



An improved reversible and secure patient data hiding algorithm for telemedicine applications

Rupali Bhardwaj¹

Received: 4 March 2020 / Accepted: 1 August 2020 / Published online: 31 August 2020
© Springer-Verlag GmbH Germany, part of Springer Nature 2020

Abstract

In the telemedicine framework, a standout among the most significant issues 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, an enhanced reversible data hiding method in the encrypted domain has been presented in this paper. All compared reversible data hiding methods have been seen to show predominant outcomes, yet just on natural images not on medical images because underflow problem may arise in medical images due to a large number of pixels have low-intensity values. Thus, an enhanced reversible data hiding method in the encrypted domain has been introduced here that gives a higher embedding rate than all the looked at reversible data hiding methods by embedding k , ($k \geq 1$) binary bits of a secret message at every pixel of a cover image without any occurrence of underflow and overflow problem. The proposed method 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 method truly reasonable for its utilization on medical images. For all test images, the proposed method altogether beat all the compared methods in its ability to embed secret information and precisely recover it with maintaining the visual quality of stego images too.

Keywords Electronic patient information (EPI) · Privacy protection · Homomorphic encryption · Variable size secret message · Reversible data hiding (RDH)

1 Introduction

The telemedicine framework 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 and its focus is on improving the healthcare framework. In the current scenario, a standout among the most significant issues 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 such type of scenario, researchers have been looking out for alternative approaches to secure the EPI in a progressively effective manner. Data hiding has

been found as an alternative to such type of scenario where steganography and watermarking are the two most common methods for data to hide. Steganography is the art of hiding secret messages into an audio, video, image, or text file to avoid detection whereas secret message is then extracted at its receiver end respectively. 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 manner that at the receiver end, secret message, as well as the cover image, is retrieved successfully.

✉ Rupali Bhardwaj
rupali.bhardwaj@thapar.edu

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

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 (2004). Afterward difference expansion based reversible data hiding technique was proposed by Tian (2003), where a single bit was embedded between two close-by pixels through difference computation. Ni et al. (2006) had given a scheme where the secret message is embedded at the histogram's peak point of the cover image. Afterward, Xiao et al. (2010) had given a method where the cover image is segmented into equal-sized blocks and each block's histogram embedded secret message in it. Celik et al. (2005) depicted a steganographic methodology for compressed cover image pixels. Qian et al. (2016) exhibited a separable reversible data hiding algorithm where the cover image is encrypted through a block cipher algorithm. In this paper (Zhang 2011), 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. Xiaotian and Sun (2014) 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. (2012) 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 (2011). In this paper Kim et al. (2015) 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 a 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. (2013) proposed a reversible data hiding method where embedding space is reserved before encryption of cover image. Liao and Shu (2015) improved computation of fluctuation function by calculating the mean difference of neighboring pixels. Paillier cryptosystem (Paillier 1999) is utilized for encryption of cover image in Chen et al. (2014) where one bit of secret message is embedded per pixel pair. Tai and Chang (2018) proposed a separable reversible data hiding algorithm where embedding space is reserved before encryption of

cover image. Puech et al. (2008) proposed a method of the local standard deviation of the encrypted image for the extraction of hidden data during the decryption phase. Bhardwaj and Aggarwal (2018) introduced a reversible data hiding algorithm in an 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, the secret message is not extracted correctly which results in a high bit error rate.

Tzu-Chuen et al. (2015) had given a method where dual stego images are generated by folded secret message centrally. Yao et al. (2017) described a dual-image method based on pixel co-ordinate system which results in minimum distortion of pixel's coordinate value. Lee and Huang (2013) presented a method where dual stego images are generated through an orientation combination of pixel coordinates. Here, binary secret message by changed over it into $base_5$ numeral framework is embedded which results in improved embedding rate. Chi et al. (2018) presented a dynamic encoding scheme where the 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. Tzu-Chuen et al. (2017) proposed a frequency encoding method to eliminate the disadvantage of Tzu-Chuen et al. (2015) strategy.

Shiu et al. (2017) 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. Bhalerao et al. (2019) 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. The most significant commitment of proposed work is its multi-purpose nature: ownership detection, tamper localization, and 100% reversibility. Mansour and Abdelrahim (2019) proposed a highly robust reversible data hiding method in encrypted domain where patient data is hidden in medical images with the help of discrete ripplelet 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.

The remaining paper is organized as follows—Sect. 3 carried out a brief description of the proposed algorithm. Further, discussions are conducted in Sect. 4 for comparison of embedding performance and visual quality of the proposed algorithm with the compared algorithms. At last, Sect. 5 concluded the paper.

3 Proposed algorithm

Nowadays, patient data privacy and security is one of the most significant challenges for telemedicine applications. Consider a scenario where the patient’s data is sent to the 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. Thus, an enhanced reversible data hiding method in the encrypted domain has been introduced here that gives higher embedding rate than all the looked at reversible data hiding methods by embedding k , ($k \geq 1$) binary bits of electronic patient information by changed over it into $base_{10}$ numeral framework at every pixel of the cover image without any occurrence of underflow and overflow problem. The data embedding algorithm is discussed in detail in Sect. 3.1 while as data extraction and image recovery algorithm is discussed in detail in Sect. 3.2.

3.1 Data embedding phase

The cover image was set to $CI = [P_{1,1}, P_{1,2}, \dots, P_{M,N}]$, where M and N are the image height and width, respectively. To avoid image distortion caused by a large value of $EPI(w)$, it was further reduced by using (Tzu-Chuen et al. 2015)’s method as follows:

$$w'_{u,v} = w_{u,v} - 2^{k-1} \tag{1}$$

Now, the range of secret message is changed from $R = [0, 1, 2, \dots, 2^k - 1]$ to $R' = [-2^{k-1}, -2^{k-1} + 1, \dots, -1, 0, 1, \dots, 2^{k-1} - 2, 2^{k-1} - 1]$

The following algorithm demonstrates the data embedding phase of our proposed approach:

Algorithm 1: Data Embedding Phase

Input: Cover image, CI of size $(M \times N)$ where each pixel $P_{u,v} \in [0..255]$, encryption key (N, g) and secret message in $base_{10}$ numeral framework of size $A \times B$.

Output: Stego image SI of size $(M \times N)$.

