compared methodologies in its ability to embed secret message and precisely recover it by maintaining the visual quality of stego images too.

Keywords Electronic Patient Information (EPI) · Separable reversible data hiding · Pixel geometry · Bit error rate

1 Introduction

Today, the Internet has turned out to be one of the significant part of our daily life. The telemedicine framework is considered as connecting objects to the Internet and utilizing that association for remote checking. The telemedicine industry is renewing the conventional healthcare system by improving efficiency, bringing down expenses, and set the consideration back on better patient care. Telemedicine has offered to ascend to E- healthcare

✉ Rupali Bhardwaj
rupali.bhardwaj@thapar.edu

¹ Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab, India

and its focus is on improving the healthcare framework. In the current scenario, a standout amongst the most significant issue is the exchange of Electronic Patient Information (EPI) between patient and a doctor that are remotely connected. A minute change to EPI may result in a wrong diagnosis for the patient. In this way, a protected and effective transmission of such information is required in the telemedicine framework. Even though Internet security protocol (IPsec), is a well-utilized for giving security to exchanged information, yet it has been provided to have lesser throughput. So that, utilization of such an algorithm for resource-constrained telemedicine framework would not yield better outcomes. In such type of scenario, researchers have been looking out for alternative approaches to secure the EPI in a progressively effective manner. Data hiding is the most robust tool that can address the security, authentication and copyright protection of the patient data issues. Various data hiding techniques are applied to protect data integrity and through these techniques, one can ensure data reliability. Sometimes, during the data hiding process, receiver is not able to reconstructed cover image successfully while in few applications, for example, medical, military, and law crime scene investigation, loss of cover image is not permitted. In these cases, an extraordinary sort of data hiding strategy called reversible or lossless data hiding is utilized. Reversible data hiding meant to embed the secret message in cover image in such a way that at receiver end, secret message as well as original cover image is recovered successfully. Encryption is the most promising solution to maintain confidentiality and privacy of data. The integration of encryption and RDH technologies plays an important role in privacy protection of data.

2 Literature review

There is a lot of research done in reversible data hiding domain; some are illustrated as follows—Firstly, the idea of hiding information from attackers was presented by Shi [22]. Afterward, difference expansion based reversible data hiding technique was proposed by Tian [25], where a single bit was embedded between two close-by pixels through difference computation. Ni et al. [16] had given a scheme where a secret message is embedded at the histogram's peak point of cover image. Afterward, Bo et al. [27] had given a method where cover image is segmented into equal-sized blocks and each block's histogram embedded secret message in it. M. Celik et al. [5] depicted a steganographic methodology for compressed cover image pixels. Qian et al. [21] exhibited a separable reversible data hiding algorithm where cover image is encrypted through block cipher algorithm. In this paper [29], firstly segmented cover image into equal-sized blocks, and after that, each block is further subdivided into two sub-blocks where one bit of secret message is embedded in it. The secret message is extracted through the computation of fluctuation function corresponding to each block. But during the computation of fluctuation function, boundary pixels are to be excluded which results in high bit error rate value. Wu and Sun [26] exhibited a method where blocks are further segmented into two sub-blocks. Embeddable pixel's neighbors are not selected for data embedding which results in high peak-signal-to-noise-ratio(PSNR) value and low bit error rate respectively. Hong et al. [8] included boundary pixels during computation of fluctuation function which results in the same PSNR value and low bit error rate value as compare to Zhang [29]. In this paper [9] segmented cover image into equal-sized blocks and after that, each block is further subdivided into two sub-blocks where one bit of secret message is embedded in it using the concept of lattice. Embeddable pixel's four-connectivity neighbors are not selected for data embedding which results in high PSNR value and low bit error rate value. Ma et al. [14] proposed a reversible data

hiding method before encryption of cover image. Liao and Changwen [11] improved computation of fluctuation function through calculating mean difference of neighboring pixels. Paillier cryptosystem [17] cryptosystem is utilized for encryption of cover image in Chen et al. [6] where one bit of secret message is embedded per pixel pair. Tai and Chang [24] proposed a separable reversible data hiding algorithm where embedding space is reserved before encryption of cover image. Puech et al. [20] proposed a method of the local standard deviation of the encrypted image for the extraction of hidden data during decryption phase. Bhardwaj and Aggarwal [4] introduced a reversible data hiding algorithm in encrypted domain where n secret bits are embedded per block by segmenting them into n sub-blocks. The drawback of this method is that for small block size, secret message is not extracted correctly which result in a high bit error rate. Lu et al. [12] had given a method where dual stego images are generated by folded secret message centrally. Yao et al. [28] described a dual-image method based on pixel co-ordinate system which results in minimum distortion of pixel's coordinate value. Lee and Huang [10] presented a method where dual stego images are generated through orientation combination of pixel coordinates. Here, binary secret message by changed over it into *base5* numeral framework is embedded which results in improved embedding rate. Chi et al. [7] presented a dynamic encoding scheme where frequent occurrence of secret digits is encoded as the minimum absolute digit. The favored stance denotes that for the same embedding rate, the proposed method gave a higher PSNR than existing methods. Lu et al. [13] proposed a frequency encoding method to eliminate the disadvantage of Lu et al. [12] strategy.

Shiu et al. [23] employed a reversible scheme for preservation of patient information in ECG signals through error correcting-coding method where $(n - m)$ bits of secret message are embedded into n number of signals with the help of (n, m) hamming code successfully. Parah et al. [18] presented a reversible data hiding scheme for embedding patient information in medical images where cover image is interpolated through Pixel to Block (PTB) conversion method to guarantee reversibility of medical images. A high capacity reversible data hiding method which is capable of tamper detection of patient information at receiver end has been presented in this paper [19]. Bhalero et al. [3] embedded patient data in ECG signals using a prediction error expansion scheme where prediction of the sample values is performed through deep neural network respectively. Mansour et al. [15] proposed a highly robust reversible data hiding method in encrypted domain where patient data is hidden in medical images with the help of Discrete Ripplet Transformation technique successfully. The most significant commitment of proposed work is to employ adaptive genetic algorithm for optimal pixel adjustment process that enhances embedding capacity as well as imperceptibility features also. Abdulla et al. [2] proposed a dual phase efficient steganography method to enhance stego image visual quality and undetectability of secret message. During first phase, secret message is losslessly compressed to reduce the number of embedding bits and in second phase reduced size secret message is embedded in the cover image through Fibonacci-based mapping scheme respectively. The advantage of this method is to improve the visual quality of stego image by embedding the compressed secret message in the cover image through Fibonacci-based mapping scheme.

A detailed review of the stated work [4, 8, 9, 11, 29] reveals that reporting schemes have low embedding capacity and they does not even support content authentication of patient data also. The motivation of this work is to present a separable reversible data hiding algorithm which is capable of content authentication for E-healthcare applications. This paper presents an enhanced dual-image separable reversible data hiding algorithm in encrypted domain to embed electronic patient information by changed over it into *base5* numeral framework respectively. In addition to embedding EPI, it also adds a fragile watermark for

authentication of EPI at receiver end. Any type of attack during transmission process, results in non-recovery of embedded watermark at receiver end that conveys that the EPI has been transformed during transmission process. The key features of the proposed algorithm are summarized as follows:

- Least pixel repetition (LPR) method is used for interpolation instead of conventional ones to avoid underflow and overflow problem during data embedding in scaled-up image.
- Pixel geometry is used instead of conventional data hiding techniques for embedding of EPI in *base5* numeral framework to improve the embedding capacity.
- Fragile watermark is used for content authentication at the receiver end.

