Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Zero watermarking scheme for privacy protection in e-Health care

Ayesha Shaik & V. Masilamani

To cite this article: Ayesha Shaik & V. Masilamani (2023) Zero watermarking scheme for privacy protection in e-Health care, Automatika, 64:3, 453-466, DOI: 10.1080/00051144.2023.2187525

To link to this article: https://doi.org/10.1080/00051144.2023.2187525

Published online: 18 Mar 2023.

AUTOMATIKA
2023, VOL. 64, NO. 3, 453–466
https://doi.org/10.1080/00051144.2023.2187525

ARTICLE

OPEN ACCESS Check for updates

Zero watermarking scheme for privacy protection in e-Health care

Ayesha Shaik [a] and V. Masilamani[b]

[a]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India; [b]Department of Computer Engineering, Indian Institute of Information Technology Design, and Manufacturing Kancheepuram (IIITDMK), Chennai, India

ABSTRACT
E-health care is an emerging field where health services and information are delivered and offered over the Internet. So the health information of the patients communicated over the Internet has to protect the privacy of the patients. The patient information is embedded into the health record and communicated online which also induces degradation to the original information. So, in this article, a zero watermarking scheme for privacy protection is proposed which protects the privacy and also eliminates the degradation done during embedding of patient information into the health record. This method is based on simple linear iterative clustering (SLIC) superpixels and partial pivoting lower triangular upper triangular (PPLU) factorization. The novelty of this article is that the use of SLIC superpixels and PPLU decomposition for the privacy protection of medical images (MI). The original image is subjected to SLIC segmentation and non-overlapping high entropy blocks are selected. On the selected blocks discrete wavelet transform (DWT) is applied and those blocks undergo PPLU factorization to get three matrices, L, U and P, which are lower triangular, upper triangular and permutation matrix respectively. The product matrix $L \times U$ is used to construct a zero-watermark. The technique has been experimented on the UCID, BOWS and SIPI databases. The test results demonstrate that this work shows high robustness which is measured using normalized correlation (NC) and bit error rate (BER) against the listed attacks.

ARTICLE HISTORY
Received 16 October 2019
Accepted 17 November 2022

KEYWORDS
Zero watermarking; PPLU decomposition; DWT; health care; privacy protection; SLIC segmentation

1. Introduction

The revolutionized advancements in digitized networking have led to the fast development of the economic society and the higher rate of digital data transfer over the internet than the previous decades. This revolution has led to the need to secure the digital data that are transferred over the internetwork. A lot of techniques have come to secure the data. All the full-form abbreviations used in this paper are tabulated in Table 1. The data hiding techniques and their goals have been briefed in Table 2. The exponential rise of technology has been highly benefited because of the advancements in electronic healthcare. The significant progress in multimedia communication has motivated an immediate necessity for protecting the privacy of the patients. The electronic healthcare system includes the exchange of medical images (MIs) and electronic patient records (EPRs) between distant places. The EPR is very sensitive information. So, the techniques need to be developed to secure such type of data. To transfer EPR, reversible data hiding (RDH) techniques became popular. In the RDH scheme, the EPR is embedded into the MI at the sender side and transferred and at the receiver end, both the MI and the EPR need to be extracted with no or minimal distortion. But when an EPR (watermark) is inserted into the data it reduces their perceptual quality. If the watermark is not embedded then privacy protection cannot be done. So, to protect privacy without degrading the perceptual quality, ZWM schemes [1] have been developed by the researchers for the general images. In these schemes, a zero-watermark will be generated depending on the properties of the digital data and EPR without disturbing digital data. The existing transform domain (TD) WMG scheme uses DCT [2], DFT [3], DWT [4], WHT [5], PCA, SVD, lifting wavelets and contourlet transform (CT) [6]. The main contribution of the proposed work is to provide a solution by the zero-watermarking scheme are as follows:

- to avoid the degradation happens during embedding of the patient information, unlike the embedded watermarking schemes;
- to protect the privacy of the patient where the patient records are communicated between the hospitals for diagnosis;
- the use of SLIC segmentation and use of high entropy blocks for extracting features;
- the combination of SLIC segmentation, DWT and PPLU decomposition for zero-watermarking;
- the permutation of the generated sequence for maintaining the security.

CONTACT Ayesha Shaik ayeshanoormd@gmail.com

Table 1. Full form of the abbreviations used in the paper.

Abbreviation	Full form
SLIC	Simple linear iterative clustering
ZWM	Zero-watermarking
PPLU	Partial pivoting lower triangular upper triangular
DWT	Discrete wavelet transform
WMG	Watermarking
DCT	Discrete cosine transform
DFT	Discrete Fourier transform
WHT	Walsh-Hadamard transform
PCA	Principal component analysis
SVD	Singular value decomposition
LPCC	linear predictive cepstral coefficients
CT	Contourlet transform
CS	Compressive sensing
BER	Bit error rate
NC	Normalized-correlation
SPN	Salt and pepper noise
GN	Gaussian noise
MF	Median filtering
AF	Average filtering
CE	Contrast enhancement
GC	Gamma correction
EPR	Electronic patient record
DICOM	Digital Imaging and Communications in Medicine

Table 2. Data hiding techniques and their goals in the research.

Data hiding method	Goal
Digital watermarking	To embed digital data for privacy protection, WMI and data authentication
Stegnography	To embed data in the cover image in such a way that the data are hidden
Cryptography	To transform the data into a noise-like form
Reversible data hiding	To get back both the cover image and the embedded information for privacy protection
Zero watermarking	Without embedding, provides privacy protection

So, we intend to use the ZWM schemes for privacy protection in e-Health care. So far, the RDH schemes have been used in medical care, but two issues have been found with them. They are (i) the RDH schemes involve disturbing the original data and (ii) most of the RDH schemes are in the spatial domain (not in the transform domain), they are vulnerable for third-party attacks. So, to protect privacy in e-Health care, a technique should include *no embedding* and *transform domain*. The block diagram for the traditional watermarking scheme is as shown in Figure 1. The block diagram for the zero-watermarking scheme is as shown in Figure 2. The difference between the traditional and ZWM schemes is that in the ZWM scheme there is no embedding of the watermark. The ZWM scheme needs the extracted features from the original image and processing happens on the original image. Because of that, quality degradation won't happen for the original image. This is the advantage of using the ZWM scheme compared to the traditional watermarking scheme. The block diagram for reversible data hiding scheme is as shown in Figure 3.

1.1. Zero-watermarking example for the sample input

For ZWM two phases are existing, one is zero-watermark generation and the other is zero-watermark extraction. An example for ZWM has two phases.

