Health and Technology (2021) 11:835–850
https://doi.org/10.1007/s12553-021-00562-6

ORIGINAL PAPER

An improved ROI-based reversible data hiding scheme completely separable applied to encrypted medical images

David Mata-Mendoza[1] · Diana Nuñez-Ramirez[1] · Manuel Cedillo-Hernandez[1] · Mariko Nakano-Miyatake[1]

Received: 21 January 2021 / Accepted: 10 May 2021 / Published online: 21 May 2021

Abstract
To protect the privacy of medical images, as well as the patient personal information associated with it, this paper proposes a reversible data hiding scheme for encrypted medical images; whose reversibility is completely separable by allowing additional data extraction and restoration of the region of interest both from the plaintext and the cipher domain of medical images. To this purpose, the pixels in the image are reordered according to the region of interest selected by the content owner and encrypted with a block cipher in counter mode; to subsequently embed additional data into the encrypted image, such as the patient's personal information and clinical diagnosis, via less significant bit substitution. Finally, according to the proper key, a legitimate receiver can perform the following tasks: a) Obtain a high visual quality approximate image with respect to the original version by directly decrypting the cryptogram with the encryption key, b) With the data hiding key, the embedded data can be extracted free of any error, either from the encrypted image or its approximate version respectively, and c) In case of having both keys, the embedded data can be extracted and the recovered image with the region of interest fully restored can be obtained without loss of information. The proposed method is suitable for applications where the information security and the management of medical images need to be ensured in terms of reliability, integrity, and confidentiality. Comparison performance with the state of the art is performed, in terms of imperceptibility, capacity and steganalysis.

Keywords —Reversible data hiding over encrypted domain · Image encryption · LSB substitution · Medical imaging · Image processing · DICOM medical images

1 Introduction

The implementation of Picture Archiving and Communications System (PACS) in the medical area has allowed the storage and distribution of medical images more efficiently, while its administration is managed by the standard of Digital Imaging and Communication in Medicine (DICOM), which provides the communication protocols for the transmission of medical information and technical specifications of the files corresponding to the stored data [1]. With the expansion and accelerated growth of the digital imaging paradigm over its analog counterpart, it is necessary to guarantee the integrity, confidentiality, and security of medical images, since they usually contain reserved information about patient health [2]; which, if not protected with adequate security levels, can be used in medical insurance frauds, identity theft, among other illegal activities.

Even though medical images contain sensitive information in their metadata, they are usually transferred from imaging stations through unencrypted or unauthenticated transmission channels to PACS servers, where they are stored and distributed to their users; like display stations, DICOM printers, CD and DVD recording equipment, clinical diagnostic equipment or even consultations via mobile services. Although these systems have various means to protect the files stored, millions of reports of security breaches related to medical information are presented every year [3]. In these incidents, attackers or intruders can accessed the medical information while it was stored on the PACS servers or during its transmission, mainly for the purpose of acquiring patient information, modifying, deleting, or hijacking the data, as illustrated in Fig. 1.

✉ Manuel Cedillo-Hernandez
mcedillohdz@hotmail.com

[1] Instituto Politecnico Nacional SEPI ESIME Culhuacan, Avenida Santa Ana 1000, San Francisco Culhuacan, CTM V, Ciudad de Mexico, CDMX C.P. 04260 Coyoacan, Mexico

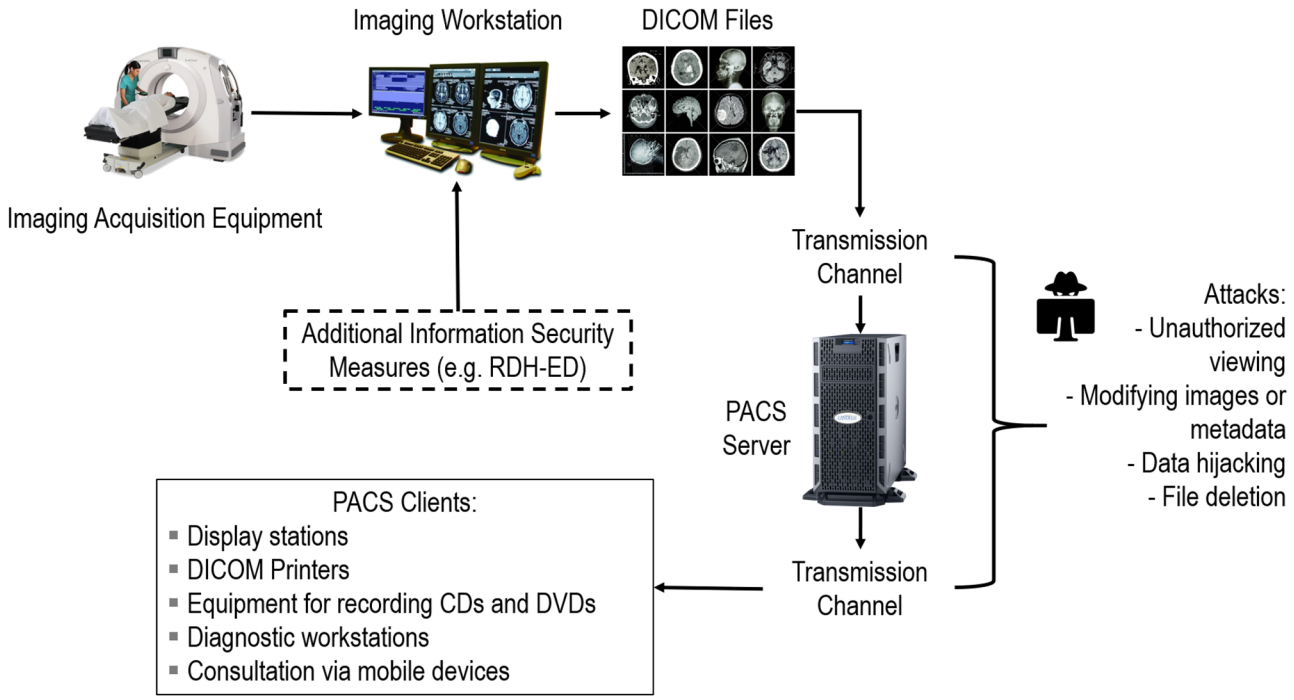

Fig. 1 Transmission of DICOM files through PACS systems

To confront some of these issues and considering that the DICOM standard allows the implementation of additional measures that increase data security, in the scientific literature several data hiding techniques in digital image watermarking modality [1, 2] have been used for this purpose. In general terms, the watermarking techniques embed a small amount of data bits called "watermarks" into the medical images to allow the authorized medical staff to extract embedded data for specific purposes. However, a drawback of watermarking methods is the visual distortion into the medical image after data embedding operation, moreover, the restoration of the image to its original form after watermark extraction/detection usually is not possible. To solve this inconvenient, reversible data hiding (RDH) techniques (also known as lossless or invertible data hiding) could be implemented since it makes possible to extract the embedded data without errors, as well as to restore the cover medium to its original state [4]. Over time, the proposals have been applied for digital media such as color and grayscale natural image, as well as digital audio and video, where the main efforts were focusing in a) improve capacity of the methods, b) obtain robustness against JPEG compression and c) conceal information meanwhile the contrast enhancement of the images is performed.

In general, the security measures were developed to verify the integrity and guarantee the privacy of the information contained in the image metadata, however, none contemplates the possibility of preventing the image pixels from being modified to the point where a healthy patient is diagnosed as sick or vice versa. In this way, e.g., in 2019 authors from [5] presented a scheme where deep learning was implemented to add and remove evidence of several pathologies in 3D medical images, which can lead to a complete misdiagnosis.

In this way, to guarantee the security and confidentiality of the hidden data and the image content respectively, reversible data hiding schemes over encrypted domain (RDH-ED) [4] are presented as a promissory solution, this refers to embed additional data into encrypted images, without losing the ability to recover both the data and the original content of the image, respectively. A characteristic that defined the first RDHE-ED schemes [6–8], and that differentiates it from other data concealment techniques, is the presence of three entities: a) the content owner who owns the original media and oversees encrypting it, b) the data hider, who embeds additional information into the encrypted media, and c) the receiver, the one who recovers the data or the original image from the encrypted marked media. Thus, the information can be embedded into the image without exposing its visual content, ensuring that the data hider does not know what the image represents, while allowing the receiver to access the content of the image or data, depending on the security elements that he owns. Likewise, RDH-ED methods can be classified into two categories: Vacating Room Before Encryption (VRBE) and Vacating Room After Encryption (VRAE), this depends on whether the image is processed to

define the space where the information will be embedded before or after it is encrypted, however, the data embedding is not carried out in the plaintext domain due to the characteristics of the entities already mentioned.

The most recent RDH-ED schemes [9–13] were designed for natural images with 8 bits of depth per pixel, authors of [9] encrypted the image with a tailored stream cipher and embedded the information through prediction-error expansion. On the other hand, in [10] Tromino scrambling is used with AES stream cipher, to later hide data by shifting a two-dimensional prediction error histogram (2D-PEH). The scheme presented in [11] used a conventional stream cipher in conjunction with the prediction errors obtained from the median-edge predictor detector to embed information using the least significant bit (LSB) substitution technique. In [12] the image was encrypted using NTRU (Number Theory Research Unit), while data embedding was done by shifting the histogram of the absolute differences of adjacent pixels. As in [11] the scheme of [13] used a conventional stream cipher and embedded the information using the LSB substitution technique, however, it employed a linear regression model to generate an error map, required to restore the image to its original state. Although the works of [9–13] used different encryption techniques, they took advantage of the spatial redundancy present in natural images to embed the additional data.

