Multimedia Tools and Applications (2021) 80:31687–31703
https://doi.org/10.1007/s11042-021-10892-2

An efficient reversible and secure patient data hiding algorithm for E-healthcare

Rupali Bhardwaj[1] · Anjali Singh[1]

Received: 30 August 2020 / Revised: 8 December 2020 / Accepted: 1 April 2021 /
Published online: 19 July 2021

Abstract
E-healthcare requires communication of patient report to a specialized doctor in a real time scenario. Therefore, any harm to patient medical data can lead to a faulty diagnosis that can be lethal for the patient. To ensure safe and secure communication in E-healthcare framework, an efficient reversible data hiding algorithm in encrypted domain has been proposed in this paper. The proposed algorithm gives a higher embedding rate by embedding a single bit of patient data in $base_2$ numeral framework at every pixel of the cover image without any occurrence of underflow and overflow problem. The proposed method has been evaluated for content authentication by subjecting it to various image processing attacks. The experimental study reveals that for test images, proposed method has higher embedding rate than the compared methods, precisely recover patient information with an average value of Peak Signal Noise Ratio value of 48.13 dB between the cover image and stego image respectively. A comparison of the observed results with that of some state-of-art methods shows that proposed method performs better and as such is an ideal candidate for content authentication of Electronic patient information in a typical E-healthcare framework.

Keywords Reversible data hiding (RDH) · Privacy Protection · Homomorphic encryption · Electronic patient information (EPI)

1 Introduction

E-healthcare systems are currently being integrated with conventional health care systems to acquire benefits of current-day technological advancements. The current E-healthcare system is doing telediagnosis of a patient, for this purpose, it requires medical reports of the patient including all image and text-based reports to share among its remote centers. Though E-healthcare systems bring

✉ Rupali Bhardwaj
rupali.bhardwaj@thapar.edu

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

the best medical facilities at your doorsteps, but during the implementation process experiences some challenges also. One of the fundamental concerns to be addressed for the implementation of E-healthcare system is security, authentication and copyright protection of the patient data respectively. Data hiding is the most robust tool that can address the above-mentioned 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 is 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 reversible data hiding technologies plays an important role in privacy protection. As a result, reversible data hiding (RDH) in encrypted image (RDH-EI) has attracted great attention from the research community. A detailed review of the stated work ([14, 17–20]) reveals that for medical images, reporting methods have low embedding capacity and they do not even support content authentication for patient data also. Keeping this in view, an enhanced reversible data hiding algorithm in encrypted domain to embed electronic patient information in cover image has been presented in this paper. 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:

- Paillier cryptosystem is used for encryption instead of conventional ones to avoid underflow and overflow problems during data embedding in cover image.
- Binary EPI is embedded at every pixel of cover image to improve the embedding capacity.
- A fragile watermark is used for content authentication at the receiver end.

The layout of paper is given as follows. Section 2 shows a compact written work outline about reversible data hiding methods. 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. Finally, paper is concluded in Section Section 5.

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 [1]. Afterward, difference expansion based reversible data hiding technique was proposed by Tian[2], where a single bit was embedded between two close-by pixels through difference computation. Ni et al. [3] had given a scheme where a secret message is embedded at the histogram's peak point of cover image. Afterward, Bo et al.[4] 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.[6] exhibited a separable reversible data hiding algorithm where cover image is encrypted through block cipher algorithm.

Zhang[7], 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[8] 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.[9] 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[7]. Young et al.[10] 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.[11] proposed a reversible data hiding method before encryption of cover image. Liao and Changwen[12] improved computation of fluctuation function through calculating mean difference of neighboring pixels. Paillier cryptosystem[13] is utilized for encryption of cover image in Chen et al.[14] where one bit of secret message is embedded per pixel pair. Wu et al.[15] presented a reversible data hiding algorithm for signals which are encrypted through Paillier cryptosystem[13] and embedded one bit of binary secret message at a single pixel successfully. Bhardwaj and Aggarwal[16] 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.[17] had given a method where dual stego images are generated by folded secret message centrally. Yao et al.[18] described a dual-image method based on pixel co-ordinate system which results in minimum distortion of pixel's coordinate value. Lee and Huang[19] presented a method where dual stego images are generated through 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.[20] 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.[21] proposed a frequency encoding method to eliminate the disadvantage of Lu et al.[17] strategy.

Shiu et al.[22] 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.[23] 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 [24]. Bhalero et al.[25] 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.[26] 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.

3 Proposed Algorithm

The current E-healthcare system is doing telediagnosis of a patient, for this purpose, it requires medical reports of the patient including all image and text-based reports to share among its remote centers. Though E-healthcare systems bring the best medical facilities at your door-steps, but during implementation process experiences some challenges also. Primary concern to be addressed for the implementation of E-healthcare system is security, authentication and copyright protection of the patient data respectively. Encryption is the most promising solution to maintain confidentiality and privacy of data. The integration of encryption and reversible data hiding technologies plays an important role in privacy protection. Keeping this in view, an enhanced reversible data hiding algorithm in the encrypted domain to embed electronic patient information(EPI) in cover image has been represented in this paper. In proposed method (Fig.1), Paillier cryptosystem is used for encryption instead of conventional ones to avoid underflow and overflow problems during data embedding in cover image.

Pailler cryptosystem[13] is discussed briefly in subsection 3.1 respectively.Data embedding algorithm is discussed in detail in subsection 3.2 while as data extraction and image recovery algorithm is discussed briefly in subsection 3.3.

