Multimedia Tools and Applications (2022) 81:1125–1152
https://doi.org/10.1007/s11042-021-11445-3

Hiding patient information in medical images : an encrypted dual image reversible and secure patient data hiding algorithm for E-healthcare

Rupali Bhardwaj[1]

Received: 19 November 2020 / Revised: 10 August 2021 / Accepted: 17 August 2021 /
Published online: 22 September 2021

Abstract
E-healthcare framework requires transfer of patient report to a specialist in a real time framework. Subsequently, any damage to patient information can prompt a wrong diagnosis that can be deadly for the patient. To guarantee a secure communication in E-healthcare framework, a high capacity dual image reversible data hiding algorithm has been presented in this paper. Highlight of proposed method is to embed $\lfloor \log_2(2 \times n + 1) \times NZ - 1 \rfloor$ binary bits of patient information whereas no overflow problem has occurred during embedding process. For authentication analysis of electronic patient information (EPI) at recipient end, a fragile watermark has also been embedded with EPI respectively. To prove the effectiveness of proposed method, experiments have been performed on different test images. The average embedding rate of 2.36 bpp for all test images which demonstrates that the method is capable for embedding high payload in comparison of others respectively.

Keywords E-healtcare · Privacy protection · Paillier cryptosystem · Reversible data hiding (RDH)

1 Introduction

Today, the Internet has turned out to be one of the significant part of our daily life. The E-healthcare framework is considered as connecting entities to the Internet and utilizing that association for remote checking of patient health. In current scenario, 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 wrong diagnosis to the patient. In this way, a protected and effective transmission of such information is required in E-healthcare framework.

✉ Rupali Bhardwaj
rupali.bhardwaj@thapar.edu

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

To ensure safe and secure transfer of patient report to a specialist, patient information is to be embedded in medical report through a data hiding method. But sometimes, at recipient end, doctor is not able to reconstruct the patient report while for a proper diagnosis, loss of information in patient report is not permitted. In such type of scenario, reversible data hiding is employed for embedding EPI in patient report respectively. 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 a great attention from the research community.

2 Literature review

There is a lot of research done in reversible data hiding domain; some are illustrated as follows- In the beginning, a reversible data hiding method was introduced by Shi [20]. Subsequently, difference expansion based reversible data hiding method was introduced by Tian [22], where a bit of secret message is hidden between a pair of pixels through difference computation. Histogram based reversible data hiding method is presented by Ni et al. [14] where secret message bits are embedded at peak of histogram of cover image respectively.

Reversible data hiding schemes in encrypted domain has attained an enormous consideration from the research community because secret message is embedded into cover image by data hider without knowing the original content of cover image and at recipient end, secret message and original cover image is recovered effectively. Zhang [26], segregated cover image into equivalent sized blocks and subsequently, every block is additionally partitioned into two sub-parts whereas a single bit of secret message is hidden in a block. Secret message is retrieved through fluctuation function computation relating to each block respectively. Yet, during computation of fluctuation value, edged pixels of cover image are to be barred which bring about a large amount of dissimilarity occurred between embedded and extracted secret message for small block sizes respectively. Disadvantage of Zhang [26] is eliminated by Hong et al. [6] through incorporation of edged pixels during fluctuation function computation. This brings about same peak-signal-to-noise-ratio(PSNR) worth and low bit error rate an incentive as contrast with Zhang [26] for small block sizes. Young-sik et al. [10] segregated cover image into equivalent sized blocks and subsequently, every block is additionally partitioned into two sub-parts where a a single bit of secret message is hidden in it utilizing idea of lattice. Using four-path connectivity, embeddable pixel's neighbors are not chosen for data hiding which brings about high PSNR worth and low bit error rate esteem. Ma et al. [12] proposed a reversible data hiding method where embedding space is reserved before encryption of original image. In the beginning, Chen et al. [4], encrypted cover image though Paillier cryptosystem [15], subsequently one bit of secret message is hidden per pixel pair respectively. Bhardwaj and Aggarwal [2] presented a reversible data hiding method where n bits of secret message are hidden per block by again partitioning them into n sub-blocks. Downside of this strategy is that for small sized blocks, secret message is not retrieved accurately which bring about a large amount of dissimilarity occurred between embedded and extracted secret message respectively. Lu et al. [23] proposed a dual reversible data hiding method where secret message is folded centrally. Subsequently, reduced secret message is embedded in cover image and produced dual stego images. Yao et al. [25] presented a dual reversible data hiding method dependent on pixel co-ordinate framework which bring about least contortion of pixel's co-ordinate esteem. Lee and Huang [11] presented a dual reversible data hiding method where secret message in $base_5$ numeral system is embedded with the help of orientation combination of pixel co-ordinates respectively. Chi et al. [5] introduced a powerful encoding method where repeatedly occurrence of secret message digits is encoded as the small absolute digit. The supported position signifies that for same embedding rate, proposed technique gave a higher PSNR than Lu et al. [23] method. Lu et al. [24] proposed a frequency encoding technique to wipe out the weakness of Lu et al. [23] method.

Rosiyadi et al. [18] proposed an efficient copyright protection scheme for e-government document images which combines the discrete cosine transform (DCT) and singular value decomposition (SVD) using a control parameter to avoid the false-positive problem. Horng et al. [8]r proposed an adaptive watermarking scheme for e-government document images. The adaptive scheme combined the discrete cosine transform (DCT) and the singular value decomposition (SVD) using luminance masking. As a core of masking model in the human visual system (HVS), luminance masking is implemented to improve noise sensitivity. Horng et al. [7] proposed an efficient blind copyright protection for e-government document images through a combination of the discrete cosine transform (DCT) and the singular value decomposition (SVD) based on genetic algorithm (GA). This combination could lead the watermarked image to be resistant to various attacks as well as to improve its performance, security and robustness. Rosiyadi et al. [19] presented a secret sharing based watermarking scheme using the Fractional Fourier Transform (FrFT) and Singular Value Decomposition (SVD). This method embeds the singular value matrix into the FrFT transformed sub-bands. The FrFT transformed sub-bands are computed from the Samir Secret Sharing (SSS) scheme. Shiu et al. [21] method used error correcting-coding technique where (n, m) hamming code is needed to embed $(n - m)$ bits of patient data into n number of ECG signals respectively. Parah et al. [16] 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 [17]. Bhalero et al. [1] used Deep neural network for predicting the sample values of ECG signal. Afterwards, patient data is embedded in ECG signals through prediction error expansion technique successfully. Mansour et al. [13] presented a robust reversible data hiding method in frequency domain where Discrete Ripplet Transformation method is used for embedding patient data in medical images effectively. The most important contribution of proposed work is to enhance embedding capacity as well as imperceptibility features through utilization of adaptive genetic algorithm for optimal pixel adjustment process effectively. Bhardwaj [3] presented an enhanced reversible data hiding method in the encrypted domain that gives a higher embedding rate 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. Table 1 presented imperceptibility analysis of some state-of-art methods respectively.

A detailed review of the stated work [3, 5, 11, 23–25] reveals that reporting methods 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 reversible and high

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[26]	Encrypted	Symmetric cryptosystem, Block division	36.81	0.25 bpp
Hong et al. [6]	Encrypted	Symmetric cryptosystem, Block division	36.82	0.25 bpp
Young et al. [10]	Encrypted	Symmetric cryptosystem, Block division	42.02	0.25 bpp
Chen et al. [4]	Encrypted	Paillier cryptosystem	40.18	1.00bpp
Bhardwaj and Aggarwal [2]	Encrypted	Symmetric cryptosystem, Block division	42.13	0.50 bpp
Lu et al. [23] (k=2)	Dual	Center folding	52.78	0.71 bpp
Yao et al. [25] (k=2)	Dual	Pixel co-ordinate system	52.75	0.80 bpp
Lee and Huang [11]	Dual	Orientation combination	47.65	0.76 bpp
Chi et al. [5] (k=2)	Dual	Dynamic encoding method	52.78	0.94 bpp
Shiu et al. [21]	E-healthcare	(1023,1013) Hamming code	17.98	66.67 (kbits)
Parah et al. [16]	E-healthcare	Intermediate significant bit substitution	46.36	0.75 bpp
Parah et al. [17]	E-healthcare	Intermediate significant bit substitution	46.55	0.9662 bpp
Bhalero et al. [1]	E-healthcare	Deep Neural Network	30.04	0.99 bps

capacity data hiding algorithm which is capable of content authentication for E-healthcare applications.

The key features of the proposed algorithm are summarized as follows:-

- Development of a high capacity dual image reversible data hiding scheme in the encrypted domain.
- $\lfloor \log_2(2 \times n + 1) \times NZ - 1 \rfloor$ binary bits of EPI is embedded in $base_{10}$ numeral framework to improve the embedding capacity.
- A fragile watermark is used for content authentication at the receiver end.

The rest of the paper is structured as follows- Proposed algorithm is described in Section3. Experimental study is described briefly in Section 4 and at last Section 5 concluded the paper.