1.1.1. Zero-watermark generation

- Let the sample image,

$$A = \begin{bmatrix} 162 & 126 & 192 & 192 \\ 182 & 20 & 192 & 98 \\ 26 & 56 & 32 & 160 \\ 182 & 110 & 194 & 28 \end{bmatrix} \tag{1}$$

- Compute mean along the columns (or rows, here for this example it is along columns), then mean vector is

$$M = \begin{bmatrix} 138 & 78 & 153 & 120 \end{bmatrix} \tag{2}$$

- Compute the features of the sample image as if the pixel value $A(i,j)$ mean value $M(j)$ then the respective feature value $F(i,j)$ is 1, else it will be considered 0, where $i, j = 0{,}1{,}2{,}3$. Then the feature image will be

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \tag{3}$$

- Now consider the unique key or copyright as

$$U = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \tag{4}$$

- Now compute the zero-watermark as

$$Z = F \oplus U = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{5}$$

- The generated zero-watermark Z will be stored for future references.

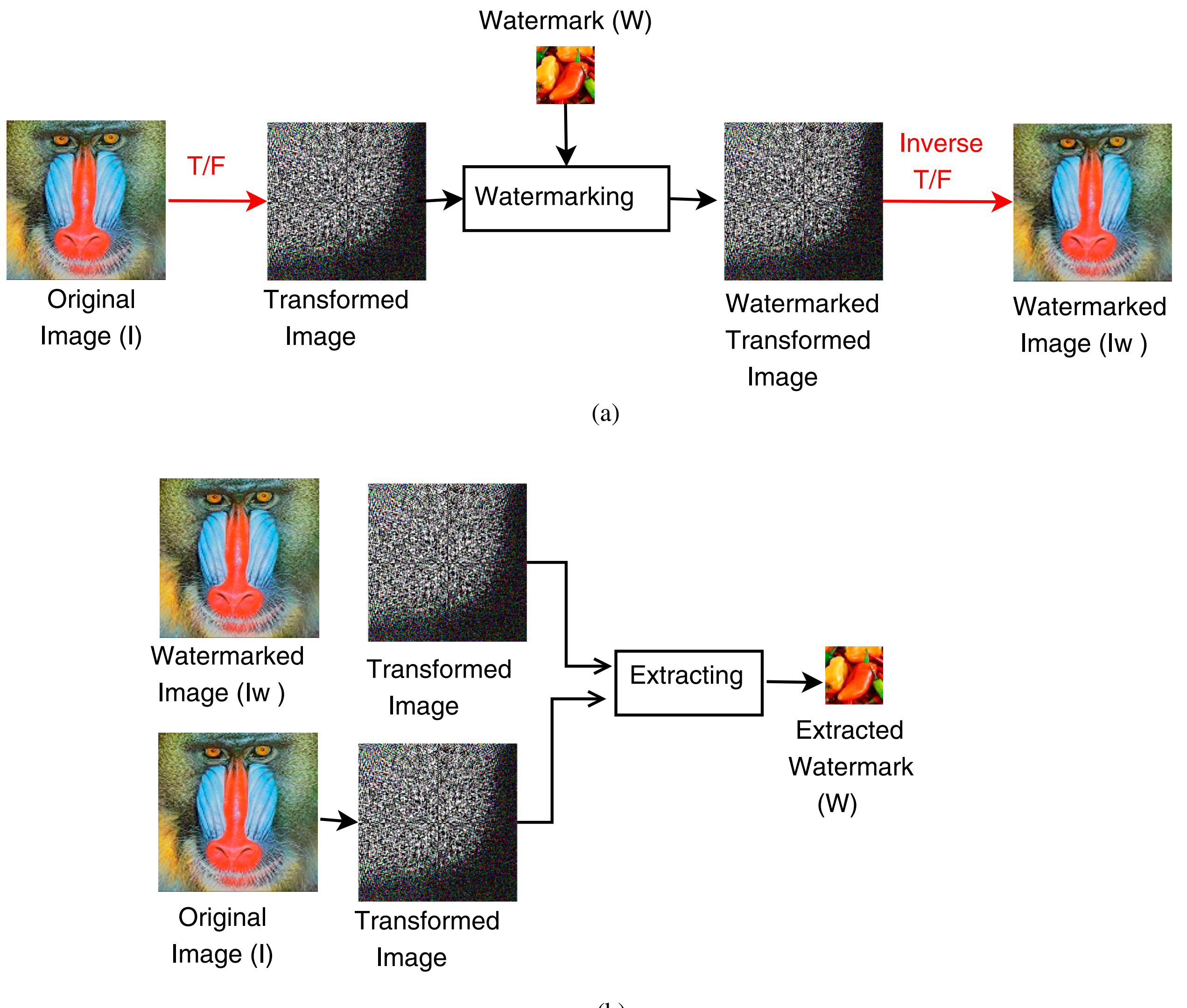
1.1.2. Zero-watermark extraction and verification without noise on the original image

- Let the sample image,

$$A_{without} = \begin{bmatrix} 162 & 126 & 192 & 192 \\ 182 & 20 & 192 & 98 \\ 26 & 56 & 32 & 160 \\ 182 & 110 & 194 & 28 \end{bmatrix} \tag{6}$$

- Compute mean along the columns (or rows, here for this example it is along columns), then the mean vector is

$$M_{without} = \begin{bmatrix} 138 & 78 & 153 & 120 \end{bmatrix} \tag{7}$$



(a)

(b)

Figure 1. Traditional watermarking scheme: (a) watermark embedding and (b) watermark extraction.

- Compute the features of the sample image as if the pixel value $A(i,j)$, mean value $M(j)$ then the respective feature value $F(i,j)$ is 1, else it will be considered 0, where $i,j = 0,1,2,3$. Then the feature image will be

$$F_{without} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad (8)$$

- Now find the unique key as

$$U_{without} = F_{without} \oplus Z = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad (9)$$

- Then find the correlation between the U and $U_{without}$ and if it is higher than the predefined threshold, then the authenticity is ensured.