Table 1 Study of some state-of-art methods in terms of imperceptibility and payload

Author	Domain	Method	Parameters	
			PSNR (dB)	Embedding Capacity Bits per pixel/ signal)
Zhang[7]	Encrypted	Symmetric cryptosystem, Block division	36.81	0.25 bpp
Hong et al.[9]	Encrypted	Symmetric cryptosystem, Block division	36.82	0.25 bpp
Young et al.[10]	Encrypted	Symmetric cryptosystem, Block division	42.02	0.25 bpp
Liao and Changwen[12]	Encrypted	Symmetric cryptosystem	36.81	0.25 bpp
Chen et al.[14]	Encrypted	Paillier cryptosystem	40.18	1.00bpp
Bhardwaj and Aggarwal[16]	Encrypted	Symmetric cryptosystem, Block division	42.13	0.50 bpp
Lu et al.[17] (k=2)	Dual	Center folding	52.78	0.71 bpp
Yao et al.[18] (k=2)	Dual	Pixel co-ordinate system	52.75	0.80 bpp
Lee and Huang[19]	Dual	Orientation combination	47.65	0.76 bpp
Chi et al.[20] (k=2)	Dual	Dynamic encoding method	52.78	0.94 bpp
Shiu et al.[22]	E-healthcare	(1023,1013) Hamming code	17.98	66.67 (kbits)
Parah et al.[23]	E-healthcare	Intermediate significant bit substitution	46.36	0.75 bpp
Parah et al.[24]	E-healthcare	Intermediate significant bit substitution	46.55	0.9662 bpp
Bhalero et al.[25]	E-healthcare	Deep Neural Netwotk	30.04	0.99 bpp

*Test medical images of size 512×512 obtained from database of The Cancer Imaging Archive (TCIA) as shown in Fig 2 and ECG signals obtained from MIT-BIH arrhythmia database respectively.

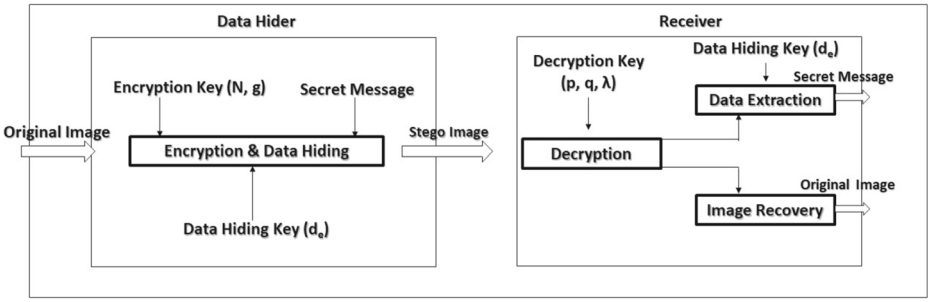

Fig. 1 Workflow of proposed algorithm

3.1 Paillier Cryptosystem

This is public key cryptosystem based on the composite residuosity class problem. It comprised three procedures: key generation, data encryption and data decryption as described as follows-

- Let p and q be two large prime numbers that are independent of each other.
- Compute $N = pq$ and $\lambda = LCM(p-1, q-1)$
- Select generator g such that $g \in Z^*_{N^2}$ and $gcd(S(g^{\lambda} mod\ N^2), N) = 1$ where

$$S(x) = \frac{x-1}{N} \tag{1}$$

- Consider a message $m \in Z^*_N$ and randomly chosen $r \in Z^*_N$. Compute the cipher text of m as

$$c = g^m r^N mod\ N^2 \tag{2}$$

- Public key is composed of (N, g) and private key is composed of (p, q, λ).
- Decryption of ciphertext c is given by

$$m = \frac{S\left(c^{\lambda} mod\ N^2\right)}{S\left(g^{\lambda} mod\ N^2\right)} mod\ N \tag{3}$$

- Given two plaintexts m_1 and m_2, corresponding ciphertexts are given by $Enc[m_1]$ and $Encr[m_2]$. The additive homomorphic property, $Encr[m_1] \times Encr[m_2] = Encr[m_1 + m_2]$ holds because of

$$\begin{aligned} Encr[m_1] \times Encr[m_2] = \left(g^{m_1} r_1^N mod\ N^2\right)\left(g^{m_2} r_2^N mod\ N^2\right) = \\ \left(g^{m_1+m_2}(r_1 r_2)^N mod\ N^2\right) = Encr[m_1 + m_2] \end{aligned} \tag{4}$$

The multiplicative homomorphic property,

$$\begin{aligned} Encr[m_1]^x = \left(g^{m_1} r_1^N mod\ N^2\right)^x = \left(g^{m_1} r_1^N\right)^x mod\ N^2 = \\ \left(g^{xm_1}\right)\left(r_1^{x^N}\right) mod N^2 = Encr[xm_1] \end{aligned} \tag{5}$$

3.2 Data Embedding Phase

Algorithm 1: Data embedding

Input: Cover image CI of size $M \times N$ where each pixel $P_{u,v} \in [0..255]$ and $u \leq [0...M-1], v \leq [0...N-1]$, secret message $(W = w_{1,1}..w_{A,B})$ in $base_2$ numeral framework of size $A \times B$, encryption key (N, g) and data hiding key d_e.
Output: Stego (and encrypted) image SI of size $M \times N$.