In the context of medical imaging, in the literature has been reported several methods based on RDH [14–21], and RDH-ED [22, 23] respectively. In this sense, the works presented in [14–21] were carried out in the plaintext domain, i.e., the image information is not encrypted, thus the content is legible to the naked eye. For the sake of brevity and to our best knowledge, we make a synthesis of the most representative works [22, 23] based on RDH-ED methods that are directly related to the field of medical imaging.

Given the importance of the region of interest (ROI) in medical diagnosis, an RDH-ED method for encrypted medical images was proposed in [22]. In general terms, the scheme in [22] divides the medical image into non-overlapping blocks and encrypts them using a conventional stream cipher [24, 25] with a public encryption key. Later, encrypted tiles of the image are classified in tiles of the ROI and the region of non-interest (RONI) respectively. Finally, control information and patient data are embedded in a customized manner using a data hiding key, modifying only the blocks belonging to the RONI, by flipping the least significant 3 bits of each encrypted pixel. In a similar way to embedding procedure, extraction and image recovery stage is performed. Thus, both patient data and control information necessary to recover the medical image could be reversibly hidden.

On the other hand, Liu et al. [23] presented an RDH-ED scheme for encrypted images based on ROI. As in their previous work reported in [21], the image is divided into the ROI, RONI and the border area, which, in general terms, is segmented, rearranged as a stack and encrypted using a conventional stream cipher [24, 25]. Using LSB substitution technique, the encrypted LSBs from ROI are concatenated with the electronic patient record (EPR) information and embedded in the encrypted domain; while the vertices that define the ROI along with the MD5 [24, 25] hash value of the ROI, are embedded in the appointed position into the border area. After the embedding process, access to the content is controlled according to the secret keys that the receiver owning. Thus, with the encryption key, a receiver could obtain an approximation of the original image; with the data hiding key, the receiver could perform the extraction of the embedded data without error; and with both keys, the ROI could be recovered without loss, as well as all data contained into the image.

However, as a drawback of the methods [22] and [23], in both the embedded data cannot be extracted when the image with hidden data is directly decrypted, i.e., in the plaintext domain. This fact implies that the recovery of data and the reversibility of the content image can only be performed in the encrypted domain, in this way, a receiver entity that possesses an approximation of the image (image with hidden data directly decrypted) as well as a data hiding key, will not be able to obtain the original content. A promissory solution to solve this problem is the use of the framework for complete separable reversible data hiding in encrypted images [26], which, in general terms, implies that a receiver entity can extract the embedded data and recover the original image not only from the image encrypted with hidden data but also from the approximate version obtained by directly decrypting it.

Since medical images contain valuable information, the proposed scheme must not alter the visual quality of the image, thus the process of data hiding should not produce perceptible changes to the human eye after the embedding of the data. Furthermore, the data embedding technique used should allow hiding enough information to store mainly patient data, clinical diagnosis and the necessary information to perform the reversibility of the image. Given the above needs, this paper proposes an RDH-ED scheme completely separable applied to DICOM [27] medical images, which allows the extraction of additional data, as well as the full restoration of the ROI, either from encrypted or plaintext domain of the DICOM medical image. Our proposal is inspired in the previous work reported in [23], which in our best knowledge, is the most recent and relevant RDH-ED scheme applied to medical images with native DICOM format, however, our proposal presents notable differences with [23]. Main contributions of this proposed paper are:

1. Tailored implementation of AES cipher in CTR mode operation for DICOM medical images with 12 or 16-bit resolution, to perform an effective extraction of hidden data either from the DICOM encrypted image with hidden data (encrypted domain) or from the directly decrypted version (plaintext domain).
2. Data embedding through LSB substitution with a pseudorandom walk in both ROI and RONI, to increase the security of the RDH-ED proposed method.
3. Implementation of the cryptographic hash function SHA-512 [24, 25] to guarantee the integrity of the embedded data as well as the fully restored ROI.
4. Evaluation of visual quality of the obtained DICOM medical images with more metrics based on the human visual system model (HVS), specifically the Structural Similarity Index (SSIM) and the Visual Information Fidelity (VIF) respectively.

The rest of this paper is organized as follows: Sect. 2 describes the materials and methods of the proposed scheme designed for embedding data in the encrypted domain of the medical image, as well as the data extraction and the full restoration processes of the ROI. The experimental results, including a discussion and a comparison with previous RDH-ED algorithms, are shown in Sect. 3. Finally, the conclusions and future work are presented in Sect. 4.

2 Material and methods

The proposed scheme consists of the ROI-based preprocessing, encryption of medical image, data embedding in the encrypted domain, extraction of data and ROI recovery stages respectively. The framework of the proposed method is shown in Fig. 2.

2.1 ROI-based preprocessing

To obtain an encrypted medical image, the process described in this paper is applied to DICOM medical images in grayscale with 12 bit/pixel resolution $[0, 2^{12} - 1 = 4095]$ and dimensions M x N.

However, to increase the level of security of the scheme and vacate the room where additional data will be embedded, a preprocessing is performed on the image to rearrange it according to an interactive selection of ROI into the medical image. The preprocessing of the image is described below:

Step 1- Read the original DICOM medical image I and supported by an interaction between the content owner and computer device, according to given clinic criteria, select a rectangular area that containing the ROI of the image I. The coordinates of vertices that define the selected region are registered and denoted as V_{ROI}. Note that the capacity of the proposed RDH-ED method is directly proportional to the sizes of ROI and RONI areas, as well as dependable on the spatial resolution of the DICOM modality of the image I, i.e., the capacity of the algorithm decreases according to the increase in ROI size. On the other hand, the maximum size of ROI is explained later in Sect. 3.

Step 2- Once ROI area is selected, to verify its integrity after the reversibility process, the hash value of ROI is calculated with the algorithm SHA-512 [24, 25], according to (1):

$$H_{ROI} = H_{SHA-512}(ROI) \tag{1}$$

where $H_{SHA512}(\cdot)$ denotes message-digest SHA-512 hash function and H_{ROI} denotes the binary representation of 512 bits generated after conversion from hexadecimal to binary values of $H_{SHA512}(\cdot)$. It should be mentioned that other

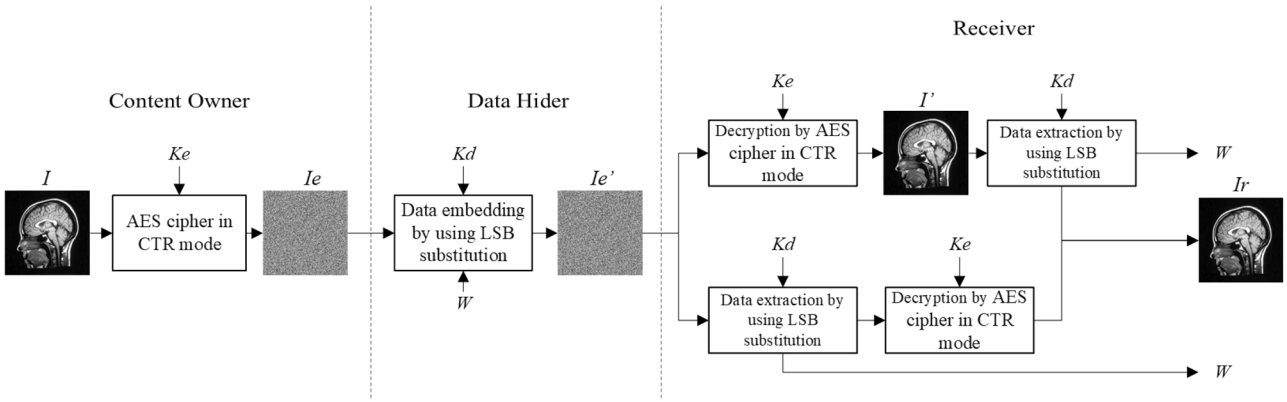

Fig. 2 Framework of the proposed scheme

cryptographic hash functions can be adapted to perform this step.

Step 3- Finally, the image is rearranged stacking all the RONI pixels followed by the pixels that belong to the ROI, preserving the original dimensions M x N. We obtain the Ind_{ROI} index of the pixel that points out the beginning of ROI in the reordered image.

2.2 Medical image encryption

After ROI-based preprocessing, the reordered medical image is encrypted using the AES-128 block cipher algorithm in counter mode (CTR) [24, 25]. This algorithm is an alternative to dedicated ciphers tailored to data hiding in the encrypted domain [28], due to the high efficiency of its implementation and the security it provides to the information systems, as well as its ability to emulate the operation of a conventional stream cipher. Unlike [23], where a conventional stream cipher is used to obtain the encrypted domain, in this paper we adapt and customize the AES-128 block cipher algorithm to achieve the completely separable reversibility explained earlier, which is a property not provided by [23]. In this way, considering 12 and 16 bit/pixel grayscale resolution of DICOM images in conjunction with the AES-128 block cipher algorithm in counter mode (CTR), the process of image encryption is described as follows:

Step 1- The rearranged image I is divided into non-overlapping blocks B_i, each of them of 4×4 pixels, according to (2).

$$I = \{B_i\}_{i=1}^{j}, where j = \frac{n}{4\times4} \tag{2}$$

where the total number of blocks is given by j, which is obtained by dividing the total number of pixels n of the image among the 16 pixels contained in each block. The size of B_i is determined by the operation specifications of the AES-CTR algorithm.