1.1.3. Zero-watermark extraction and verification without noise on the original image

- Let the image without noise,

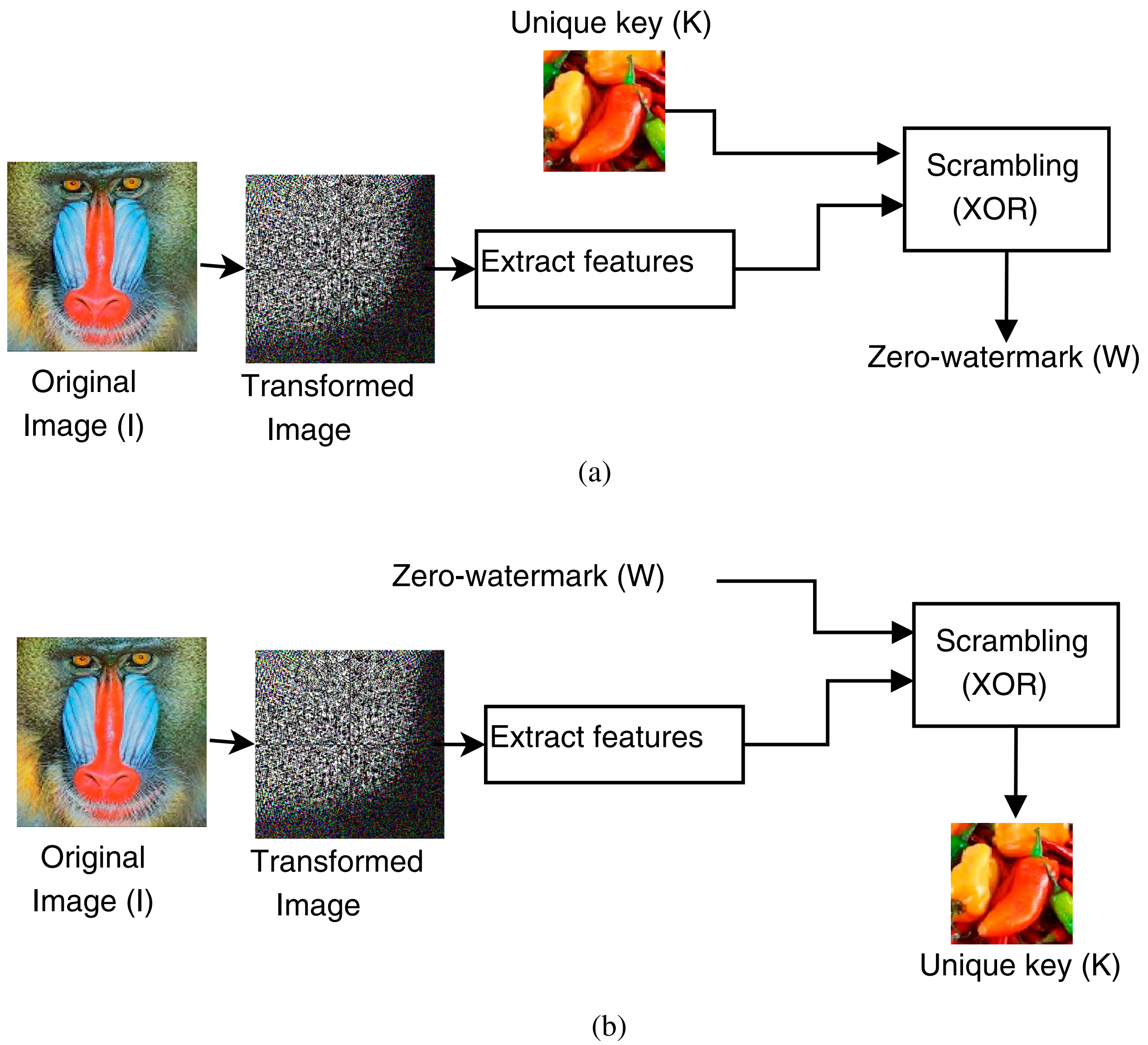
$$A_{without} = \begin{bmatrix} 162 & 126 & 192 & 192 \\ 182 & 20 & 192 & 98 \\ 26 & 56 & 32 & 160 \\ 182 & 110 & 194 & 28 \end{bmatrix} \qquad (10)$$

- Compute mean along the columns (or rows, here for this example, it is along columns), then mean vector is

$$M_{without} = \begin{bmatrix} 138 & 78 & 153 & 120 \end{bmatrix} \qquad (11)$$

- Compute the features of the sample image as if the pixel value $A(i,j)$ mean value $M(j)$ then the respective feature value $F(i,j)$ is 1, else it will be considered 0, where $i,j = 0,1,2,3$. Then the feature image will be

$$F_{without} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad (12)$$



(a)

(b)

Figure 2. Zero-watermarking scheme: (a) zero-watermark construction and (b) zero-watermark extraction.

- Now find the unique key as

$$U_{without} = F_{without} \oplus Z = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad (13)$$

- Then find the correlation between the U and $U_{without}$ and if it is higher than the predefined threshold then the authenticity is ensured.
- One can observe that the U and $U_{without}$ are the same. So authenticity is provided for this sample image as the noise has not been added.

1.1.4. Zero-watermark extraction and verification with noise on the original image

- Let the image with noise,

$$A_{with} = \begin{bmatrix} 162 & 0 & 192 & 0 \\ 182 & 0 & 192 & 0 \\ 26 & 0 & 32 & 0 \\ 182 & 0 & 194 & 0 \end{bmatrix} \qquad (14)$$

- Compute mean along the columns (or rows, here for this example, it is along columns), then the mean vector is

$$M_{without} = \begin{bmatrix} 138 & 0 & 153 & 0 \end{bmatrix} \qquad (15)$$

- Compute the features of the sample image as if the pixel value $A(i,j)$ mean value $M(j)$ then the respective feature value $F(i,j)$ is 1, else it will be considered 0, where $i, j = 0,1,2,3$. Then the feature image will be

$$F_{with} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \qquad (16)$$

- Now find the unique key as

$$U_{with} = F_{with} \oplus Z = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \qquad (17)$$