1: Cover image is set to $CI = [P_{1,1}, P_{1,2}, ..., P_{M,N}]$, 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 three units $x_{u,v}, y_{u,v}, z_{u,v}$ as follows-

$$\begin{cases} P_{u,v} = x_{u,v} + y_{u,v} + z_{u,v} \\ where \quad x_{u,v},\ y_{u,v} = \lfloor \frac{P_{u,v}}{2} \rfloor, \quad z_{u,v} = mod\ (P_{u,v}, 2) \end{cases} \tag{6}$$

2: Now $x_{u,v}, y_{u,v}, z_{u,v}$ are encrypted through Paillier cryptosystem[18] with encryption key (N, g) to produce encrypted pixel values as follows-

$$[P_{u,v}] = [x_{u,v}] + [y_{u,v}] + [z_{u,v}] \tag{7}$$

Here, symbol [ ] meant for encrypted value. To improve the security of secret message, secret message W is also encrypted through Paillier cryptosystem[18].

3: Assumed $[P_{u,v}] = [P_i],\ [x_{u,v}] = [x_i],\ [y_{u,v}] = [y_i],\ [z_{u,v}] = [z_i]$ and $[w_{u,v}] = [w_i]$. With the help of data hiding key (d_e), embed the secret message $[w_i]$ into $[P_i]$ to produce $[P_i^*] = [x_i^* + y_i^* + z_i^*] = [x_i^*]\,[y_i^*]\,[z_i^*]$ as follows:-

if $([P_i] < [255])$ **then**
  $[x_i^*] = [x_i + w_i]$
  $[y_i^*] = [y_i - w_i + 1]$
  $[z_i^*] = [z_i]$
else
  if $([w_i] = [0])$ **then**
    $[x_i^*] = [x_i - 1]$
    $[y_i^*] = [y_i + 1]$
    $[z_i^*] = [z_i]$
  else
    if $([w_i] = [1])$ **then**
      $[x_i^*] = [x_i + 1]$
      $[y_i^*] = [y_i - 1]$
      $[z_i^*] = [z_i]$

end if
end if
end if

3.3 Data extraction and image recovery phase

In our method, firstly stego image is decrypted through Paillier cryptosystem[13] at receiver end, then it is conceivable to extract the secret message and recuperate original cover image with no error.

Algorithm 2: Data extraction and image recovery

Input: Encrypted stego image SI of size $M \times N$ where $u \leq [0...M-1], v \leq [0...N-1]$, decryption key (p, q, λ) and data hiding key d_e.
Output: Cover image CI of size $M \times N$ where each pixel $CI \in [0..255]$ and and secret message($W = w_{1,1}..w_{A,B}$) in $base_2$ numeral framework of size $A \times B$

1: Firstly, $[x_i^*], [y_i^*]$ and $[z_i^*]$ are decrypted through Paillier cryptosystem[18] with decryption key (p, q, λ) where each directly decrypted pixel is considered as a unit of $P_i* = x_i^* + y_i^* + z_i^*$.

2: With the help of data hiding key (d_e), original pixel value (P_i) corresponding to cover image as well as secret message (w_i) in $base_2$ numeral framework is extracted from P_i^* as follows:-

if $(x_i^* < y_i^*)$ **then**
$w_i = 0$
else
if $(x_i^* > y_i^*)$ **then**
$w_i = 1$
end if
end if

Original pixel P_i is reconstructed from the stego pixel $P_i^* = x_i^* + y_i^* + z_i^*$ as follows:

$m_i^* = x_i^* + y_i^*$
if $(mod\ (m_i^*, 2 = 1))$ **then**
$P_i = x_i^* + y_i^* + z_i^* - 1$
else
$P_i = x_i^* + y_i^* + z_i^*$
end if

Assume $P_i = P_{u,v},\ x_i = x_{u,v},\ y_i = y_{u,v},\ z_i = z_{u,v},$ and $w_i = w_{u,v}$.

Now, extraction of secret message $w_{u,v}$ and recovery of cover image is as follows:-

$$\begin{cases} W = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} w_{u,v} \\ CI = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} P_{u,v} \end{cases} \tag{8}$$

Example: Working of proposed algorithm on sample pixel values 0, 64, 127 and 255 is shown in Table2.

4 Experimental Study

The experimental study has been carried out using MATLAB R2017a platform for different 512×512 test images obtained from database of The Cancer Imaging Archive (TCIA) as shown in Fig.2 respectively. The exhibition of the proposed method has been assessed as far as metrics like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index Matrix (SSIM), Normalized Cross-correlation (NCC), 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. Let $f(x, y)$ denote the value of pixel (x, y) in the cover 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 -

$$PSNR = 10\ log_{10} \frac{255^2}{MSE} \tag{9}$$

where

$$\begin{aligned} MSE &= \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(f(x,y) - \widetilde{f}(x,y) \right)^2 \\ SSIM(x,y) &= \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_1\right)}{\left(\mu_x^2 + \mu_y^2 c_1\right)\left(\sigma_x^2 + \sigma_y^2 c2\right)} \end{aligned} \tag{10}$$

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, $c_1 = (k_1 L)^2, c_2 = (k2L)^2, L = (2^8 - 1), k_1 = 0.01$ and $k_2 = 0.03$ respectively.

$$NAE = \frac{\sum_{x=1}^{M} \sum_{y=1}^{M} \left| f(x,y) - \widehat{f}(x,y) \right|}{\sum_{x=1}^{M} \sum_{y=1}^{M} f(x,y)} \tag{11}$$

$$NCC = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} f(x,y) \widetilde{f}(x,y)}{\sqrt{\sum_{x=1}^{M} \sum_{y=1}^{N} f(x,y)^2 \sum_{x=1}^{2M} \sum_{y=1}^{2N} \widetilde{f}(x,y)^2}} \tag{12}$$

$$R = \frac{Payload}{M \times N} \tag{13}$$

$$BER = \frac{\sum_{i=1}^{A} \sum_{j=1}^{B} \left(sm(i,j) \oplus sm'(i,j) \right) \times 100}{Count\_of\_embedded\_bits} \tag{14}$$

