# A 3-layer RDH method in encrypted domain for medical information security

Jayanta Mondal*

University of Engineering and Management,
University Area, Street Number 03, Action Area III, B/5,
Newtown, Kolkata, West Bengal 700156, India
Email: jayantamondal777@gmail.com
*Corresponding author

Debabala Swain

Rama Devi Women's University,
Bhoinagar P.O., Bhubaneswar, Odisha 751022, India
Email: debabala.swain@gmail.com

**Abstract:** Digitisation of sensitive images demands a lossless security mechanism and a sophisticated privacy preservation technique. Sensitive imagery, e.g., medical, forensic, military images, etc., needs special care during transmission as a little distortion can lead to catastrophic diagnosis mistake. With immense advancements, popularity, and success of service-oriented architecture (SOA), providing safe and secure online medical facility is one hard challenge for both research community and the industry. This paper proposes a 3-layer embedding mechanism enabled reversible data hiding (RDH) scheme with additional electronic patient record (EPR) hiding technique for encrypted medical images. LSB modification and LSB substitution technique are used for the embedding and EPR hiding. The experiments carried out on the medical test images on three levels of embedding and the experimental results show great potential in terms of security, embedding capacity, and recovered image quality.

**Keywords:** reversible data hiding; RDH; least significant bit; LSB; electronic patient record; EPR; encryption; data embedding.

**Reference** to this paper should be made as follows: Mondal, J. and Swain, D. (2020) 'A 3-layer RDH method in encrypted domain for medical information security', *Int. J. Electronic Security and Digital Forensics*, Vol. 12, No. 1, pp.1–15.

**Biographical notes:** Jayanta Mondal is an Associate Professor in the Department of CSE at UEM, Kolkata. He has received his PhD in CSE from the KIIT Deemed to be University, Bhubaneswar in 2018. His research interests include sensitive image security, data hiding, and data mining.

Debabala Swain is an Associate Professor in Computer Science Department at the Rama Devi Women's University, Bhubaneswar. Her research interests include information security, information hiding and computer architecture.

## 1 Introduction

Sensitive images hold huge importance and different properties compared to normal images. An astronomical image or a medical image carries much more vital information than any normal digital image because each and every pixel can be of importance and any distortion can lead to the wrong diagnosis. Any kind of strong encryption does affect an image up to some extent which can be ignored for any normal image as the margin of redundancy in images is generally high. In case of sensitive imagery, the margin of redundancy is very minimum. Therefore many alterations in pixel values or compression are harmful to such images. As the degree of redundancy is very minimum and importance of pixel values is high, the capacity of additional data embedding in sensitive images is very low. There are several conventional data hiding mechanisms for embedding additional data into images such as watermarking, steganography and others. In most of them, the cover image cannot be fully recovered due to the data embedding and compression. Watermarking delivers a way of embedding a message in a portion of the digital content without rescinding its value. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked (Lu, 2014).

Digital watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or 'covered' and graphos or 'to write'). Steganography is the science of communicating information while hiding the existence of the communication. The goal of steganography is to hide an information message inside harmless messages in such a way that it is not possible even to detect that there is a secret message present. Both steganography and watermarking belong to a category of information hiding, but the objectives and conditions for the two techniques are just the opposite. In watermarking, for example, the important information is the 'external' data (e.g., images, voices, etc.). The 'internal' data (e.g., watermark) are additional data for protecting the external data and to prove ownership. In steganography, however, the external data (referred to as a vessel, container, or dummy data) are not very important. They are just a carrier of the important information the internal data are the most important (Lu, 2014). On the other hand, watermarking and steganography are not like encryption. Watermarking does not restrict access to the data while encryption has the aim of making messages unintelligible to any unauthorised persons who might intercept them. Once encrypted data is decrypted, the media is no longer protected. A watermark is designed to permanently reside in the host data. If the ownership of a digital work is in question, the information can be extracted to completely characterise the owner. Steganography does hide secret data into a cover image but generally does not care much about the cover image (Lu, 2014).

The answer to the above-mentioned concern is reversible data hiding (RDH). RDH fulfils each and every concern assigned to sensitive image digitisation. In modern days RDH technique received more attention because of its high efficiency and simplicity. Reversibility is the main criterion to achieve in a certain situation. RDH technique allows

implanting data into a target image in such a manner that the embedded data may be extracted and an identical lossless copy of the original image can be redeemed. Embedding vital information into sensitive images had saved a huge amount of space and complexity and provides privacy. RDH has become a trendy research topic in the area of information hiding and security. A huge number of research papers published on RDH in the past two decades and the numbers are growing every day. It is evident that research on RDH and its real-time applications will continue moving further. Barton proposed the very first RDH approach in 1997 for embedding authentication signature (Barton, 1997). Considerable advances have been made in real time application of RDH in both spatial and frequency domain. Efficient application of RDH in compressed images and encrypted sensitive images still remain hard challenges as compressed domain or encryption introduces more distortion in the cover image. Research on RDH can be basically categorised into four domains:

1 RDH into uncompressed images

2 RDH into encrypted images

3 RDH into compressed images

4 RDH for image authentication and contrast enhancement.

In this paper, we propose an efficient RDH method with an additional EPR hiding mechanism and a 3-layer data embedding technique implemented on encrypted medical images. Section 2 contains an updated literature survey on the recent work done on RDH aimed at medical images and different LSB-based RDH schemes for encrypted images. Section 3 shows the proposed work and Section 4 represents the experimental results and the performance analysis. Finally, we conclude in Section 5.