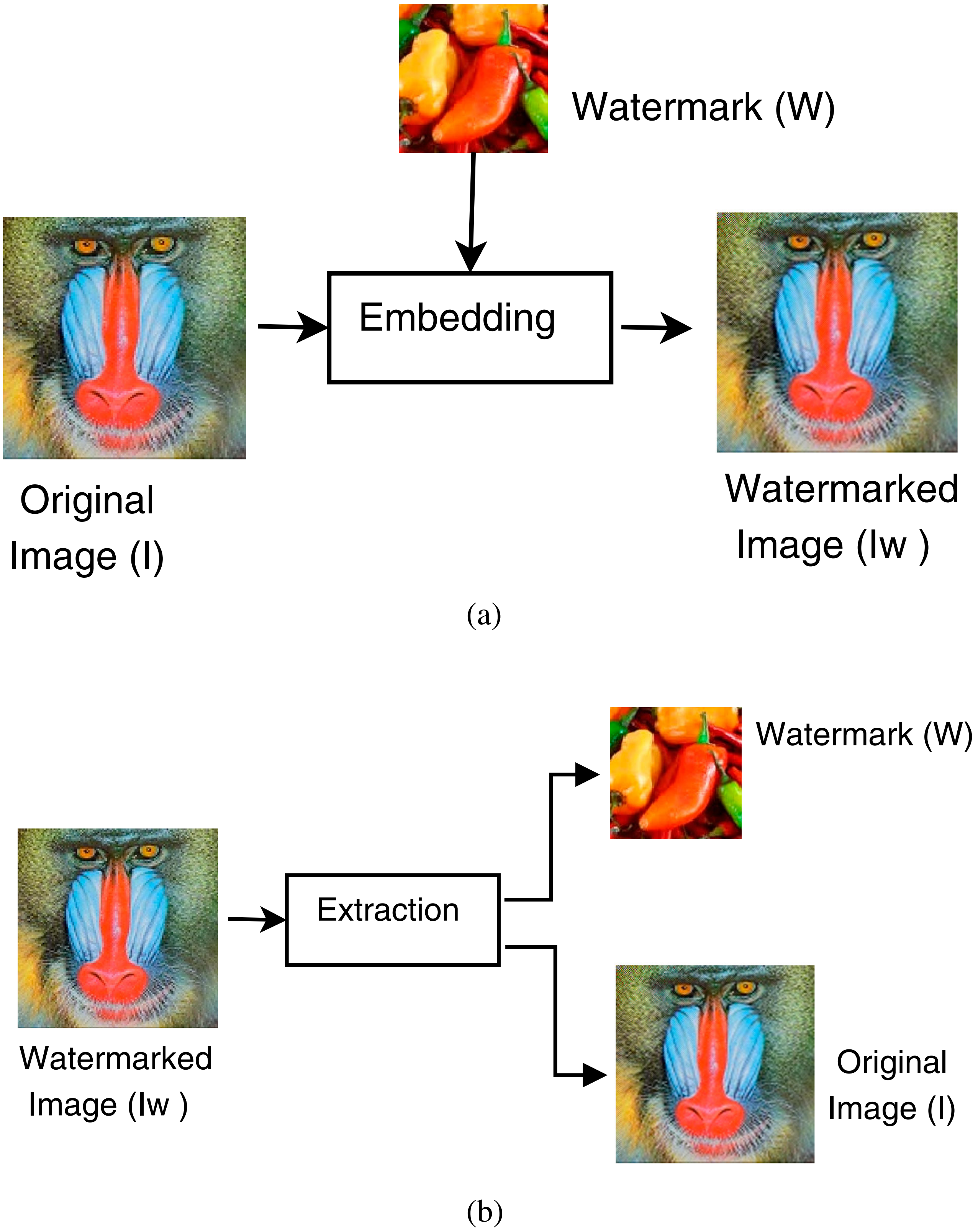


Figure 3. Reversible data hiding scheme: (a) watermark embedding and (b) watermark extraction.

- Then find the correlation between the U and U_{with} and if it is higher than the predefined threshold, then the authenticity is ensured.
- One can observe that the U and U_{with} are different as the noise been added to the original image.

This is a basic ZWM process for the sample input in the spatial domain. The proposed watermarking scheme will provide a transform domain technique as explained in Section 4.

In this article, a novel SLIC and PPLU decomposition-based ZWM technique is proposed in the wavelet domain for e-healthcare privacy protection. Here the original image is subjected to SLIC, then DWT and PPLU decomposition. The product of the lower $\triangle^{lar}$ and the upper $\triangle^{lar}$ matrices is used to generate a zero watermark by using EPR, which is the patient's information. This watermark is used to verify whether the patient is protected or not, in the case of availability of illegal copies of the data.

The rest of the article is presented as Literature Survey (Section 2), Related work (Section 3), Proposed method (Section 4), Results (Section 5), Conclusion and future work (Section 6) followed by References.

2. Literature survey

Unlike traditional WMG schemes ZWM schemes achieve copyright protection without embedding the watermark into the digital data. The audio ZWM scheme has been discussed in [7]. An LPCC-based ZWM scheme is presented in [8] and an audio ZWM scheme using energy comparison is discussed in [9]. DWT- and DCT-based audio ZWM scheme where zero-watermark is generated using wavelet and cosine coefficients as discussed in [10]. A contourlet ZWM scheme using entropy is presented in [11] and a DWT, DCT and log-polar mapping (LPM)-based ZWM scheme is discussed in [12]. In [13], a compressive sensing (CS)-based ZWM is presented. Another CS-based ZWM scheme depending on the CS measurement matrix is discussed in [14]. A DFT ZWM technique for copyright protection is discussed in [15]. A DWT-based ZWM technique in which the message bit will be embedded at different levels as discussed in [16].

Many MI watermarking algorithms have been proposed in both the spatial domain (SD) technique and transform domain (TD) technique. To verify the integrity and authenticity of digital Mammography images [17] and Digital Imaging and Communications in Medicine (DICOM) ultrasound images [18], SD watermarking schemes have been proposed. A lossless watermarking scheme based on difference expansion has been proposed in [19]. A reversible watermarking technique where EPR data are embedded using advanced encryption standard in non-ROI (calculated using adjacent pixel values) is proposed in [20]. A TD technique based on DCT where EPR-related data are embedded in quantized DCT coefficients of watermarked image as proposed in [21]. A DCT-based scheme where ECG and encrypted text data of the patient are combined with MIs to reduce the overheads of storage and transmission is proposed in [22]. A wavelet-based watermarking scheme to embed data other than the ROI region is proposed in [23] for the integrity of DICOM images. A reversible EPR data hiding using IWT is proposed in [24]. A reversible contrast mapping robust watermarking scheme using IWT is proposed in [25].

A spatial domain image watermarking scheme that utilizes MinEigen value features, chaotic sequence and Quantization Index Modulation (QIM) for ensuring the authenticity of medical images is discussed in [26]. The 3×3 non-overlapping blocks are chosen for blindly embedding the watermark bits in this method and are robust against DICOM JPEG compression. A blind and fragile watermarking scheme is discussed in [27]. This scheme uses Schur decomposition for authenticating medical images. A medical image watermarking scheme that uses DCT, Weber descriptors (WDs) and Arnold chaotic map is discussed in [28]. This technique uses mid-DCT coefficients for embedding the watermark data. An efficient encryption scheme for telecare medical information systems (TMIS) based on elliptical curve cryptography and linear cryptography is discussed in [29]. In this work, the authors have analysed the existing security scheme and improved the scheme to overcome the flaws and weaknesses. A ZWM scheme in [1] has been presented using multi-channel-shifted Gegenbauer moments of fractional orders for medical images. In this work, the zero-watermark is constructed with scrambling and XOR operation. Multiple ZWM schemes for colour images using local quaternion polar harmonic Fourier moments have been discussed in [30]. A PPLU decomposition-based digital image watermarking in the transform domain has been presented in [31]. A zero-watermarking technique with Zernike and DCT moments for medical images has been discussed in [32]. In [33], a robust and secure ZWM scheme using Harris-SURF-DCT and Chaotic Map for medical images has been discussed.