Step 2- The decimal representation of the pixels of a given block B_i is converted to 3-digit hexadecimal numbers when bit-depth of the image is 12 bit/pixel and 4-digit hexadecimal numbers when bit-depth of the image is 16 bit/pixel, in order to facilitate the manipulation of the bits of each pixel.
Step 3- A partition is performed to each hexadecimal number in such a way that the first two digits from left to right, that representing the eight most significant bits denoted as MSB_{B_i}, are separated from the 3rd digit when 12 bit/pixel or 4th digit when 16 bit/pixel, i.e. the least significant bits denoted as LSB_{B_i}.

Step 4- To obtain the encrypted block $MSB_{B_i^e}$ of the MSB_{B_i}, an encryption key K_e is required, which determines the result of the application of the AES-CTR stream cipher to the hexadecimal digits MSB_{B_i}. If not specified, the default length of K_e is 128 bits.
Step 5- Once the encrypted block $MSB_{B_i^e}$ is obtained, concatenate the unaltered LSB_{B_i} with the encrypted $MSB_{B_i^e}$.
Step 6- Values obtained of the concatenation in Step 5 are converted from hexadecimal to decimal representation, to generate the final encrypted block of pixels B_i^e. This block encryption procedure could be expressed as (3):

$$B_i^e = e\left(B_i, K_e\right) = B_i \oplus K \tag{3}$$

where the encryption function $e(B_i, K_e)$, denotes all steps described above. The ciphertext is obtained by an XOR operation between plaintext domain of the bits and the pseudorandom bitstream K, generated by AES-CTR stream cipher and the encryption key K_e. To illustrative purposes, Fig. 3 shows an example of the above encryption procedure considering a 12 bit/pixel bit depth.

Step 7- In this way, by repeating the procedure described from Steps 2 to 6 for each one of the blocks B_i in plaintext domain, the encrypted version of the DICOM medical image I_e is obtained by (4):

$$I_e = \{B_i^e\}_{i=1}^{j} \tag{4}$$

where $i=1, \ldots, j=n/4\times4$, e denotes encryption domain.

Finally, to complete the creation of the encrypted medical image I_e and considering an appointed position $R(x,y)$ in the first pixels of the RONI, conceal into RONI the data of V_{ROI} and Ind_{ROI} using LSB substitution technique.

The V_{ROI} parameter allows a receiver with the key K_e reconstruct the ROI and RONI when the image is decrypted. On the other hand, Ind_{ROI} is required by the data hider to embed additional data in the corresponding region; this guarantees that the plaintext of the image will not be exposed, either when embedding or extracting data.

2.3 Data embedding in the encrypted domain

Once preprocessed and encrypted DICOM medical image I_e is obtained by the content owner, as shown in Fig. 4, the data hider is capable of embed data into the encrypted medical image, without knowing the image content.

To embed additional data, LSB substitution technique is used, which has been widely used in data hiding schemes [29–31], due to its high capacity to embed data into images without affecting its visual quality. This technique consists of the substitution of the pixel LSB by a bit $b=\{0,1\}$, the changes caused in the value of the modified pixel are:

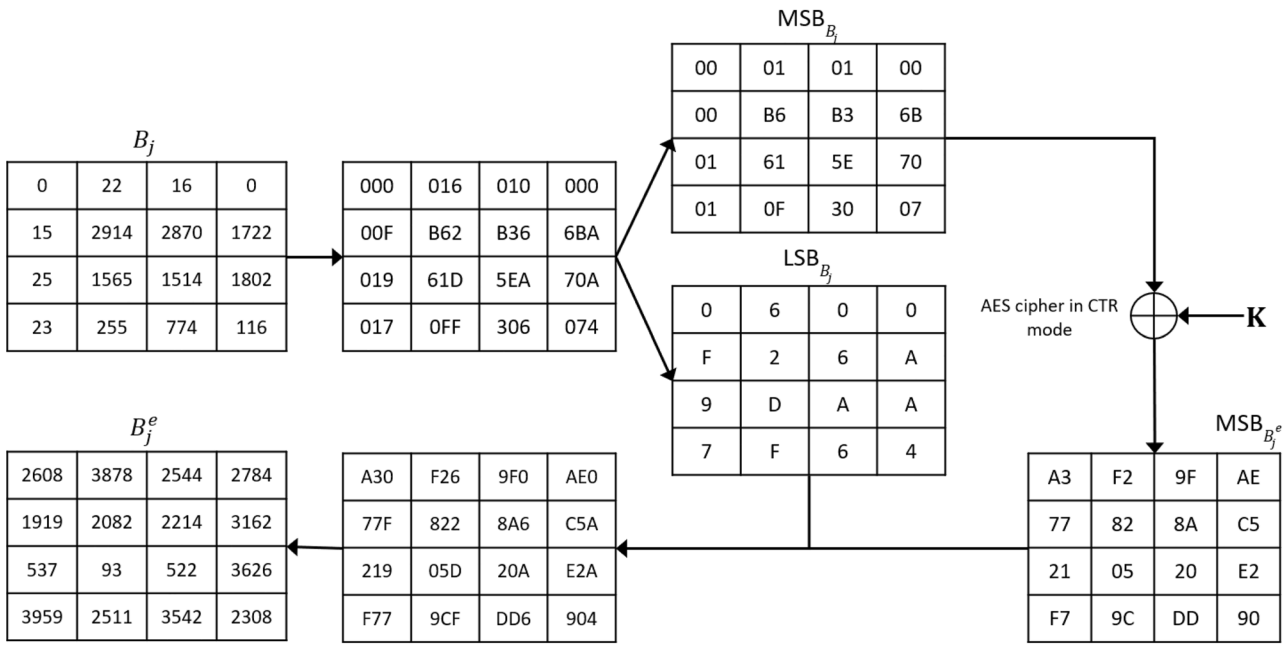

Fig. 3 Example of tailored encryption for medical images with 12 bit/pixel depth

Considering the value of a pixel pair as $2i$, with $i=0, \ldots, (2^{12}/2-1)=2047$, the value changes according to (5):

$$2i \xrightarrow[LSB-substitution]{} \begin{cases} 2i, & \text{if } b=0 \\ 2i+1, & \text{if } b=1 \end{cases} \tag{5}$$

Considering the value of an odd pixel as $2i+1$, with $i=0, \ldots, 2047$, its value is given by (6):

$$2i+1 \xrightarrow[LSB-substitution]{} \begin{cases} 2i, & \text{if } b=0 \\ 2i+1, & \text{if } b=1 \end{cases} \tag{6}$$

In order to guarantee patient privacy, as well as the integrity of their associated information, before embedding data into I_e, the following additional information is required:

- From metadata of DICOM medical image I_e, the fields associated with the name, date of birth, gender, and patient identifier are obtained and stored in binary form into M_p.

- From the DICOMDIR file associated with DICOM medical image I_e, the diagnosis summary of the patient is obtained and stored in binary form into D_p.

- To verify the integrity of M_p and D_p information after the extraction-data and ROI-recovery procedures, SHA-512 bits hash of M_p and D_p denoted as H_M and H_D are obtained applying (7) and (8) respectively.

$$H_M = H_{SHA-512}(M_p) \tag{7}$$

$$H_D = H_{SHA-512}(M_p) \tag{8}$$

The embedding process is performed by the data hider entity, which is described in detail as follows:

Step 1- From DICOM medical image I_e, read the LSBs embedded into I_e according to the appointed position

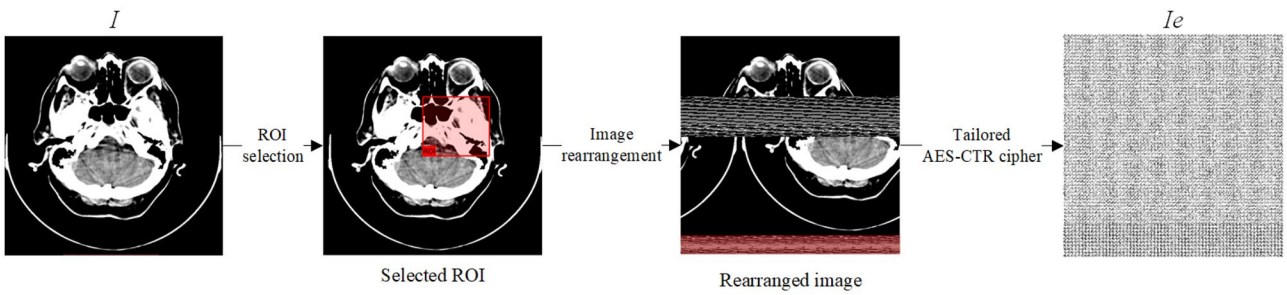

Fig. 4 Sample of the preprocessing in conjunction with medical image encryption according to the selection of ROI

$R(x,y)$ and recover the index Ind_{ROI}, which determines the pixels belonging to ROI and RONI, respectively.
Step 2- Supported by the information of the hash values H_{ROI}, H_M and H_D, a set of control data L_{ROI} composed by indexes location of each one, is obtained.
Step 3- Concatenate the data bits of H_{ROI}, H_M, H_D, and L_{ROI}, and obtain the information that will be concealed into the ROI, which is denoted as W_{ROI} and generated by (9):

$$W_{ROI} = L_{ROI} + H_{ROI} + H_M + H_D \tag{9}$$

the operator " + " in (9) indicates the concatenation of data bits.