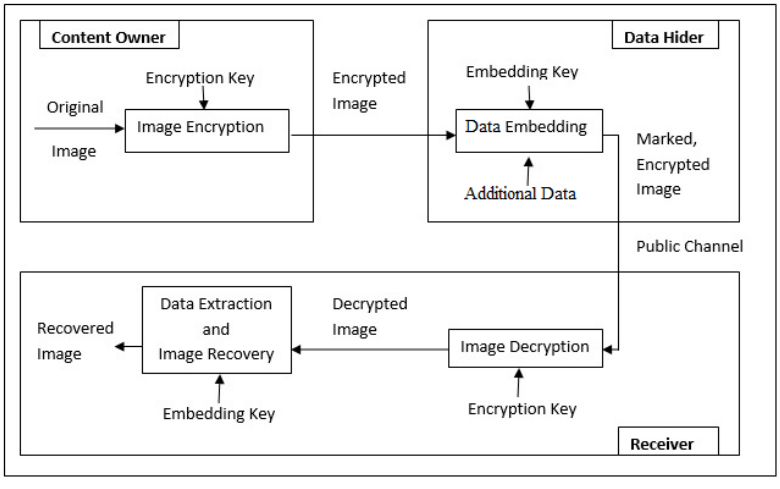
## 2 Literature survey

Several efficient RDH mechanisms have been proposed in the last decade. Least significant bits (LSB) substitution (Chen, 2011; Chan and Cheng, 2004), histogram shifting (Tai et al., 2009), and difference expansion (Al-Qershi and Khoo, 2011) are extensively used for RDH into uncompressed images. However, in the compressed domain, it is not possible to modify the pixels of the cover image directly. Discrete cosine transformation (DCT) (Chang et al., 2007), discrete wavelength transform (DWT) (Chandra and Pandey, 2010) are famous examples of image transformation. Vector quantisation (Chen and Huang, 2009; Yang and Lin, 2009) and BTC (Guo and Lin, 2010) are the most common techniques used in the frequency domain for image compression. General standard digital images and sensitive images are very different based on their inherent properties. A slight distortion can cause a catastrophic error in diagnosis. Several RDH methods have been proposed for medical images in recent years (Al-Qershi and Khoo, 2011; Lou et al., 2009; Huang et al., 2013; Fallahpour et al., 2011; Chang and Xu, 2011; Ahmad et al., 2013; Liu et al., 2016; Al-Qershi and Khoo, 2011). After going through all the pre-existing RDH schemes we found RDH in the encrypted domain is the most secure and effective way to address the research problem and LSB manipulation is the simplest, most cost-effective, and efficient technique for ensuring security, authentication and privacy preservation relating to sensitive digital images.

### 2.1 LSB-based RDH in the encrypted domain

RDH in the encrypted domain is the best way in terms of security and privacy preservation and LSB manipulation is the best mechanism to achieve it. A good amount of work has been carried out on this topic in recent years. In Zhang (2011) first proposed an LSB-based RDH scheme for encrypted images. In this method, the original image is fully encrypted in the first step. In the second step, the encrypted image is divided into same size non-overlapping blocks, then for half of the pixels, three LSBs are flipped to generate room for data hiding. Finally, in each block, a secret bit is embedded. The decryption process follows the exact opposite way. In the third step the embedded bits are extracted and in the final step, the plain text image is recovered utilising spatial correlation. The basic architecture of this RDH scheme proposed by Zhang is shown in Figure 1.

**Figure 1** Architecture of RDH in encrypted domain proposed in Zhang (2011)




Hong et al. enhanced Zhang's method by decreasing the error rate of the extracted bits. Two metrics are used for this purpose smoothness evaluation and side-matching. For each block, every horizontal and vertical pixel are utilised for smoothness evaluation and for side-matching neighbouring blocks are considered and using pixel correlation in the border the recovered and unrecovered blocks are identified. It helps in decreasing error rate of the extracted image with small block size (Hong et al., 2012).

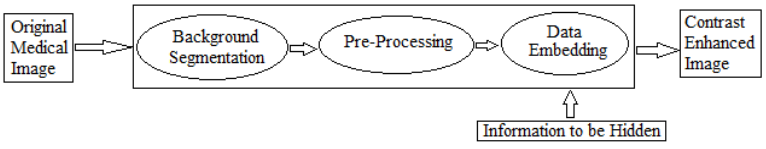
In Qin and Zhang (2015), advanced the effectiveness of the previous method (Zhang, 2011) where data hiding room is vacated after encryption. Previously the LSB half of the pixels of the LSB are flipped after encryption, this scheme selects a fewer number of pixels and flips them instead. This improves the visual quality remarkably of the marked image after decryption. An adaptive judging function is introduced centred on the distribution characteristics which helps in decreasing the error rate (Qin and Zhang, 2015).