4.1 Result Analysis

Here, we examined the performance of the proposed method and compared it with the existing state-of-the-art algorithms of Lu et al. $(k = 2)$ [17], Yao et al. $(k = 1, k = 2)$ [18], Lee & Huang[19] and Chi et al. $(k = 2)$ [20] respectively. Table 3 demonstrates the examination of the proposed method with all other compared methods with reference to embedding rate and the PSNR value attained on test images as shown in Fig.2 respectively. From Table 3, it can be observed that the proposed method achieved maximum embedding rate for all test images (approx.) and similarity of cover and stego image with one another in a degree to yield an average PSNR value of 48.13 dB. The same can also be observed from Fig.3 which graphically represents the comparison of the different payloads achieved by the proposed and compared methods. The embedding rate of proposed scheme is most prominent than other compared methods with an average visual quality of the stego images. Indeed, even as far as bits per pixel value, in most of the cases, embedding rate produced by the proposed method is at par with all the compared methods (Fig.4). After data embedding phase, proposed method successfully recovered original pixel values from stego image to facilitate reversibility. The unrivaled performance of the proposed method on all test images is attributed to its ability to manage the low-intensity pixels, which can cause the underflow issue during the procedure of data embedding. In the compared methods, they fundamentally neglect these low-intensity pixels, or by the day's end mark them as non-embeddable cases. Since, in medical images, the count of such type of pixels is high as compared to natural images. The comparable can be seen from the outcomes introduced in Fig.4 too. The explanation behind this immense improvement in the embedding performance of the proposed method lies in its ability to hide information properly without any occurrence of underflow problem respectively. In this manner, all the compared methods were capable to give great embedding rate on natural images in contrast with medical images. Table 4 demonstrates the examination of the proposed algorithm with state-of-the-art algorithms with reference to image quality metrics like SSIM, NAE, NCC and Embedding Rate attained on medical images respectively. It is obvious from the obtained average values of quality metrics, 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 one bpp respectively. It is also examined from Table 4 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. In this manner it very well may be inferred that proposed method altogether beated all the compared methods in its ability to embed secret information and precisely recover it with maintaining the visual nature of stego images too. The purpose behind this enormous improvement in the embedding performance of the proposed methods lies in its capacity to embed data properly at low intensity pixels without any occurrence of underflow problem. Since, larger part of the pixels are black in medical images, so the proposed method performed extraordinarily well as compared to other methods for medical images.

4.2 Authentication Analysis

To evaluate performance of proposed scheme for its hidden message security at receiver end, we embedded a watermark inside the cover image. At the receiver end, 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 performance of proposed scheme for its embedded message authentication, we subject stego image to well

Table 2 Example

Example 1	Example 2	Example 3	Example 4
P =0	P=64	P=127	P=255
$x = 0$	$x = 32$	$x = 63$	$x = 127$
$y = 0$	$y = 32$	$y = 63$	$y = 127$
$z = 0$	$z = 0$	$z = 1$	$z = 1$
Secret Message			
$w = 0$	$w = 1$	$w = 1$	$w = 0$
Data Embedding			
$[x^*] = [0]$	$[x^*] = [33]$	$[x^*] = [64]$	$[x^*] = [126]$
$[y^*] = [1]$	$[y^*] = [32]$	$[y^*] = [63]$	$[y^*] = [128]$
$[z^*] = [0]$	$[z^*] = [0]$	$[z^*] = [1]$	$[z^*] = [1]$
Data Extraction			
$x^* < y^*$	$x^* > y^*$	$x^* > y^*$	$x^* < y^*$
$w = 0$	$w = 1$	$w = 1$	$w = 0$
Image Recovery			
$P = 0 + 1 + 0 - 1$ = 0	$P = 33 + 32 + 0 - 1$ = 64	$P = 64 + 63 + 1 - 1$ = 127	$P = 126 + 128 + 1$ = 255

known image processing attacks on $Med_4(512 \times 512)$ cover image with embedding of watermark (cameraman) of size (256×256) Fig 5 respectively. From the outcomes for different attacks which are referenced in Fig 5, 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. High bit error rate value of the order of about (18-60)% 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. **Theorem 1**:-The proposed method is reversible in nature so