The remaining paper is organized as follows. Section 3 described proposed algorithm in detail. Further, discussions are conducted in Section 4 for comparison of embedding performance and reversibility nature of proposed algorithm with the compared algorithms. At last, Section 5 concluded the paper.

3 Proposed algorithm

Nowadays, patient data privacy and security is one of the most significant challenge for telemedicine applications. Consider a scenario where patient's data is sent to doctor/surgeon; the hacker may observe the healthcare information. Later, an attacker may float this information on social sites and this action may put tremendous threats to the patient's confidentiality. The appropriate encryption and authentication schemes can be useful to prevent these types of attacks. The proposed method demonstrated a block-based dual-image separable reversible data hiding algorithm to embed electronic patient information by changed over it into *base5* numeral framework which is based on pixel geometry (Fig. 1). Firstly, cover image of size $M \times N$ is scaled-up to a $(M + \frac{M}{2}) \times (N + \frac{N}{2})$ image by using the method of Least Pixel Repetition (LPR) which is based on simple arithmetic and is discussed in detail in Section 3.1.

Data embedding algorithm is discussed in detail in Section 3.2 while as data extraction and Image recovery algorithm is discussed in detail in Section 3.3.

3.1 Least Pixel Repetition (LPR)

To facilitate reversibility and carry out data embedding based on pixel geometry, the original image is subjected to LPR method. The two main key points that need to be kept in mind while carrying out LPR process are given as follows:

- Least pixel value is minimal pixel value from 2×2 block.
- Average of scaled-up block is very close to original block's average.
- pixels of block are segmented into two types—seed pixels (corner pixels) and non-seed pixels (non corner pixels) whereas non-seed pixels should have different values.

Algorithm 1 Least Pixel Repetition method.

Input: Cover grey scale image (CI) of size $M \times N$

Output: Scaled-up image (IOI) of size $(M + \frac{M}{2}) \times (N + \frac{N}{2})$

- 1: Firstly, cover image is segmented into 2×2 blocks which is scaled-up into a block size of 3×3 through LPR method whereas pixels are segmented into two types—seed pixels (corner pixels) and non-seed pixels (non corner pixels) and non-seed pixels should have different values.
- 2: Let $CI'_{x,y}$ represent least pixel value of 2×2 block of input image (CI) and $IOI_{x,y}$ is center non-seed pixel of resultant image (Fig. 2). Generation process of 3×3 block corresponding to 2×2 block of cover image using LPR method is explained by the given equation:

$$\begin{cases} IOI_{x-1,y-1} = CI_{x-1,y-1} \\ IOI_{x-1,y} = CI'_{x,y} \\ IOI_{x-1,y+1} = CI_{x-1,y+1} \\ IOI_{x,y-1} = CI'_{x,y} + 1 \\ IOI_{x,y} = CI'_{x,y} + 2 \\ IOI_{x,y+1} = CI'_{x,y} + 3 \\ IOI_{x+1,y-1} = CI_{x+1,y-1} \\ IOI_{x+1,y} = CI'_{x,y} + 4 \\ IOI_{x+1,y+1} = CI_{x+1,y+1} \end{cases} \quad (1)$$

- 3: The generation of 3×3 block using LPR method given in (1) is valid only for the least seed pixel value ($CI'_{x,y}$), where $0 \leq CI'_{x,y} \leq 251$. For other values of $CI'_{x,y}$, where $252 \leq CI'_{x,y} \leq 255$, following equation is used for generation of 3×3 block corresponding to 2×2 block of cover image using LPR method:

$$\begin{cases} IOI_{x-1,y-1} = CI_{x-1,y-1} \\ IOI_{x-1,y} = CI'_{x,y} \\ IOI_{x-1,y+1} = CI_{x-1,y+1} \\ IOI_{x,y-1} = CI'_{x,y} - 1 \\ IOI_{x,y} = CI'_{x,y} - 2 \\ IOI_{x,y+1} = CI'_{x,y} - 3 \\ IOI_{x+1,y-1} = CI_{x+1,y-1} \\ IOI_{x+1,y} = CI'_{x,y} - 4 \\ IOI_{x+1,y+1} = CI_{x+1,y+1} \end{cases} \quad (2)$$

- 4: Similarly, each 2×2 block of cover image CI is scaled up through Least Pixel Repetition process.
- 5: Lastly, scaled-up output image IOI can be reconstructed block-by-block, as follows-

$$IOI = IOI_1 || IOI_2 || \dots || IOI_r \quad (3)$$

Here, symbol $||$ represents block concatenation respectively.

It is apparent from Fig. 3 that seed pixels are original cover image pixels and these are not used for data embedding purpose. Figures 4, 5 and 6 demonstrates the visual quality of various original and corresponding scaled-up images. Figure 6 demonstrated the iterations of 4-connectivity respectively.

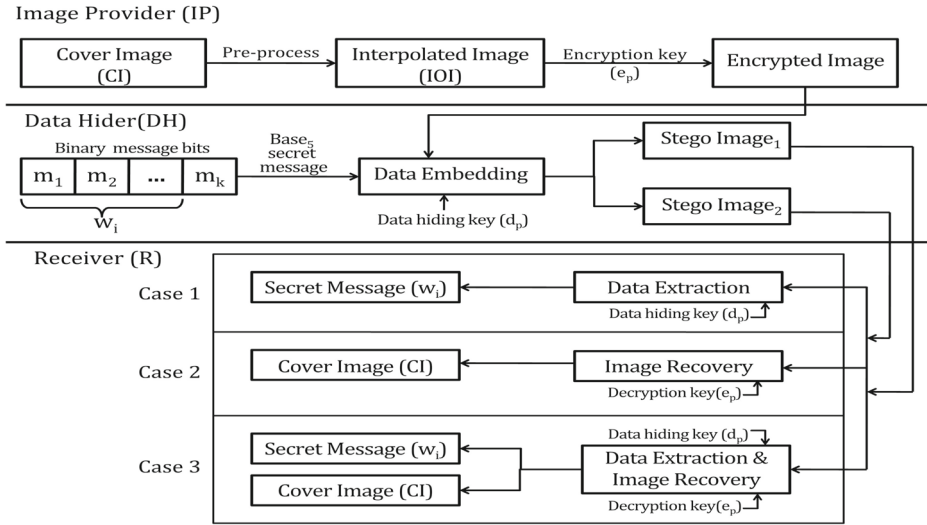


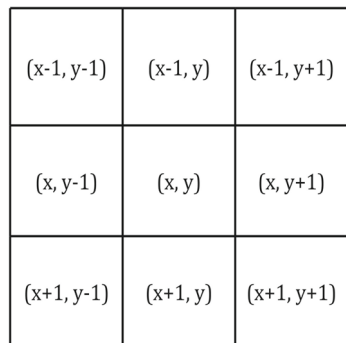
Fig. 1 Proposed algorithm

3.2 Data embedding phase

Before data embedding, proposed algorithm changes over binary secret message into a succession of digits in $base_5$ numeral framework. For dual $base_5$ numeral framework, maximum value is $4 \times 5^1 + 4 \times 5^0 = (24)_{10}$. Assumed, a secret message S_i is changed over into a binary sequence BS , which is traversed from left to right as follows:-

- If $(bs_{n+1})_{10} \in [16, 17 \dots 23, 24]$ then $bs_i = bs_{n+1}$ bits, otherwise $bs_i = bs_n$ bits where $n = 4$ bits and bs_n or bs_{n+1} is the succession of n or $n + 1$ bits from the binary sequence BS .
- Now convert binary secret message bs_i into two continuous digits $w_1 w_2$ of $base_5$ numeral framework which are embedded into non-seed center pixel $S_{x,y}$ or $S'_{x,y}$ of encrypted dual stego images as per pixel geometry respectively.