In 2017 we proposed an LSB-based RDH method (Mondal et al., 2017) and the experimental results shows better efficiency than Zhang (2011), Hong et al. (2012), and Qin and Zhang (2015). This scheme follows the same basic framework as of Zhang (2011) and the encryption and embedding procedures are of same nature. In the embedding phase among the half number of blocks are subjected to change if the XOR of the last three LSB with the upper row is not zero. The last three-LSBs are being left rotated and the 4th LSB is flipped.

### *2.2 Recent works on RDH aimed at medical image*

There has been little recent advancement in RDH schemes aimed at medical images. In Wu et al. (2015) proposed contrast enhancement capability-based RDH method for medical images. Instead of directly applying the embedding algorithm into the cover image in this method a mechanism is proposed to select the region of interest (ROI) for embedding additional medical information. Automatic background segmentation is done for the ROI selection. The additional bits embedding are carried out by histogram modification of the enhanced ROI region. The experimental results show improvement in peak signal to noise ratio (PSNR) and structural similarity index (SSIM) values. The data hiding process proposed in this scheme is described in Figure 2.

**Figure 2** Data hiding process in Wu et al. (2015)




In Chandrasekaran and Sevugan (2017) applied RDH method for medical images using histogram modification in the hybrid domain. It uses the pixel difference of neighbouring pixel histograms. The payload is embedded in the frequency domain through a 2D DWT haar transform. The experimental results show a huge improvement in image quality.

In Qian et al. (2016) proposed a joint RDH scheme which is also implemented on some medical images. In this paper, a dual LSB-based RDH scheme is proposed and successfully implemented in medical images. In the data embedding phase, a combination of cyclic shifting and LSB swapping is carried out for generating the marked image. This process works in the encrypted domain and thus much more secure than other methods.

## 3 Proposed work

Here, an RDH model is proposed with 3-layer data embedding mechanism with additional EPR hiding technique for encrypted medical images. The proposed scheme primarily includes six processes: image encryption, EPR hiding, data embedding, EPR recovery, de-embedding, and image decryption. The work proposed in this paper covers all the concerned research problems for sensitive image digitisation. Privacy of image

content is preserved through encryption. Security and authentication are dealt with the 3-layer data embedding. The privacy and security of the patient data are restored through additional EPR embedding. The scope of this paper includes successful transmission and management of medical imagery for cloud service-oriented systems. For example, in online healthcare systems where patients need to consult a doctor via some online healthcare provider. In this scenario, the patient sends the encrypted version of the medical image with additional private data hidden in it to the service provider in the cloud. The data hider marked the image through 3-layer data embedding without knowing the image content for authentication and sends to the doctor. The receiver needs to have both the keys to recover the original image because a little-distorted image will result in the wrong diagnosis.

In case the image falls in unauthorised hand this scheme guarantees one step better security than encryption. If we assume that the eavesdropper decrypts the image then the secret EPR bits are lost thus privacy prevails. Furthermore, the image quality will not be good enough for a proper diagnosis of the medical image without proper de-embedding. To prove this, we decrypted the EPR embedded marked image directly, which shows good visual quality, then, de-embedding is applied to the directly decrypted images, which shows a huge improvement in image quality.

### *3.1 Proposed architecture*

Figure 3 shows the proposed architecture with three actors. Encryption and EPR embedding are done by the content owner, 3-layer data embedding is performed by the data hider, and the decryption and image recovery phases are carried out by the receiver. In Figures 4(a) and 4(b) the layer-3 embedding technique and EPR embedding process are pictorially represented.

**Figure 3** Proposed RDH architecture

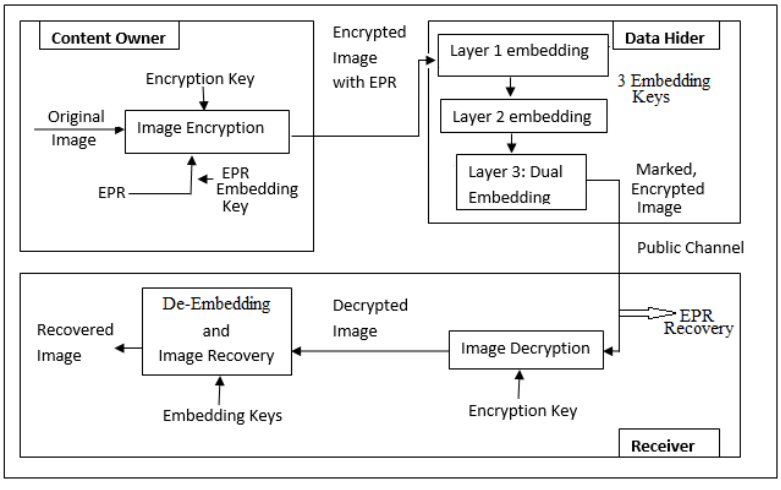
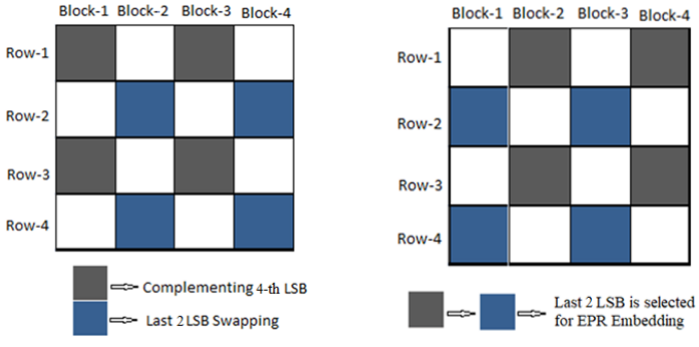