3 Proposed algorithm

One of the vital concern to be addressed for the implementation of E-healthcare framework is security, authentication and copyright protection of the patient data respectively. Encryption is the most promising solution to maintain confidentiality and

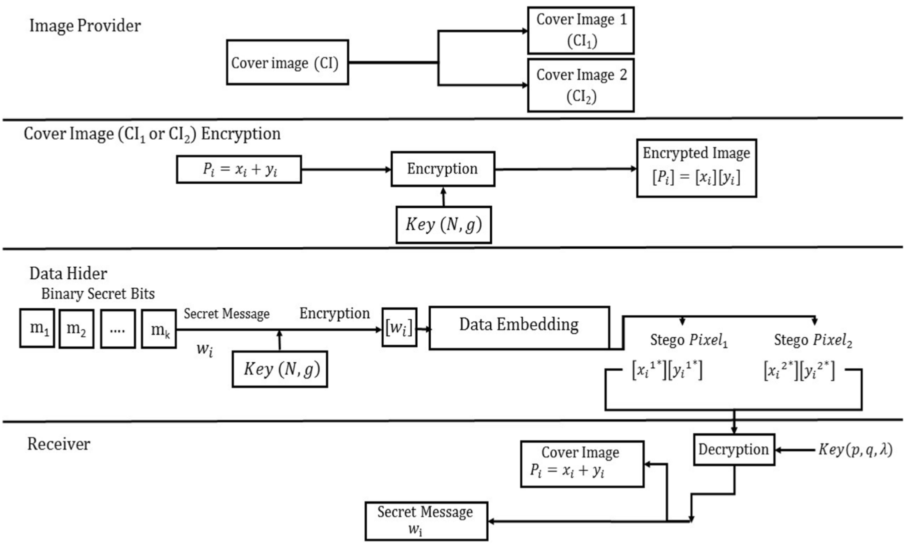


Fig. 1 Workflow of proposed algorithm

privacy of data. The integration of encryption and reversible data hiding technologies plays an important role in privacy protection. Dual-image reversible data hiding method can be functional in situations where embedding capacity and visual quality of stego images matter. From a security viewpoint, attackers cannot extract secret message without access to the dual images concurrently. Keeping this in view, an enhanced dual image reversible data hiding algorithm in the encrypted domain to embed electronic patient information(EPI) in cover image has been represented in this paper. Workflow diagram of proposed method has been shown in Fig. 1 respectively.

Cover image and secret message are encrypted through Paillier cryptosystem which is described briefly in subsection 3.1. Subsection 3.2 presented data embedding algorithm while subsection 3.3 presented data extraction and image recovery algorithm respectively.

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

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

- 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

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

The multiplicative homomorphic property,

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

3.2 Data embedding phase

Firstly, cover image (CI) of size $M \times N$ was set to $CI^1 = [P^1_{1,1}, P^1_{1,2}, ..., P^1_{M,N}]$ and $CI^2 = [P^2_{1,1}, P^2_{1,2}, ..., P^2_{M,N}]$, where M and N are the image height and width, respectively. Pixels of CI^1 and CI^2 are segmented into two types - seed pixels [(NZ^* ...255),(2n...255)] and the remaining pixels are called non-seed pixels. Now, embedded $\lfloor \log_2(2 \times n + 1) \times NZ - 1 \rfloor$ binary bits of secret message by changed over it into $base_{10}$ numeral framework at seed pixels of CI^2 and corresponding zone values are embedded at seed pixels of CI^1 respectively. Data embedding algorithm is discussed below as-

Algorithm 1: Data embedding phase

Input: Dual cover images CI^1 and CI^2 of size $M \times N$ where each pixel $P_{u,v} \in [0..255]$ and $u \leq [0...M-1], v \leq [0...N-1]$, binary secret message $(w = w_{1,1}||w_{1,2}||.......||w_{r,s})$ of size $A \times B$ and encryption key (N, g).
Output: Stego images SI_1 and SI_2 of size $M \times N$.

```
1: Each value $P^t_{u,v}$ (either $P^1_{u,v}$ in $CI^1$ or $P^2_{u,v}$ in $CI^2$) where $P^t_{u,v} \in (0....255)$ is
   divided into two units $x^t_{u,v}$ and $y^t_{u,v}$(either $x^1_{u,v}$ and $y^1_{u,v}$ in $CI^1$ or $x^2_{u,v}$ and $y^2_{u,v}$
   in $CI^2$ ) as follows-

   $$\begin{cases} P^t_{u,v} = x^t_{u,v} + y^t_{u,v} \\ where \quad x^t_{u,v} = \lfloor \frac{P^t_{u,v}}{2} \rfloor, \\ y^t_{u,v} = P^t_{u,v} - x^t_{u,v} \end{cases} \tag{6}$$

   Now $x^t_{u,v}$ and $y^t_{u,v}$ are encrypted through Paillier cryptosystem [9] to produce
   encrypted $Encr[x^t_{u,v}]$ and $Encr[y^t_{u,v}]$ respectively.

2: To avoid image distortion caused by a large value of secret message $(w_{r,s})$, it is
   further reduced by dividing $w_{r,s}$ into multiple zones, $z_{u,v}$ using method of Lu et
   al.[26]. Total number of elements in a zone is $(2 \times n + 1)$ where maximum folded
   value is $n$ and minimum folded value is $-n$ and total number of zones is $NZ$
   respectively. Reduced zone value, $z^*_{u,v}$ for embedding in $CI^1$ and reduced secret
   message value, $w^*_{r,s}$ for embedding in $CI^2$ is computed as follows-

   $$\begin{cases} z_{u,v} = \lfloor \frac{w_{r,s}}{2 \times n+1} \rfloor \\ NZ^* = \lceil \frac{2^{\lfloor \log_2 (2 \times n+1) \times NZ-1 \rfloor}}{2n+1} \rceil \\ z^*_{u,v} = z_{u,v} - \lfloor \frac{NZ^*}{2} \rfloor \\ CZ_{u,v} = z_{u,v} \times (2 \times n + 1) + n \\ w^*_{r,s} = w_{r,s} - CZ_{u,v} \end{cases} \tag{7}$$

   Now $z^*_{u,v}$ and $w^*_{r,s}$ are encrypted through Paillier cryptosystem[9] to produce
   encrypted $Encr[z^*_{u,v}]$ and $Encr[w^*_{r,s}]$ respectively.

3: Assumed $Encr[P^t_{u,v}] = Encr[P^t_i]$, $Encr[x^t_{u,v}] = Encr[x^t_i]$, $Encr[y^t_{u,v}] =
   Encr[y^t_i]$, $Encr[z^*_{u,v}] = Encr[z^*_i]$ and $Encr[w^*_{r,s}] = Encr[w^*_i]$ respectively.

4: After that, embedded secret message $Encr[w^{t'}_i]$(either $Encr[w^{1'}_i]$ or $Encr[w^{2'}_i]$)
   into $Encr[P^t_i]$ (either $Encr[P^2_i]$ where $Encr[w^{2'}_i]$ represented $Encr[w^*_i]$ and cor-
   responding zone value $Encr[z^*_i]$ is represented through $Encr[w^{1'}_i]$ into $Encr[P^{1'}_i]$
   respectively.

5: Embed the secret message $Encr[w^{t'}_i]$ into $Encr[x^t_i]$ and $Encr[y^t_i]$ to produce
   $Encr[x^{t^*}_i + y^{t^*}_i] = Encr[x^{t^*}_i]\, Encr[y^{t^*}_i]$ as follows:-
   a: if $(Encr[P^t_i] = Encr[P^1_i])$ then
   b:     $Encr[R] = Encr[NZ^*]$
   c: else
   d:     if $(Encr[P^t_i] = Encr[P^2_i])$ then
   e:         $Encr[R] = Encr[2n]$
   f:     end if
   g: end if
   h: if $(Encr[P^t_i] \geq Encr[R])$ then
   i:     $Encr[x^{t^*}_i] = Encr[x^t_i] + Encr[w^{t'}_i] = Encr[x^t_i + w^{t'}_i]$
   j:     $Encr[y^{t^*}_i] = Encr[y^t_i] - Encr[w^{t'}_i] = Encr[y^t_i - w^{t'}_i]$
   k: end if

6:   Repeat steps from 1 to 5 for all the pixel values of dual cover images to construct
   stego images, $SI_1$ and $SI_2$ respectively.
```

3.3 Data extraction and image recovery phase

The process of extraction of secret message in *base*$_2$ numeral framework and recovery of original cover image is shown in the following algorithm-

Algorithm 2: Data extraction and image recovery

Input: Stego images SI_1 and SI_2 of size $M \times N$, value of n and NZ 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, $(w = w_{1,1}||w_{1,2}||.......||w_{r,s})$ of size $A \times B$.