3. Related work

3.1. PPLU decomposition

PPLU decomposition [34] is a factoring technique that outputs three matrices using the partial pivoting (PP) procedure. PPLU decomposition of C is defined as follows:

$$PPLU(C) = (L, U, P) \text{ such that } PC = LU, \tag{18}$$

where L, U and P which are lower triangular, upper triangular and permutation matrix, respectively. An illustrated example for PPLU decomposition of a 3 × 3 matrix is given below. Let

$$C = \begin{bmatrix} 1 & 0 & 4 \\ 0 & 0 & 1 \\ 3 & 2 & 13 \end{bmatrix} \tag{19}$$

Then C can be decomposed into

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad L = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$U = \begin{bmatrix} 1 & 0 & 4 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$P \times A = \begin{bmatrix} 1 & 0 & 4 \\ 3 & 2 & 13 \\ 0 & 0 & 1 \end{bmatrix} \quad L \times U = \begin{bmatrix} 1 & 0 & 4 \\ 3 & 2 & 13 \\ 0 & 0 & 1 \end{bmatrix} \tag{20}$$

3.2. SLIC superpixels

Superpixels are used to categorize the image into purposeful sections using similarity and contiguity in the image plane [35]. SLIC superpixels are fast, easy to use and contribute segmentation of high quality [36] compared to other existing superpixel techniques [37–40]. It is a 5D CIELAB color space (L, a, b, t, s) based local clustering algorithm where (L, a, b) is the pixel color vector and (t, s) are pixel coordinates. CIELAB colour space is based on the Richard Hunter (L, a, b) colour space [41]. It is device independent model of the international color consortium (ICC) device profile. It is not possible to use Euclidean distance measure in 5D space without normalizing the spatial distances. So, a new distance measure is discussed in [36].

$$M_{Lab} = \sqrt{(L_c - L_r)^2 + (a_c - a_r)^2 + (b_c - b_r)^2}$$
$$M_{ts} = \sqrt{(t_c - t_r)^2 + (s_c - s_r)^2}$$
$$M_W = M_{Lab} + \frac{n}{W} \times D_{xy} \tag{21}$$

where M_{Lab} and M_W are the sum of the *Lab* distance and normalized *ts* distance, *n* is the scale parameter and *W* is the grid interval. In the SLIC algorithm, *C* regularly spaced cluster centres are sampled and moved to seed locations corresponding to the lowest gradient position in 3 × 3 neighbourhood. Image gradients are computed as follows:

$$Grad(p,q) = \|O(p+1,q) - O(p-1,q)\|^2 + \|O(p,q+1) - O(p,q-1)\|^2 \tag{22}$$

where $O(p,q)$ is the *Lab* vector and $\|\cdot\|^2$ is the L2 norm. SLIC performs clustering in $O(N)$ as the $K \leq 8$ and the number of iterations (4 to 10) is constant [36]. An example of SLIC segmentation for different region sizes is given in 6.

4. The proposed method

ZWM schemes have become popular as we can protect privacy and the data, without inserting any digital data (watermark) into the original data. Due to this perceptual degradation will not happen to the original image, i.e. high imperceptibility which is one of the main requirements of digital WMG. The selection of scale factors plays an important role to decide the WMG scheme to be robust or imperceptible and selecting the optimal scale factor is difficult. But in ZWM schemes there is no overhead of scale factor because embedding of the watermark is not required. The ZWM scheme will not have embedding of the watermark. So as the watermark is not embedded the scale factor prediction for the watermark is also not required. In this way, the selection of scaling overhead is reduced. It provides high imperceptibility and high robustness, using the zero-watermark generated from the properties of the original data. This type of watermarking is very helpful for e-health care privacy issues.

4.1. Zero-watermark generation

The proposed zero-watermark generation algorithm block diagram for general images is shown in Figure 4. For MIs, the zero-watermark generation algorithm block diagram is shown in Figure 7. The difference in the block diagrams of general and MIs is the unique key for the general image which is replaced with the EPR for MI. Let the original image be *I* of size M × N. It is segmented using the SLIC superpixel algorithm discussed in preliminaries. In those segments, assume *N* segments *H* (*H* < *N*) high entropy segments are selected. The high entropy segments will be containing high information. So *H* segments are chosen from *N* segments such that the security is also maintained

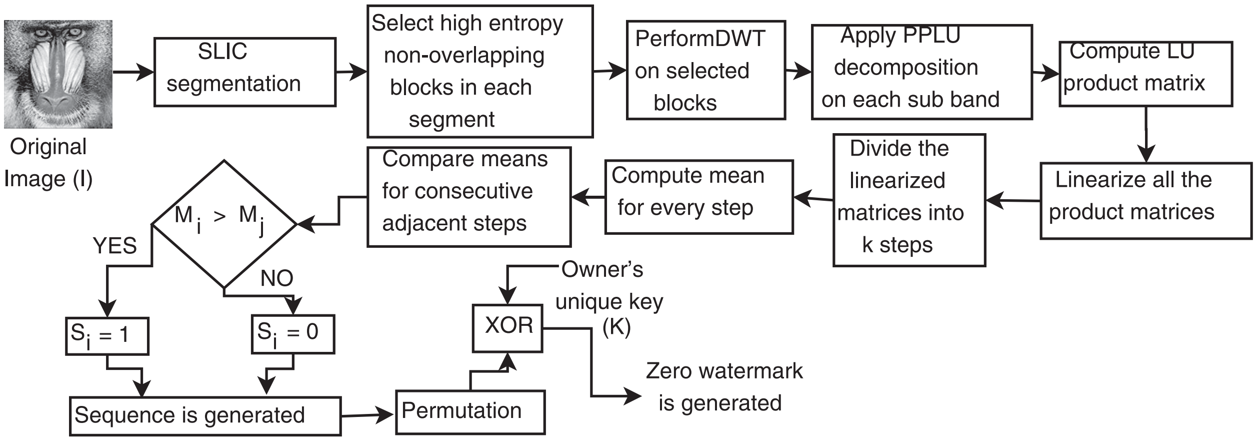

Original Image (I)
SLIC segmentation
Select high entropy non-overlapping blocks in each segment
PerformDWT on selected blocks
Apply PPLU decomposition on each sub band
Compute LU product matrix
Linearize all the product matrices
Divide the linearized matrices into k steps
Compute mean for every step
Compare means for consecutive adjacent steps
$M_i > M_j$
YES
NO
$S_i = 1$
$S_i = 0$
Sequence is generated
Permutation
XOR
Owner's unique key (K)
Zero watermark is generated

Figure 4. The proposed zero-watermark generating scheme for privacy protection for general images.