**Figure 4** (a) Layer-3 dual embedding process and (b) EPR hiding process (see online version for colours)




(a) (b)

## *3.2 Proposed algorithms*

### *3.2.1 Encryption*

Here the original grey-scale image is $I_{M\times N}$ whose pixel values range in 0 to 255.

Step-1 The image matrix in 8-bit binary format can be generated as:

$b_{i,j,u}$ = 8 bit binary value of each pixel

$$b_{i,i,u} = \left[ I_{i,j} / 2^{u} \right] \% 2 \tag{1}$$

where $(i, j)$ denotes pixel position and $u$ = 0, 1, 2, 3, 4, 5, 6, 7

$$\text{Original image inbinary format} = I_{i,j,u} = \sum_{0}^{255} b_{i,j,u} \tag{2}$$

Step-2 The key matrix ($K_{M\times N}$) can be generated using MATLAB random function.

Step-3 The encrypted image $E_{i,j,u}$ can be produced using bit-wise XOR operation between the image and key matrix as:

$$E_{i,j,u} = I_{i,j,u} \oplus K_{i,j,u} \tag{3}$$

Step-4 Further the encrypted image in 8-bit binary format is:

$$E_{M\times N} = \sum_{u=0}^{7} E_{i,j,u} \times 2^{u} \tag{4}$$

### *3.2.2 EPR hiding*

Step-1 Then the encrypted image can be divided into non-overlapping blocks of order $r \times r$. Let the total number of blocks be R.

Step-2 In the odd rows, all even number blocks (block 2 to block R) and in the even rows all odd number blocks (block 1 to block R-1) are subjected to EPR embedding.

Step-3 In the subjected blocks the last two LSBs are replaced by the binary EPR data. Here the maximum EPR embedding is considered by embedding in all blocks, where the maximum value is 16384 bits when the block size is 4×4.

### *3.2.3 Data embedding*

Here the embedding phase consists of three different layers, which uses two LSB management techniques for image marking.

#### *3.2.3.1 Layer 1*

Only for the odd row blocks. It covers 19% of total image pixels.

Step-1 Divide the EPR embedded encrypted image ($[E_{epr}]_{M\times N}$) into non-overlapping blocks of size $r \times r$.

Step-2 In all odd number blocks:

1 1st-row pixels remain unchanged

2 2nd row onwards XOR the last 2 LSB with the previous row

3 IF result is zero then no alteration ELSE complement the 3rd LSB.

The final marked image after layer-1 embedding is denoted by $[E'_{epr}]_{M\times N}$.

#### *3.2.3.2 Layer 2*

Only the even row blocks. It covers maximum 25% of total image pixels.

Step-1 Divide the marked image ($[E'_{epr}]_{M\times N}$) into non-overlapping blocks of size $r \times r$.

Step-2 In all the even blocks last LSB of each pixel are swapped with the next even block. For example, Block-0 with Block-2, Block-4 with Block-6, and so on.

The final marked image after layer-2 embedding is denoted by $[E''_{epr}]_{M\times N}$.

#### *3.2.3.3 Layer 3*

For all the even blocks in the even rows and all odd blocks in the odd rows. It covers maximum 45% of total image pixels. The process is similar but the degree of LSB modification is higher in layer-3.

Step-1 Divide the encrypted image ($[E''_{epr}]_{M\times N}$) into non-overlapping blocks ofsize .

Step-2 For every even row:

In all the even blocks last two LSBs of each pixel is swapped with the next even block. For example, Block-0 with Block-2, Block-4 with Block-6, and so on.

Step-3 For every odd row of blocks in all odd number of blocks:

1 1st-row pixels remain unchanged
2 2nd row onwards XOR the last 3 LSB with the previous row
3 IF result is zero then no alteration is done ELSE complement the 4th LSB.

The final encrypted embedded image is denoted by $[E'''_{epr}]_{M\times N}$.