- 1: Cover image was set to $CI = [P_{1,1}, P_{1,2}, \dots, P_{M,N}]$, where M and N are the image height and width, respectively. Each value $P_{u,v}$ in CI where $P_{u,v} \in (0...255)$ is divided into two units $x_{u,v}, y_{u,v}$ as follows-

$$\begin{cases} P_{u,v} = x_{u,v} + y_{u,v} \\ \text{where } x_{u,v} = \lfloor \frac{P_{u,v}}{2} \rfloor, \quad y_{u,v} = P_{u,v} - x_{u,v} \end{cases} \tag{2}$$

- 2: Assumed $P_{u,v} = P_i$, $x_{u,v} = x_i$, $y_{u,v} = y_i$ and $w'_{u,v} = w'_i$.
- 3: Embed the reduced secret message w'_i into P_i to produce x_i^*, y_i^* as follows:-
 - a: **if** ($P_i \geq 2^k$) **then**
 - b: $x_i^* = x_i + w'_i$
 - c: $y_i^* = y_i - w'_i$
 - d: **else**
 - e: $x_i^* = w'_i + 2^{k-1} + 2^k - 1 + x_i + y_i$
 - f: $y_i^* = x_i + y_i$
 - g: **end if**
- 4: Now x_i^* and y_i^* are encrypted through Paillier cryptosystem [13] to produce $Encr[x_i^*]$ and $Encr[y_i^*]$.

3.2 Data extraction and image recovery phase

The process of extraction of secret message in $base_{10}$ numeral framework and recovery of cover image is shown in the following algorithm:

Algorithm 2: Data Extraction and Image Recovery

Input: Stego images SI of size $M \times N$ and decryption key (p, q, λ) .

Output: Cover image CI of size $M \times N$ where each pixel $CI \in [0..255]$ and secret message in $base_{10}$ numeral framework of size $A \times B$.

- 1: Firstly, $Encr[x_i^*]$ and $Encr[y_i^*]$ are decrypted through Paillier cryptosystem [13] where each directly decrypted pixel is considered as a unit of $P_i' = x_i^* + y_i^*$.
- 2: Extract the secret message w_i' as follows:-
 - a: $d_i' = x_i^* - y_i^*$
 - b: **if** ($d_i' \in [-2^k \dots (2^k - 2)]$) **then**
 - c: **if** ($d_i' \% 2 = 0$) **then**
 - d: $w_i' = \frac{d_i'}{2}$
 - e: $w_i = w_i' + 2^{k-1}$
 - f: $z_i = x_i^* + y_i^*$
 - g: **end if**
 - h: **else**
 - i: **if** ($d_i' \in [(-2^k - 1) \dots (2^k - 1 - 2)]$) **then**
 - j: **if** ($d_i' \% 2 \neq 0$) **then**
 - k: $w_i' = \frac{d_i' + 1}{2}$
 - l: $w_i = w_i' + 2^{k-1}$
 - m: $z_i = x_i^* + y_i^*$
 - n: **end if**
 - o: **else**
 - p: $w_i = d_i' - \sum_{r=1}^k 2^{(k-r)}$
 - q: $z_i = y_i^*$
 - r: **end if**
 - s: **end if**
- 3: Assumed $P_i = P_{u,v}$, $x_i = x_{u,v}$, $y_i = y_{u,v}$, $z_i = z_{u,v}$, $d_i' = d_{u,v}'$ and $w_i = w_{u,v}$. Now, extraction of secret message $w_{u,v}$ and recovery of cover image is as follows:-

$$\begin{cases} w_{u,v} = w_{u,v} \\ P_{u,v} = z_{u,v} \end{cases} \quad (3)$$

Example Detailed execution of proposed algorithm ($k = 3$) is shown in Table 1.

4 Results and discussions

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), structural similarity index matrix (SSIM), normalized cross-correlation (NCC), normalized absolute error (NAE), bit error rate (BER) and embedding rate (bpp) respectively. PSNR, SSIM, NCC are used to evaluate the quality of stego images while BER is used to evaluate the error between embedded and extracted watermark. The experimental study is performed on test

images of size 512×512 and binary watermark of size (256×256) , as shown in Figs. 1 and 2. Let $f(x, y)$, $\hat{f}(x, y)$ denote the value of pixel (x, y) in the cover and stego image of size $M \times N$ 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:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (4)$$

where

$$MSE = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N (f(x, y) - \hat{f}(x, y))^2 \quad (5)$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

where μ_x is average of x , μ_y is average of y , σ_x^2 is variance of x , σ_y^2 is variance of y , σ_{xy} is covariance of x and y , $c_1 = (k_1L)^2, c_2 = (k_2L)^2, L = (2^8 - 1), k_1 = 0.01$ and $k_2 = 0.03$ respectively.

$$NCC = \frac{\sum_{x=1}^M \sum_{y=1}^N f(x, y)\hat{f}(x, y)}{\sqrt{\sum_{x=1}^M \sum_{y=1}^N f(x, y)^2 \sum_{x=1}^M \sum_{y=1}^N \hat{f}(x, y)^2}} \quad (6)$$

$$NAE = \frac{\sum_{x=1}^M \sum_{y=1}^N |f(x, y) - \hat{f}(x, y)|}{\sum_{x=1}^M \sum_{y=1}^N |f(x, y)|} \quad (7)$$

$$R = \frac{Payload}{M \times N} \quad (8)$$

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

4.1 Imperceptibility analysis

Imperceptibility points out to the capability of a data hiding method that assures, no perceptible degradation occurs to cover image during the data embedding process respectively. Here, we examined the performance of the proposed method with the existing state-of-the-art algorithms of Tzu-Chuen et al. (2015), Yao et al. (2017), Lee and Huang (2013), Chi et al. (2018) and Tzu-Chuen et al. (2017) respectively. It is obvious from the obtained values of quality metrics, average PSNR value (48.65 dB), high SSIM value coupled with NCC value of approximate unity specify that proposed algorithm is capable of providing high-quality images for a payload of 262,144 bits respectively (Table 2). Table 3 demonstrates the examination of the proposed algorithm

Table 1 Execution of proposed method

Cover image (CI) =
$$\begin{bmatrix} 11 & 11 & 16 & 16 \\ 9 & 10 & 15 & 12 \\ 7 & 6 & 10 & 12 \\ 11 & 12 & 7 & 6 \end{bmatrix}$$

Each value $P_{u,v}$ in CI where $P_{u,v} \in (0 \dots 255)$ is divided into two units $x_{u,v}, y_{u,v}$ using Eq. (4) which are given as follows-

$$x_{u,v} = \begin{bmatrix} 5 & 5 & 8 & 8 \\ 4 & 5 & 7 & 6 \\ 3 & 3 & 5 & 6 \\ 5 & 6 & 3 & 3 \end{bmatrix} \quad y_{u,v} = \begin{bmatrix} 6 & 6 & 8 & 8 \\ 5 & 5 & 8 & 6 \\ 4 & 3 & 5 & 6 \\ 6 & 6 & 4 & 3 \end{bmatrix}$$