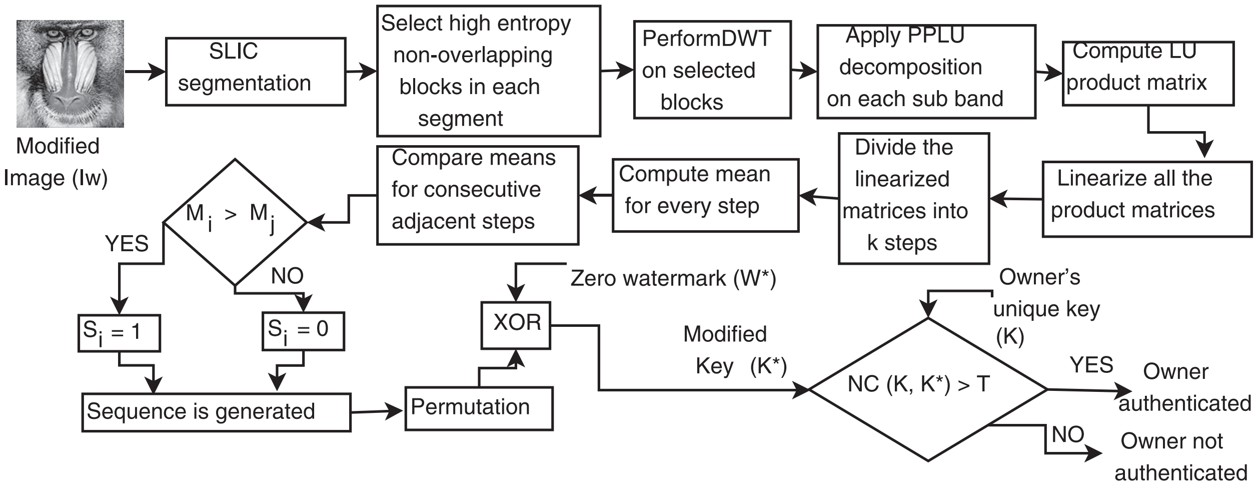
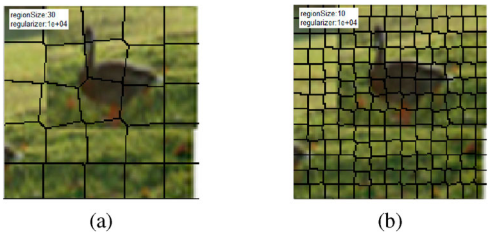

Modified Image (Iw)
SLIC segmentation
Select high entropy non-overlapping blocks in each segment
PerformDWT on selected blocks
Apply PPLU decomposition on each sub band
Compute LU product matrix
Linearize all the product matrices
Divide the linearized matrices into k steps
Compute mean for every step
Compare means for consecutive adjacent steps
$M_i > M_j$
YES
NO
$S_i = 1$
$S_i = 0$
Sequence is generated
Permutation
XOR
Zero watermark (W*)
Modified Key (K*)
Owner's unique key (K)
NC (K, K*) > T
YES
Owner authenticated
NO
Owner not authenticated

Figure 5. The proposed zero watermark extracting scheme for privacy protection for general images.



(a) (b)

Figure 6. Segmented image with region size 10 (left) and region size 20 (right).

with the value of selected H as the whole image is not considered for generating the features. From the high entropy segments, n non-overlapping blocks of size $2b \times 2b$ are chosen. These blocks are subjected to DWT and then PPLU decomposition to produce three matrices. The product of L and U matrices of all the blocks is linearized and then divided into G steps. The mean of each step is computed and a mean vector is generated. A unique sequence is generated by comparing the adjacent samples of the mean vector. This sequence is permuted by a secure key and then XORed with EPR (unique key of patient information) to generate the zero-watermark. This watermark contains the properties of the original data and the transforms applied, as they are highly involved in generating it. The zero-watermark generation algorithm is given in Algorithm 1.

4.2. Zero-watermark extraction for general images

The zero-watermark extraction algorithm is explained in Algorithm 2. The procedure is similar to the zero-watermark generation process except that after generating a unique sequence it has to be XORed with the zero-watermark to obtain EPR. The block diagram for privacy protection for general images is shown in Figure 5. The block diagram for privacy protection for general images is shown in Figure 8. If the correlation between the input EPR and extracted EPR is higher than the threshold then the privacy of the patient is protected. Otherwise, it is not protected.

5. Results

To validate the proposed work, it is tested against a set of attacks and listed in Tables 3–5. The

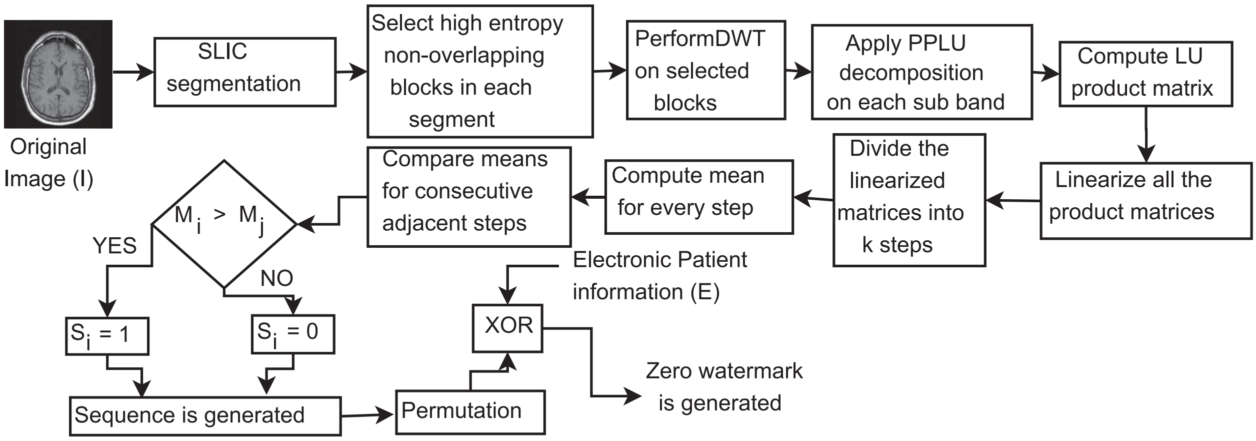

Original Image (I)
SLIC segmentation
Select high entropy non-overlapping blocks in each segment
PerformDWT on selected blocks
Apply PPLU decomposition on each sub band
Compute LU product matrix
Linearize all the product matrices
Divide the linearized matrices into k steps
Compute mean for every step
Compare means for consecutive adjacent steps
$M_i > M_j$
YES
NO
$S_i = 1$
$S_i = 0$
Sequence is generated
Permutation
XOR
Electronic Patient information (E)
Zero watermark is generated

Figure 7. The proposed zero-watermark generating scheme for privacy protection for MIs.