### *3.2.4 Decryption*

Step-1 Generate the decrypted image.

$$[I^D]_{M\times N} = [E'''_{epr}]_{M\times N} \oplus [K]_{M\times N} \tag{5}$$

### *3.2.5 De-embedding*

Step-1 Divide the decrypted image $[I^D]_{M\times N}$ into non-overlapping blocks of size $r \times r$.

Step-2 Repeat the data embedding process in reverse order i.e., layer-3 first, then layer-2 and layer-1 at last.

## 4 Experimental results and analysis

To demonstrate the potential of our proposed method, experiments were carried out on standard 512 × 512 test images. Experiments are performed on a computer with 2.00 GHz AMD-A10 processor, 8 GB RAM, Windows 8 operating system, and the programming environment was MATLAB 13.

**Figure 5** Eight original test images

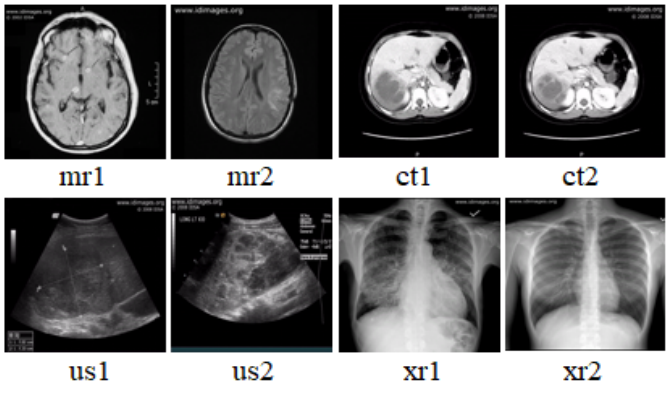
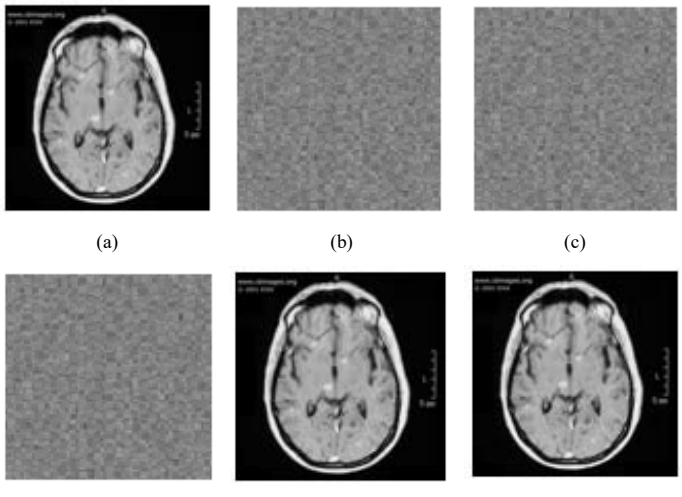



Figure 5 shows the original medical images taken for experimental analysis from microbes digital library (idimages.org, 2016). There are 2 MRI images (mr1 and mr2), two CT scan images (ct1 and ct2), two ultrasonography images (us1 and us2), and two x-ray images (xr1 and xr2), thus eight test images in total. Different experiments have

been conducted on these test images for measuring recovered image quality and embedding capacity. To prove the overall efficiency of the proposed work, we have compared the findings with pre-existing methods (Zhang, 2011; Hong et al., 2012; Wu et al., 2015; Chandrasekaran and Sevugan, 2017; Qian et al., 2016). All the previous works that we have referred have used 512 × 512 grey-scale images as test cases which, allowed us to use 512 × 512 grey-scale images as our test cases. Figure 6 shows the different implementation phase of the mr1 test image, where (a), (b), (c), (d), (e), and (f) consecutively represents original image, encrypted image, EPR embedded encrypted image, marked image, directly decrypted image, and recovered image.

**Figure 6** Different experimental phases of the mr1 test image



(a) (b) (c)

(d) (e) (f)

**Table 1** Comparison table between decrypted and recovered images for layer-1 embedding when the block size is 32 × 32

| *Test medical images* | *Layer-1 embedding when the block size is 32 × 32* | | | | | |
|---|---|---|---|---|---|---|
| | *Decrypted image* | | | *Recovered image* | | |
| | *PSNR* | *MSE* | *SSIM* | *PSNR* | *MSE* | *SSIM* |
| ct1 | 47.89 | 0.18 | 0.9538 | 79.01 | 0 | 0.9998 |
| ct2 | 47.78 | 0.15 | 0.9530 | 77.08 | 0.01 | 0.9994 |
| mr1 | 46.84 | 0.08 | 0.9450 | 74.05 | 0.01 | 0.9995 |
| mr2 | 49.99 | 0.06 | 0.9635 | 75.16 | 0.01 | 0.9993 |
| us1 | 50.56 | 0.06 | 0.9653 | 78.11 | 0 | 0.9999 |
| us2 | 49.63 | 0.12 | 0.9646 | 76.48 | 0.01 | 0.9998 |
| xr1 | 46.49 | 0.22 | 0.9483 | 73.12 | 0.01 | 0.9992 |
| xr2 | 45.91 | 0.24 | 0.9406 | 72.57 | 0.01 | 0.9992 |