Secret message, $w_{u,v}$ (assumed) =
$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 3 \end{bmatrix}$$
 Reduced secret message, $w'_{u,v} = w_{u,v} - 2^{k-1} = \begin{bmatrix} -4 & -3 & -2 & -1 \\ 0 & 1 & 2 & 3 \\ -3 & -2 & -1 & 0 \\ 1 & 2 & 3 & -1 \end{bmatrix}$

Data embedding

Embed the reduced secret message $w'_{u,v}$ into $P_{u,v}$ (Algorithm [1]'s step:3) to produce $x^*_{u,v}, y^*_{u,v}$ as follows:

$$x^*_{u,v} = \begin{bmatrix} 1 & 2 & 6 & 7 \\ 4 & 6 & 9 & 9 \\ 15 & 15 & 4 & 6 \\ 6 & 8 & 21 & 16 \end{bmatrix} \quad y^*_{u,v} = \begin{bmatrix} 10 & 9 & 10 & 9 \\ 5 & 4 & 6 & 3 \\ 7 & 6 & 6 & 6 \\ 5 & 4 & 7 & 6 \end{bmatrix}$$

Data encryption

Encrypted $x^*_{u,v}$ and $y^*_{u,v}$ through Paillier cryptosystem (Paillier 1999) to produce $Encr[x^*_{u,v}]$ and $Encr[y^*_{u,v}]$ as follows:
 Encrypted value presented by [] symbol

$$Encr[x^*_{u,v}] = \begin{bmatrix} [1] & [2] & [6] & [7] \\ [4] & [6] & [9] & [9] \\ [15] & [15] & [4] & [6] \\ [6] & [8] & [21] & [16] \end{bmatrix} \quad Encr[y^*_{u,v}] = \begin{bmatrix} [10] & [9] & [10] & [9] \\ [5] & [4] & [6] & [3] \\ [7] & [6] & [6] & [6] \\ [5] & [4] & [7] & [6] \end{bmatrix}$$

Data extraction

Firstly, $Encr[x^*_{u,v}]$ and $Encr[y^*_{u,v}]$ are decrypted through Paillier cryptosystem (Paillier 1999)

$$x^*_{u,v} = \begin{bmatrix} 1 & 2 & 6 & 7 \\ 4 & 6 & 9 & 9 \\ 15 & 15 & 4 & 6 \\ 6 & 8 & 21 & 16 \end{bmatrix} \quad y^*_{u,v} = \begin{bmatrix} 10 & 9 & 10 & 9 \\ 5 & 4 & 6 & 3 \\ 7 & 6 & 6 & 6 \\ 5 & 4 & 7 & 6 \end{bmatrix}$$

Reduced secret message is extracted through Algorithm [2]'s step:2.

$$Difference\ matrix(d'_i) = x^*_{u,v} - y^*_{u,v} = \begin{bmatrix} -9 & -7 & -4 & -2 \\ -1 & 2 & 3 & 6 \\ 8 & 9 & -2 & 0 \\ 1 & 4 & 14 & 10 \end{bmatrix} \quad Reduced\ secret\ message, w'_{u,v} = \begin{bmatrix} -4 & -3 & -2 & -1 \\ 0 & 1 & 2 & 3 \\ -3 & -2 & -1 & 0 \\ 1 & 2 & 3 & -1 \end{bmatrix}$$

Finally, secret message is extracted and cover image is reconstructed through Algorithm [2]

$$Secret\ message, w_{u,v} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 3 \end{bmatrix} \quad Reconstructed\ cover\ image \quad CI = \begin{bmatrix} 11 & 11 & 16 & 16 \\ 9 & 10 & 15 & 12 \\ 7 & 6 & 10 & 12 \\ 11 & 12 & 7 & 6 \end{bmatrix}$$

with all other compared algorithms regarding the embedding rate and PSNR value attained on test images exhibited in Fig. 1 respectively. It is examined from the Table 3 that the proposed algorithm gives a high embedding rate in encrypted domain with content authentication at receiver end while all other compared methods did not. 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 quite comparable to

those obtained by compared methods. From the Table 3, it can be examined effectively that the proposed scheme gave maximum embedding rate for all test images with maintaining a good visual quality of stego images respectively. For some test images, after data embedding phase, the proposed method successfully preserved original pixel values of the cover image which implied that cover image and stego image are identical to one another and yield a PSNR value ∞ dB (Fig. 3a).

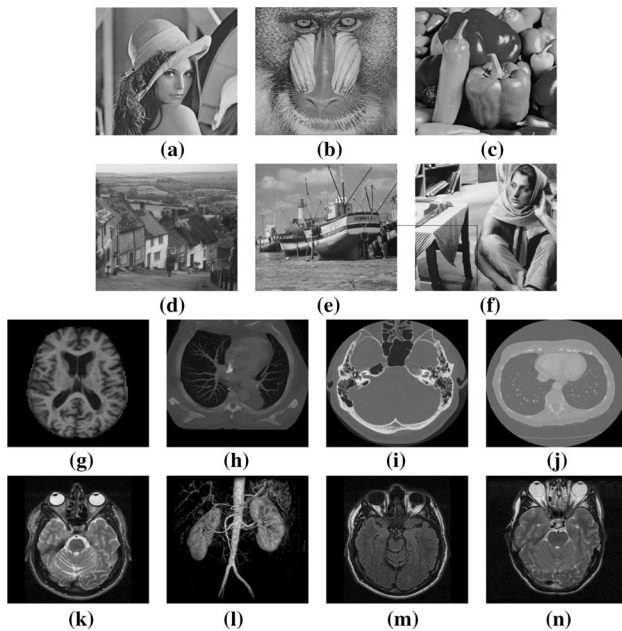


Fig. 1 Test images



Fig. 2 Watermark

Table 2 Study of proposed method in terms of imperceptive parameters (payload=262,144 bits)

Test images	Imperceptive parameters			
	PSNR (dB)	SSIM	NCC	NAE
<i>Med</i> ₁	45.67	0.9554	0.9998	0.0209
<i>Med</i> ₂	50.87	0.9669	0.9999	0.0051
<i>Med</i> ₃	49.25	0.9469	1.0000	0.0045
<i>Med</i> ₄	49.36	0.9484	1.0000	0.0036
<i>Med</i> ₅	48.19	0.9247	0.9999	0.0097
<i>Med</i> ₆	44.90	0.9538	0.9998	0.0329
<i>Med</i> ₇	48.31	0.9253	0.9998	0.0136
<i>Med</i> ₈	52.67	0.9924	1.0000	0.0028

It is noted from Fig. 3 that even at high payloads, the proposed method gave good quality stego image while compared methods did not because their decreased

embedding rates can't work at high payloads. The unparalleled performance of the proposed method on all test images is ascribed to its capacity to deal with the low as well as high-intensity pixels which can arise the underflow and overflow issue during data embedding phase in compared methods. Some compared methods, simply avoid these pixels, or as it named them as non-embeddable cases. Noted that, in natural images, the proportion of low-intensity pixels is extremely less as compared to medical images. So that, all the compared methods have good embedding rate in contrast with those achieved by them on medical images. The embedding rate of the proposed strategy is most prominent than other compared methods and the visual quality of stego image produced by the proposed method is at standard with all the compared methods (Fig. 4). The predominant performance of the proposed methodology on medical images is credited to its ability to deal with the low-intensity pixels, which can cause the underflow problem while embedding data into them. In the compared methods, they overlooked these low-intensity pixels, or at the end of the day name them as non-embeddable cases. Since, in medical images, the number of low-intensity pixels is exceptionally high, neglecting them causes loss of embedding rate. The proposed method 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 method truly reasonable for its utilization on medical images. In this manner it very well may be inferred that, for medical images, the proposed method altogether beat all the compared methods in its ability to embed secret information and precisely recover it with maintaining the visual nature of stego images too.