Fig. 2 Pixel geometry



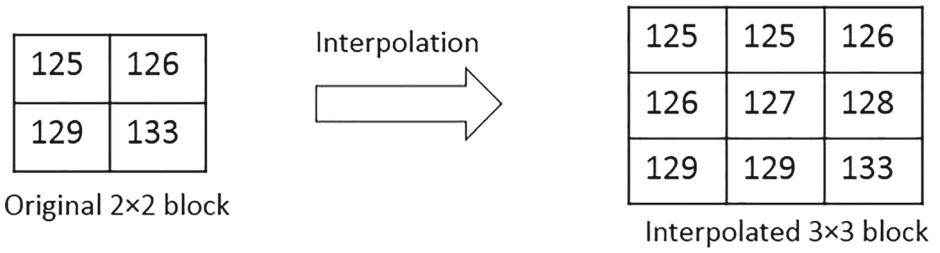


Fig. 3 Least pixel repetition method



Fig. 4 Original test images



Fig. 5 Scaled-up test images

Algorithm 2 Image encryption and data embedding.

Input: Scaled-up original image (*IOI*) of size $(M + \frac{M}{2}) \times (N + \frac{N}{2})$, secret message in *base5* numeral framework, encryption key (e_p) and data hiding key (d_p).

Output: Dual stego (and encrypted) images (*SI* & *SI'*) of size $(M + \frac{M}{2}) \times (N + \frac{N}{2})$.

1: Consider a grey scale scaled-up original image *IOI* of size $(M + \frac{M}{2}) \times (N + \frac{N}{2})$, which is encrypted using symmetric cryptosystem where eight bit encryption key (e_p) is generated by random seed. Exclusive-OR operation is performed (bit by bit) between encryption key and scaled-up original cover image pixels.

2: Now, encrypted scaled-up image, *Encr[IOI]* is divided into a block size of 3×3 as described in Section 3.1, where data embedding is carried out only in center non-seed pixel while no embedding is done in seed pixels to facilitate reversibility. For center non-seed pixel, consider 4-connectivity into clock wise direction for generation of pixel geometry based data embedding rules respectively (Fig. 6). Data is embedded only in center non-seed pixel which is replaced by non-seed pixel value corresponding to non-seed pixel geometry designated through *base5* based secret message (w_1w_2) through consideration of (Table 1).

For example, embed $(24)_5$ into 3×3 encrypted scaled-up block to generate dual stego blocks as follows-

$$\left\{ \begin{array}{l} SI_{x-1,y-1}, SI'_{x-1,y-1} = Encr[IOI_{x-1,y-1}] \\ SI_{x-1,y}, SI'_{x-1,y} = Encr[IOI_{x-1,y}] \\ SI_{x-1,y+1}, SI'_{x-1,y+1} = Encr[IOI_{x-1,y+1}] \\ SI_{x,y-1}, SI'_{x,y-1} = Encr[IOI_{x,y-1}] \\ SI_{x,y} = Encr[IOI_{x-1,y}] \\ SI'_{x,y} = Encr[IOI_{x,y}] \\ SI_{x,y+1}, SI'_{x,y+1} = Encr[IOI_{x,y+1}] \\ SI_{x+1,y-1}, SI'_{x+1,y-1} = Encr[IOI_{x+1,y-1}] \\ SI_{x+1,y}, SI'_{x+1,y} = Encr[IOI_{x+1,y}] \\ SI_{x+1,y+1}, SI'_{x+1,y+1} = Encr[IOI_{x+1,y+1}] \end{array} \right. \tag{4}$$

where $SI_{x,y}$ and $SI'_{x,y}$ is center pixel of a 3×3 block of dual stego (and encrypted) images respectively. Similarly, according to data hiding key d_p , secret message (w_1w_2) in *base5* numeral framework is embedded throughout the encrypted scaled-up image (*Encr[IOI]*).

3: Lastly, stego image can be reconstructed block-by-block as follows-

$$\begin{aligned} SI &= SI_1 || SI_2 || \dots || SI_r \\ SI' &= SI'_1 || SI'_2 || \dots || SI'_r \end{aligned} \tag{5}$$

Here, symbol || represents block concatenation respectively.

3.3 Data extraction and image recovery phase

During this phase, a decryption key and a data hiding key is required according to different cases. As presented in Fig. 1, three cases are to be considered at receiver side. In proposed algorithm, receiver with only the data hiding key can extract the secret message without



Fig. 6 Iterations of 4-connectivity into clock wise direction

having any knowledge of cover image. If the receiver has only decryption key, it can recoup original cover image without extraction of secret message. When the receiver has both the data hiding key and the decryption key, it is conceivable to extract the secret message and recuperate original cover image without any error. First of all, dual stego images are divided into a block size of 3×3 . The process of extraction of secret message in $base_5$ numeral framework and recovery of the original cover image is shown in Algorithm 3.

Table 1 Pixel geometry based data embedding

$base_5$ numeral framework	Center pixel value ($SI_{x,y}$) in $stego_image_1$	Center pixel value ($SI'_{x,y}$) in $stego_image_2$
00	(x, y)	(x, y)
01	(x, y)	$(x, y - 1)$
02	(x, y)	$(x - 1, y)$
03	(x, y)	$(x, y + 1)$
04	(x, y)	$(x + 1, y)$
10	$(x, y - 1)$	$(x, y - 1)$
11	$(x, y - 1)$	$(x - 1, y)$
12	$(x, y - 1)$	$(x, y + 1)$
13	$(x, y - 1)$	$(x + 1, y)$
14	$(x, y - 1)$	(x, y)
20	$(x - 1, y)$	$(x - 1, y)$
21	$(x - 1, y)$	$(x, y + 1)$
22	$(x - 1, y)$	$(x + 1, y)$
23	$(x - 1, y)$	$(x, y - 1)$
24	$(x - 1, y)$	(x, y)
30	$(x, y + 1)$	$(x, y + 1)$
31	$(x, y + 1)$	$(x + 1, y)$
32	$(x, y + 1)$	$(x, y - 1)$
33	$(x, y + 1)$	$(x - 1, y)$
34	$(x, y + 1)$	(x, y)
40	$(x + 1, y)$	$(x + 1, y)$
41	$(x + 1, y)$	$(x, y - 1)$
42	$(x + 1, y)$	$(x - 1, y)$
43	$(x + 1, y)$	$(x, y + 1)$
44	$(x + 1, y)$	(x, y)

Algorithm 3 Data extraction and image recovery.