1: Firstly, $Encr[x_i^{1^*}]$, $Encr[y_i^{1^*}]$, $Encr[x_i^{2^*}]$ and $Encr[y_i^{2^*}]$ are decrypted through Paillier cryptosystem [9] where each directly decrypted pixel is considered as a unit of $P_i^{1'} = x_i^{1^*} + y_i^{1^*}$ and $P_i^{2'} = x_i^{2^*} + y_i^{2^*}$. After that extracted secret message $w_i^{t'}$ (either $w_i^{1'}$ or $w_i^{2'}$) from $P_i^{t'}$ (either $P_i^{2'}$ where $w_i^{2'}$ represented w_i^* and corresponding zone value z_i^* is represented through $w_i^{1'}$ into $P_i^{1'}$ respectively.

2: Extract the secret message $w_i^{'}$ from $P_i^{t'}$ as follows:-

```
a: if ($P_i^{t'} \geq R$) then;($R = NZ^*$ ,$if$ ($P_i^{t'} = P_i^{1'}$)) $or$ ($R = 2n$ ,$if$ ($P_i^{t'} = P_i^{2'}$))
b:     $diff_i^{t'} = x_i^{t^*} - y_i^{t^*}$
c:     if ($mod$ ($diff_i^{t'}$ ,2 = 0)) then
d:         $w_i^{t'} = \frac{diff_i^{t'}}{2}$
e:     else
f:         $w_i^{t'} = \frac{diff_i^{t'}+1}{2}$
g:     end if
h: end if
```

3: Final zone value(z_i) and corresponding secret message value(w_i) is computed as follows-

$$\begin{cases} NZ^* = \lceil \frac{2^{\lfloor \log_2(2\times n+1)\times NZ-1\rfloor}}{2n+1} \rceil \\ z_i = z_i^* + \lfloor \frac{NZ^*}{2} \rfloor \\ w_i = (2\times n+1)\times z_i + w_i^* + n \end{cases} \tag{8}$$

Now, final secret message(w_i) is represented in $base_2$ numeral framework by representing them through $\lfloor \log_2(2\times n+1)\times NZ - 1\rfloor$ bits in sequence.

4: Assume $P_i^{t'} = P_{u,v}^{t'}$ and $w_i = w_{r,s}$. Now, recovery of original pixel value is given as follows:-

$$\begin{cases} P_{u,v} = \frac{P_{u,v}^{1'}+P_{u,v}^{2'}}{2} \end{cases} \tag{9}$$

5: Repeat the steps from 1 to 4 for all the pixel values of stego images to reconstruct original cover image (CI) and secret message (w) respectively.

$$\begin{cases} w = w_{1,1}||w_{1,2}||.......||w_{r,s} \end{cases} \tag{10}$$

Table 2 Working of proposed method

Dual cover images, $CI^1 = \begin{bmatrix}112 & 153\\ 167 & 255\end{bmatrix}$ and $CI^2 = \begin{bmatrix}112 & 153\\ 167 & 255\end{bmatrix}$

$x^1_{u,v} = \begin{bmatrix}56 & 76\\ 83 & 127\end{bmatrix}$, $y^1_{u,v} = \begin{bmatrix}56 & 77\\ 84 & 128\end{bmatrix}$, $x^2_{u,v} = \begin{bmatrix}56 & 76\\ 83 & 127\end{bmatrix}$, $y^2_{u,v} = \begin{bmatrix}56 & 77\\ 84 & 128\end{bmatrix}$

$Encrypted\ x^1_{u,v} = [x^1_{u,v}] = \begin{bmatrix}[56] & [76]\\ [83] & [127]\end{bmatrix}$, $Encrypted\ y^1_{u,v} = [y^1_{u,v}] = \begin{bmatrix}[56] & [77]\\ [84] & [128]\end{bmatrix}$

$Encrypted\ x^2_{u,v} = [x^2_{u,v}] = \begin{bmatrix}[56] & [76]\\ [83] & [127]\end{bmatrix}$, $Encrypted\ y^2_{u,v} = [y^2_{u,v}] = \begin{bmatrix}[56] & [77]\\ [84] & [128]\end{bmatrix}$

Data Embedding Phase (Algorithm 1)

Convert w_i into $base_{10}$ numeral framework by taking $\lfloor \log_2(2\times n+1)\times NZ-1\rfloor = \lfloor \log_2(2\times 1+1)\times 3-1\rfloor = \log_2(2^3)$=3 bits in sequence.

To avoid image distortion caused by a large value of secret message(w_i), it is divided into multiple zones as follows-

$Secret\ message, w_i$ (assumed) = 1 0 1 0 0 0 0 1 1 1 1 1

So, w_i into $base_{10}$ numeral framework is as follows-5 0 3 7

Corresponding zone value (z_i) is calculated as follows-

$z_1 = \lfloor \frac{w_1}{2\times n+1} \rfloor = \lfloor \frac{5}{2\times 1+1} \rfloor = 1$

$z_2 = \lfloor \frac{w_2}{2\times n+1} \rfloor = \lfloor \frac{0}{2\times 1+1} \rfloor = 0$

$z_3 = \lfloor \frac{w_3}{2\times n+1} \rfloor = \lfloor \frac{3}{2\times 1+1} \rfloor = 1$

$z_4 = \lfloor \frac{w_4}{2\times n+1} \rfloor = \lfloor \frac{7}{2\times 1+1} \rfloor = 2$

Reduced zone value (z^*_i) for embedding in CI^1 is calculated as follows-

$NZ^* = \lceil \frac{2^{\lfloor \log_2(2\times n+1)\times NZ-1\rfloor}}{2n+1} \rceil = \lceil \frac{2^3}{3} \rceil = \lceil \frac{8}{3} \rceil = 3$

$z^*_1 = z_1 - \lfloor \frac{NZ^*}{2} \rfloor = 1 - \lfloor \frac{3}{2} \rfloor = 0$

$z^*_2 = z_2 - \lfloor \frac{NZ^*}{2} \rfloor = 0 - \lfloor \frac{3}{2} \rfloor = -1$

$z^*_3 = z_3 - \lfloor \frac{NZ^*}{2} \rfloor = 1 - \lfloor \frac{3}{2} \rfloor = 0$

$z^*_4 = z_4 - \lfloor \frac{NZ^*}{2} \rfloor = 2 - \lfloor \frac{3}{2} \rfloor = 1$

Reduced secret message (w^*_i) for embedding in CI^2 is calculated as follows-

$CZ_1 = z_1 \times (2\times n+1) + n = 1\times(2\times 1+1)+1 = 4$

$w^*_1 = w_1 - CZ_1 = 5 - 4 = 1$

$CZ_2 = z_2 \times (2\times n+1) + n = 0\times(2\times 1+1)+1 = 1$

$w^*_2 = w_2 - CZ_2 = 0 - 1 = -1$

$CZ_3 = z_3 \times (2\times n+1) + n = 1\times(2\times 1+1)+1 = 4$

$w^*_3 = w_3 - CZ_3 = 3 - 4 = -1$

$CZ_4 = z_4 \times (2\times n+1) + n = 2\times(2\times 1+1)+1 = 7$

$w^*_4 = w_4 - CZ_4 = 7 - 7 = 0$

Now z^*_i and w^*_i are encrypted through Paillier cryptosystem [15] to produce $[z^*_i]$ and $[w^*_i]$ respectively.

Reduced zone value (z^*_i) is embedded in CI^1 as follows-

$[x^{1^*}_{u,v}] = \begin{bmatrix}[56] & [75]\\ [83] & [128]\end{bmatrix}$, $[y^{1^*}_{u,v}] = \begin{bmatrix}[56] & [78]\\ [84] & [127]\end{bmatrix}$

Reduced secret message (w^*_i) is embedded in CI^2 as follows-

Table 2 (continued)

Dual cover images, $CI^1=\begin{bmatrix}112 & 153\\167 & 255\end{bmatrix}$ and $CI^2=\begin{bmatrix}112 & 153\\167 & 255\end{bmatrix}$

$[x^{2^*}_{u,v}]=\begin{bmatrix}[57] & [75]\\ [82] & [127]\end{bmatrix}$, $[y^{2^*}_{u,v}]=\begin{bmatrix}[55] & [78]\\ [85] & [128]\end{bmatrix}$

Data Extraction and Image Recovery Phase (Algorithm 2)

Firstly $[x^{1^*}_{u,v}]$, $[y^{1^*}_{u,v}]$, $[x^{2^*}_{u,v}]$ and $[y^{2^*}_{u,v}]$ are decrypted. So that,

$x^{1^*}_{u,v}=\begin{bmatrix}56 & 75\\83 & 128\end{bmatrix}$, $y^{1^*}_{u,v}=\begin{bmatrix}56 & 78\\84 & 127\end{bmatrix}$, $x^{2^*}_{u,v}=\begin{bmatrix}57 & 75\\82 & 127\end{bmatrix}$, $y^{2^*}_{u,v}=\begin{bmatrix}55 & 78\\85 & 128\end{bmatrix}$