Step 4- Embed W_{ROI} information into encrypted ROI pixels, using the index Ind_{ROI} and LSB substitution with pseudorandom walk defined by the secret key K_d. For this purpose, Kd seeds a pseudorandom number generator to produce a pseudorandom permutation of the pixel positions, from the beginning of ROI to the last pixel of the image, so that increases the security level of hidden data.
Step 5.- During the process of LSB replacing, the original LSBs of the ROI that were modified are recorded in a string denoted as LSB_{ROI}. A set of control data L_{RONI} composed by indexes location corresponding to LSB_{ROI}, the metadata, and the patient diagnosis, is obtained.
Step 6- Concatenate the data bits of L_{RONI}, LSB_{ROI}, M_p, and D_p, to obtain the information that will be concealed into the RONI, which is denoted as W_{RONI} and generated by (10).

$$W_{RONI} = L_{RONI} + LSB_{ROI} + M_p + D_p \tag{10}$$

Step 7- Embed W_{RONI} information into encrypted RONI pixels, using LSB substitution with pseudorandom walk defined by the secret key K_d, excluding the first encrypted pixels of the RONI where V_{ROI} and Ind_{ROI} were concealed by the content owner according to the appointed position $R(x,y)$.

In summary, RONI conceals sensitive patient and diagnostic information, as well as the LSBs required for the full restoration of ROI; meanwhile, ROI conceals data for integrity verification related to patient, diagnostics and ROI data respectively. In this way, the capacity W is defined as the total sum of bits embedded in both the ROI and the RONI, as shown in (11).

$$W = W_{ROI} + W_{RONI} \tag{11}$$

Note that this embedding process can be done in any LSB plane. In this way, when embedding W in the vacated room reserved during preprocessing and encryption procedures, the encrypted image with data hidden I'_e could be as represented in (12):

$$I'_e = RDHED(I_e, W, K_d) \tag{12}$$

where $RDHED(\bullet)$ refers to the embedding procedure by using LSB substitution in the encrypted domain which was described earlier in Steps 1–7. Finally, the image I'_e is written in DICOM format.

2.4 Data extraction and ROI restoration

In this stage, a receiver entity with the image I'_e will perform several operations, depending on whether he has the encryption key K_e or the data hiding key K_d or both. Different from non-separable RDH-ED methods such as [23], in the schemes completely separable such as this proposed method, it is possible to extract the concealed data and recover the ROI either from the plaintext or encrypted domain. Cases available to a legitimate receiver entity are illustrated in Fig. 5. Cases 1, 2 and 3 in Fig. 5 are performed in the encrypted domain, while cases 4 and 5 are carried out in the plaintext domain.

2.4.1 Case 1: Data extraction from the encrypted domain

A receiver with the pseudorandom walk data hiding key K_d will have access to the additional data embedded inside I'_e, without being able to decrypt the image. To achieve this, the following procedure is required.

Step 1- Read the DICOM image file and obtain the image I'_e.
Step 2- From I'_e, obtain the parameter Ind_{ROI} by reading the LSBs embedded in the appointed position $R(x,y)$.
Step 3- Using the pseudorandom walk data hiding key K_d and the parameter Ind_{ROI} that contains the beginning of ROI, read the LSBs of ROI and RONI, and obtain the sequences W_{ROI} and W_{RONI} respectively.
Step 4- From sequences W_{ROI} and W_{RONI}, identify the control information L_{ROI} and L_{RONI}, and extract all data bits from ROI and RONI, respectively.
Step 5- Binary sequences corresponding to the metadata M_p and patient diagnosis D_p are converted to ASCII code, on the other hand, bits of the hash values H_M and H_D are formatted to hexadecimal representation.
Step 6- Finally, using the recovered information of metadata and diagnosis M_p, D_p, H_M and H_D we can verify its data integrity.

In Case 1, the original LSBs of ROI, LSB_{ROI}, and the hash value H_{ROI} are not employed.

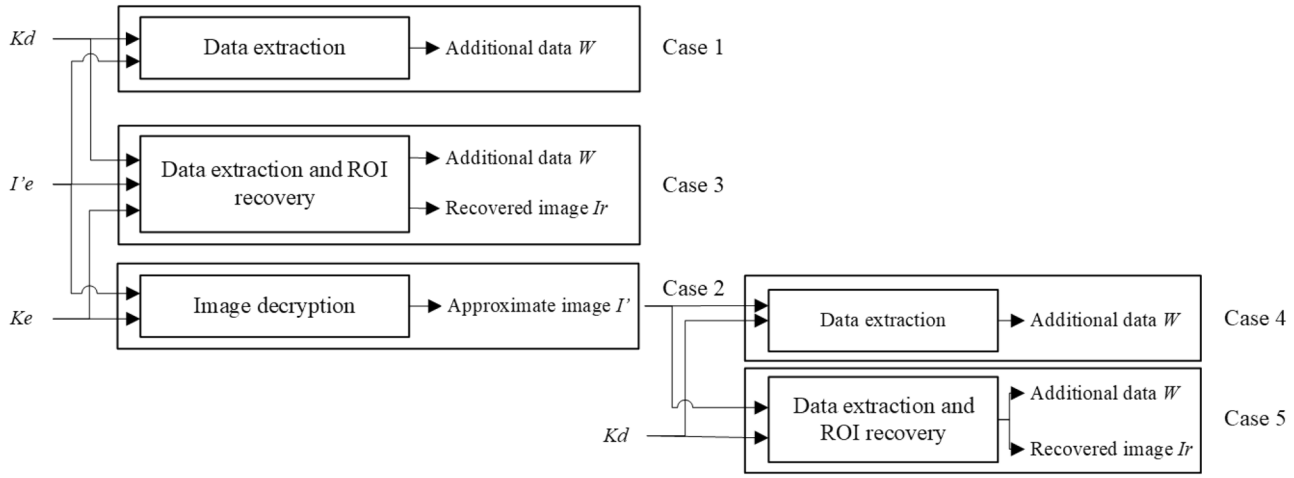

Fig. 5 Reception cases in the receiver stage of the complete separable RDH-ED scheme proposed

2.4.2 Case 2: Obtaining of the medical image approximation from the encrypted domain

A receiver that has only the encryption key K_e is able to directly decrypt the image to generate an approximate version of the original image, however, he cannot extract another data embedded. This process is described as follows:

Step 1- Read the DICOM image file and obtain the image I'_e.
Step 2- To re-arrange the approximate image after the decryption process, it is necessary to recover the vertices of ROI, in this way, V_{ROI} is obtained from reading the LSBs in the appointed position $R(x,y)$. We would like to emphasize that obtaining this parameter can also be done after the decryption procedure.
Step 3- To decrypt the image I'_e and obtain its approximate version in plaintext, the decryption process is performed to each block of pixels, according to (13).

$$B_i = d\left(B_i^e, K_e\right) = B_i^e \oplus K \tag{13}$$

where the decryption function $d\left(B_i^e, K_e\right)$ implies the same operations as in (3) in a decryption mode operation. Once the image I'_e has been decrypted, with V_{ROI} information, ROI and RONI pixels are arranged to their original positions and the approximate version of the medical image I' is obtained, whose visual quality is close to the original in spite of the hidden data that remains in its content.

2.4.3 Case 3: Recovery of ROI from the encrypted medical image

A receiver with the encryption key K_e and the pseudorandom walk data hiding key K_d can extract error-free embedded data as well as recover the ROI with lossless, both procedures from the encrypted medical image I'_e, as follows:

Step 1- Read the DICOM medical image I'_e and extract the V_{ROI} and Ind_{ROI} parameters from the LSBs of the pixels in the appointed position $R(x,y)$.
Step 2- Using the pseudorandom walk data hiding key K_d and the Ind_{ROI} parameter, all data bits W concealed in the image I'_e are extracted.
Step 3- Recover the LSB_{ROI} from the extracted data bits W and, in the order given by the secret key K_d, restore the LSBs of the encrypted ROI to its original state, i.e., the state prior to the LSB substitution.
Step 4- Once ROI is restored, decrypt the DICOM medical image I'_e with encryption key K_e using (13).
Step 5- The decrypted image in Step 4 is rearranged using the information of V_{ROI}. The resultant medical image is denoted by I_r and contains the ROI information completely restored to its original form.
Step 6- Finally, ROI integrity can be verified using the hash value H_{ROI} and ROI restored information.

Note that the extraction of all data bits W, as well as the restoration of the ROI LSBs, can be performed after the decryption procedure or before the reconstruction of the image.

2.4.4 Case 4: Data extraction from the plaintext domain

The receiver entity with the approximate version of the medical image *I'* and the pseudorandom walk data hiding key K_d, can extract the additional data *W* from the plaintext domain, using the control parameters V_{ROI} and Ind_{ROI} from the appointed position $R(x,y)$ of the image *I'*. This is possible because the encryption method does not modify the first LSB planes of the pixels, allowing them to keep the embedded bits even after decryption.

In this way, the image *I'* is rearranged using the parameter V_{ROI} and subsequently, the receiver can extract the additional data *W* employing K_d and Ind_{ROI} parameters.

2.4.5 Case 5: ROI recovery from the decrypted image

This case extends the capabilities of Case 4. In this way, once the image *I'* is rearranged and the additional data *W* was extracted, the modified LSBs into ROI are replaced by the bits of LSB_{ROI} using K_d and, as a consequence, ROI is restored to its original condition; thus, employing the V_{ROI} information, an image I_r can be obtained, which contains the ROI completely restored with lossless data.

3 Results and discussion

To evaluate the performance of the algorithm applied to DICOM imaging, this section presents the experimental results and discussion of the proposed scheme. A set of 200 computed tomography (CT) scans in DICOM format [27] were used, composed of skull, thorax and abdomen images; of 512×512 pixels in size and 12 bit/pixel resolution in grayscale. Considering the spatial and grayscale resolutions of CT images, experiments were performed using a ROI with a size of 25% of the spatial resolution of the original image.