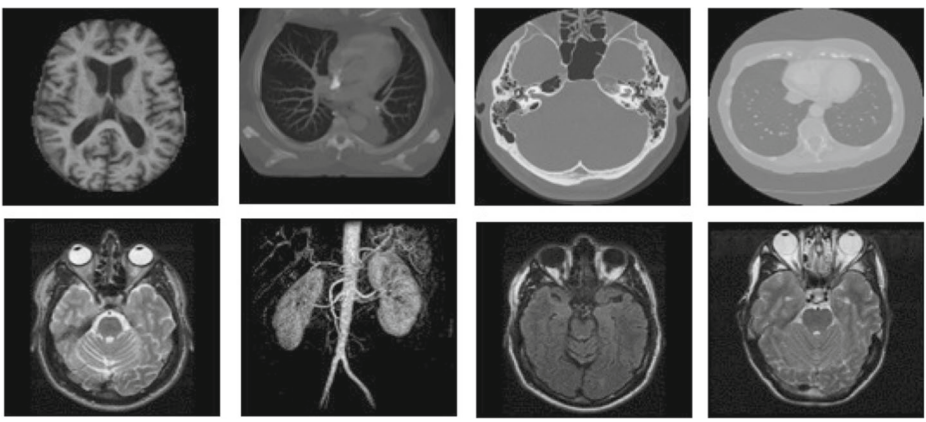

Fig. 2 Test images

Table 3 Comparative study of proposed method

Test Images	Parameters	Method						
		Chen et al.[14]	Lu et al.[17] (k=2)	Yao et al.[18] (k=1)	Yao et al.[18] (k=2)	Lee & Huang[19]	Chi et al.[20] (k=2)	Proposed Algorithm
Med_1	Embedding capacity (bits)	131,072	263,938	198,447	297,113	283,172	263,938	262,144
	Embedding rate (bpp)	0.5	0.5	0.38	0.57	0.54	0.5	1.00
	PSNR of stego image (dB)	40.43	54.13	57.11	54.12	46.44	54.11	48.13
Med_1	Embedding capacity (bits)	131,072	263,938	198,447	297,113	283,172	263,938	262,144
	Embedding rate (bpp)	0.5	0.5	0.38	0.57	0.54	0.5	1.00
	PSNR of stego image (dB)	40.43	54.13	57.11	54.12	46.44	54.11	48.13
Med_2	Embedding capacity (bits)	131,072	435,042	326,395	489,949	466,982	435,042	262,144
	Embedding rate (bpp)	0.5	0.83	0.62	0.93	0.89	0.83	1.00
	PSNR of stego image (dB)	40.03	51.93	54.96	51.94	48.27	51.93	48.13
Med_3	Embedding capacity (bits)	131,072	410,056	307,349	461,536	439,633	410,056	262,144
	Embedding rate (bpp)	0.5	0.78	0.59	0.88	0.84	0.78	1.00
	PSNR of stego image (dB)	40.09	52.21	55.22	52.20	47.94	52.20	48.13
Med_4	Embedding capacity (bits)	131,072	412,744	309,832	464,394	442,530	412,744	262,144
	Embedding rate (bpp)	0.5	0.79	0.59	0.89	0.84	0.79	1.00
	PSNR of stego image (dB)	40.18	52.17	55.17	52.17	47.97	52.18	48.13
Med_5	Embedding capacity (bits)	131,072	389,730	296,039	444,105	422,548	389,730	262,144
	Embedding rate (bpp)	0.5	0.74	0.57	0.85	0.81	0.74	1.00
	PSNR of stego image (dB)	40.13	52.41	55.38	52.37	47.75	52.43	48.13
Med_6	Embedding capacity (bits)	131,072	187,118	141,527	212,163	198,637	187,118	262,144
	Embedding rate (bpp)	0.5	0.36	0.27	0.40	0.38	0.36	1.00
	PSNR of stego image (dB)	40.61	55.61	58.57	55.56	45.81	55.60	48.13
Med_7	Embedding capacity (bits)	131,072	391,546	296,119	444,103	422,931	391,546	262,144
	Embedding rate (bpp)	0.5	0.75	0.57	0.85	0.81	0.75	1.00
	PSNR of stego image (dB)	40.13	52.40	55.38	52.36	47.75	52.40	48.13
Med_8	Embedding capacity (bits)	131,072	491,094	378,955	568,746	542,176	491,094	262,144
	Embedding rate (bpp)	0.5	0.94	0.72	1.09	1.03	0.94	1.00
	PSNR of stego image (dB)	39.86	51.43	54.31	51.30	49.31	51.43	48.13

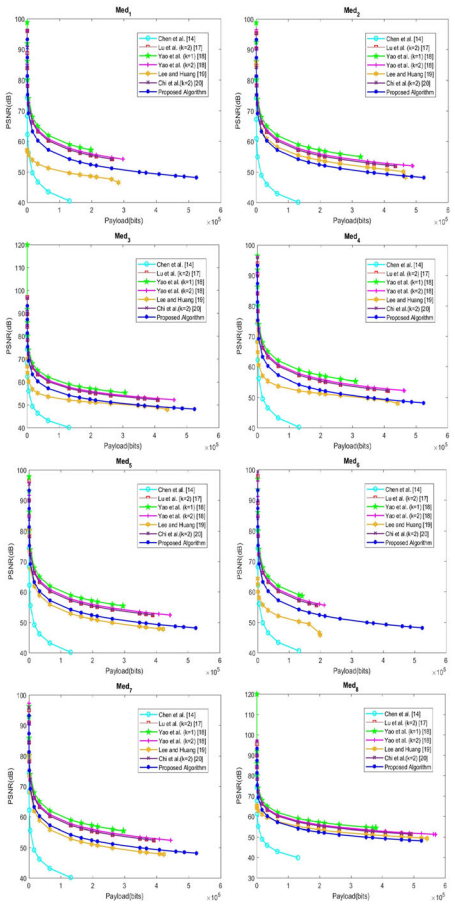

Fig. 3 PSNR value comparison against different payload on test images

that after extraction of the secret message, it reconstructs the original cover image at the receiver end successfully. **Proof**:-Consider any pixel value $(P_{u,v} = 2^k, k \leq 7)$ in cover image(CI) which is divided into three units $x_{u,v}$, $y_{u,v}$ and $z_{u,v}$ as follows-

$$\begin{cases} P_{u,v} = x_{u,v} + y_{u,v} + z_{u,v} \\ where \quad x_{u,v}, y_{u,v} = \left\lfloor \dfrac{P_{u,v}}{2} \right\rfloor = 2^{(k-1)} \\ z_{u,v} = mod\ \left(2^k, 2\right) = 0 \end{cases} \tag{15}$$

Assumed secret message ($w_{u,v} > 0$), after embedding $[w_{u,v}]$ into $[x_{u,v}]$, $[y_{u,v}]$ and $[z_{u,v}]$, they will be changed into $[x^*_{u,v}]$, $[y^*_{u,v}]$ and $[z^*_{u,v}]$ as follows-

$$\begin{cases} \left[x^*_{u,v}\right] = \left[2^{(k-1)} + w_{u,v}\right] \\ \left[y^*_{u,v}\right] = \left[2^{(k-1)} - w_{u,v} + 1\right] \\ \left[z^*_{u,v}\right] = [0] \end{cases} \tag{16}$$