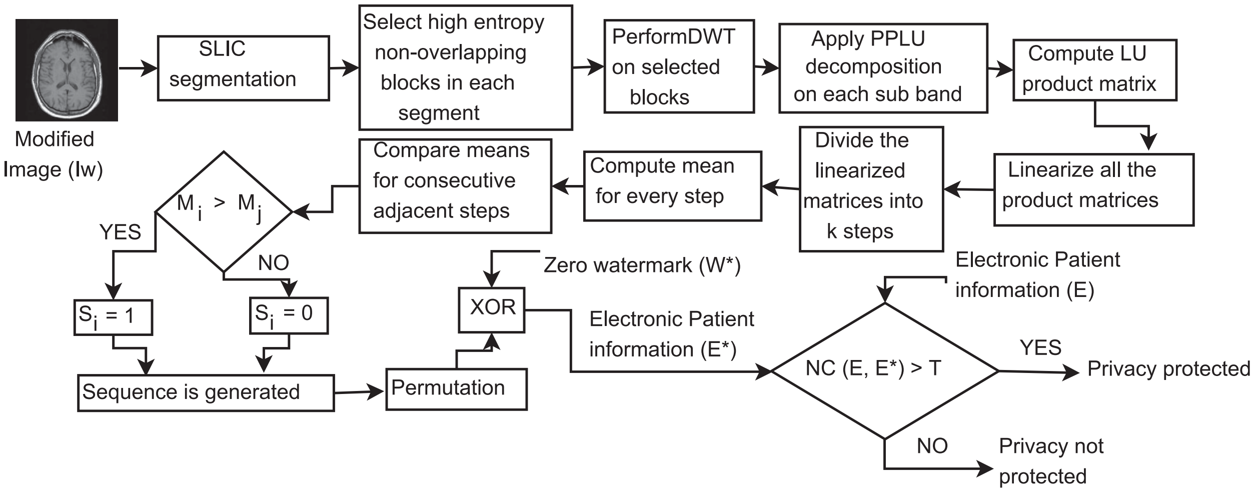

Modified
Image (Iw)
SLIC segmentation
Select high entropy non-overlapping blocks in each segment
PerformDWT on selected blocks
Apply PPLU decomposition on each sub band
Compute LU product matrix
Linearize all the product matrices
Divide the linearized matrices into k steps
Compute mean for every step
Compare means for consecutive adjacent steps
M_i > M_j
YES
NO
S_i = 1
S_i = 0
Sequence is generated
Permutation
XOR
Zero watermark (W*)
Electronic Patient information (E*)
Electronic Patient information (E)
NC (E, E*) > T
YES
Privacy protected
NO
Privacy not protected

Figure 8. The proposed zero watermark extracting scheme for privacy protection for MIs.

```
Algorithm 1 Zero-watermark generation
Input: Original Image ($I$), EPR ($E$), Permutation key ($K$)
Output: Zero watermark ($W$)
  Perform SLIC segmentation on $I$ to divide into segments.
  From each segment $N$ high entropy non-overlapping blocks of size $2b \times 2b$ are selected.
  On each block apply DWT to obtain sub-bands $(LL_i, LH_i, HL_i, HH_i)$ of size $b \times b$.
  These sub-bands are subjected to PPLU decomposition to get three matrices $L_i, U_i$, and $Pv$ of size $b \times b$.
  Then the product of $L$ and $U$ is computed say $Y_i$.
  Linearize all $Y_i$ matrices into single row and divide it into $L$ steps.
  Compute mean vector by computing means of each step.
  Generate a binary sequence by comparing means of adjacent samples in the mean vector.
  Then the sequence is permuted by a secure key ($K$) to obtain the permuted sequence.
  The permuted sequence is encrypted using $\oplus$ operation by EPR ($E$) to obtain zero-watermark ($W$).
```

```
Algorithm 2 Zero-watermark extraction
Input: Possibly modified image ($I^*$), EPR ($E$), Permutation key ($K$), Zero watermark ($W$)
Output: Privacy is protected or not
  Perform SLIC segmentation on $I^*$ to divide into segments.
  From each segment $N$ high entropy non-overlapping blocks of size $2b \times 2b$ are selected.
  On each block apply DWT to obtain sub-bands $(LL_i^*, LH_i^*, HL_i^*, HH_i^*)$ of size $b \times b$.
  These sub-bands are subjected to PPLU decomposition to get three matrices $L_i^*, U_i^*$, and $P_i^*$ of size $b \times b$.
  Then the product of $L_i^*$ and $U_i^*$ is computed say $Y_i^*$.
  Linearize all $Y_i^*$ matrices into single row and divide it into $L^*$ steps.
  Compute mean vector by computing means of each step.
  Generate a binary sequence by comparing means of adjacent samples in the mean vector.
  Then the sequence is permuted by a secure key ($K$) to obtain a permuted sequence.
  The permuted sequence is encrypted using $\oplus$ operation by zero-watermark ($W^*$) to obtain possibly modified EPR ($E^*$).
  Find the normalized correlation (NC) between ($E$) and ($E^*$). If NC is greater than the predefined threshold then the privacy is protected otherwise not protected.
```

normalized-correlation (NC) and bit error rate (BER) between the generated and received watermarks for the proposed and existing method against a salt and pepper noise (SPN) and Gaussian noise (GN) attacks are tabulated in Table 3. To validate the proposed method the test images are taken from UCID, SIPI, and BOWS datasets. A few MRI and CT scan images of the brain from the UCID database on which experimentation was carried out are as shown in Figures 9 and 10 respectively. The test images from SIPI and BOWS datasets on which experimentation was carried out are shown in Figures 12 and 11 respectively. The proposed scheme is robust to the set of attacks listed in the paper because for other attacks the zero-watermark constructed will be fragile as it can't hold the properties of the original image. So, the authors state that the proposed scheme is robust only to the listed attacks provided in the article. The size of the images considered is 256×256 and the

Table 3. Correlation and BER values between the generated and received watermark against listed attacks for the proposed method and the existing method for general images.

		Proposed		Existing [32]	
Attack		BER	NC	BER	NC
No attack		0	1	0	1
SPN	0.1	0	1	0.001	0.998
	0.01	0	1	0.001	0.998
	0.001	0	1	0.001	0.999
GN	1	0	1	0	1
	2	0	1	0.002	0.999
MF	3 × 3	0	1	0.003	0.904
	5 × 5	0	1	0.02	0.9993
	7 × 7	0	1	0.148	0.999
AF	3 × 3	0	1	0.005	0.9924
	5 × 5	0	1	0.064	0.9856
	7 × 7	0	1	0.072	0.9968

Table 4. Correlation and BER values between the generated and received watermark against listed attacks for the proposed method and the existing method.

	Proposed		Existing [32]	
Attack	BER	NC	BER	NC
CE	0	1	0.003	0.956
GC	0	1	0.001	0.986

Table 5. Extracted watermarks against listed attacks for the proposed method and the existing method for general images.

Attack	Proposed	Existing [32]
SPN		
GN		
AF with 3 × 3 window		
AF with 5 × 5 window		
AF with 7 × 7 window		
MF with 3 × 3 window		
MF with 5 × 5 window		
MF with 7 × 7 window		
Contrast enhancement		
Gamma correction		