Although the schemes of the works [9–13] are more recent and have obtained competitive results, they cannot be directly implemented in medical imaging, since they are based on the spatial correlation present in the image pixels. As can be seen in Fig. 6a, the regions that appear to be flat in a DICOM image are represented by very different intensities and the pixel values are in a range that goes from 0 to 1024, 4096, or 65,536, because DICOM images can have resolutions of 10, 12 or 16 bit/pixel depth, depending on the modality. On the other hand, the intensities of the pixels in a natural image are usually approximate to each other and are in a range from 0 to 255, as shown in Fig. 6b, which allows the use of methods based on predicting pixel values or calculating the difference between pixels. Therefore, the comparison of results will be performed between the schemes that have been designed for medical images.

Lengths of parameters V_{ROI} and Ind_{ROI} are: V_{ROI} control parameter consists of 4 coordinates represented by 10 bits each one, obtaining a length of 40 bits; while Ind_{ROI} is a sequence of 18 bits that indicates the pixel index at which ROI begins, obtaining a total length of $V_{ROI}+Ind_{ROI}=58$ bits. These control data are embedded into the LSBs of the first 58 pixels of the medical image. To perform data extraction, the control information L_{ROI} and L_{RONI} is formed by 3 indexes, each one allows to identify the beginning and the end of the binary sequences embedded in ROI and RONI respectively; thus each index is represented by 18 bits, hence, $3\times18=54$ bits is the length of L_{ROI} and L_{RONI} respectively. Since message-digest algorithm SHA-512 cause an output of 512 bits in length, the total amount of data to recover ROI region is $LSB_{ROI}=L_{ROI}+H_{ROI}+H_M+H_D=54+512+512+512=1590$ bits. The patient sensitive information M_p is obtained from the metadata of DICOM medical images and is composed of the fields associated with the name, date of birth, gender, and patient identifier. Meanwhile, the size of the patient diagnosis D_p is variable and, for illustrative purposes, in the experimental results its length was adjusted with pseudorandom data.

All tests were carried out on a personal computer with Microsoft Windows 10 © operating system, Intel © Core ™ i7

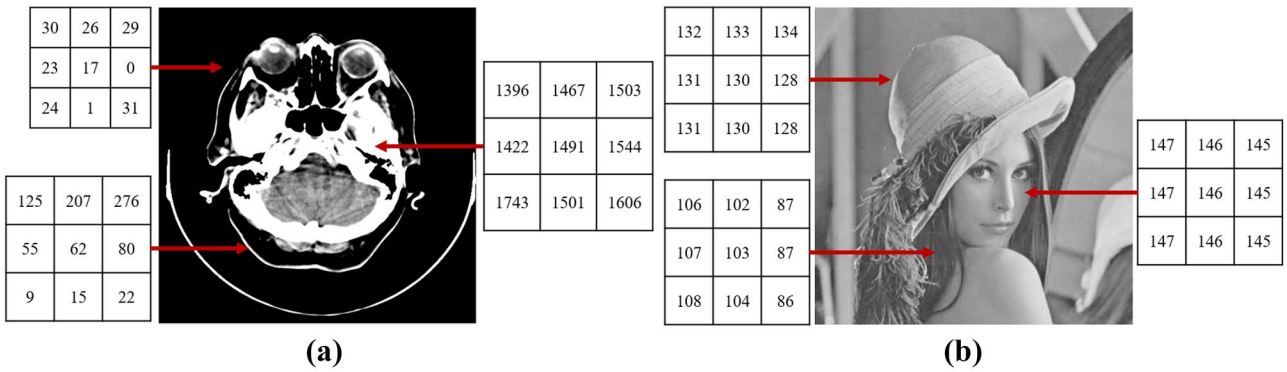

Fig. 6 Samples of pixel values from 3×3 flat regions (**a**) from a DICOM CT scan with 12 bit/pixel grayscale resolution, and (**b**) from the conventional image Lena with 8 bit/pixel grayscale resolution

(2.66 GHz) processor and 8 Gb of RAM, where the algorithms of the proposed scheme were implemented in MATLAB © R2017b. For the encryption stage, the average processing time was 10.06 s. The restoration of ROI with embedding rates of 0.01 to 0.7 bits per pixel (bpp) in the encrypted domain was carried out in an interval from 9.95 to 11.24 s; meanwhile, in

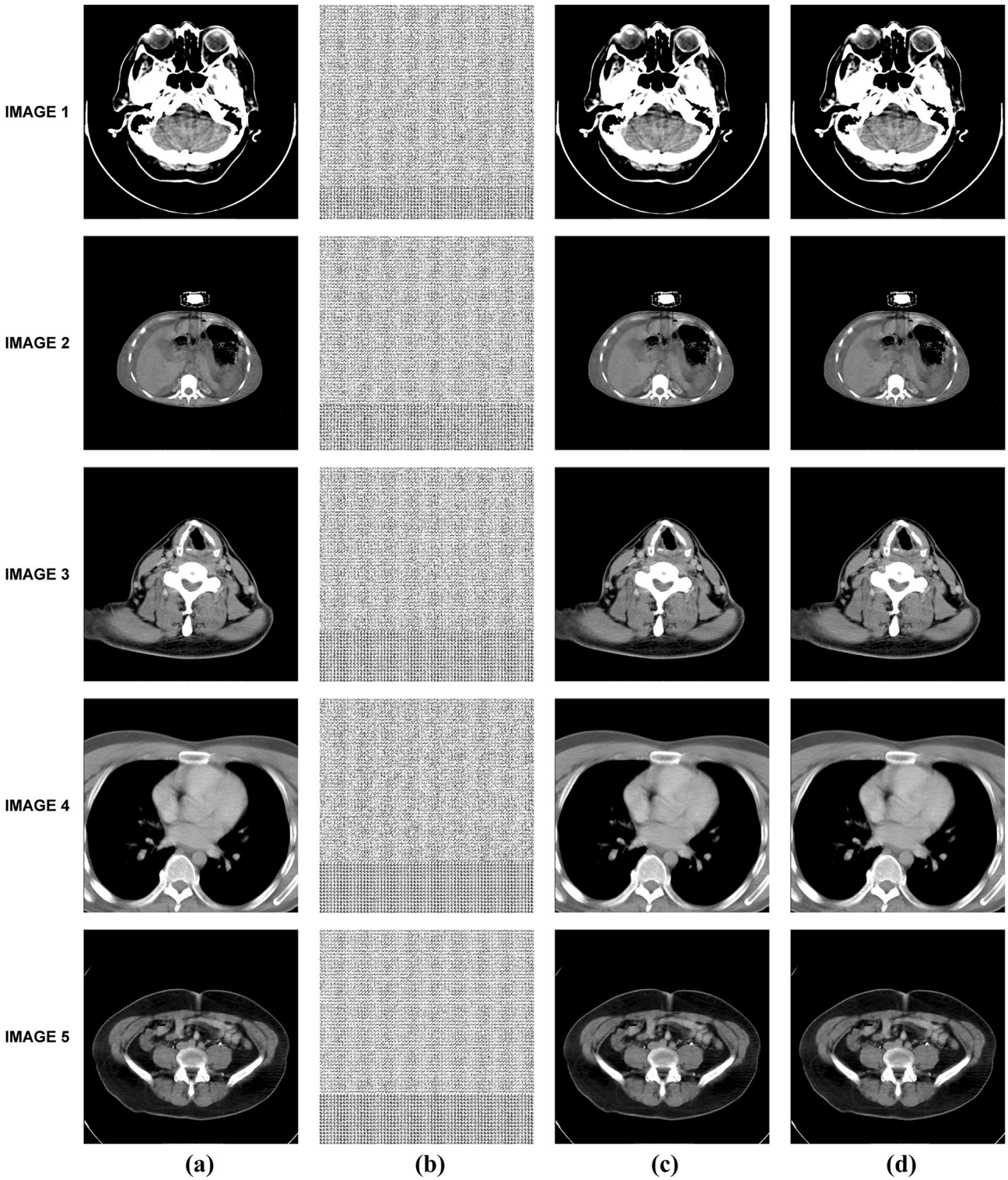

Fig. 7 (**a**) Original test medical images, (**b**) Encrypted medical images with data hidden, (**c**) Approximate images without ROI restored and (**d**) Images with restored ROI. Embedding rate of 0.5 bpp in the 1st LSB plane and a ROI size of 25% of the original image

the plaintext domain, the restoration time was in an interval from 0.53 to 1.48 s. Considering an embedding rate of 0.5 bpp in the 1st LSB plane and a ROI size of 25% of the original image, Fig. 7 shows five test DICOM medical images used in the proposed scheme with its encrypted version with hidden data, as well as their approximated and recovered versions with ROI restored, respectively. DICOM images in Fig. 7 were obtained using the specialized software Radiant DICOM Viewer ©.

The performance of the proposed algorithm is evaluated in terms of imperceptibility using several embedding rates for the first 3 LSB planes. A widely used conventional metric to evaluate the visual quality of images with data concealed in its content is the Peak Signal to Noise Ratio (PSNR) [32], given by (14):

$$PSNR(dB) = 10\log_{10}\left(\frac{N \cdot M \cdot MaxPixel\ Value^2}{\sum_{x=1}^{N}\sum_{y=1}^{M}\left(I(x,y) - I'(x,y)\right)^2}\right) \quad (14)$$

where N and M are the image dimensions, while I and I' are the original and the image with data hidden in its content, respectively.