Input: Dual stego (and encrypted) images (SI & SI') of size $(M + \frac{M}{2}) \times (N + \frac{N}{2})$, decryption key (e_p) and data hiding key (d_p)

Output: Cover image (CI) of size $M \times N$, secret message in *base5* numeral framework

Case1 :

1: If the receiver has only the data hiding key, the receiver can extract the secret message without being aware of the original image content. For each 3×3 block, assumed $P_{x,y} = Z_{x,y}$ or $Z'_{x,y}$ where $Z_{x,y} = SI_{x,y}$ or $Z'_{x,y} = SI'_{x,y}$ is center non-seed pixel of 3×3 block of dual stego (and encrypted) images respectively.

```

a: for each  $P_{x,y}$  do
b:   if ( $P_{x,y} = P_{x-1,y}$ ) then
c:     return ( $x - 1, y$ )
d:   else if ( $P_{x,y} = P_{x,y+1}$ ) then
e:     return ( $x, y + 1$ )
f:   else if ( $P_{x,y} = P_{x+1,y}$ ) then
g:     return ( $x + 1, y$ )
h:   else if ( $P_{x,y} = P_{x,y-1}$ ) then
i:     return ( $x, y - 1$ )
j:   else
k:     return ( $x, y$ )
l:   end if
m: end for
    
```

2: After retrieving non-seed pixel co-ordinate value corresponding to center non-seed pixel $P_{x,y}$ for each 3×3 block in dual stego images, secret message in *base5* numeral framework is extracted through consideration of Table 1 with the help of data hiding key (d_p).

Case2:

If the receiver has only the decryption key, the receiver can decrypt the encrypted blocks for recovery of cover image from seed pixels only without knowing the secret message.

1: Decrypt the dual encrypted stego images using the decryption key (e_p) to obtain decrypted dual stego images, $Decr[SI]$ and $Decr[SI']$.

2: Now recover original 2×2 block from decrypted 3×3 block for $Decr[SI]$ as follows-

$$\begin{cases}
 RI_{i,j} & = Decr[SI]_{x-1,y-1} \\
 RI_{i,j+1} & = Decr[SI]_{x-1,y+1} \\
 RI_{i+1,j} & = Decr[SI]_{x+1,y-1} \\
 RI_{i+1,j+1} & = Decr[SI]_{x+1,y+1}
 \end{cases} \tag{6}$$

$\forall i, j ((i \bmod 2 = 1) \ \& \ (j \bmod 2 = 1))$

Repeat above procedure for each 3×3 block of $Decr[SI]$ to recover original 2×2 block of cover image CI .

3: Lastly, original cover image CI can be reconstructed block-by-block, as follows-

$$CI = RI_1 || RI_2 || \dots || RI_r \tag{7}$$

Case3: If the receiver has decryption key and the data hiding key, the receiver can extract the secret message from the decrypted image as well as totally recover the original image by using both the keys, which is a combination of case 1 and case 2 scenario respectively.

Table 2 Example

$$\text{Original } 2 \times 2 \text{ block of cover image CI} = \begin{bmatrix} 123 & 125 \\ 128 & 123 \end{bmatrix}$$

$$\text{Scaled-up } 3 \times 3 \text{ block of cover image CI} = \begin{bmatrix} 123 & 123 & 125 \\ 124 & 125 & 126 \\ 128 & 127 & 123 \end{bmatrix}$$

Encryption key, $e_p = 11111111$

$$\text{Encrypted block} = \begin{bmatrix} 132 & 132 & 130 \\ 131 & 130 & 129 \\ 127 & 128 & 132 \end{bmatrix}$$

Assumed secret message to be embedded is $(10001)_2 = (17)_{10}$ so that, $w_1w_2 = (32)_5$. Data is embedded only in central non-seed pixel which is replaced by non-seed pixel value corresponding to pixel geometry designated through $base_5$ based secret message (w_1w_2) with the help of Table 1. So, for embedding $(32)_5$ according to Table 1, center non-seed pixel values are replaced by pixel values corresponding to $(x, y + 1)$ and $(x, y - 1)$ to produce $stego_block_1$ and $stego_block_2$ respectively.

$$Stego_block_1 = \begin{bmatrix} 132 & 132 & 130 \\ 131 & 129 & 129 \\ 127 & 128 & 132 \end{bmatrix}$$

$$Stego_block_2 = \begin{bmatrix} 132 & 132 & 130 \\ 131 & 131 & 129 \\ 127 & 128 & 132 \end{bmatrix}$$

At receiver end firstly, dual $stego_blocks$ are decrypted with decryption key, $e_p = 11111111$

$$Decrypted_block_1 = \begin{bmatrix} 123 & 123 & 125 \\ 124 & 126 & 126 \\ 128 & 127 & 123 \end{bmatrix}$$

$$Decrypted_block_2 = \begin{bmatrix} 123 & 123 & 125 \\ 124 & 124 & 126 \\ 128 & 127 & 123 \end{bmatrix}$$

Only center pixel (P_{xy}) in decrypted $block_1$ and decrypted $block_2$ carry hidden message. Center pixel in decrypted $block_1$ and decrypted $block_2$ has pixel values corresponding to pixel coordinates $(x, y + 1)$ and $(x, y - 1)$. It is clear with the help of Table 1 (redesigned by receiver according to pixel geometry in clockwise direction) that corresponding to $(x, y + 1)$ and $(x, y - 1)$, secret message value is $(32)_5 = (17)_{10} = (10001)_2$.

Original block is reconstructed through scaled-up block by considering only corner seed pixels of it.

Reconstructed original 2×2 block of cover image

$$CI = \begin{bmatrix} 123 & 125 \\ 128 & 123 \end{bmatrix}$$

Example: The execution of proposed algorithm on sample block value is shown in Table 2.

4 Result and discussion

Here, we examine the performance of the proposed method which is evaluated using metrics like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Embedding Capacity

(bits) and Bit Error Rate (BER) respectively. PSNR is used to evaluate the quality of stego images while BER is used to evaluate the error between embedded and extracted watermark (Abdulla et al. [1]). The experimental study is performed on test images of size 512×512 as shown in Fig. 7 respectively.

Let $f(x, y)$ and $\hat{f}(x, y)$ denote the value of pixel (x, y) in the cover and stego image of size $(M + \frac{M}{2}) \times (N + \frac{N}{2})$ and sm and sm' is embedded and extracted watermark, where $A \times B$ is the size of the watermark.