$diff^{1'}_{u,v}=\begin{bmatrix}0 & -3\\-1 & 1\end{bmatrix}$, $diff^{2'}_{u,v}=\begin{bmatrix}2 & -3\\-3 & -1\end{bmatrix}$

$z_i^* = [0-1\ 0\ 1]$, $w_i^* = [1-1-10]$

Zone value (z_i) is computed as follows-

$NZ^* = \lceil \frac{2^{\lfloor \log_2(2\times n+1)\times NZ-1\rfloor}}{2n+1}\rceil = \lceil \frac{2^3}{3}\rceil = \lceil \frac{8}{3}\rceil = 3$

$z_1 = z_1^* + \lfloor \frac{NZ^*}{2}\rfloor = 0 + \lfloor \frac{3}{2}\rfloor = 1$

$z_2 = z_2^* + \lfloor \frac{NZ^*}{2}\rfloor = -1 + \lfloor \frac{3}{2}\rfloor = 0$

$z_3 = z_3^* + \lfloor \frac{NZ^*}{2}\rfloor = 0 + \lfloor \frac{3}{2}\rfloor = 1$

$z_4 = z_4^* + \lfloor \frac{NZ^*}{2}\rfloor = 1 + \lfloor \frac{3}{2}\rfloor = 2$

Secret message (w_i) is computed as follows-

$w_1 = (2\times n+1)\times z_1 + w_1^* + n = (2\times 1+1)\times 1+1+1 = 5$

$w_2 = (2\times n+1)\times z_2 + w_2^* + n = (2\times 1+1)\times 0-1+1 = 0$

$w_3 = (2\times n+1)\times z_3 + w_3^* + n = (2\times 1+1)\times 1-1+1 = 3$

$w_4 = (2\times n+1)\times z_4 + w_4^* + n = (2\times 1+1)\times 2+0+1 = 7$

Convert $w_1w_2w_3w_4$ into $base_2$ numeral framework by representing them through $\lfloor \log_2(2\times n+1)\times NZ-1\rfloor = \lfloor \log_2(2\times 1+1)\times 3-1\rfloor = \log_2(2^3) = 3$ bits in sequence.

so that, extraced secret message, $w_i = 1\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1$

Reconstructed cover images, $CI^1=\begin{bmatrix}112 & 153\\167 & 255\end{bmatrix}$ and $CI^2=\begin{bmatrix}112 & 153\\167 & 255\end{bmatrix}$

Reconstructed cover images, $CI = \frac{CI^1+CI^2}{2} = \begin{bmatrix}112 & 153\\167 & 255\end{bmatrix}$

Example: Execution of proposed algorithm for ($n = 1$) and ($NZ = 3$) on cover image(CI) is shown in Table 2 where cover image(CI) is $\begin{bmatrix}112 & 153\\167 & 255\end{bmatrix}$ respectively.

4 Results and discussion

This section presented experimental study of proposed method carried out using MATLAB R2017a platform on different 512×512 test images obtained from open-source image database (USC-SIPI) whereas medical images obtained from the database of The Cancer Imaging Archive (TCIA) as shown in Fig. 2 respectively. The performance of the proposed method has been evaluated in terms of metrics like Peak Signal to Noise

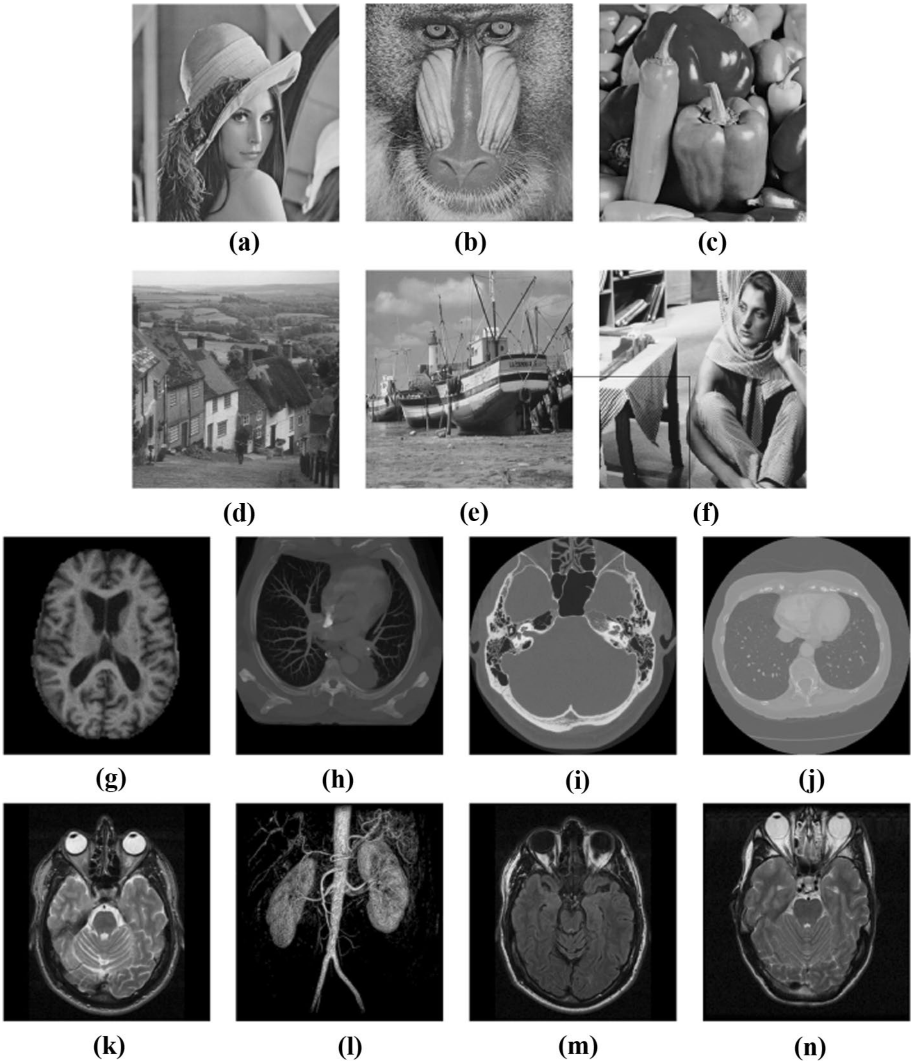


Fig. 2 Test images

Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index Matrix (SSIM), Normalized Absolute Error (NAE), Normalized Cross-correlation (NCC) and Embedding Rate (bpp) respectively. These metrics are defined as follows -

$$PSNR = 10log_{10}\frac{255^2}{MSE} \tag{6}$$

where

$$MSE = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}(f(x,y) - \bar{f}(x,y))^2 \tag{7}$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c2)} \tag{8}$$

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, $c_1 = (k_1L)^2, c_2 = (k2L)^2, L = (2^8 - 1), k_1 = 0.01$ and $k_2 = 0.03$ respectively.

$$NAE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} |f(x, y) - \hat{f}(x, y)|}{\sum_{x=1}^{M}\sum_{y=1}^{N} f(x, y)} \tag{9}$$

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} f(x, y)\hat{f}(x, y)}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N} f(x, y)^2 \sum_{x=1}^{M}\sum_{y=1}^{N} \hat{f}(x, y)^2}} \tag{10}$$

The embedding rate indicated by R is described as pure payload of cover image (CI^2) of size $M \times N$ respectively. It is defined as pursues:-

$$R = \frac{Pure\_payload}{2 \times M \times N} \tag{11}$$

where pure payload is the total number of binary bits of secret message which are embedded in cover image (CI^2) respectively.

4.1 Result analysis

In this section, performance of the proposed method is evaluated and compared it with some existing state-of-the-art methods of Lu et al. ($k = 3$)[23], Yao et al. ($k = 3$)[25], Lee & Huang [11], Chi et al. ($k = 3$)[5], Lu et al. ($k = 3$)[24] and Bhardwaj [3] respectively. Table 3 exhibits the assessment of the proposed method with all other compared methods with reference to maximum embedding capacity (bits), maximum embedding rate (bpp) and visual quality of stego images observed on test images (Fig. 2) respectively. It tends to be observed from Table 3 that maximum average embedding rate (2.36 bpp) is obtained by proposed method with an average visual quality of stego images (∞ dB) respectively. The maximum embedding rate of proposed method is higher than other compared methods with maintaining a good visual quality of the stego images too. Hence, embedding rate achieved by the proposed method is at standard with all the looked at methods. Fig. 4 presents the comparative study of visual quality of stego images vs embedding rate achieved by the proposed and compared methods on different payload values respectively. It is observed from Fig. 4 that even at high payload value, the proposed method gave good visual quality of stego image while looked at strategies didn't on the grounds that their decreased embedding rates can't work at high payloads. Fig. 5 presents the comparison in maximum embedding rate and average embedding rate attained by the proposed and compared strategies respectively. It is noted from Fig. 5 that proposed method gave a high embedding rate while compared schemes did not because their decreased embedding rates can't work at high payloads. The superior performance of the proposed method on all test images is credited to its capacity to deal with the high-intensity pixels, which could cause the overflow issue during process of data embedding respectively. In the looked at strategies, they disregard these high-intensity pixels, or continuously end mark them as non-embeddable cases.