4.2 Security and robustness analysis

4.2.1 Histogram analysis

Stego images attained through a specific data hiding method are generally exposed to histogram analysis by attackers to get a hint about what has been embedded in it. Generally, a steganalyst gets a hint about embedded information through a comparison of corresponding histograms. A data hiding method is viewed as robust to this sort of attack if corresponding histograms are closely identical to each other. Figure 5 show histograms of different medical cover images and corresponding stego images. As is observed from the Fig. 5 that the proposed method is robust to this attack because corresponding histograms are closely identical to each other and their absolute difference is zero for almost all the intensity values.

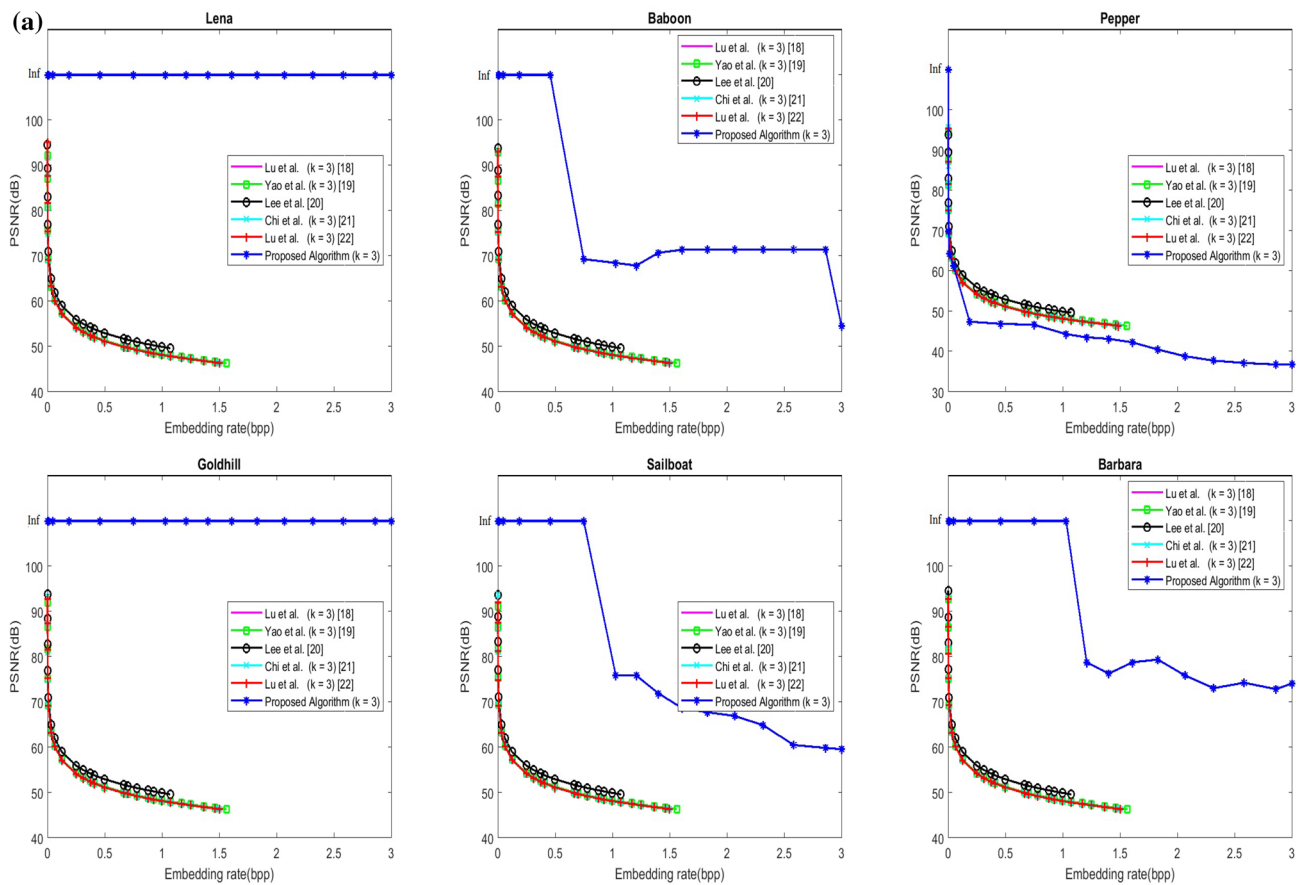


Fig. 3 a, b Graphs comparing PSNR value on different payload values obtained by the proposed and the compared methods

4.2.2 Authentication analysis

To evaluate the performance of the proposed method for its hidden message authentication, we subject stego image to well-known image processing attacks. As the secret message is embedded in the spatial domain so that the proposed algorithm is fragile in nature. The authentication analysis is carried out to calculate the degree of degradation in secret message due to a predefined attack which has been calculated in terms of BER (bit error rate) respectively. For the hidden message authentication at the receiver end, we embedded a watermark inside the cover image. At the receiver end, the extracted watermark is compared with the original one, if both watermarks are not matched with each other, it is accepted that the stego image and the hidden message is not legitimate. To assess the performance of the proposed method for its embedded message authentication, we subject stego image to well-known image processing attacks on random test images with the embedding of the watermark (cameraman) of size (256×256) respectively. From the outcomes for different attacks which are referenced in Table 4, it is obvious that our strategy is profoundly fragile to every

one of the attacks completed on different stego images and is approved by the way that the recovered watermark in the majority of the cases is not recognizable, thus demonstrative that the stego image has been attacked during transmission. Bit error rate value is around (35–55)% which concluded that extracted secret message in all of the cases is not recognizable, hence this is indicated that stego image has been attacked during transmission. High bit error rates for test images, approve the way that the proposed method 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 5 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 5, it is obvious that the difference image is perfectly black with each pixel intensity equivalent to zero and corresponding