In this context, Fig. 8 shows a performance comparison in terms of PSNR using test images 1, 2, 3 and 4 shown in Fig. 7, with several embedding rates from 0 to 0.5 bpp. The RDH-ED methods included in the comparative are [6–8, 22] and [23]. PSNR in Fig. 8 is measured directly from decrypted images versions that still have data concealed in its content. From Fig. 8 we show that the imperceptibility decreases quickly in the works [6–8] and [22]

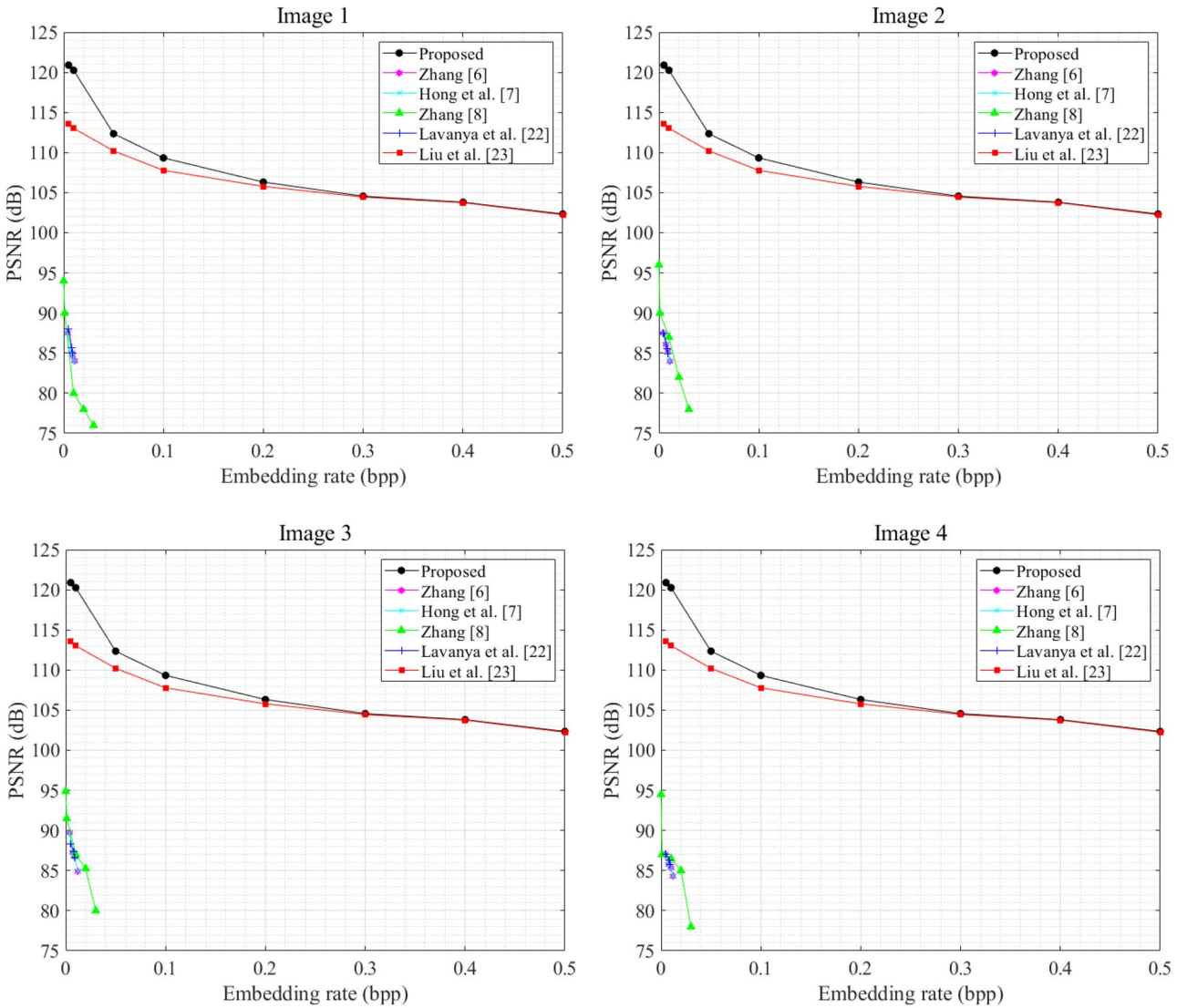

Fig. 8 PSNR comparison obtained from directly decrypted images with the methods Zhang [6], Hong et al. [7], Zhang [8], Lavanya et al. [22] and Liu et al. [23]

Table 1 Average PSNR comparison obtained in approximate images for the first three LSB planes with respect to several embedding rates

Embedding rate (bpp)		PSNR (dB)							
		0.005	0.01	0.05	0.1	0.2	0.3	0.4	0.5
Proposed method (approximated image)	LSB plane 1	120.89	120.26	112.35	109.33	106.32	104.56	103.81	102.34
	LSB plane 2	114.88	114.26	106.34	103.32	101.02	99.55	98.80	97.03
	LSB plane 3	108.87	108.24	100.33	97.31	95.79	94.03	92.78	91.66
Liu et al. [23] (approximated image)	LSB plane 1	113.58	113.02	110.21	107.78	105.78	104.45	103.75	102.25
	LSB plane 2	108.31	108.52	105.12	102.44	100.54	98.23	97.90	96.31
	LSB plane 3	102.22	102.00	99.32	97.23	95.66	93.99	92.26	91.56

for embedding rates below 0.1, obtaining PSNR values of less than 80 dB. This fact indicates that the methods [6–8] and [22] inevitably introduce visual distortion when the embedding rate is increased, as a consequence, its application in medical images seems not suitable to scenarios that require high data embedding capacity.

On the other hand, Fig. 8 shows that the RDH-ED method reported in [23] and the proposed one in this paper, both obtained PSNR values greater than 102 dB for embedding rates from 0 to 0.5 bpp, avoiding any visual distortion into the medical images and allowing a high data embedding capacity. Based on these results and considering that the algorithm presented by Liu et al. [23], in our best knowledge, is nowadays the most recent and relevant method in the context of RDH-ED for DICOM medical images, from now on the comparison is performed between the method of [23] and our proposed scheme.

In this way, considering embedding rates of 0.005, 0.01, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5, LSB planes 1, 2, 3, and decrypted images with and without restored ROI, the comparison between the PSNR average values obtained from Liu et al. [23] scheme and the proposed one is shown in Tables 1 and 2, respectively. From Tables 1 and 2 we show that the visual quality provided by our proposed method outperforms the offered by Lui et al. [23] in terms of PSNR. In this way, when the embedding rate is small (less than 0.1), PSNR differences between our proposed RDH-ED scheme and Lui et al. [23] are around 1.5–7.5 dB, becoming smaller when the embedding rate is increased, obtaining PSNR differences of 1.5–0.15 dB approximately.

In order to evaluate more strictly the performance of the proposed method in this paper, the literature reports metrics that allow evaluating the visual quality of the image more accurately than the PSNR, based on the perceptible distortions of an image with respect to another reference. One of these metrics is the SSIM (Structural Similarity Index) [33], defined by (15):

$$SSIM(I, I') = \frac{\left(2\mu_I\mu_{I'} + C_1\right)\left(2\sigma_{I'} + C_2\right)}{\left(\mu_I^2 + \mu_{I'}^2 + C_1\right)\left(\sigma_I^2 + \sigma_{I'}^2 + C_2\right)} \tag{15}$$

In (15), I is the original medical image, I' is the decrypted medical image with or without restored ROI, while C_1 and C_2 are small constant values defined in [33].

Another well-known criterion to determine the level of fidelity of a processed image with respect to the original, based on the human visual system model (HVS), is the VIF (Visual Information Fidelity) [32], given by (16):

$$VIF = \frac{\sum_{k \in channels} I(\vec{C}^{Z,k}; \vec{G}^{Z,k} | s^{Z,k})}{\sum_{k \in channels} I(\vec{C}^{Z,k}; \vec{E}^{Z,k} | s^{Z,k})} \tag{16}$$

where, E and G refer to the visual signals of the original medical image and the processed one, respectively, obtained from the HSV model and from which the brain extracts

Table 2 Average PSNR comparison obtained in recovered images for the first three LSB planes with respect to several embedding rates

Embedding rate (bpp)		PSNR (dB)							
		0.005	0.01	0.05	0.1	0.2	0.3	0.4	0.5
Proposed method (recovered image with ROI restored)	LSB plane 1	134.16	132.68	115.90	111.60	108.46	106.65	105.38	103.60
	LSB plane 2	127.15	125.67	109.90	105.59	102.45	100.64	99.47	97.89
	LSB plane 3	121.15	118.98	103.89	99.58	96.43	94.62	93.35	91.81
Liu et al. [23] (recovered image with ROI restored)	LSB plane 1	131.02	131.12	114.20	109.68	107.06	105.01	103.66	102.37
	LSB plane 2	113.25	112.32	106.67	103.78	101.15	99.43	98.32	97.01
	LSB plane 3	104.67	103.05	100.49	97.46	95.80	93.78	92.88	91.65

Table 3 Comparison of SSIM and VIF average values obtained in the approximate images for the first three planes LSB with respect to several embedding rates

Embedding rate (bpp)		0.01	0.05	0.1	0.2	0.3	0.4	0.5	0.6
SSIM (approximate image)	LSB plane 1	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
	LSB plane 2	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
	LSB plane 3	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
VIF (approximate image)	LSB plane 1	0.9990	0.9984	0.9969	0.9940	0.9913	0.9886	0.9860	0.9835
	LSB plane 2	0.9956	0.9940	0.9886	0.9786	0.9698	0.9619	0.9548	0.9482
	LSB plane 3	0.9827	0.9787	0.9619	0.9364	0.9174	0.9025	0.8903	0.88 00

cognitive information. $I\left(\vec{C}^{Z,k};\vec{G}^{Z,k}|s^{Z,k}\right)$ denotes the information that, theoretically, the brain extracts from a specific channel of the original image, while $I\left(\vec{C}^{Z,k};\vec{E}^{Z,k}|s^{Z,k}\right)$ corresponds to information extracted from the processed image.