**Table 2** Comparison table between decrypted and recovered images when the block size is 16 × 16

| *Medical test images* | *Layer-1 + layer-2 embedding when the block size is 16 × 16* | | | | | |
|---|---|---|---|---|---|---|
| | *Decrypted image* | | | *Recovered image* | | |
| | *PSNR* | *MSE* | *SSIM* | *PSNR* | *MSE* | *SSIM* |
| ct1 | 45.98 | 0.20 | 0.9448 | 77.91 | 0.01 | 0.9995 |
| ct2 | 44.98 | 0.18 | 0.9440 | 76.58 | 0.02 | 0.9993 |
| mr1 | 44.94 | 0.11 | 0.9360 | 73.55 | 0.02 | 0.9992 |
| mr2 | 46.29 | 0.10 | 0.9545 | 74.56 | 0.02 | 0.9989 |
| us1 | 47.66 | 0.10 | 0.9563 | 76.88 | 0.01 | 0.9995 |
| us2 | 46.93 | 0.16 | 0.9556 | 75.88 | 0.02 | 0.9994 |
| xr1 | 43.09 | 0.26 | 0.9393 | 72.32 | 0.02 | 0.9989 |
| xr2 | 42.31 | 0.28 | 0.9336 | 71.58 | 0.02 | 0.9988 |

**Table 3** Comparison table between decrypted and recovered images when the block size is 8 × 8

| *Medical test images* | *Layer-3 embedding only when the block size is 8 × 8* | | | | | |
|---|---|---|---|---|---|---|
| | *Decrypted image* | | | *Recovered image* | | |
| | *PSNR* | *MSE* | *SSIM* | *PSNR* | *MSE* | *SSIM* |
| ct1 | 44.76 | 0.22 | 0.9443 | 74.86 | 0.03 | 0.9991 |
| ct2 | 43.58 | 0.20 | 0.9435 | 72.53 | 0.02 | 0.9989 |
| mr1 | 43.84 | 0.14 | 0.9355 | 69.51 | 0.02 | 0.9990 |
| mr2 | 45.5x4 | 0.12 | 0.9540 | 71.98 | 0.03 | 0.9985 |
| us1 | 46.28 | 0.12 | 0.9559 | 72.65 | 0.02 | 0.9992 |
| us2 | 45.66 | 0.18 | 0.9551 | 71.72 | 0.02 | 0.9990 |
| xr1 | 42.98 | 0.28 | 0.9388 | 69.54 | 0.03 | 0.9985 |
| xr2 | 41.78 | 0.30 | 0.9331 | 68.64 | 0.03 | 0.9986 |

**Table 4** Comparison table between decrypted and recovered images when the block size is 4 × 4

| *Medical test images* | *Layer-1 + layer-2 + layer-3 embedding when the block size is 4×4* | | | | | |
|---|---|---|---|---|---|---|
| | *Decrypted image* | | | *Recovered image* | | |
| | *PSNR* | *MSE* | *SSIM* | *PSNR* | *MSE* | *SSIM* |
| ct1 | 43.67 | 0.25 | 0.9354 | 71.75 | 0.04 | 0.9990 |
| ct2 | 42.85 | 0.24 | 0.9346 | 70.40 | 0.03 | 0.9988 |
| mr1 | 42.48 | 0.18 | 0.9233 | 67.38 | 0.03 | 0.9988 |
| mr2 | 44.25 | 0.17 | 0.9488 | 69.67 | 0.04 | 0.9981 |
| us1 | 44.98 | 0.15 | 0.9459 | 70.22 | 0.03 | 0.9989 |
| us2 | 43.88 | 0.22 | 0.9478 | 68.98 | 0.03 | 0.9988 |
| xr1 | 41.02 | 0.31 | 0.9228 | 66.34 | 0.03 | 0.9982 |
| xr2 | 39.98 | 0.33 | 0.9288 | 65.89 | 0.03 | 0.9983 |

Table 1 shows the difference between directly decrypted and recovered image in terms of PSNR, MSE, and SSIM for layer-1 embedding only when the block size is 32 × 32. Table 2 shows the difference between directly decrypted and recovered image in terms of PSNR, MSE, and SSIM for (layer-1 + layer-2) embedding when the block size is 16 × 16. Table 3 shows the difference between directly decrypted and recovered image in terms of PSNR, MSE, and SSIM for layer-3 embedding only when the block size is 8 × 8. Table 4 shows the difference between directly decrypted and recovered image in terms of PSNR, MSE, and SSIM for all 3-layer embedding (layer-1 + layer-2 + layer-3) embedding when the block size is 4 × 4. Table 5 shows the embedding capacity of layer-3 embedding and EPR embedding when the block size is 4 × 4.