Table 4 demonstrates the examination of the proposed algorithm($n = 5, NZ = 8$) with state-of-the-art algorithms Lu et al. ($k = 3$)[23], Yao et al. ($k = 3$)[25], Lee & Huang [11], Chi et al. ($k = 3$)[5] and Lu et al. ($k = 3$)[24] with reference to image quality metrics like with reference to Structural Similarity Index Matrix (SSIM), Normalized Absolute error (NAE), Normalized Cross-correlation (NCC) and Embedding Rate attained on medical images respectively. It is evident from the average values of quality metrics, high SSIM value combined with low NAE value and NCC value of approximate unity indicate that proposed method is able to provide a high visual quality of stego image for an embedding rate of 2.30 bpp respectively. Proposed method provides a high embedding capacity in encrypted domain with content authentication at recipient end while all other compared methods didn't as observed from Table 4 respectively. Hence, it is concluded that, for all kind of test images, a high embedding capacity is achieved by the proposed method with maintaining the visual nature of stego images as well.

4.2 Authentication analysis

To assess the performance of the proposed algorithm for its secret message validation, some well known image processing attacks are executed on dual stego images respectively. For secret message validation at the recipient end, a watermark (Fig. 3) of size 256 × 256 is hidden within the cover image. At the beneficiary end, extracted watermark is matched with original watermark, if the compared watermarks are not same to each other, it is acknowledged that the stego images and the secret message is not authentic. The validation examination is completed to figure out the level of deterioration in secret message through computation of BER (bit error rate) as follows-

$$BER = \frac{\sum_{x=1}^{P} \sum_{y=1}^{Q} \left(z(x,y) \oplus z^{'}(x,y) \right) \times 100}{Count\_of\_embedded\_bits} \tag{12}$$

Here, z and $z^{'}$ of size $P \times Q$ is embedded and extracted watermark respectively. From the results for various attacks on proposed algorithm as shown in Table 5, it is observed that

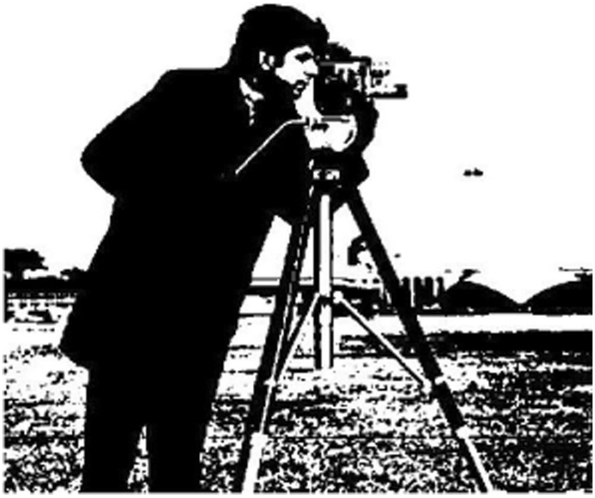


Fig. 3 Watermark

Table 3 Comparative study of proposed method

Test Images	Parameters	Method								
		Lu et al. [23]	Yao et al. [25]	Lee & Huang [11]	Chi et al. [5]	Lu et al. [24]	Bhardwaj [3]	Proposed Algorithm	Proposed Algorithm	Proposed Algorithm
		$(k = 3)$	$(k = 3)$		$(k = 3)$	$(k = 3)$		$(n = 2)$	$(n = 3)$	$(n = 5)$
								$(NZ = 5)$	$(NZ = 6)$	$(NZ = 8)$
Lena	Payload (bits)	786,432	819,155	562,388	786,432	786,432	524,288	1,048,576	1,310,720	1,572,864
	Embedding rate (bpp)	1.50	1.56	1.07	1.50	1.50	2.00	2.00	2.50	3.00
	PSNR of stego image (dB)	46.38	46.35	49.63	46.35	46.38	∞	∞	∞	∞
Baboon	Payload (bits)	786,042	819,020	561,965	786,042	786,042	524,288	1,048,144	1,309,980	1,571,568
	Embedding rate (bpp)	1.49	1.56	1.07	1.49	1.49	2.00	1.99	2.49	2.99
	PSNR of stego image (dB)	46.36	46.37	49.63	46.38	46.38	63.96	∞	∞	∞
Pepper	Payload (bits)	777,474	818,266	562,113	777,474	777,474	524,288	1,048,328	1,309,845	1,569,342
	Embedding rate (bpp)	1.48	1.56	1.07	1.48	1.48	2.00	1.99	2.49	2.99
	PSNR of stego image (dB)	46.41	46.38	49.63	46.39	46.43	49.20	∞	∞	∞
Goldhill	Payload (bits)	786,432	819,260	786,432	786,432	786,432	524,288	1,048,576	1,310,720	1,572,864
	Embedding rate (bpp)	1.50	1.56	1.07	1.50	1.50	2.00	2.00	2.50	3.00

Table 3 (continued)

Test Images	**Parameters**	**Method**								
		Lu et al. [23]	Yao et al. [25]	Lee & Huang [11]	Chi et al. [5]	Lu et al. [24]	Bhardwaj [3]	Proposed Algorithm	Proposed Algorithm	Proposed Algorithm
		($k = 3$)	($k = 3$)		($k = 3$)	($k = 3$)		($n = 2$)	($n = 3$)	($n = 5$)
								($NZ = 5$)	($NZ = 6$)	($NZ = 8$)
	PSNR of stego image (dB)	46.36	46.36	49.63	46.37	46.38	∞	∞	∞	∞
Sailboat	Payload (bits)	786,348	819,042	562,019	786,348	786,348	524,288	1,048,576	1,310,720	1,572,864
	Embedding rate (bpp)	1.49	1.56	1.07	1.49	1.49	2.00	2.00	2.50	3.00
	PSNR of stego image (dB)	46.37	46.36	49.63	46.36	46.38	71.12	∞	∞	∞
Barbara	Payload (bits)	786,432	819,321	562,465	786,432	786,432	524,288	1,048,576	1,310,720	1,572,864
	Embedding rate (bpp)	1.50	1.56	1.07	1.50	1.50	2.00	2.00	2.50	3.00
	PSNR of stego image (dB)	46.37	46.35	49.63	46.37	46.38	∞	∞	∞	∞
Med_1	Embedding capacity (bits)	394,863	412,320	283,172	394,863	394,863	524,288	526,484	657,665	788,058
	Embedding rate (bpp)	0.75	0.79	0.54	0.75	0.75	2.00	1.00	1.25	1.50
	PSNR of stego image (dB)	49.35	49.35	46.44	49.36	49.37	36.13	∞	∞	∞

Table 3 (continued)

Test Images	Parameters	Method								
		Lu et al. [23] ($k = 3$)	Yao et al. [25] ($k = 3$)	Lee & Huang [11]	Chi et al. [5] ($k = 3$)	Lu et al. [24] ($k = 3$)	Bhardwaj [3]	Proposed Algorithm ($n = 2$) ($NZ = 5$)	Proposed Algorithm ($n = 3$) ($NZ = 6$)	Proposed Algorithm ($n = 5$) ($NZ = 8$)
Med_2	Embedding capacity (bits)	637,011	679,816	466,982	637,011	637,011	524,288	849,348	1,053,795	1,255,200
	Embedding rate (bpp)	1.22	1.30	0.89	1.22	1.22	2.00	1.62	2.01	2.39
	PSNR of stego image (dB)	47.29	47.17	48.27	47.29	47.29	40.16	∞	∞	∞
Med_3	Embedding capacity (bits)	615,084	640,863	439,633	615,084	615,084	524,288	820,112	1,025,140	1,230,168
	Embedding rate (bpp)	1.17	1.22	0.83	1.17	1.17	2.00	1.56	1.95	2.34
	PSNR of stego image (dB)	47.44	47.42	47.94	47.44	47.45	39.73	∞	∞	∞
Med_4	Embedding capacity (bits)	619,116	644,666	442,530	619,116	619,116	524,288	825,488	1,031,860	1,238,232
	Embedding rate (bpp)	1.18	1.23	0.84	1.18	1.18	2.00	1.57	1.96	2.36
	PSNR of stego image (dB)	47.41	47.41	47.97	47.41	47.41	39.83	∞	∞	∞