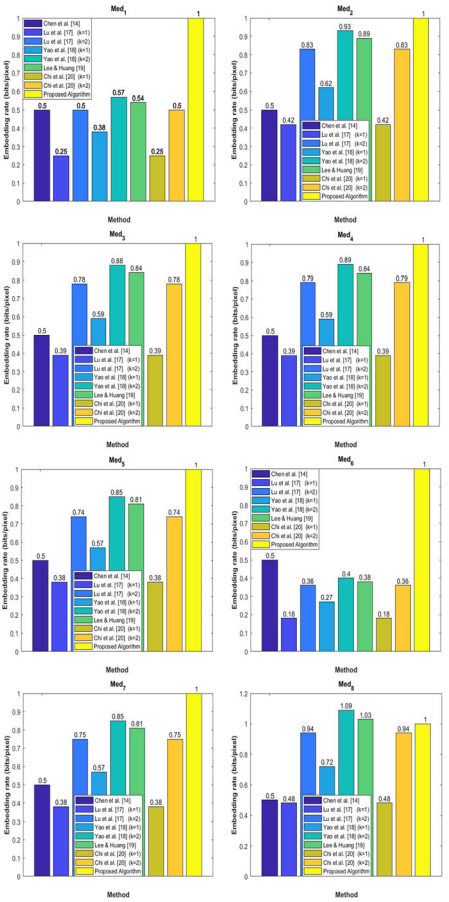

Fig. 4 Maximum Embedding rate comparison on test images

At receiver end, firstly $[x^*_{u,v}], [y^*_{u,v}], [z^*_{u,v}]$ are decrypted through Paillier cryptosystem[13] and extract the secret message $w_{u,v}$ and reconstruct cover image(CI) as follows:-

$$\begin{cases} x^*_{u,v} > y^*_{u,v}, w_{u,v} = 1 \\ m^*_{u,v} = x^*_{u,v} + y^*_{u,v} = 2^{(k-1)} + 2^{(k-1)} = 2^k \\ mod\left(\left(m^*_{u,v}, 2\right) \neq 1\right) \\ P_{u,v} = x^*_{u,v} + y^*_{u,v} + z^*_{u,v} = 2^{k-1} + 2^{k-1} + 0 = 2^k = P_{u,v} \end{cases} \tag{17}$$

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 done successfully at the receiver end. So, it is to be concluded that proposed method is reversible in nature.

Table 4 Comparative study of proposed method in terms of imperceptibility, payload and authenticity

Image	Method	Parameters					
		Imperceptibility			Payload (bpp)	Authentication Analysis	Encrypted Domain
		SSIM	NAE	NCC			
Med_1	Lu et al.[17]($k=2$)	0.9955	0.0123	0.9998	0.50	No	No
	Yao et al.[18] ($k=2$)	0.9954	0.0123	0.9999	0.57	No	No
	Lee & Huang[19]	0.9474	0.0179	0.9998	0.54	No	No
	Chi et al.[20]($k=2$)	0.9955	0.0122	0.9999	0.50	No	No
	Proposed Algorithm	0.9377	0.0145	0.9999	1.00	Yes	Yes
Med_2	Lu et al.[17]($k=2$)	0.9870	0.0175	0.9998	0.83	No	No
	Yao et al.[18] ($k=2$)	0.9860	0.0181	0.9998	0.93	No	No
	Lee & Huang[19]	0.9770	0.0155	0.9998	0.89	No	No
	Chi et al.[20]($k=2$)	0.9870	0.0176	0.9998	0.83	No	No
	Proposed Algorithm	0.9788	0.0117	0.9999	1.00	Yes	Yes
Med_3	Lu et al.[17]($k=2$)	0.9902	0.0096	0.9999	0.78	No	No
	Yao et al.[18] ($k=2$)	0.9898	0.0096	0.9999	0.88	No	No
	Lee & Huang[19]	0.9759	0.0088	0.9999	0.84	No	No
	Chi et al.[20]($k=2$)	0.9902	0.0096	0.9999	0.78	No	No
	Proposed Algorithm	0.9763	0.0123	1.0000	1.00	Yes	Yes
Med_4	Lu et al.[17]($k=2$)	0.9860	0.0080	1.0000	0.79	No	No
	Yao et al.[18] ($k=2$)	0.9854	0.0080	1.0000	0.89	No	No
	Lee & Huang[19]	0.9742	0.0073	1.0000	0.84	No	No
	Chi et al.[20]($k=2$)	0.9860	0.0080	1.0000	0.79	No	No
	Proposed Algorithm	0.9770	0.0102	1.0000	1.00	Yes	Yes
Med_5	Lu et al.[17]($k=2$)	0.9936	0.0141	0.9999	0.74	No	No
	Yao et al.[18] ($k=2$)	0.9917	0.0157	0.9999	0.85	No	No
	Lee & Huang[19]	0.9712	0.0151	0.9999	0.81	No	No
	Chi et al.[20]($k=2$)	0.9936	0.0139	0.9999	0.74	No	No
	Proposed Algorithm	0.9650	0.0110	0.9999	1.00	Yes	Yes
Med_6	Lu et al.[17]($k=2$)	0.9993	0.0114	0.9999	0.36	No	No
	Yao et al.[18] ($k=2$)	0.9993	0.0115	0.9999	0.40	No	No
	Lee & Huang[19]	0.9415	0.0237	0.9998	0.38	No	No
	Chi et al.[20]($k=2$)	0.9993	0.0113	0.9999	0.36	No	No
	Proposed Algorithm	0.9276	0.0122	0.9999	1.00	Yes	Yes
Med_7	Lu et al.[17]($k=2$)	0.9922	0.0208	0.9998	0.75	No	No
	Yao et al.[18] ($k=2$)	0.9909	0.0225	0.9998	0.85	No	No
	Lee & Huang[19]	0.9708	0.0216	0.9998	0.81	No	No
	Chi et al.[20]($k=2$)	0.9922	0.0206	0.9998	0.75	No	No
	Proposed Algorithm	0.9658	0.0101	0.9999	1.00	Yes	Yes
Med_8	Lu et al.[17]($k=2$)	0.9890	0.0184	0.9999	0.94	No	No
	Yao et al.[18] ($k=2$)	0.9871	0.0200	0.9999	1.09	No	No
	Lee & Huang[19]	0.9929	0.0151	0.9999	1.03	No	No
	Chi et al.[20]($k=2$)	0.9890	0.0181	0.9999	0.94	No	No
	Proposed Algorithm	0.9920	0.0114	0.9999	1.00	Yes	Yes
Average	Lu et al.[17]($k=2$)	0.9916	0.0140	0.9998	0.71	No	No
	Yao et al.[18] ($k=2$)	0.9907	0.0147	0.9998	0.80	No	No
	Lee & Huang[19]	0.9688	0.0156	0.9998	0.76	No	No
	Chi et al.[20]($k=2$)	0.9916	0.0139	0.9998	0.94	No	No
	Proposed Algorithm	0.9650	0.0116	0.9999	1.00	Yes	Yes