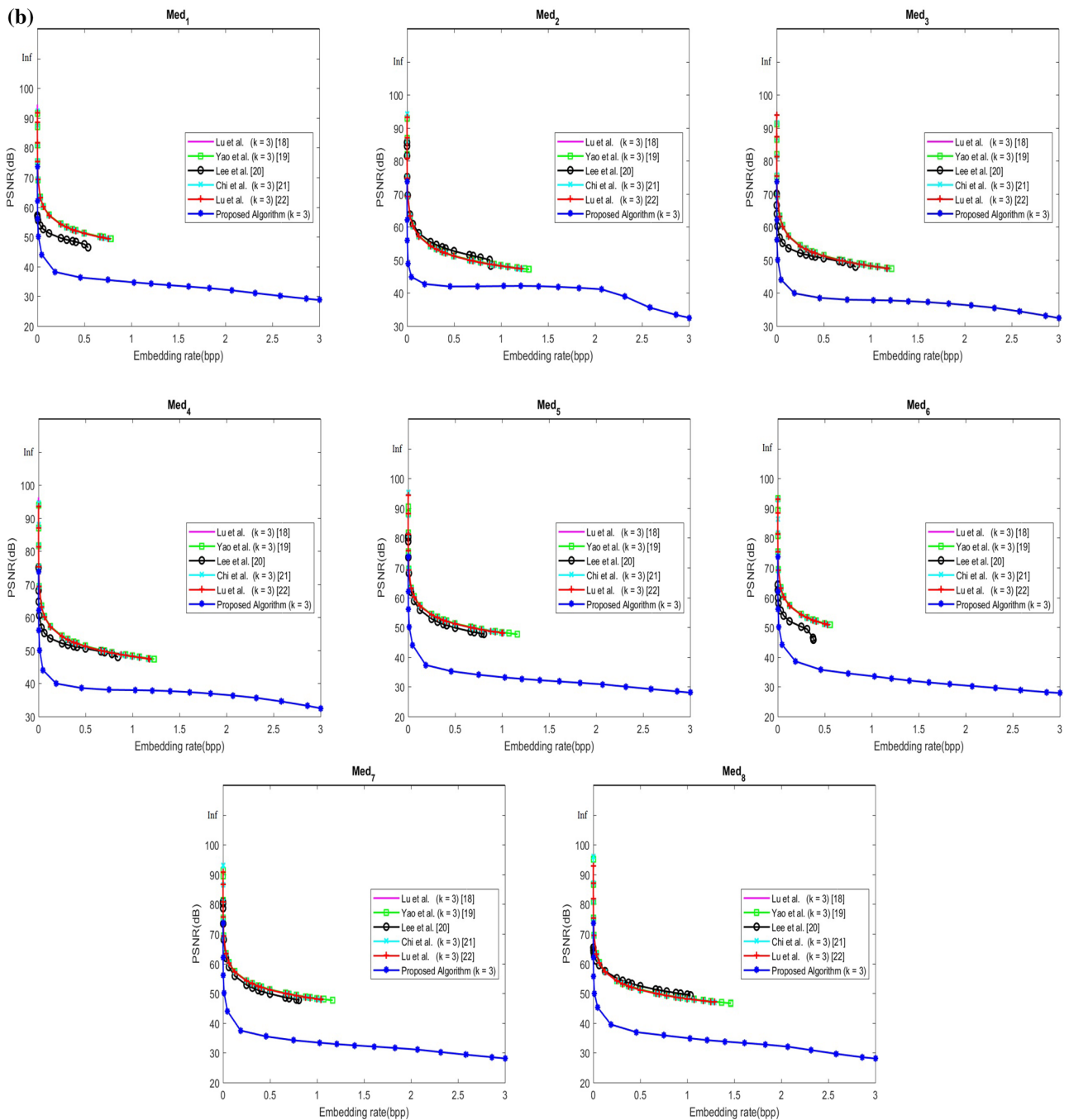


Fig. 3 (continued)

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 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.

Theorem 1 *The proposed method can not extract the secret message and reconstruct the original cover image at the receiver end successfully if stego image has been attacked during transmission.*

Proof Consider any pixel value ($P_{u,v} = 2^k$) in cover image (CI) which is divided into two units $x_{u,v}$ and $y_{u,v}$ as follows:

$$\begin{cases} P_{u,v} = x_{u,v} + y_{u,v} \\ \text{where } x_{u,v} = \lfloor \frac{P_{u,v}}{2} \rfloor = 2^{(k-1)} \\ y_{u,v} = P_{u,v} - x_{u,v} = 2^{(k-1)} \end{cases}$$

To avoid image distortion caused by a large value of $w_{u,v}$ (EPI), it was further reduced by using (Tzu-Chuen et al. 2015)’s method as follows:

$$\begin{cases} w'_{u,v} = w_{u,v} - 2^{k-1} \end{cases}$$

After embedding $w'_{u,v}$ into $x_{u,v}$ and $y_{u,v}$, they will be changed into $x^*_{u,v}$ and $y^*_{u,v}$ as follows:

$$\begin{cases} x^*_{u,v} = 2^{(k-1)} + w'_{u,v} \\ y^*_{u,v} = 2^{(k-1)} - w'_{u,v} \end{cases}$$

Assume noise (δ) is introduced due to attack on stego image which has been taken place during transmission process. It is introduced into $x^*_{u,v}$ and $y^*_{u,v}$ as follows:

$$\begin{cases} x^*_{u,v} = 2^{(k-1)} + \delta + w'_{u,v} \\ y^*_{u,v} = 2^{(k-1)} - w'_{u,v} \end{cases}$$

At receiver end, firstly compute $d'_{u,v} = x^*_{u,v} - y^*_{u,v} = 2w'_{u,v} + \delta$

$$\begin{cases} \text{Now } d'_i \in [(-2^k - 1) \dots (2^k - 1 - 2)] \\ d'_{u,v} \% 2 \neq 0 \\ w'_{u,v} = \frac{d'_{u,v} + 1}{2} = \frac{2w'_{u,v} + \delta + 1}{2} \\ w_{u,v} = w'_{u,v} + 2^{k-1} \\ = \frac{2w'_{u,v} + \delta + 1}{2} + 2^{k-1} \neq w_{u,v} \\ z_{u,v} = x^*_{u,v} + y^*_{u,v} = 2^{k-1} + \delta + 2^{k-1} = 2^k + \delta \neq P_{u,v} \end{cases}$$

□

Theorem 2 *The proposed method is reversible in nature so that after extraction of the secret message, it reconstructs the original cover image at the receiver end successfully.*