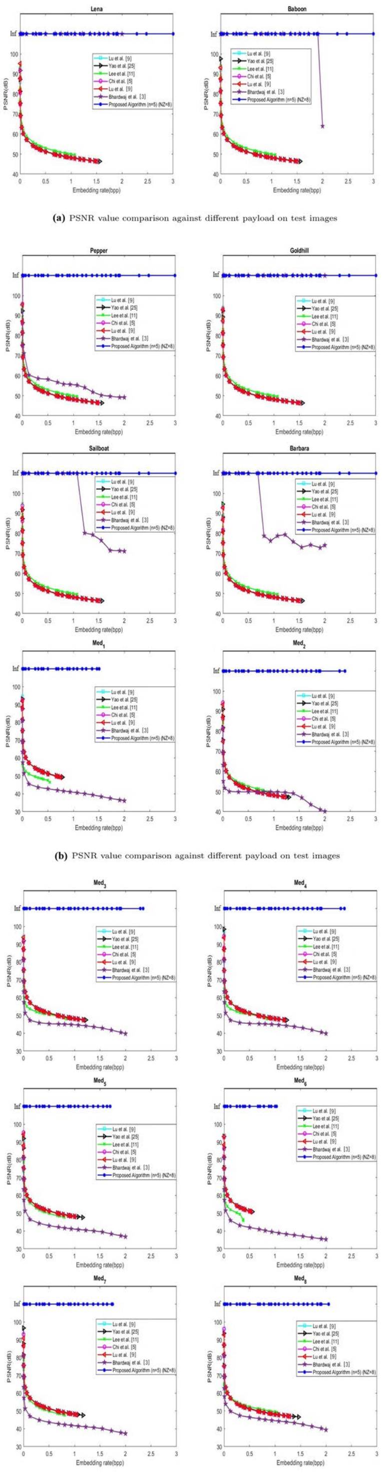
Table 3 (continued)

Test Images	Parameters	Method								
		Lu et al. [23]	Yao et al. [25]	Lee & Huang [11]	Chi et al. [5]	Lu et al. [24]	Bhardwaj [3]	Proposed Algorithm	Proposed Algorithm	Proposed Algorithm
		($k = 3$)	($k = 3$)		($k = 3$)	($k = 3$)		($n = 2$)	($n = 3$)	($n = 5$)
								($NZ = 5$)	($NZ = 6$)	($NZ = 8$)
Med_5	Embedding capacity (bits)	527,349	608,914	422,548	527,349	527,349	524,288	703,132	819,415	890,820
	Embedding rate (bpp)	1.00	1.16	0.80	1.00	1.00	2.00	1.34	1.56	1.69
	PSNR of stego image (dB)	48.11	47.66	47.75	48.11	48.12	36.85	∞	∞	∞
Med_6	Embedding capacity (bits)	276,678	292,414	198,637	276,678	276,678	524,288	368,908	457,825	541,542
	Embedding rate (bpp)	0.53	0.56	0.37	0.53	0.53	2.00	0.70	0.87	1.03
	PSNR of stego image (dB)	50.90	50.83	45.81	50.90	50.93	35.32	∞	∞	∞
Med_7	Embedding capacity (bits)	545,532	611,734	422,931	545,532	545,532	524,288	727,376	854,765	916,806
	Embedding rate (bpp)	1.04	1.17	0.80	1.04	1.04	2.00	1.38	1.63	1.74
	PSNR of stego image (dB)	47.95	47.63	47.75	47.96	47.96	37.36	∞	∞	∞

Table 3 (continued)

Test Images	Parameters	Method								
		Lu et al. [23]	Yao et al. [25]	Lee & Huang [11]	Chi et al. [5]	Lu et al. [24]	Bhardwaj [3]	Proposed Algorithm	Proposed Algorithm	Proposed Algorithm
		$(k = 3)$	$(k = 3)$		$(k = 3)$	$(k = 3)$		$(n = 2)$	$(n = 3)$	$(n = 5)$
								$(NZ = 5)$	$(NZ = 6)$	$(NZ = 8)$
Med_8	Embedding capacity (bits)	675,663	767,346	542,176	675,663	675,663	524,288	900,884	1,049,780	1,075,650
	Embedding rate (bpp)	1.29	1.46	1.03	1.29	1.29	2.00	1.71	2.00	2.05
	PSNR of stego image (dB)	47.02	46.66	49.31	47.02	47.04	39.44	∞	∞	∞

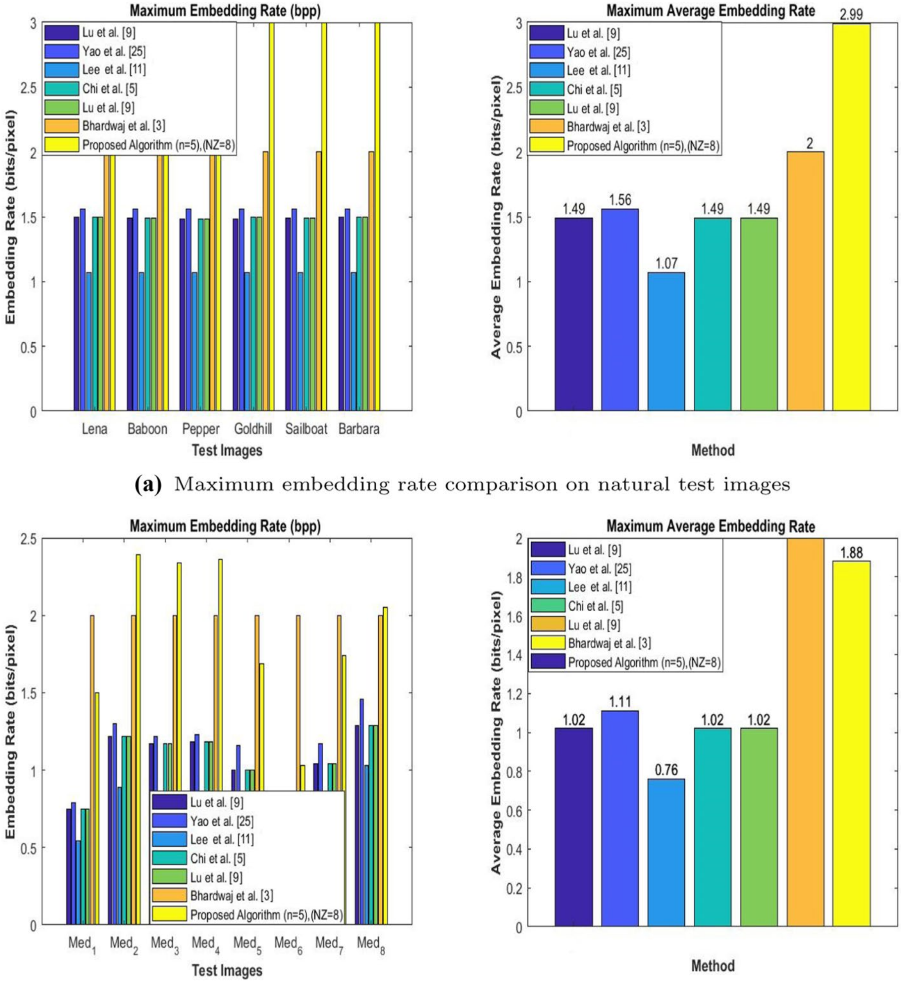
Fig. 4 Experimental study of proposed method



(a) PSNR value comparison against different payload on test images

(b) PSNR value comparison against different payload on test images

(c) PSNR value comparison against different payload on test images



(a) Maximum embedding rate comparison on natural test images

(b) Maximum embedding rate comparison on medical test images

Fig. 5 Comparative study of proposed method

extracted watermark in most of the cases is not matched with original one hence the proposed method is fragile against all type of attacks.

4.3 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. Fig. 6 show histograms of different medical cover images and corresponding stego images for a payload