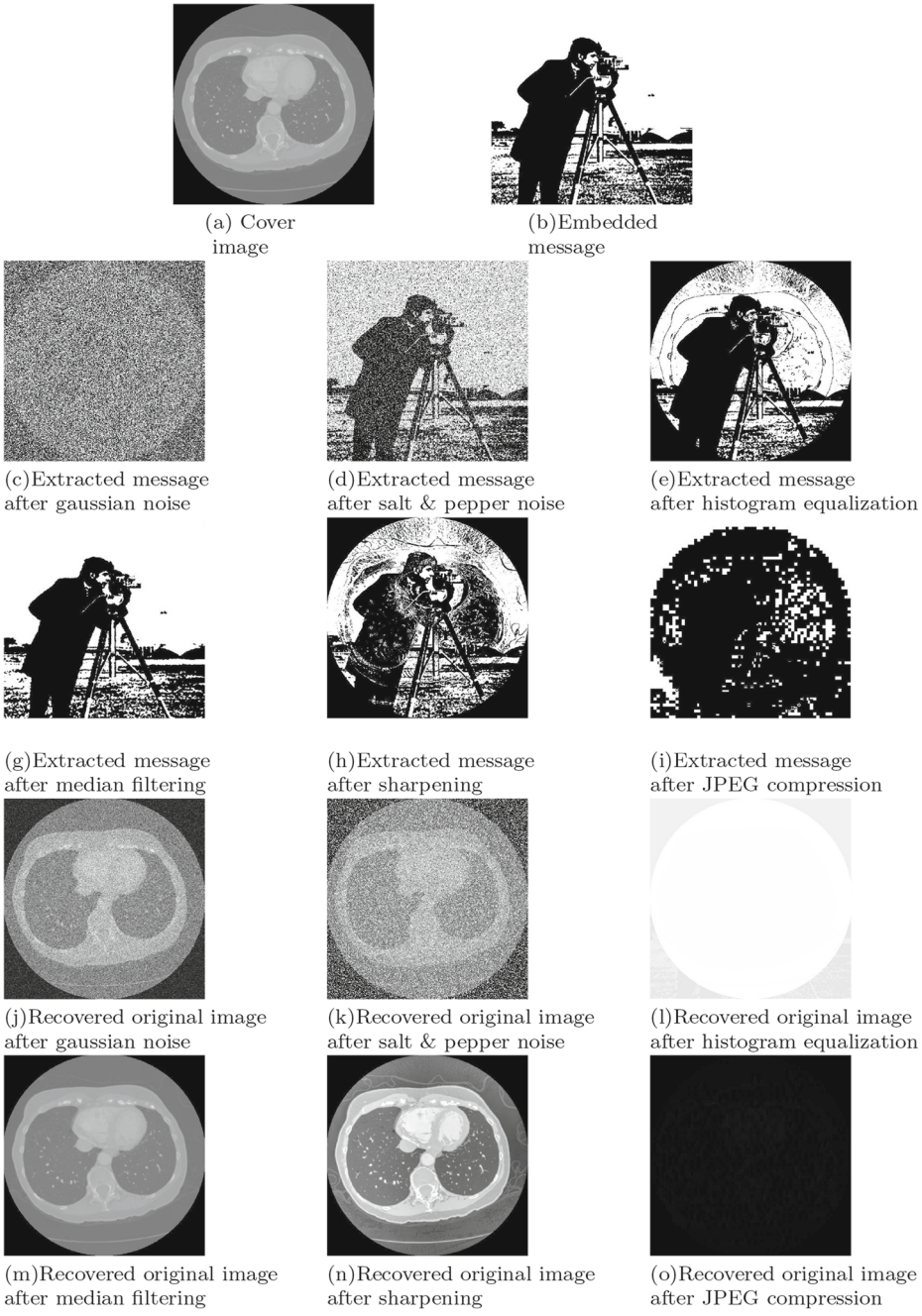

Fig. 5 Image quality under different type of attacks

5 Conclusion

Data hiding applications in the E-healthcare framework have an extreme indulgence with reversibility, high payload and content authentication. To recover the original medical image at the receiver end for diagnosis and transfer of high payload, an enhanced reversible data hiding technique in an encrypted domain has been proposed in this paper. The proposed algorithm gives higher embedding rate by embedding a single bit of patient data in $base_2$ numeral framework at every pixel of the cover image without any occurrence of underflow and overflow problem. As the proposed method does not incur underflow and overflow problem now it has been commissioned to embed and recover patient information precisely from low-intensity pixels too. This superlative quality makes the proposed method appropriate for utilization on medical images. An evaluation of the proposed algorithm with some state-of-the-art algorithms shows that the proposed method has higher embedding capacity and as such as far suitable for content authentication of EPI in a typical E-healthcare system. The proposed algorithm has been tested out in the spatial domain so that the embedded EPI is not robust to various types of noise attacks. In the future, we need to improve the robustness of the proposed method.

References

1. Yun Q Shi. Reversible data hiding. In *Int. workshop on digital watermarking*, pages 1–12. Springer, 2004
2. Tian Jun (2003) Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Technol. 13:890–6
3. Ni Zhicheng, Shi Yun-Qing, Ansari Nirwan, Wei Su (2006) Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol. 16:354–8
4. B Xiao, Lizhi Ying, and Yongfeng Huang. Reversible data hiding using histogram shifting in small blocks. In *Communications (ICC), 2010 IEEE Int. Conf on*, pages 1–6. IEEE, 2010
5. Mehmet Utku Celik, Gaurav Sharma, A Murat Tekalp, and Eli Saber. Lossless generalized-lsb data embedding. *IEEE Trans. Image Process.*, 14:253–13, 2005
6. Qian Zhenxing, Zhang Xinpeng, Ren Yanli, Feng Guorui (2016) Block cipher based separable reversible data hiding in encrypted images. Multimed Tools Appl 75:13749–17
7. Zhang Xinpeng (2011) Reversible data hiding in encrypted image. IEEE Signal Process Lett. 18:255–3
8. Xiaotian Wu, Sun Wei (2014) High-capacity reversible data hiding in encrypted images by prediction error. Signal Process. 104:387–13
9. Hong Wien, Chen Tung-Shou, Han-Yan Wu (2012) An improved reversible data hiding in encrypted images using side match. IEEE Signal Process Lett. 19:199–3
10. Kim Young-Sik, Kang Kyungjun, Lim Dae-Woon (2015) New reversible data hiding scheme for encrypted images using lattices. Appl Math Inform Sci 9:2627