Proof Consider any pixel value ($P_{u,v} = 2^k$) in cover image (CI) which is divided into two units $x_{u,v}$ and $y_{u,v}$ as follows:

$$\begin{cases} P_{u,v} = x_{u,v} + y_{u,v} \\ \text{where } x_{u,v} = \lfloor \frac{P_{u,v}}{2} \rfloor = 2^{(k-1)} \\ y_{u,v} = P_{u,v} - x_{u,v} = 2^{(k-1)} \end{cases}$$

So that, to avoid image distortion caused by a large value of $w_{u,v}$ (EPI), it was further reduced by using (Tzu-Chuen et al. 2015)’s method as follows:

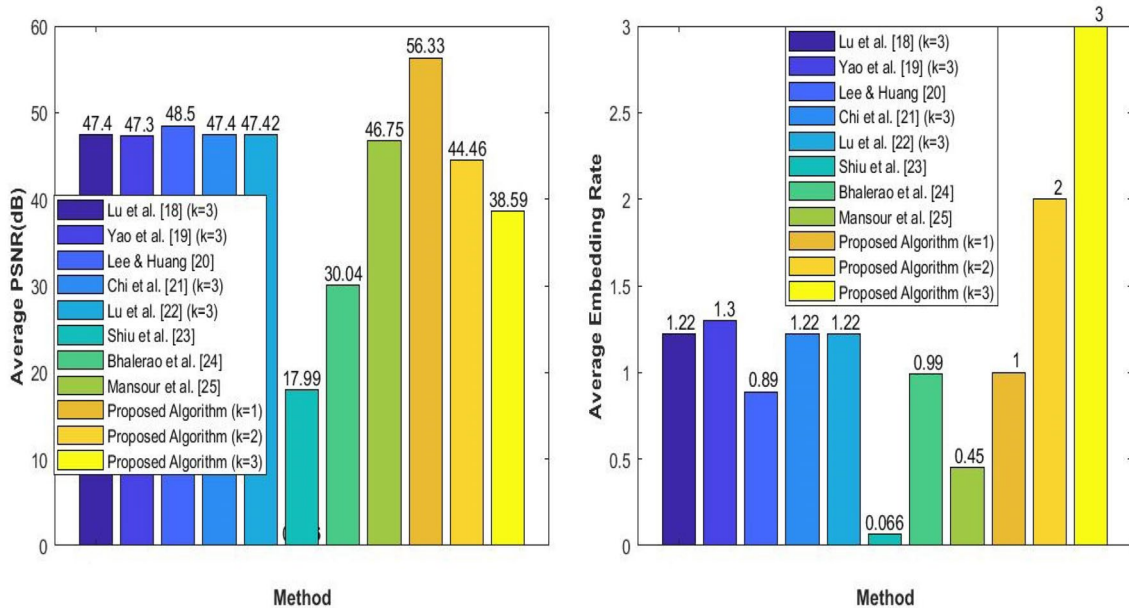


Fig. 4 Comparative study of proposed method

Table 3 Comparative study of proposed method

Test images	Parameters	Method							
		Tzu-Chuen et al. (2015) ($k = 3$)	Yao et al. (2017) ($k = 3$)	Lee and Huang (2013)	Chi et al. (2018) ($k = 3$)	Tzu-Chuen et al. (2017) ($k = 3$)	Proposed algorithm ($k = 1$)	Proposed algorithm ($k = 2$)	Proposed algorithm ($k = 3$)
<i>Lena</i>	Payload (bits)	786,432	819,155	562,388	786,432	786,432	262,144	524,288	786,432
	Embedding rate (bpp)	1.50	1.56	1.07	1.50	1.50	1	2	3
	PSNR of stego image (dB)	46.38	46.35	49.63	46.35	46.38	∞	∞	∞
<i>Baboon</i>	Payload (bits)	786,042	819,020	561,965	786,042	786,042	262,144	524,288	786,432
	Embedding rate (bpp)	1.49	1.56	1.07	1.49	1.49	1	2	3
	PSNR of stego image (dB)	46.36	46.37	49.63	46.38	46.38	77.76	63.96	54.56
<i>Pepper</i>	Payload (bits)	777,474	818,266	562,113	777,474	777,474	262,144	524,288	786,432
	Embedding rate (bpp)	1.48	1.56	1.07	1.48	1.48	1	2	3
	PSNR of stego image (dB)	46.41	46.38	49.63	46.39	46.43	69.26	49.20	36.83
<i>Goldhill</i>	Payload (bits)	786,432	819,260	562,349	786,432	786,432	262,144	524,288	786,432
	Embedding rate (bpp)	1.50	1.56	1.07	1.50	1.50	1	2	3
	PSNR of stego image (dB)	46.36	46.36	49.63	46.37	46.38	∞	∞	∞
<i>Sailboat</i>	Payload (bits)	786,348	819,042	562,019	786,348	786,348	262,144	524,288	786,432
	Embedding rate (bpp)	1.49	1.56	1.07	1.49	1.49	1	2	3
	PSNR of stego image (dB)	46.37	46.36	49.63	46.36	46.38	83.39	71.12	59.58
<i>Barbara</i>	Payload (bits)	786,432	819,321	562,465	786,432	786,432	262,144	524,288	786,432
	Embedding rate (bpp)	1.50	1.56	1.07	1.50	1.50	1	2	3
	PSNR of stego image (dB)	46.37	46.35	49.63	46.37	46.38	∞	∞	74.08
<i>Med₁</i>	Embedding capacity (bits)	394,863	412,320	283,172	394,863	394,863	262,144	524,288	786,432
	Embedding rate (bpp)	0.75	0.79	0.54	0.75	0.75	1	2	3
	PSNR of stego image (dB)	49.35	49.35	46.44	49.36	49.37	45.67	36.13	28.75
<i>Med₂</i>	Embedding capacity (bits)	637,011	679,816	466,982	637,011	637,011	262,144	524,288	786,432
	Embedding rate (bpp)	1.22	1.30	0.89	1.22	1.22	1	2	3
	PSNR of stego image (dB)	47.29	47.17	48.27	47.29	47.29	50.87	40.16	32.48

Table 3 (continued)