These metrics are defined as follows -

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{8}$$

where

$$MSE = \frac{1}{(M + \frac{M}{2}) \times (N + \frac{N}{2})} \sum_{x=1}^{(M+\frac{M}{2})} \sum_{y=1}^{(N+\frac{N}{2})} (f(x, y) - \hat{f}(x, y))^2$$

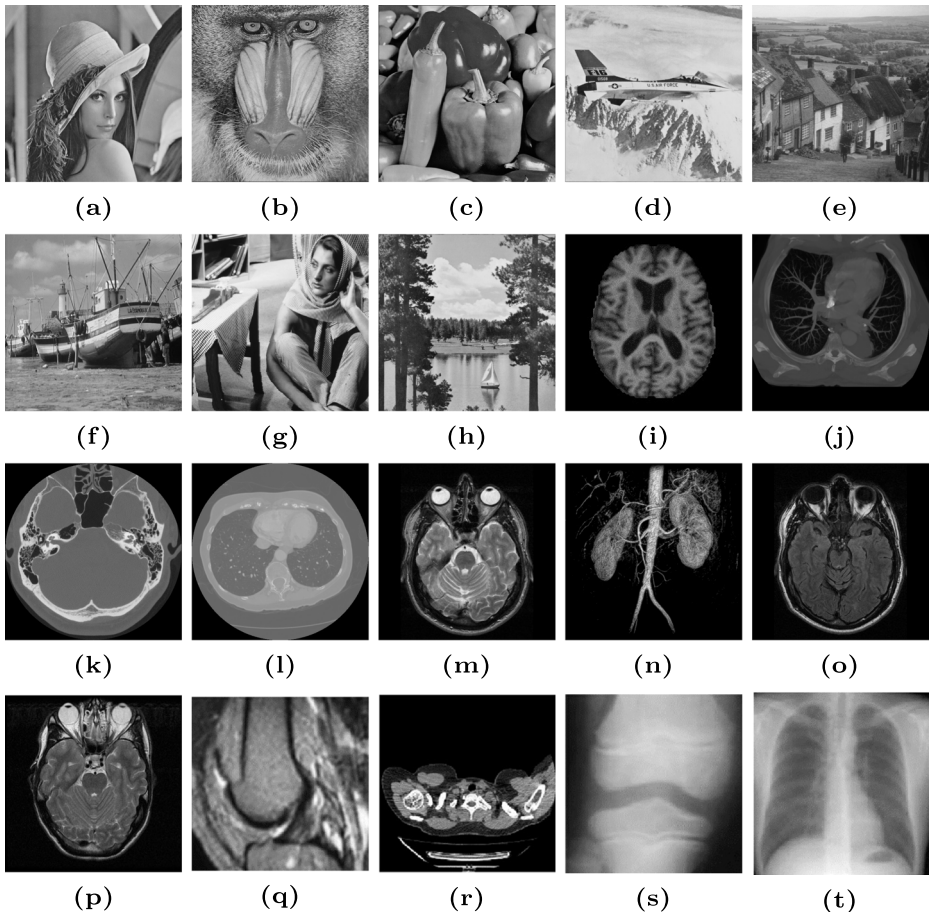


Fig. 7 Test images

Table 3 Comparative study of proposed method

Test images	Parameters	Method					
		Zhang [29]	Hong et al. [8]	Young-Sik et al. [9]	Liao et al. [11]	Bhardwaj et al. [4] ($n = 2$)	Proposed algorithm
<i>Lena</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0	0	0	0	0	0
	PSNR of stego image (dB)	37.92	37.94	40.94	37.95	40.61	54.10
<i>Baboon</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.0078	0.0039	0.0039	0.0039	0.0175	0
	PSNR of stego image (dB)	37.91	37.93	40.93	37.91	40.59	54.10
<i>Pepper</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0	0	0	0	0.2695	0
	PSNR of stego image (dB)	37.95	37.92	40.94	37.94	40.66	54.12
<i>F16</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0	0	0	0	0	0
	PSNR of stego image (dB)	37.95	37.94	40.94	37.94	40.66	54.10
<i>Goldhill</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.2617	0.2031	0.0156	0.2656	0.0156	0
	PSNR of stego image (dB)	38.60	38.60	41.56	38.55	41.54	54.10
<i>Sailboat</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0	0	0	0	0.1757	0
	PSNR of stego image (dB)	37.95	37.91	40.22	37.92	40.59	54.11
<i>Barbara</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1718	0.1523	0.0078	0.1562	0.1640	0
	PSNR of stego image (dB)	38.81	38.83	41.87	38.86	40.66	54.11
<i>Boat</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0	0	0	0.0078	0.0640	0
	PSNR of stego image (dB)	37.81	37.83	40.87	37.86	40.60	54.11
<i>Med₁</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1953	0.2421	0.2265	0.1914	0.2949	0
	PSNR of stego image (dB)	35.61	35.60	43.55	35.62	43.91	54.11
<i>Med₂</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.0781	0.0937	0.0703	0.0664	0.2792	0
	PSNR of stego image (dB)	37.35	37.38	42.25	37.30	42.10	54.11
<i>Med₃</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.0937	0.0976	0.0546	0.0859	0.2890	0
	PSNR of stego image (dB)	36.77	36.72	41.87	36.73	41.91	54.10
<i>Med₄</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1289	0.1445	0.0468	0.1484	0.2929	0
	PSNR of stego image (dB)	36.57	36.62	41.60	36.65	41.80	54.11
<i>Med₅</i>	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1289	0.1289	0.0390	0.1210	0.2832	0
	PSNR of stego image (dB)	36.97	37.00	42.42	36.98	42.84	54.11

Table 3 (continued)

Test images	Parameters	Method					
		Zhang [29]	Hong et al. [8]	Young-Sik et al. [9]	Liao et al. [11]	Bhardwaj et al. [4] ($n = 2$)	Proposed algorithm
Med_6	Cover Image	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.3867	0.5273	0.1992	0.3750	0.3398	0
	PSNR of stego image (dB)	35.26	35.27	42.53	35.24	43.79	54.10
Med_7	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1406	0.0976	0.0585	0.1132	0.2832	0
	PSNR of stego image (dB)	36.88	36.90	45.65	36.91	42.70	54.11
Med_8	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1243	0.1824	0.1615	0.1214	0.2695	0
	PSNR of stego image (dB)	37.95	37.95	41.37	37.89	41.54	54.10
Med_9	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.0406	0.0776	0.0385	0.1232	0.2882	0
	PSNR of stego image (dB)	35.95	35.95	40.37	35.89	40.54	54.11
Med_{10}	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.0837	0.0867	0.0564	0.0895	0.1695	0
	PSNR of stego image (dB)	36.82	36.83	40.17	36.80	41.54	54.11
Med_{11}	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.0718	0.0973	0.0730	0.0646	0.1495	0
	PSNR of stego image (dB)	37.75	37.75	41.17	37.89	41.44	54.10
Med_{12}	Embedding capacity (bits)	65,536	65,536	65,536	65,536	131,072	327,680
	Bit Error rate (BER)	0.1198	0.1454	0.0486	0.1448	0.2085	0
	PSNR of stego image (dB)	37.95	37.95	41.37	37.89	41.54	54.10

$$BER = \frac{\sum_{i=1}^A \sum_{j=1}^B (sm(i, j) \oplus sm'(i, j)) \times 100}{\text{Count_of_embedded_bits}} \quad (9)$$

4.1 Imperceptibility analysis

Here, we examine the performance of the proposed scheme and compare it with the existing state-of-the-art algorithms of Zhang [29], Hong et al. [8], Young-Sik et al. [9], Liao et al. [11] and Bhardwaj et al. [4] respectively. Table 3 demonstrates the examination of the proposed algorithm with all other compared algorithms regarding embedding capacity, bit error rate, and the PSNR value attained on random test images, exhibited in Fig. 7 respectively. Proposed algorithm embedded binary secret message by changed over it into *bases* numeral framework to produce dual stego images simultaneously. Embedding capacity and PSNR value are reciprocal to each other, with the increase in embedding capacity there is an inherent loss of PSNR value respectively. Even then, the PSNR values obtained by the proposed approach are superior to those obtained by compared methods. It is noted from Fig. 8 that even at high payloads, the proposed method gave high-quality stego image while compared schemes did not because their decreased embedding rates can't work at high payloads. It

is visible from Fig. 9 that for the proposed algorithm with $block_size = 3 \times 3$, maximum embedding capacity is 327,680 bits, bit error rate is zero and PSNR is 54.10 dB(approx.) for all test images which is far better than other compared algorithms. Indeed, even as far as PSNR values, the visual quality of the stego image produced by the proposed method is at par with all the compared methods. The proposed scheme has not been suffering from underflow and overflow problem so that empowering it to embed and recover information precisely from low-intensity pixels too. This property makes our proposed methodology truly reasonable for its utilization on medical images. In this manner it very well may be