**Table 5** Embedding capacity of different test images for layer-3 embedding when the block size is 4 × 4

| *Layer-3 total embedding capacity when the block size is 4 × 4* | | |
|---|---|---|
| *Image* | *EPR bits* | *Marked bits* |
| ct1 | 16384 | 111654 |
| ct2 | 16384 | 111744 |
| mr1 | 16384 | 111491 |
| mr2 | 16384 | 111617 |
| us1 | 16384 | 111682 |
| us2 | 16384 | 111706 |
| xr1 | 16384 | 111791 |
| xr2 | 16384 | 111770 |

**Table 6** A comparison table of standard 512 × 512 Baboon image after recovery for different block size

| *Block size* | | *4 × 4* | *8 × 8* | *16 × 16* |
|---|---|---|---|---|
| PSNR | Zhang (2011) | 38.96 | 43.28 | 48.41 |
| | Hong et al. (2012) | 39.32 | 44.98 | 50.46 |
| | Mondal et al. (2017) | 41.14 | 46.84 | 55.23 |
| | Proposed | 61.83 | 63.58 | 67.07 |
| SSIM | Zhang (2011) | 0.98885 | 0.99445 | 0.99816 |
| | Hong et al. (2012) | 0.98978 | 0.99609 | 0.99889 |
| | Mondal et al. (2017) | 0.99246 | 0.99695 | 0.99953 |
| | Proposed | 0.99571 | 0.99922 | 0.9998 |

Table 6 shows PSNR and SSIM comparison between Zhang (2011), Hong et al. (2012), Mondal et al. (2017) and proposed method for standard 512 × 512 Baboon test image. Figure 7 shows a graphical comparison of PSNR values of four medical test images after recovery between Wu et al. (2015), Chandrasekaran and Sevugan (2017) and the proposed method. Figure 8 shows the SSIM comparison between Wu et al. (2015), Chandrasekaran and Sevugan (2017) and the proposed method. Figure 9 shows a graphical comparison of EPR embedding capacity between Zhang (2011), Hong et al. (2012), Wu et al. (2015), Chandrasekaran and Sevugan (2017) and proposed method.

These comparisons clearly prove the superiority of the proposed method in terms of recovered image quality and embedding capacity.

**Figure 7** PSNR comparison between Wu et al. (2015), Chandrasekaran and Sevugan (2017) and proposed method (see online version for colours)

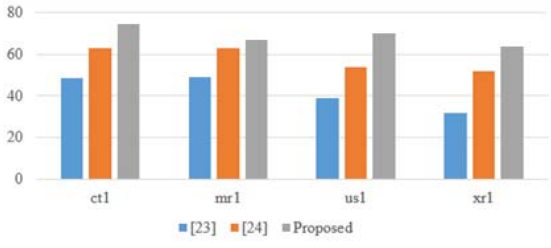



**Figure 8** SSIM comparison between Wu et al. (2015), Chandrasekaran and Sevugan (2017) and proposed method (see online version for colours)

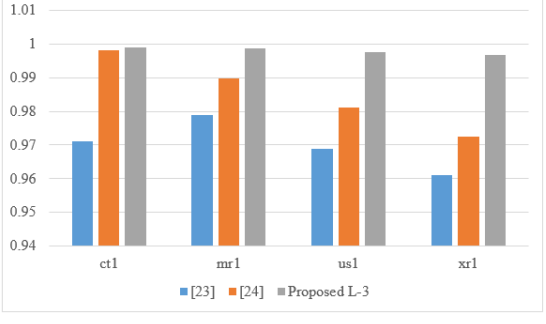
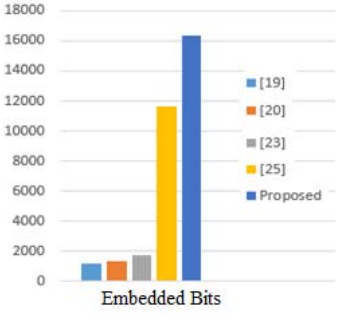



**Figure 9** Comparison between Zhang (2011), Hong et al. (2012), Wu et al. (2015), Qian et al. (2016) and proposed method on embedding capacity (see online version for colours)



## 5 Conclusions

This paper proposes a novel LSB-based RDH model for encrypted medical images with additional EPR embedding facility. Security is enhanced through encryption and three different data embedding mechanism for authentication and additional security. Data embedding procedure is carried out through LSB swapping and LSB complementing. The experimental results clearly show superiority in terms of PSNR which is enhanced by 60% after recovery. The error rate is hugely reduced after data extraction. EPR embedding capacity is increased by almost 100% than the previous methods. In terms of PSNR, SSIM, and MSE values and embedding capacity, the proposed method clearly outperforms the pre-existing methods. This work can be further enhanced by implementing other types of sensitive images, for example, forensic or astronomical images. The method can work on colour images also through transforming the colour image into grey-scale value. There are ample scope for future research and modification based on different image formats. Large-scale implementation of the proposed model can solve the security problems in electronic healthcare services.

## References

Ahmad, T., Holil, M., Wibisono, W. and Muslim, I.R. (2013) 'An improved quad and RDE-based medical data hiding method', *Computational Intelligence and Cybernetics (CYBERNETICSCOM)*, *2013 IEEE International Conference on*, IEEE.