Test images	Parameters	Method							
		Tzu-Chuen et al. (2015) ($k = 3$)	Yao et al. (2017) ($k = 3$)	Lee and Huang (2013)	Chi et al. (2018) ($k = 3$)	Tzu-Chuen et al. (2017) ($k = 3$)	Proposed algorithm ($k = 1$)	Proposed algorithm ($k = 2$)	Proposed algorithm ($k = 3$)
Med_3	Embedding capacity (bits)	615,084	640,863	439,633	615,084	615,084	262,144	524,288	786,432
	Embedding rate (bpp)	1.17	1.22	0.83	1.17	1.17	1	2	3
	PSNR of stego image (dB)	47.44	47.42	47.94	47.44	47.45	49.25	39.73	32.37
Med_4	Embedding capacity (bits)	619,116	644,666	442,530	619,116	619,116	262,144	524,288	786,432
	Embedding rate (bpp)	1.18	1.23	0.84	1.18	1.18	1	2	3
	PSNR of stego image (dB)	47.41	47.41	47.97	47.41	47.41	49.36	39.83	32.48
Med_5	Embedding capacity (bits)	527,349	608,914	422,548	527,349	527,349	262,144	524,288	786,432
	Embedding rate (bpp)	1.00	1.16	0.80	1.00	1.00	1	2	3
	PSNR of stego image (dB)	48.11	47.66	47.75	48.11	48.12	48.19	36.85	28.00
Med_6	Embedding capacity (bits)	276,678	292,414	198,637	276,678	276,678	262,144	524,288	786,432
	Embedding rate (bpp)	0.53	0.56	0.37	0.53	0.53	1	2	3
	PSNR of stego image (dB)	50.90	50.83	45.81	50.90	50.93	44.90	35.32	27.86
Med_7	Embedding capacity (bits)	545,532	611,734	422,931	545,532	545,532	262,144	524,288	786,432
	Embedding rate (bpp)	1.04	1.17	0.80	1.04	1.04	1	2	3
	PSNR of stego image (dB)	47.95	47.63	47.75	47.96	47.96	48.31	37.36	28.07
Med_8	Embedding capacity (bits)	675,663	767,346	542,176	675,663	675,663	262,144	524,288	786,432
	Embedding rate (bpp)	1.29	1.46	1.03	1.29	1.29	1	2	3
	PSNR of stego image (dB)	47.02	46.66	49.31	47.02	47.04	52.67	39.44	28.05

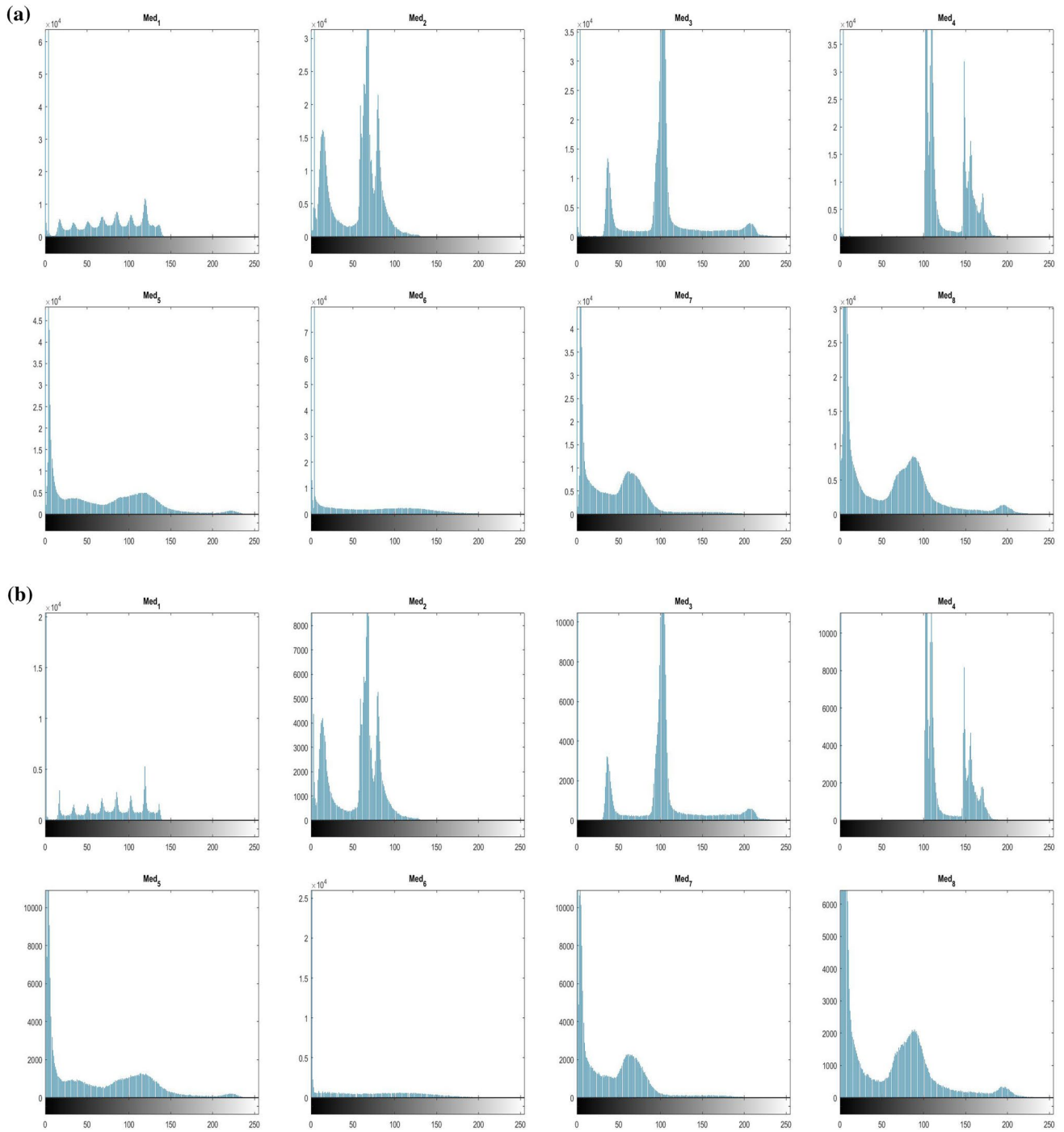


















Fig. 5 a Histogram of cover images, b Histogram of corresponding stego images

Table 6 Computational complexity comparison of proposed method

Test images	Parameters	Method					
		Tzu-Chuen et al. (2015)	Yao et al. (2017)	Lee and Huang (2013)	Chi et al. (2018)	Tzu-Chuen et al. (2017)	Proposed algorithm
<i>Med</i> ₁	Embedding rate (bpp)	0.75	0.79	0.54	0.75	0.75	1.00
	Execution time (s)	2.03	1.89	7.20	3.30	1.26	3.25 × 10 ³
<i>Med</i> ₂	Embedding rate (bpp)	1.22	1.30	0.89	1.22	1.22	1.00
	Execution time (s)	2.72	2.25	9.90	5.80	1.75	1.64 × 10 ³
<i>Med</i> ₃	Embedding rate (bpp)	1.17	1.22	0.83	1.17	1.17	1.00
	Execution time (s)	2.87	2.20	9.57	4.52	1.83	1.18 × 10 ³
<i>Med</i> ₄	Embedding rate (bpp)	1.18	1.23	0.84	1.18	1.18	1.00
	Execution time (s)	2.62	2.14	9.76	4.55	1.50	1.34 × 10 ³
<i>Med</i> ₅	Embedding rate (bpp)	1.00	1.16	0.80	1.00	1.00	1.00
	Execution time (s)	2.40	2.12	9.36	4.10	1.58	1.48 × 10 ³
<i>Med</i> ₆	Embedding rate (bpp)	0.53	0.56	0.37	0.53	0.53	1.00
	Execution time (s)	1.63	1.51	5.75	2.73	1.04	3.74 × 10 ³
<i>Med</i> ₇	Embedding rate (bpp)	1.04	1.17	0.80	1.04	1.04	1.00
	Execution time (s)	2.49	2.06	9.35	4.18	1.49	1.80 × 10 ³
<i>Med</i> ₈	Embedding rate (bpp)	1.29	1.46	1.03	1.29	1.29	1.00
	Execution time (s)	2.77	2.35	11.41	4.74	1.68	3.77 × 10 ²