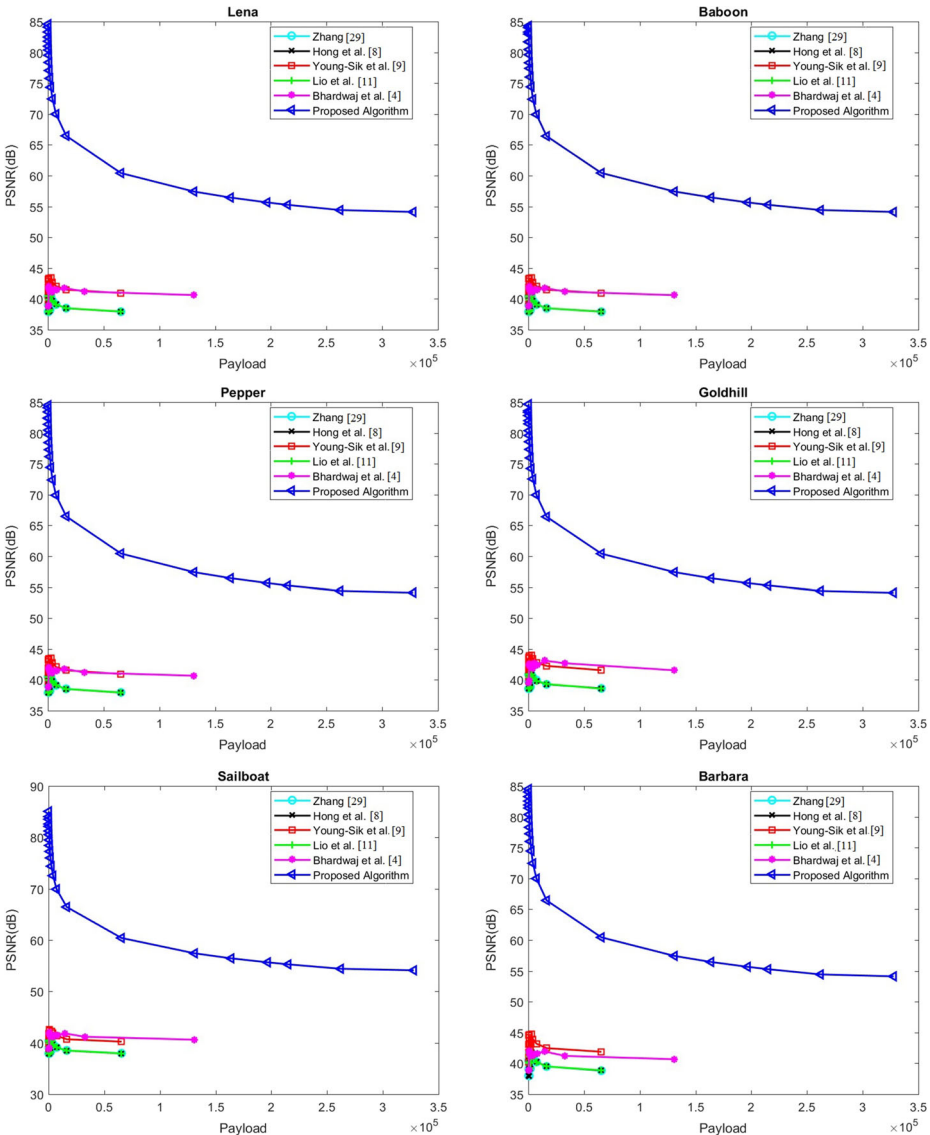


Fig. 8 PSNR value comparison against different payload on test images

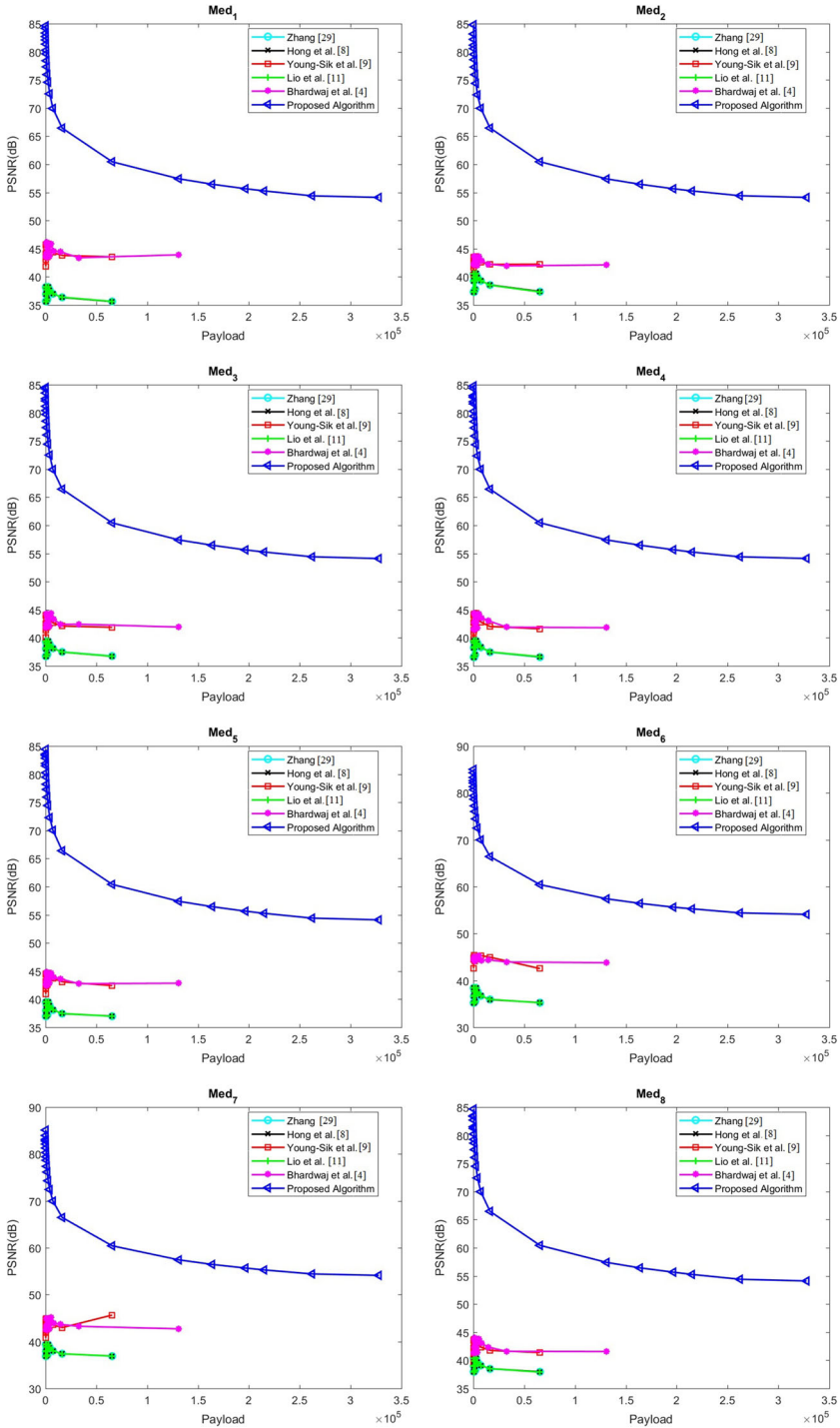


Fig. 8 (continued)