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

Image	**Method**	**Parameters**					
		Imperceptibility			**Payload**	**Authentication**	**Encrypted**
					(bpp)	**Analysis**	**Domain**
		SSIM	NAE	NCC			
Med_1	Lu et al. [23]($k = 3$)	0.9955	0.0123	0.9998	0.75	No	No
	Yao et al. [25] ($k = 3$)	0.9954	0.0123	0.9999	0.79	No	No
	Lee & Huang [11]	0.9474	0.0179	0.9998	0.54	No	No
	Chi et al. [5]($k = 3$)	0.9955	0.0122	0.9999	0.75	No	No
	Lu et al. [24] ($k = 3$)	0.9956	0.0123	0.9999	0.75	No	No
	Proposed Algorithm ($n = 5, NZ = 8$)	0.9734	0.0144	0.9996	1.50	Yes	Yes
Med_2	Lu et al. [23]($k = 3$)	0.9870	0.0175	0.9998	1.22	No	No
	Yao et al. [25] ($k = 3$)	0.9860	0.0181	0.9998	1.30	No	No
	Lee & Huang [11]	0.9770	0.0155	0.9998	0.89	No	No
	Chi et al. [5]($k = 3$)	0.9870	0.0176	0.9998	1.22	No	No
	Lu et al. [24] ($k = 3$)	0.9871	0.0175	0.9998	1.22	No	No
	Proposed Algorithm ($n = 5, NZ = 8$)	0.9807	0.0133	0.9995	2.39	Yes	Yes
Med_3	Lu et al. [23]($k = 3$)	0.9902	0.0096	0.9999	1.17	No	No
	Yao et al. [25] ($k = 3$)	0.9898	0.0096	0.9999	1.22	No	No
	Lee & Huang [11]	0.9759	0.0088	0.9999	0.83	No	No
	Chi et al. [5]($k = 3$)	0.9902	0.0096	0.9999	1.17	No	No
	Lu et al. [24] ($k = 3$)	0.9902	0.0096	0.9999	1.17	No	No
	Proposed Algorithm ($n = 5, NZ = 8$)	0.9697	0.0107	0.9996	2.34	Yes	Yes
Med_4	Lu et al. [23]($k = 3$)	0.9860	0.0080	1.0000	1.18	No	No
	Yao et al. [25] ($k = 3$)	0.9854	0.0080	1.0000	1.23	No	No
	Lee & Huang [11]	0.9742	0.0073	1.0000	0.84	No	No
	Chi et al. [5]($k = 3$)	0.9860	0.0080	1.0000	1.18	No	No
	Lu et al. [24] ($k = 3$)	0.9860	0.0080	1.0000	1.18	No	No
	Proposed Algorithm ($n = 5, NZ = 8$)	0.9670	0.0089	0.9997	2.36	Yes	Yes
Med_5	Lu et al. [23]($k = 3$)	0.9936	0.0141	0.9999	1.00	No	No
	Yao et al. [25] ($k = 3$)	0.9917	0.0157	0.9999	1.16	No	No
	Lee & Huang [11]	0.9712	0.0151	0.9999	0.80	No	No
	Chi et al. [5]($k = 3$)	0.9936	0.0139	0.9999	1.00	No	No
	Lu et al. [24] ($k = 3$)	0.9936	0.0080	0.9999	1.00	No	No
	Proposed Algorithm ($n = 5, NZ = 8$)	0.9750	0.0130	0.9997	1.69	Yes	Yes
Med_6	Lu et al. [23]($k = 3$)	0.9993	0.0114	0.9999	0.53	No	No
	Yao et al. [25] ($k = 3$)	0.9993	0.0115	0.9999	0.56	No	No
	Lee & Huang [11]	0.9415	0.0237	0.9998	0.37	No	No
	Chi et al. [5]($k = 3$)	0.9993	0.0113	0.9999	0.53	No	No
	Lu et al. [24] ($k = 3$)	0.9993	0.0080	0.9999	0.53	No	No

Table 4 (continued)

Image	**Method**	**Parameters**					
		Imperceptibility			**Payload**	**Authentication**	**Encrypted**
					(bpp)	**Analysis**	**Domain**
		SSIM	NAE	NCC			
	Proposed Algorithm $(n = 5, NZ = 8)$	0.9781	0.0240	0.9990	1.03	Yes	Yes
Med_7	Lu et al. [23]$(k = 3)$	0.9922	0.0208	0.9998	1.04	No	No
	Yao et al. [25] $(k = 3)$	0.9909	0.0225	0.9998	1.17	No	No
	Lee & Huang [11]	0.9708	0.0216	0.9998	0.80	No	No
	Chi et al. [5]$(k = 3)$	0.9922	0.0206	0.9998	1.04	No	No
	Lu et al. [24] $(k = 3)$	0.9923	0.0080	0.9998	1.04	No	No
	Proposed Algorithm $(n = 5, NZ = 8)$	0.9832	0.0251	0.9986	1.74	Yes	Yes
Med_8	Lu et al. [23]$(k = 3)$	0.9890	0.0184	0.9999	1.29	No	No
	Yao et al. [25] $(k = 3)$	0.9871	0.0200	0.9999	1.46	No	No
	Lee & Huang [11]	0.9929	0.0151	0.9999	1.03	No	No
	Chi et al. [5]$(k = 3)$	0.9890	0.0181	0.9999	1.29	No	No
	Lu et al. [24] $(k = 3)$	0.9892	0.0080	0.9999	1.29	No	No
	Proposed Algorithm $(n = 5, NZ = 8)$	0.9687	0.0178	0.9993	2.05	Yes	Yes
Average	Lu et al. [23]$(k = 3)$	0.9916	0.0140	0.9998	1.02	No	No
	Yao et al. [25] $(k = 3)$	0.9907	0.0147	0.9998	1.11	No	No
	Lee & Huang [11]	0.9688	0.0156	0.9998	0.76	No	No
	Chi et al. [5]$(k = 3)$	0.9916	0.0139	0.9998	1.02	No	No
	Lu et al. [24] $(k = 3)$	0.9916	0.0099	0.9999	1.02	No	No
	Proposed Algorithm $(n = 5, NZ = 8)$	0.9719	0.0159	0.9993	2.30	Yes	Yes

of 512×512. As is observed from the Fig. 6 that the proposed system is robust to this attack because corresponding histograms are closely identical to each other because their absolute difference is zero for all the intensity values.

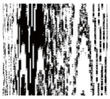
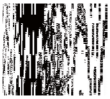
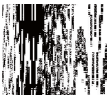
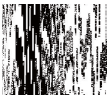
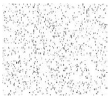
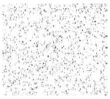
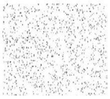
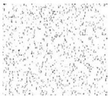
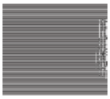
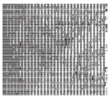
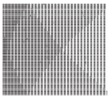
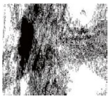
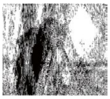
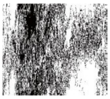
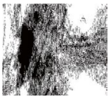
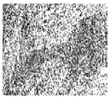
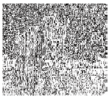
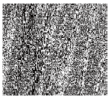
Theorem 1:- The proposed scheme can not extract the secret message and reconstruct the original cover image at the receiver end successfully if stego image has been attacked during transmission.

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

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

To avoid image distortion caused by a large value of $w_{u,v}(EPI)$, it was further reduced by using Lu et al. [9] method as follows-

Table 5 Authentication Analysis

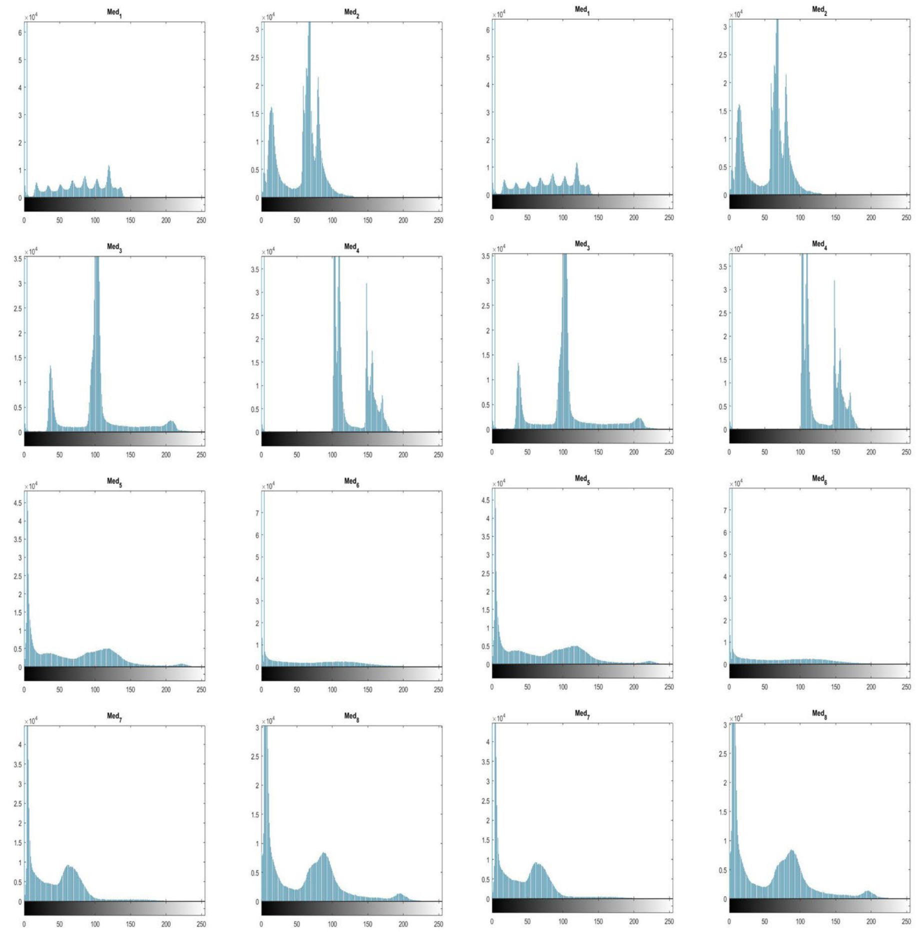
Attacks	Med_1	Med_3	Med_4	Med_6	*Average BER*(%)
Reflection	 *BER=41.25*	 *BER=44.17*	 *BER=42.64*	 *BER=40.32*	*42.09*
Salt & Pepper noise	*BER=32.78*	*BER=25.35*	*BER=15.30*	*BER=29.14*	*25.64*
Gaussian noise	 *BER=40.99*	 *BER=40.98*	 *BER=41.11*	 *BER=41.09*	*41.04*
Histogram Equalization	 *BER=49.18*	 *BER=46.79*	 *BER=45.69*	*BER=44.32*	*46.49*
Median Filtering	 *BER=43.27*	 *BER=27.85*	*BER=26.02*	 *BER=43.51*	*35.16*
Cropping	 *BER=39.17*	*BER=34.91*	*BER=35.69*	*BER=42.29*	*38.01*
Sharpening	 *BER=46.80*	 *BER=52.08*	*BER=59.44*	 *BER=47.46*	*51.44*