Both the SSIM and the VIF metrics provide more accuracy than the conventional PSNR to determine perceptible distortions in a given image and have a range of values of [0, 1]. SSIM and VIF values close to 1 indicate a good visual quality regarding the original image. The average values of SSIM and VIF obtained with embedding rates ranging from 0.01 to 0.6 bpp for each of the first three LSB planes, are shown in Tables 3 and 4, for directly decrypted images and those with ROI completely restored, respectively.

Regarding the above analysis between the imperceptibility and capacity of the proposed method, several points should be noted. Since the length of bits embedded into ROI (W_{ROI}) is fixed, the number of bits required for ROI restoration (LSB_{ROI}) does not depend on the size of the selected ROI area. However, a large ROI selected in the preprocessing stage limits the embedding capacity for the patient data M_p and the patient diagnosis D_p, because the number of pixels belonging to the RONI (where M_p and D_p are concealed) decreases when the selected ROI is bigger. In this way, considering images with 512×512 pixels in size and 12 bit/pixel resolution in grayscale, the proposed scheme requires a selected ROI with a minimum size of 40×40 pixels, so that it can store the 1,590 bits of W_{ROI}, allowing a maximum capacity in RONI to host 260,544 bits, which corresponds to a maximum embedding capacity of 0.99 bpp in a single LSB plane. On the other hand, the maximum size of the ROI depends on the amount of information that the data hider wants to embed; considering a case where no additional data is embedded, and only the control information (1648 bits) is stored in the RONI, the ROI can be made up of 260,496 bits, and like the RONI, the ROI can have a maximum size of 99% from the image.

Finally, from Tables 1, 2, 3 and 4, it can be seen that the proposed scheme allows the creation of approximate versions, as well as recovered versions with restored ROI, both with high visual quality, obtaining average values of PSNR, SSIM and VIF greater than 101 dB, 0.98 and 0.97 respectively when the embedding rate is 0.5 bpp in the first LSB plane; fact that shows that a receiver entity that possesses only the decryption key K_e is able to obtain decrypted DICOM medical images with hidden data which are visually identical to the original ones.

Another aspect analyzed is the capability of the RDH-ED proposed scheme to be unnoticed against the steganalysis technique. For this purpose, we employed the steganalysis method of Pairs of Values (PoV) [34], because it is one of the most efficient algorithms to detect hidden data when the embedding technique is LSB substitution. In general terms, PoV is based on statistical analysis using the probability density function (PDF) of χ^2 distribution [34]. In this way, considering embedding rates ranging from 0 to 0.6 bpp and the first three LSB planes of medical images, Fig. 9a shows the behavior of χ^2 distribution for approximated versions, meanwhile, Fig. 9b shows the results obtained from recovered versions with restored ROI. As shown in Fig. 9, the pseudorandom walk implemented in the data embedding stage of the proposed RDH-ED method allows obtaining

Table 4 Comparison of SSIM and VIF average values obtained in the recovered images for the first three planes LSB with respect to several embedding rates

Embedding rate (bpp)		0.01	0.05	0.1	0.2	0.3	0.4	0.5	0.6
SSIM (recovered image with ROI restored)	LSB plane 1	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
	LSB plane 2	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
	LSB plane 3	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
VIF (recovered image with ROI restored)	LSB plane 1	0.9992	0.9986	0.9971	0.9943	0.9915	0.9888	0.9862	0.9837
	LSB plane 2	0.9965	0.9949	0.9894	0.9795	0.9706	0.9628	0.9556	0.9491
	LSB plane 3	0.9859	0.9819	0.9651	0.9396	0.9206	0.9056	0.8934	0.8831

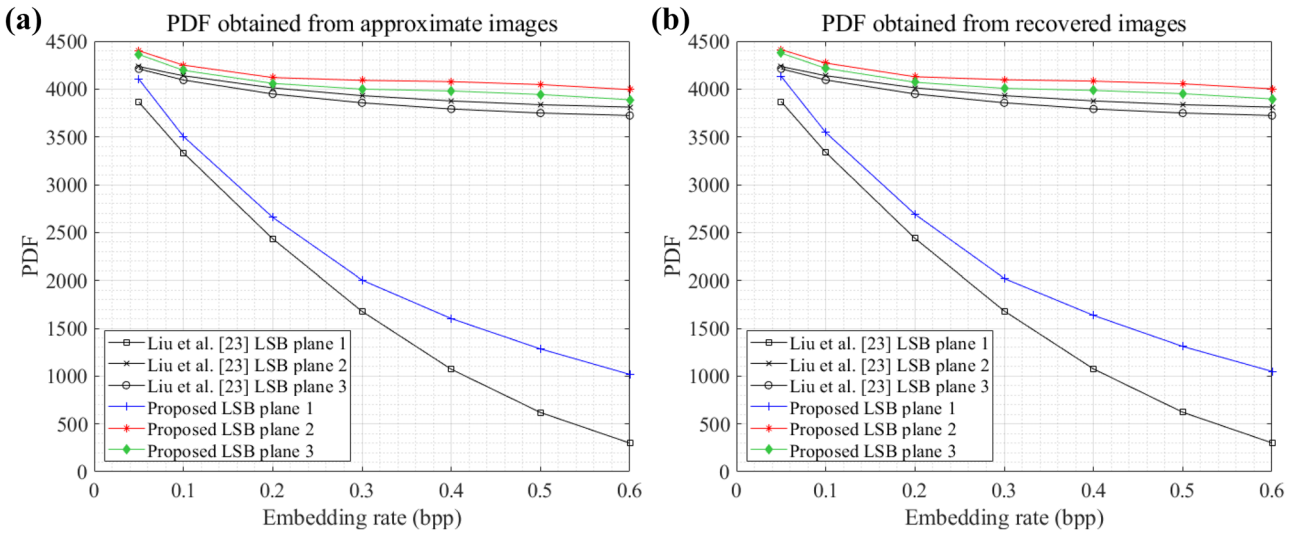

Fig. 9 Comparison of the values of PoV steganalysis obtained from (**a**) approximate images and (**b**) images with restored ROI, for several embedding rates

higher PDF values regarding the sequential walk used in the method of Lui et al. [23]. Thus, considering that with a low value of PDF, the probability of detecting the presence of hidden data in an image is high, from Fig. 9a and b we show that our proposed RDH-ED method compared with [23], provides a better capability in terms of allowing concealed data in medical images to be unnoticed against the steganalysis technique, demonstrating the benefits of using a pseudorandom-walk in RDH-ED schemes, as in the case of our proposed algorithm.

To complete the test, a performance comparison is presented in Table 5, regarding the state of the art reported in [6–8, 22] and [23] in terms of capability to be separable (data extraction and image recovery could be done from the encrypted or plaintext domain, not in both), the ability to be completely separable (data extraction and image recovery can be performed either in encrypted domain or plaintext domain), as well as the presence of errors in data extraction and image recovery, respectively. Therefore, in Table 5 we show that the methods of Zhang [6], Hong et al. [7] and Lavanya et al. [22] are not separable in their stages of data extraction and image recovery, meanwhile, the works of Zhang [8], Liu et al. [23] and our proposed method are separable. On the other hand, our proposed RDH-ED method is completely separable, while the other schemes are not. Regarding errors in data extraction, Zhang [8], Liu et al. [23] and our proposed method are error-free, although the rest of the methods present errors in the extracted bits. Finally, concerning errors in image recovery, we show that Lavanya et al. [22], Liu et al. [23] and our proposed method present errors in recovered images only in the RONI content, this fact is because these three RDH-ED methods are ROI-based, i.e., they recover in an intact manner only the ROI information. The rest of the methods [6, 7] and [8] contains errors in the recovered image, in both the ROI and RONI areas. Although the results obtained are very similar to those of [23], the proposed method has managed to increase the recovery options of the receiver, since it allows restoring the image and extracting the data from the plaintext domain of the approximate image, without losing embedding capacity

Table 5 Performance comparison

Methods	Performance			
	Separable	Complete separable	Error in data extraction	Error in image recovery
Zhang [6]	No	No	Yes	Yes
Hong et al. [7]	No	No	Yes	Yes
Zhang [8]	Yes	No	No	Yes
Lavanya et al. [22]	No	No	Yes	Only RONI
Liu et al. [23]	Yes	No	No	Only RONI
Proposed	Yes	Yes	No	Only RONI

and visual quality of the approximation, whereas this is not possible with the work of [23]. Additionally, the proposed scheme provides a higher level of protection against steganalysis, thanks to the implementation of the LSB substitution in pseudo-random order.

4 Conclusions

To protect the privacy of a medical image, as well as the patient personal information associated with it, in this paper we propose a reversible data hiding scheme for encrypted medical images; whose reversibility, unlike related works in the state of the art, is completely separable by allowing the extraction of the additional data and the restoration of the region of interest, both from the plaintext domain and the encrypted domain of DICOM medical images. According to the proper key, a legitimate receiver can perform the following tasks: a) Obtain a high visual quality approximate image with respect to the original version by directly decrypting the cryptogram with the encryption key, b) With the data hiding key, the embedded data can be extracted free of any error, either from the encrypted image or its approximate version respectively, and c) In case of having both keys, the embedded data can be extracted and the recovered image with the region of interest fully restored can be obtained without loss of information. In this context, the proposed RDH-ED method is suitable for applications where the information security and the management of medical images need to be ensured in terms of reliability, integrity and, confidentiality.