Table 4 Authentication analysis

Attacks	<i>Med</i> ₁	<i>Med</i> ₃	<i>Med</i> ₄	<i>Med</i> ₆	Average BER(%)
Reflection					42.09
Salt & Pepper noise					55.64
Median Filtering					35.16
Sharpening					40.47

$$\{ w'_{u,v} = w_{u,v} - 2^{k-1}$$

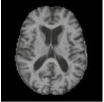


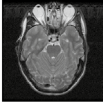
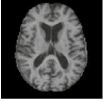


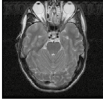




After embedding $w'_{u,v}$ into $x_{u,v}$ and $y_{u,v}$, they will be changed into $x^*_{u,v}$ and $y^*_{u,v}$ as follows:

$$\begin{cases} x^*_{u,v} = 2^{(k-1)} + w'_{u,v} \\ y^*_{u,v} = 2^{(k-1)} - w'_{u,v} \end{cases}$$

At receiver end extract the secret message $w_{u,v}$ and reconstruct cover image (*CI*) as follows:

Firstly, compute $d'_{u,v} = x^*_{u,v} - y^*_{u,v} = 2w'_{u,v}$ as follows:

Table 5 Reversibility analysis

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

$$\left\{ \begin{array}{l} \text{Now } d'_{u,v} \in [-2^k \dots (2^k - 2)] \\ d'_{u,v} \% 2 = 0 \\ w'_{u,v} = \frac{d'_{u,v}}{2} = w'_{u,v} \\ w_{u,v} = w'_{u,v} + 2^{k-1} = w_{u,v} \\ z_{u,v} = x^*_{u,v} + y^*_{u,v} = 2^{k-1} + 2^{k-1} = 2^k = P_{u,v} \end{array} \right.$$

□

4.4 Computational complexity

The time complexity is computed when proposed method and compared methods are run on a laptop with Intel i5@2.40 GHz CPU and 8 GB RAM. As shown in Table 6, execution time of proposed method is more as compared to the methods of Tzu-Chuen et al. (2015), Yao et al. (2017), Lee and Huang (2013), Chi et al. (2018), Tzu-Chuen et al. (2017) for test medical images but the embedding rate of the proposed strategy is most prominent than other compared methods and the visual quality of stego image produced by the proposed method is at standard with all the compared methods (Fig. 3).

5 Conclusion

In this work, an enhanced reversible data hiding method in the encrypted domain has been implemented and tests against well-known image processing attacks also. The proposed algorithm has not been suffering from underflow

and overflow problem and altogether beat all the compared methods with yielded an embedding rate of three bits per pixel ($k = 3$) for medical images respectively. In future, the focus will be on improving the robustness of the proposed method because it has been carried out in the spatial domain so that not robust to various image processing attacks.

References

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

Bhardwaj R, Aggarwal A (2018) An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. *Pattern Recognit Lett*. <https://doi.org/10.1016/j.patrec.2018.01.014>

Celik MU, Sharma G, Murat TA, Saber E (2005) Lossless generalized-LSB data embedding. *IEEE Trans Image Process* 14(2):253–266

Chen Y-C, Shiu C-W, Horng G (2014) Encrypted signal-based reversible data hiding with public key cryptosystem. *J Vis Commun Image Represent* 25(5):1164–1170

Chi L-P, Chang-Han W, Chang H-P (2018) Reversible data hiding in dual stegano-image using an improved center folding strategy. *Multimed Tools Appl* 77(7):8785–8803

Hong W, Chen T-S, Han-Yan W (2012) An improved reversible data hiding in encrypted images using side match. *IEEE Signal Process Lett* 19(4):199–202

Kim Y-S, Kang K, Lim D-W (2015) New reversible data hiding scheme for encrypted images using lattices. *Appl Math Inf Sci* 9(5):2627

Lee C-F, Huang Y-L (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommun Syst* 52(4):2237–2247

Liao X, Shu C (2015) Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. *J Vis Commun Image Represent* 28:21–27

- Ma K, Zhang W, Zhao X, Nenghai Yu, Li F (2013) Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans Inf Forensics Secur* 8(3):553–562
- 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
- Ni Z, Shi Y-Q, Ansari N, Wei S (2006) Reversible data hiding. *IEEE Trans Circuits Syst Video Technol* 16(3):354–362
- 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 223–238
- 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
- Qian Z, Zhang X, Ren Y, Feng G (2016) Block cipher based separable reversible data hiding in encrypted images. *Multimed Tools Appl* 75(21):13749–13763
- Shi YQ (2004) Reversible data hiding. In: *International workshop on digital watermarking*. Springer, pp 1–12
- Shiu H-J, 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
- Tai W-L, Chang Y-F (2018) Separable reversible data hiding in encrypted signals with public key cryptography. *Symmetry* 10(1):23
- Tian J (2003) Reversible data embedding using a difference expansion. *IEEE Trans Circuits Syst Video Technol* 13(8):890–896
- Tzu-Chuen L, Jhih-Huei W, Huang C-C (2015) Dual-image-based reversible data hiding method using center folding strategy. *Signal Process* 115:195–213
- Tzu-Chuen L, Chi L-P, Chang-Han W, Chang H-P (2017) Reversible data hiding in dual stego-images using frequency-based encoding strategy. *Multimed Tools Appl* 76(22):23903–23929
- Xiao B, Lizhi Y, Yongfeng H (2010) Reversible data hiding using histogram shifting in small blocks. In: *2010 IEEE international conference on communications (ICC)*. IEEE, pp 1–6
- Xiaotian W, Sun W (2014) High-capacity reversible data hiding in encrypted images by prediction error. *Signal Process* 104:387–400
- 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* 135:26–35
- Zhang X (2011) Reversible data hiding in encrypted image. *IEEE Signal Process Lett* 18(4):255–258
- Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.