11. Ma Kede, Zhang Weiming, Zhao Xianfeng, Nenghai Yu, Li Fenghua (2013) Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. Inf. Forensics Secur. 8:553–9
12. Liao Xin, Shu Changwen (2015) Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J. Visual Commun. Image Represent. 28:21–6
13. Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 223–15. Springer, 1999
14. Chen Yu-Chi, Shiu Chih-Wei, Horng Gwoboa (2014) Encrypted signal-based reversible data hiding with public key cryptosystem. J. Visual Commun. Image Represent. 25:1164–6
15. Xiaotian Wu, Chen Bing, Weng Jian (2016) Reversible data hiding for encrypted signals by homomorphic encryption and signal energy transfer. Journal of Visual Communication and Image Representation 41:58–64
16. Bhardwaj Rupali, Aggarwal Ashutosh (2018) An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. Pattern Recognit. Lett
17. Tzu-Chuen Lu, Jhih-Huei Wu, Huang Chun-Chih (2015) Dual-image-based reversible data hiding method using center folding strategy. Signal Process. 115:195–18

18. Yao Heng, Qin Chuan, Tang Zhenjun, Tian Ying (2017) Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion. Signal Process. 135:26–9
19. Lee Chin-Feng, Huang Yu-Lin (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. Telecommun Syst 52:2237–10
20. Chi Li-Pin, Chang-Han Wu, Chang Hsung-Pin (2018) Reversible data hiding in dual stegano-image using an improved center folding strategy. Multimed Tools Appl 77:8785–18
21. Tzu-Chuen Lu, Chi Li-Pin, Chang-Han Wu, Chang Hsung-Pin (2017) Reversible data hiding in dual stego-images using frequency-based encoding strategy. Multimed Tools Appl 76:23903–26
22. Shiu Hung-Jr, Lin Bor-Sing, Huang Chien-Hung, Chiang Pei-Ying, Lei Chin-Laung (2017) Preserving privacy of online digital physiological signals using blind and reversible steganography. Computer methods and programs in biomedicine 151:159–170
23. Shabir A Parah, Farhana Ahad, Javaid A Sheikh, and Ghulam Mohiuddin Bhat. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. *Journal of biomedical informatics*, 66:214–230, 2017
24. Shabir A Parah, Farhana Ahad, Javaid A Sheikh, Nazir A Loan, and Ghulam Mohiuddin Bhat. A new reversible and high capacity data hiding technique for e-healthcare applications. *Multimedia Tools and Applications*, 76(3):3943–3975, 2017
25. Siddharth Bhalerao, Irshad Ahmad Ansari, Anil Kumar, and Deepak Kumar Jain. A reversible and multipurpose ecg data hiding technique for telemedicine applications. *Pattern Recognition Letters*, 125: 463–473, 2019
26. Romany F Mansour and Elsaid M Abdelrahim. An evolutionary computing enriched rs attack resilient medical image steganography model for telemedicine applications. *Multidimensional Systems and Signal Processing*, 30(2):791–814, 2019