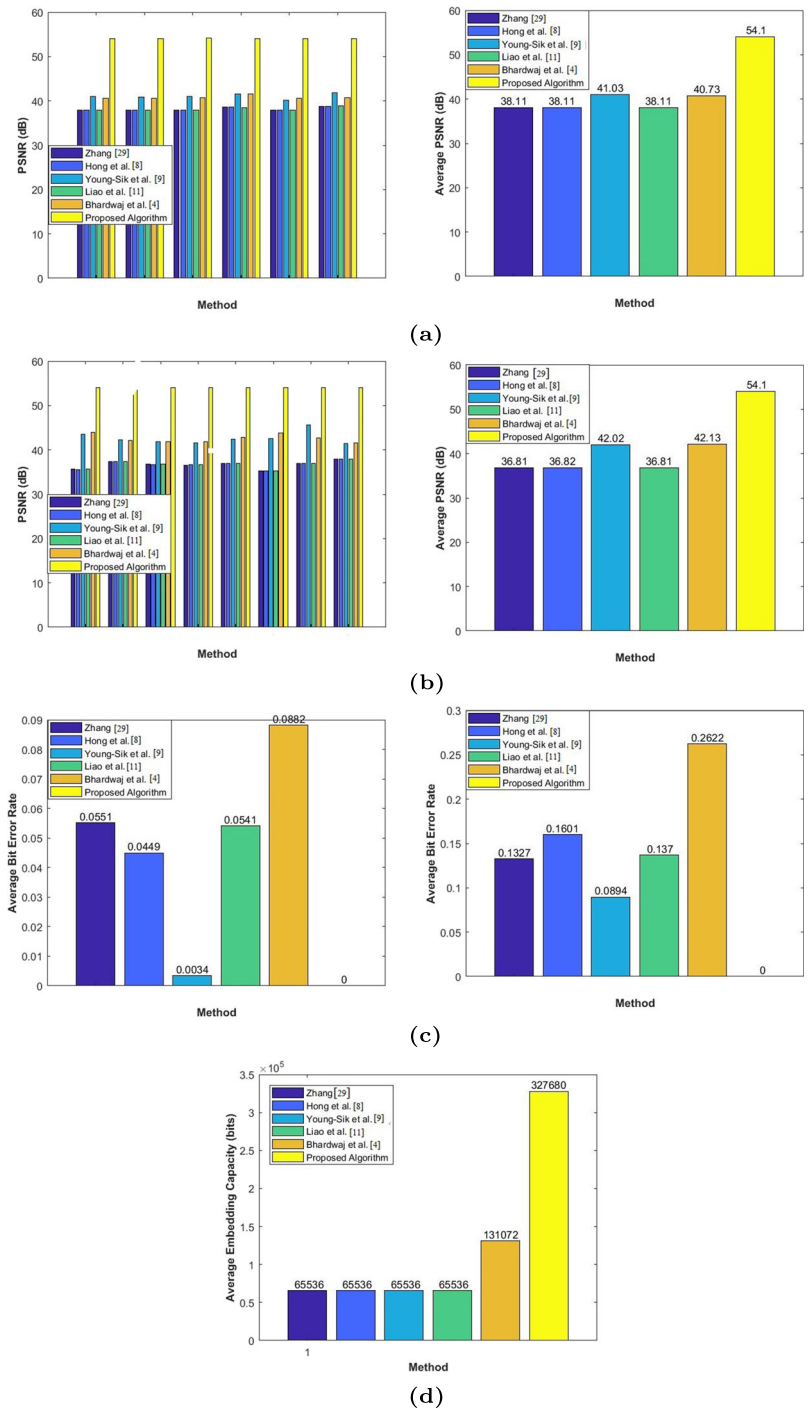


Fig. 9 Comparative study of proposed method

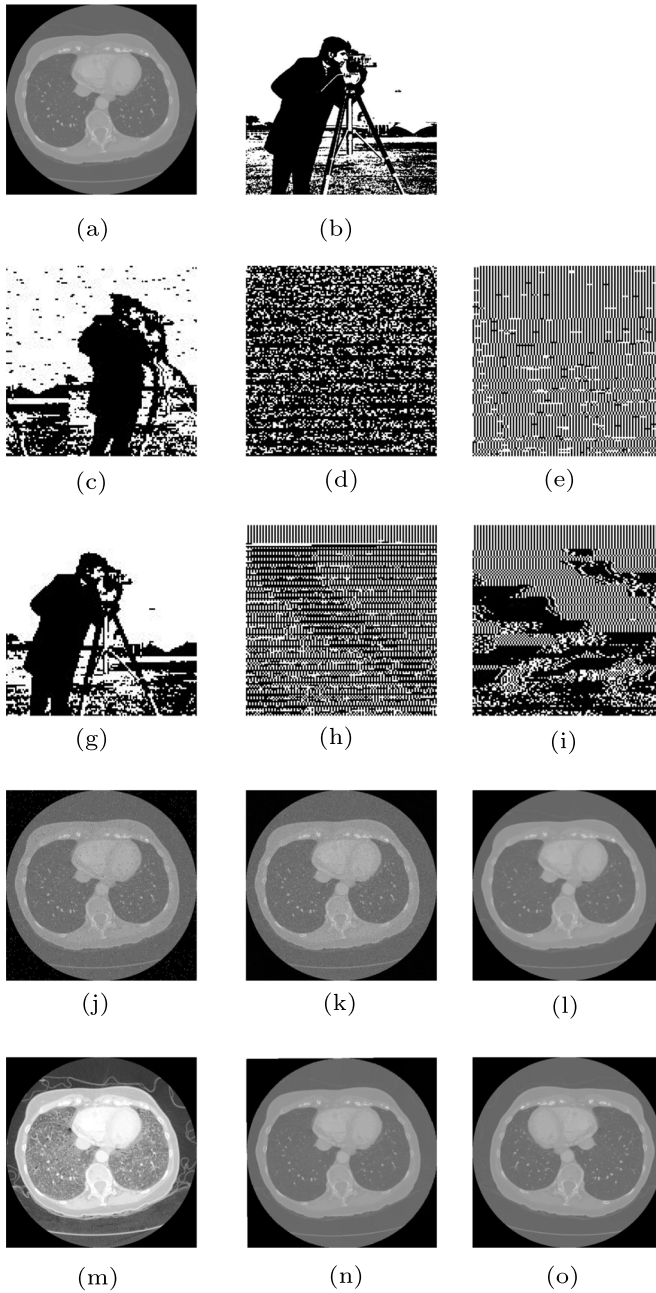


Fig. 10 Image quality under different type of attacks

inferred that, on all types of test images, the proposed methodology altogether beaten all the compared methodologies in its ability to embed secret information and precisely recover it by maintaining the visual nature of stego images too.