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

Now $x_{u,v}$, $y_{u,v}$ and $w'_{u,v}$ are encrypted through Paillier cryptosystem [15] to produced encrypted $Encr[x_{u,v}]$, $Encr[y_{u,v}]$ and $Encr[w'_{u,v}]$ respectively. After embedding $Encr[w'_{u,v}]$ into $Encr[x_{u,v}]$ and $Encr[y_{u,v}]$, they will be changed into $Encr[x^*_{u,v}]$ and $Encr[y^*_{u,v}]$ as follows-

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

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-



(a) Histogram of cover images

(b) Histogram of corresponding stego images

Fig. 6 Histogram analysis of proposed method

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

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

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

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 2:-The proposed scheme 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^2) which is divided into two units $x_{u,v}$ and $y_{u,v}$ as follows-

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

So that, to avoid image distortion caused by a large value of $w_{u,v}(EPI)$, it was further reduced by using Lu et al. [9] method as follows-

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

Now $x_{u,v}$, $y_{u,v}$ and $w'_{u,v}$ are encrypted through Paillier cryptosystem [15] to produced encrypted $Encr[x_{u,v}]$, $Encr[y_{u,v}]$ and $Encr[w'_{u,v}]$ respectively. After embedding $Encr[w'_{u,v}]$ into $Encr[x_{u,v}]$ and $Encr[y_{u,v}]$, they will be changed into $Encr[x^*_{u,v}]$ and $Encr[y^*_{u,v}]$ as follows-

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

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

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

$$\begin{cases} Nowdiff'_{u,v} \in [-2^k....(2^k - 2)] \\ diff'_{u,v}\%2 = 0 \\ w'_{u,v} = \frac{diff'_{u,v}}{2} = w'_{u,v} \\ w_{u,v} = w'_{u,v} + 2^{k-1} = w_{u,v} \\ z_{u,v} = x^*_{u,v} + y^*_{u,v} = 2^{k-1} + 2^{k-1} = 2^k = P_{u,v} \end{cases}$$

Hence, proved that that the proposed scheme is purely reversible in nature.

4.4 Computational complexity

The time complexity is computed when proposed method and compared schemes are run on a machine 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 (Lu et al. [23], Yao et al. [25], Chi et al. [5], Lu et al. [24]) but less than the method of Lee & Huang [11] for test medical images. Embedding rate of the proposed strategy is most prominent than other compared schemes and the visual quality of stego images produced by the proposed method is at standard with all the compared methods.

Table 6 Computational complexity comparison of proposed method

Test Images	**Parameters**	**Method**					
		Lu et al. [23]	Yao et al. [25]	Lee & Huang [11]	Chi et al. [5]	Lu et al. [24]	Proposed Algorithm
Med_1	Embedding rate (bpp)	0.75	0.79	0.54	0.75	0.75	1.50
	Execution time (sec)	2.03	1.89	7.20	3.30	1.26	4.34
Med_2	Embedding rate (bpp)	1.22	1.30	0.89	1.22	1.22	2.39
	Execution time (sec)	2.72	2.25	9.90	5.80	1.75	6.46
Med_3	Embedding rate (bpp)	1.17	1.22	0.83	1.17	1.17	2.34
	Execution time (sec)	2.87	2.20	9.57	4.52	1.83	6.40
Med_4	Embedding rate (bpp)	1.18	1.23	0.84	1.18	1.18	2.36
	Execution time (sec)	2.62	2.14	9.76	4.55	1.50	6.56
Med_5	Embedding rate (bpp)	1.00	1.16	0.80	1.00	1.00	1.69
	Execution time (sec)	2.40	2.12	9.36	4.10	1.58	4.49
Med_6	Embedding rate (bpp)	0.53	0.56	0.37	0.53	0.53	1.03
	Execution time (sec)	1.63	1.51	5.75	2.73	1.04	3.10
Med_7	Embedding rate (bpp)	1.04	1.17	0.80	1.04	1.04	1.74
	Execution time (sec)	2.49	2.06	9.35	4.18	1.49	4.53
Med_8	Embedding rate (bpp)	1.29	1.46	1.03	1.29	1.29	2.05
	Execution time (sec)	2.77	2.35	11.41	4.74	1.68	4.96

5 Conclusion

One of the basic problem for the execution of E-medical platform is security, verification, and copyright protection of the patient information. To ensure safe and secure transfer of patient report at a specialist, patient information is to be embedded in medical report through proposed method. Proposed method embed

$$\lfloor \log_2(2 \times n + 1) \times NZ - 1 \rfloor$$

binary bits of patient information at seed pixels of the report (cover image) whereas no overflow problem has occurred during embedding process respectively. Maximum average embedding rate (2.36 bpp) is achieved by proposed method with an average visual quality of stego images (∞ dB) respectively. A comparative study of the proposed method with some state-of-the-art methods shows that at higher payloads compared methods wriggled to perform because of failing to recompense the overflow problem in high-intensity pixels, proposed method thus surpasses all the compared methods as it is able to embed data at high intensity pixels too. Since the proposed method has been carried out in the spatial domain so that embedded electronic patient information (EPI) is not robust to well known image processing attacks. Constraint of proposed method is robustness which can be dispensed with in coming future.

References

1. Bhalerao S, Ansari IA, Kumar A Jain DK (2019) A reversible and multipurpose ecg data hiding technique for telemedicine applications. Pattern Recognition Letters 125:463–473
2. Bhardwaj R, Aggarwal A (2018) An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. Pattern Recognition Letters
3. Bhardwaj R (2020) An improved reversible and secure patient data hiding algorithm for telemedicine applications. J Ambient Intell Humaniz Comput. pages 1–15
4. Chen Yu-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
5. Chi Li-P, Chang-Han Wu, Chang H-P (2018) Reversible data hiding in dual stegano-image using an improved center folding strategy. Multimed Tools Appl 77(7):8785–8803
6. Hong W, Chen T-S, Han-Yan Wu (2012) An improved reversible data hiding in encrypted images using side match. IEEE Signal Process Lett 19(4):199–202
7. Horng SJ, Rosiyadi D, Li T, Takao T, Guo M, Khan MK (2013)A blind image copyright protection scheme for e-government. J Vis Commun Image Represent. 24(7):1099–1105
8. Horng SJ, Rosiyadi D, Fan P, Wang X, Khan MK (2014) An adaptive watermarking scheme for e-government document images. Multimed Tools Appl. 72(3):3085–3103
9. Lu TC, Lu YC, Vo TN (2019) Dual-image based high image quality reversible hiding scheme with multiple folding zones. Multimed Tools Appl. 78(24):34397–34435
10. Kim Y-S, Kang K, Lim D-W (2015) New reversible data hiding scheme for encrypted images using lattices. Applied Mathematics &; Inform Sci 9(5):2627
11. Lee C-F, Huang Yu-L (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. Telecommun Syst 52(4):2237–2247
12. 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
13. 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
14. Ni Z, Shi Y-Q, Ansari N, Wei Su (2006) Reversible data hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362

15. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 223–238. Springer
16. Parah SA, Ahad F, Sheikh JA, Bhat GM (2017)&nbsp;Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inform. 66:214–230
17. 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
18. Rosiyadi D, Horng SJ, Fan P, Wang X (2011) MuhammadKhurram Khan, and YiPan. Copyright protection for e-government document images. IEEE MultiMedia, 19(3):62–73
19. Rosiyadi D, Prasetyo H, Horng SJ, Basuki AI (2020) Security attack on secret sharing based watermarking using fractional fourier transform and singular value decomposition. In 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), pages 343–347. IEEE
20. Shi YQ (2004) Reversible data hiding. In International workshop on digital watermarking, pages 1–12. Springer, 2004
21. Shiu H-Jr, 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 Programs Biomed 151:159–170
22. Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 13(8):890–896
23. Tzu-Chuen Lu, Jhih-Huei Wu, Huang C-C (2015) Dual-image-based reversible data hiding method using center folding strategy. Signal Process 115:195–213
24. Tzu-Chuen Lu, Chi Li-P, Chang-Han Wu, Chang H-P (2017) Reversible data hiding in dual stego-images using frequency-based encoding strategy. Multimed Tools Appl 76(22):23903–23929
25. 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
26. 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.