The high visual quality of DICOM images with restored ROI has been demonstrated by obtaining average values of PSNR, SSIM and VIF higher than 101 dB, 0.98 and 0.97, respectively. These values ensure that the medical images do not present perceptible distortions to the human eye that may alter the visual content of medical images and, as a result, lead to an erroneous diagnosis. Moreover, a high capacity for concealing data is warranted with embedding rates up to 0.6 bpp in the first three LSB planes. Also, information security is improved by using AES cipher in CTR operation mode to obtain the encrypted domain, SHA-512 algorithm to verify data integrity, as well as the implementation of pseudorandom-walk in data embedding to be unnoticed against steganalysis. A performance comparison with the most recent work reported in the state of the art was provided, demonstrating the superiority of our proposed method in terms of visual quality of the obtained medical images, as well as an improvement in the versatility of separability, by allowing data extraction and ROI restoration, either from the encrypted domain or from the plaintext domain; preserving in all cases the performance in terms of data embedding capacity.

As future work, we consider the implementation of a reversible data hiding technique that allows the restoration of the whole image or the use of lossless data compression methods, in order to achieve total reversibility and not only of the region of interest ROI. Also, extending the application of our method to other modalities of medical imaging, such as magnetic resonance imaging (MRI), radio fluoroscopy (RF), computerized radiography (CR), among others.

Acknowledgments Authors thank the Instituto Politecnico Nacional (IPN) as well as the Consejo Nacional de Ciencia y Tecnologia de Mexico (CONACYT) by the support provided during the realization of this research.

Funding This research was supported by Instituto Politecnico Nacional (IPN) as well as the Consejo Nacional de Ciencia y Tecnologia (CONACYT) of Mexico.

Declarations

Informed consent All patients data in DICOM images used in this research was anonymized considering the DICOM standard in https://www.dicomstandard.org/using/security. In this way, none patients data appears in all content of the paper.

Research involving human participants and/or animals This research not involving human participants and/or animals.

Conflicts of interest The authors declare that they have no potential conflicts of interest that could have appeared to influence the work reported in this paper.

References

1. Coatrieux G, Maitre H, Sankur B, et al. Relevance of watermarking in medical imaging. Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. 2000;250–5. https://doi.org/10.1109/ITAB.2000.892396.
2. Coatrieux G, Quantin C, Montagner J, Fassa M, Allaert FA, Roux C. Watermarking medical images with anonymous patient identification to verify authenticity. Stud Health Technol Inform. 2008;136:667–72 (PMID: 18487808).
3. U.S. Department of Health and Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf2021. Accessed 28 March 2021.
4. Shi Y, Li X, Zhang X, Wu H, Ma B. Reversible data hiding: Advances in the past two decades. IEEE Access. 2016;4:3210–37. https://doi.org/10.1109/ACCESS.2016.2573308.
5. Mirsky Y, Mahler T, Shelef I, Elovici YCT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning, Cornell University. 2019. https://arxiv.org/abs/1901.03597.
6. Zhang X. Reversible Data Hiding in Encrypted Image. IEEE Signal Process Lett. 2011;18(4):255–8. https://doi.org/10.1109/LSP.2011.2114651.
7. Hong W, Chen T, Wu H. An improved reversible data hiding in encrypted images using side match. IEEE Signal Process. 2012;19:199–202. https://doi.org/10.1109/LSP.2012.2187334.

8. Zhang X. Separable reversible data hiding in encrypted image. IEEE Transactions on Information Forensics and Security. 2012;7:826–32. https://doi.org/10.1109/tifs.2011.2176120.
9. Yu M, Liu Y, Sun H, et al. Adaptive and separable multiary reversible data hiding in encryption domain. J Image Video Proc. 2020;2020:16. https://doi.org/10.1186/s13640-020-00502-w.
10. Min Long Yu, Zhao XZ, Peng F. A separable reversible data hiding scheme for encrypted images based on Tromino scrambling and adaptive pixel value ordering. Signal Process. 2020;176:107703. https://doi.org/10.1016/j.sigpro.2020.107703.
11. Liu L, Wang A, Chang C. Separable Reversible Data Hiding in Encrypted Images With High Capacity Based on Median-Edge Detector Prediction. IEEE Access. 2020;8:29639–47. https://doi.org/10.1109/ACCESS.2020.2972736.
12. Zhou N, Zhang M, Wang H, Ke Y, Di F. Separable Reversible Data Hiding Scheme in Homomorphic Encrypted Domain Based on NTRU. IEEE Access. 2020;8:81412–24. https://doi.org/10.1109/ACCESS.2020.2990903.
13. Chen K, Chang CC. Error-free separable reversible data hiding in encrypted images using linear regression and prediction error map. Multimed Tools Appl. 2019;78:31441–65. https://doi.org/10.1007/s11042-019-07946-x.
14. Bao F, Deng R-H, Ooi B-C, Yang Y. Tailored reversible watermarking schemes for authentication of electronic clinical atlas. IEEE Trans Inf Technol Biomed. 2005;9(4):554–63. https://doi.org/10.1109/TITB.2005.855556.
15. Coatrieux G, Le Guillou C, Cauvin J-M, Roux C. Reversible watermarking for knowledge digest embedding and reliability control in medical images. IEEE Trans Inf Technol Biomed. 2009;13(2):158–65. https://doi.org/10.1109/TITB.2008.2007199.
16. Wu H-T, Huang J, Shi Y-Q. A reversible data hiding method with contrast enhancement for medical images. J Vis Commun Image Represent. 2015;31:146–53. https://doi.org/10.1016/j.jvcir.2015.06.010.
17. Zain JM, Clarke M. Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images, IJCSNS International Journal of Computer Science and Network Security. 2007;7(9):19–28. https://arxiv.org/ftp/arxiv/papers/1101/1101.1603.pdf
18. Kundu MK, Das S. Lossless ROI medical image watermarking technique with enhanced security and high payload embedding. Proc. of 2010 Int. Conf. on Pattern Recognition. IEEE Computer Society. 2010;1457–60. https://doi.org/10.1109/ICPR.2010.360
19. Tan CK, Ng JC, Xu X, et al. Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability. J Digit Imaging. 2011;24:528–40. https://doi.org/10.1007/s10278-010-9295-4.
20. Coatrieux G, Puentes J, Roux C, Lamard M, Daccache W. A low distorsion and reversible watermark: application to angiographic images of the retina. Conf Proc IEEE Eng Med Biol Soc. 2005;2005:2224–7. https://doi.org/10.1109/IEMBS.2005.1616905 (PMID: 17282674).
21. Liu YL, Qu XX, Xin GJ. ROI-based reversible data hiding scheme for medical images with tamper detection. IEICE Trans. Inf Syst. 2015;E98-D(4):769–74. https://doi.org/10.1587/transinf.2014ICP0001
22. Lavanya A, Natarajan V. Watermarking patient data in encrypted medical images. Sadhana-Acad. Proc Eng Sci. 2012;37:723–9. https://www.ias.ac.in/public/Volumes/sadh/037/06/0723-0729.pdf
23. Liu, Yuling, Xinxin Qu, Guojiang Xin. A ROI-based reversible data hiding scheme in encrypted medical images. J. Visual Communication and Image Representation. 2016;39:51–7. https://doi.org/10.1016/j.jvcir.2016.05.008
24. Schneier B. Applied Cryptography. 2nd ed. New York: Wiley; 1996.
25. C.Paar and J. Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg. 2010; https://doi.org/10.1007/978-3-642-04101-3.
26. Z. Yin, H. Wang, H. Zhao, B. Luo, and X. Zhang. Complete separable reversible data hiding in encrypted image. Proc. 1st Int. Conf. Cloud Comput. Secur.; 2015. pp. 101–10.
27. Digital Imaging and Communications in Medicine. Current Edition. 2021. https://www.dicomstandard.org/current/ Accessed 1 January 2021.
28. Zhou J, Sun W, Dong L, Liu X, Au OC, Tang YY. Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation. IEEE Trans Circuits Syst Video Technol. 2016;26(3):441–52. https://doi.org/10.1109/TCSVT.2015.2416591.
29. Fridrich J, Goljan M, Du R. Lossless Data Embedding—New Paradigm in Digital Watermarking. EURASIP J Adv Signal Process. 2002;2002:986842. https://doi.org/10.1155/S1110865702000537.
30. Jessica Fridrich, Miroslav Goljan, Rui Du. "Invertible authentication", Proc. SPIE 4314, Security and Watermarking of Multimedia Contents III, (1 August 2001); https://doi.org/10.1117/12.435400
31. Celik MU, Sharma G, Tekalp AM. Lossless generalized-LSB data embedding. IEEE Trans Image Process. 2005;14(2):253–66. https://doi.org/10.1109/TIP.2004.840686.
32. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process. 2004;13(4):600–12. https://doi.org/10.1109/TIP.2003.819861.
33. Sheikh HR, Bovik AC. Image information and visual quality. IEEE Trans Image Process. 2006;15(2):430–44. https://doi.org/10.1109/TIP.2005.859378.
34. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems. In: Pfitzmann A. (eds) Information Hiding. IH 1999. Lecture Notes in Computer Science. 2000;1768. Springer, Berlin, Heidelberg. https://doi.org/10.1007/10719724_5