4.2 Security and robustness analysis

To evaluate the performance of proposed scheme for its hidden message authentication, we subject stego image to popular image processing attacks. It is appropriate to mention here that the proposed algorithm is fragile in nature as a secret message is embedded in spatial domain. The authentication analysis is aimed to calculate the degree of degradation in secret message due to a predefined attack which has been evaluated in terms of Bit error rate respectively. We had given example of some popular image processing attacks on *Med₄*(512 × 512) cover image with binary Cameraman (128 × 128) data embedding (Fig. 10). From the outcomes for different attacks, referenced in Fig. 10, it is clear that the proposed strategy is highly fragile to all the attacks except histogram equalization attack carried on different stego images. Bit error rate value is around 0-52% which concluded that recovered secret message in most of the cases is not recognizable, hence indicated that stego image has been attacked during transmission. High Bit Error Rates for test images, approve the way that the proposed scheme is profoundly fragile, irrespective of the type of cover image.

4.3 Reversibility analysis

At the receiver end, after extraction of the secret message, cover image is also reconstructed through stego image successfully. Table 4 shows reversibility analysis of the proposed method which consists of the original cover image, corresponding recovered image, difference image, and PSNR value between the original and reconstructed cover image in dB. From the outcomes which are referenced in Table 4, it is obvious that the difference image is perfectly black with each pixel intensity equivalent to zero and corresponding PSNR value is ∞ dB thus demonstrative that the proposed scheme is purely reversible in nature. Similarly, all pixel values of the cover image are retrieved and finally, the extraction of secret message

Table 4 Reversibility analysis

	<i>Med₁</i>	<i>Med₄</i>	<i>Med₆</i>	<i>Med₈</i>
Original Image				
Recovered Image				
Difference Image				
PSNR (dB)	∞	∞	∞	∞

and reconstruction of the original cover image is not done successfully at the receiver end. So, it is to be concluded that stego image has been attacked during the transmission process.

5 Conclusion

To ensure secure and safe communications for telemedicine applications, an enhanced separable reversible data hiding scheme in encrypted domain has been presented in this paper where binary secret message by changed over it into *base5* numeral framework is embedded according to pixel geometry to produce dual stego images respectively. The secret message is extracted through the access of dual stego-images simultaneously. The proposed technique has not been suffering from underflow and overflow problem so that empowering it to embed and recover patient information precisely from low-intensity pixels too. Since the proposed algorithm has been carried out in spatial domain so that embedded electronic patient information (EPI) is not robust to various image processing attacks. In future, we need to improve the robustness of the proposed method.

References

1. Abdulla AA (2019) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Doctoral thesis University of Buckingham
2. Abdulla AA, Sellahewa H, Jassim SA (2020) Stego quality enhancement by message size reduction and fibonacci bit-plane mapping. arXiv:2004.12467
3. Bhalerao S, Ansari IA, Kumar A, Jain DK (2019) A reversible and multipurpose ecg data hiding technique for telemedicine applications. *Pattern Recognit Lett* 125:463–473
4. Bhardwaj R, Aggarwal A (2018) An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. *Pattern Recognition Letters* 139(2020):60–68
5. Celik MU, Sharma G, Tekalp AM, Saber E (2005) Lossless generalized-lsb data embedding. *IEEE Trans Image Process* 14:253–13
6. Chen Y-C, Shiu C-W, Horng G (2014) Encrypted signal-based reversible data hiding with public key cryptosystem. *J Visual Commun Image Represent* 25:1164–1166
7. Chi L-P, Wu C-H, Chang H-P (2018) Reversible data hiding in dual stegano-image using an improved center folding strategy. *Multimed Tools Appl* 77:8785–18
8. Hong W, Chen T-S, Wu H-Y (2012) An improved reversible data hiding in encrypted images using side match. *IEEE Signal Process Lett* 19:199–3
9. Kim Y-S, Kang K, Lim D-W (2015) New reversible data hiding scheme for encrypted images using lattices. *Appl Math Inform Sci* 9:2627
10. Lee C-F, Huang Y-L (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommun Syst* 52:2237–10
11. Liao X, Shu C (2015) Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. *J Visual Commun Image Represent* 28:21–26
12. Lu T-C, Wu J-H, Huang C-C (2015) Dual-image-based reversible data hiding method using center folding strategy. *Signal Process* 115:195–18
13. Lu T-C, Chi L-P, Wu C-H, Chang H-P (2017) Reversible data hiding in dual stego-images using frequency-based encoding strategy. *Multimed Tools Appl* 76:23903–26
14. Ma K, Zhang W, Zhao X, Yu N, Li F (2013) Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans Inf Forensics Secur* 8:553–559
15. Mansour RF, Abdelrahim EM (2019) An evolutionary computing enriched rs attack resilient medical image steganography model for telemedicine applications. *Multidimens Syst Signal Process* 30(2):791–814
16. Ni Z, Shi Y-Q, Ansari N, Su W (2006) Reversible data hiding. *IEEE Trans Circ Syst Video Technol* 16:354–358
17. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: *International conference on the theory and applications of cryptographic techniques*. Springer, pp 223–15

18. Parah SA, Ahad F, Sheikh JA, Bhat GM (2017) Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. *J Biomed Inform* 66:214–230
19. Parah SA, Ahad F, Sheikh JA, Loan NA, Bhat GM (2017) A new reversible and high capacity data hiding technique for e-healthcare applications. *Multimed Tools Appl* 76(3):3943–3975
20. Puech W, Chaumont M, Strauss O (2008) A reversible data hiding method for encrypted images. In: *Security, forensics, steganography, and watermarking of multimedia contents X*, vol 6819. International Society for Optics and Photonics, p 68191E
21. Qian Z, Zhang X, Ren Y, Feng G (2016) Block cipher based separable reversible data hiding in encrypted images. *Multimed Tools Appl* 75:13749–17
22. Shi YQ (2004) Reversible data hiding. In: *International workshop on digital watermarking*. Springer, pp 1–12
23. Shiu HJ, Lin B-S, Huang C-H, Chiang P-Y, Lei C-L (2017) Preserving privacy of online digital physiological signals using blind and reversible steganography. *Comput Methods Progr Biomed* 151:159–170
24. Tai W-L, Chang Y-F (2018) Separable reversible data hiding in encrypted signals with public key cryptography. *Symmetry* 10:23
25. Tian J (2003) Reversible data embedding using a difference expansion. *IEEE Trans Circ Syst Video Technol* 13:890–896
26. Wu X, Sun W (2014) High-capacity reversible data hiding in encrypted images by prediction error. *Signal Process* 104:387–13
27. Xiao B, Ying L, Huang Y (2010) Reversible data hiding using histogram shifting in small blocks. In: *2010 IEEE International conference on communications (ICC)*. IEEE, pp 1–6
28. Yao H, Qin C, Tang Z, Tian Y (2017) Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion. *Signal Process* 135:26–29
29. Zhang X (2011) Reversible data hiding in encrypted image. *IEEE Signal Process Lett* 18:255–3

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.