Al-Qershi, O.M. and Khoo, B.E. (2011) 'Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images', *Journal of Digital Imaging*, Vol. 24, No. 1, pp.114–125.

Al-Qershi, O.M. and Khoo, B.E. (2011) 'High capacity data hiding schemes for medical images based on difference expansion', *Journal of Systems and Software*, Vol. 84, No. 1, pp.105–112.

Barton, J.M. (1997) *Method and Apparatus for Embedding Authentication Information within Digital Data*', US Patent No. 5,646,997, 8 July.

Chan, C-K. and Cheng, L-M. (2004) 'Hiding data in images by simple LSB substitution', *Pattern Recognition*, Vol. 37, No. 3, pp.469–474.

Chandra, M. and Pandey, S. (2010) 'A DWT domain visible watermarking techniques for digital images', *Electronics and Information Engineering (ICEIE)*, *2010 International Conference On*, IEEE, Vol. 2.

Chandrasekaran, V. and Sevugan, P. (2017) 'Applying reversible data hiding for medical images in hybrid domain using Haar and modified histogram', *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 4.

Chang, C-C. et al. (2007) 'Reversible hiding in DCT-based compressed images', *Information Sciences*, Vol. 177, No. 13, pp.2768–2786.

Chang, Z. and Xu, J. (2011) 'Reversible run length data embedding for medical images', *Communication Software and Networks (ICCSN)*, *2011 IEEE 3rd International Conference on*, IEEE.

Chen, S-K. (2011) 'A module-based LSB substitution method with lossless secret data compression', *Computer Standards and Interfaces*, Vol. 33, No. 4, pp.367–371.

Chen, W-J. and Huang, W-T. (2009) 'VQ indexes compression and information hiding using hybrid lossless index coding', *Digital Signal Processing*, Vol. 19, No. 3, pp.433–443.

Fallahpour, M., Megias, D. and Ghanbari, M. (2011) 'Reversible and high-capacity data hiding in medical images', *IET Image Processing*, Vol. 5, No. 2, pp.190–197.

Guo, J-M. and Lin, C-Y. (2010) 'Parallel and element-reduced error-diffused block truncation coding', *IEEE Transactions on Communications*, Vol. 58, No. 6, pp.1667–1673.

Hong, W., Chen, T.S. and Wu, H.Y. (2012) 'An improved reversible data hiding in encrypted image using side match', *IEEE Signal Processing Letters*, April, Vol. 19, No. 5, pp.199–203.

Huang, L.C., Tseng, L.Y. and Hwang, M.S. (2013) 'A reversible data hiding method by histogram shifting in high quality medical images', *Journal of Systems and Software*, Vol. 86, No. 3, pp.716–727.

idimages.org (2016) *Partners Infectious Disease Images*, Emicrobes Digital Library, June [online] http://www.idimages.org/images/browse/ImageTechnique/. (accessed 21 December 2017).

Liu, Y., Qu, X. and Xin, G. (2016) 'A ROI-based reversible data hiding scheme in encrypted medical images', *Journal of Visual Communication and Image Representation*, August, Vol. 39, pp.51–57.

Lou, D.C., Hu, M.C. and Liu, J.L. (2009) 'Multiple layer data hiding scheme for medical images', *Computer Standards and Interfaces*, Vol. 31, No. 2, pp.329–335.

Lu, C.S. (Ed.) (2004) *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*, IGI Global; 31 July, Chun-Shien Lu Institute of Information Science Academia Sinica, Taiwan, ROC.

Mondal, J., Swain, D., Singh, D.P. and Mohanty, S. (2017) 'An improved LSB-based RDH technique with better reversibility', *International Journal of Electronic Security and Digital Forensics*, Vol. 9, No. 3, pp.254–268.

Qian, Z. et al. (2016) 'Improved joint reversible data hiding in encrypted images', *Journal of Visual Communication and Image Representation*, Vol. 40, pp.732–738.

Qin, C. and Zhang, X. (2015) 'Effective reversible data hiding in encrypted image with privacy protection for image content', *Journal of Visual Communication and Image Representation*, August, Vol. 31, pp.154–164.

Tai, W-L., Yeh, C-M. and Chang, C-C. (2009) 'Reversible data hiding based on histogram modification of pixel differences', *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 19, No. 6, pp.906–910.

Wu, H-T., Huang, J. and Shi, Y-Q. (2015) 'A reversible data hiding method with contrast enhancement for medical images', *Journal of Visual Communication and Image Representation*, August, Vol. 31, pp.146–153.

Yang, C-H. and Lin, Y-C. (2009) 'Reversible data hiding of a VQ index table based on referred counts', *Journal of Visual Communication and Image Representation*, Vol. 20, No. 6, pp.399–407.

Zhang, X. (2011) 'Reversible data hiding in encrypted image', *IEEE Signal Processing Letters*, April, Vol.18, No. 4, pp.255–258.