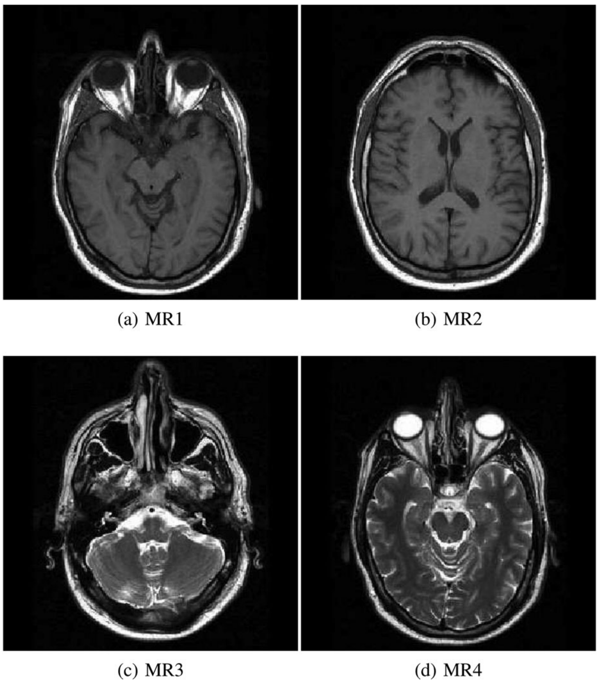
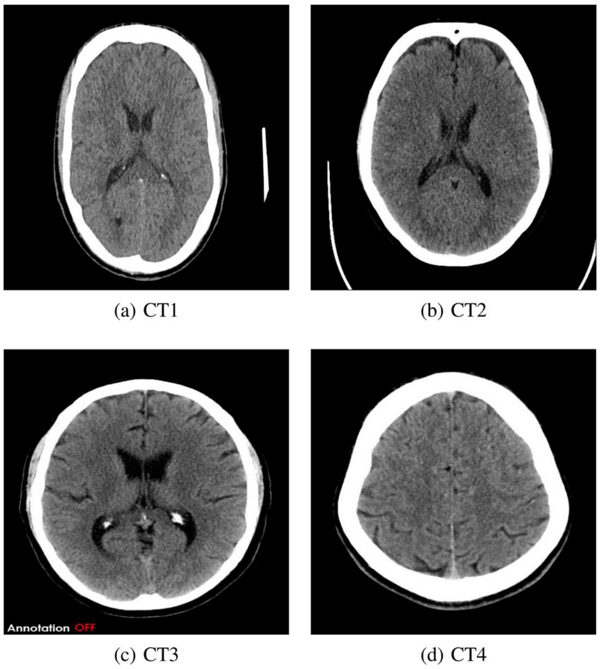

(a) MR1
(b) MR2
(c) MR3
(d) MR4

Figure 9. MRI brain images: (a) MR1, (b) MR2, (c) MR3 and (d) MR4.



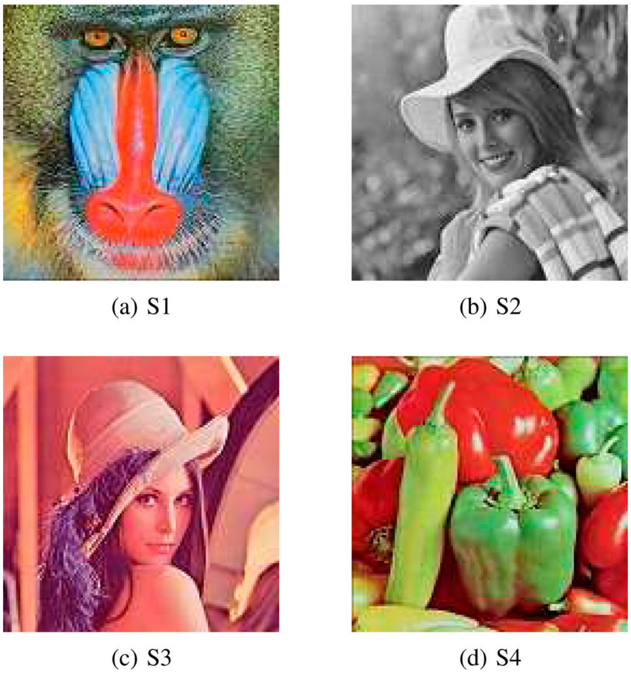
(a) CT1
(b) CT2
(c) CT3
(d) CT4

Figure 10. CT brain images: (a) CT1, (b) CT2, (c) CT3 and (d) CT4.

experimentation was done using Matlab 2015 with an Intel Core i7 processor with 8 GB DDR3 RAM.

In this table, the seco*nd* row corresponds to BER and NC values obtained when no modification is done to the image. The 3^{rd} row corresponds to BER and NC obtained against attack with intensities 0.1, 0.01, and 0.001. One can note that if the intensity of SPN is increasing the proposed method is performing superior. Then the 4th row provides the BER and NC values obtained against GN attack with zero mean and different variances, where the equal performance is shown by the proposed and existing methods. The fir*st* and seco*nd* rows in Table 3 provide the BER and NC values for median filtering (MF) and average filtering (AF) attacks with various window sizes, where the proposed scheme is performing better. Then the BER and NC values obtained against contrast enhancement (CE) and gamma correction (GC) attacks are listed in the first and second rows of Table 4 respectively, where the proposed scheme is performing better.

In this article, for MIs, the EPR information is the patient's record and for general images, the EPR information is assumed as the owner's unique key. In Table 6, the owner's key received by the proposed and existing [32] ZWM schemes against SPN, GN, AF and MF with 3 × 3, 5 × 5 and 7 × 7 window sizes, CE and GC attacks have been shown. The seco*nd* column of the table shows the key obtained from the proposed



(a) S1

(b) S2

(c) S3

(d) S4

Figure 11. SIPI test images: (a) S1, (b) S2, (c) S3 and (d) S4.

(a) B1

(b) B2

(c) B3

(d) B4

(e) B5

(f) B6

Figure 12. BOWS test images: (a) B1, (b) B2, (c) B3, (d) B4, (e) B5 and (f) B6.

Table 6. Correlation and BER values between the generated and received watermark against MF attack for different window sizes for MRI images, where $Lo = 0, Hi = 1$.

	Median filtering					
	3×3		5×5		7×7	
MRI Image	BER	NC	BER	NC	BER	NC
MR1	Lo	Hi	Lo	Hi	Lo	Hi
MR2	Lo	Hi	Lo	Hi	Lo	Hi
MR3	Lo	Hi	Lo	Hi	Lo	Hi
MR4	Lo	Hi	Lo	Hi	Lo	Hi

Table 7. Correlation and BER values between the generated and received watermark against MF attack for different window sizes for CT images, where $Lo = 0, Hi = 1$.

	Median filtering					
	3×3		5×5		7×7	
CT image	BER	NC	BER	NC	BER	NC
CT1	Lo	Hi	Lo	Hi	Lo	Hi
CT2	Lo	Hi	Lo	Hi	Lo	Hi
CT3	Lo	Hi	Lo	Hi	Lo	Hi
CT4	Lo	Hi	Lo	Hi	Lo	Hi

Table 8. Correlation and BER values between the generated and received watermark against AF attack for different window sizes for MRI images, where $Lo = 0, Hi = 1$.

	Average filtering					
	3×3		5×5		7×7	
MRI Image	BER	NC	BER	NC	BER	NC
MR1	Lo	Hi	Lo	Hi	Lo	Hi
MR2	Lo	Hi	Lo	Hi	Lo	Hi
MR3	Lo	Hi	Lo	Hi	Lo	Hi
MR4	Lo	Hi	Lo	Hi	Lo	Hi

method and the third column shows the key obtained from the existing method.

The NC and BER calculated between the generated and received watermarks for brain MRI and CT scan images are tabulated for AF and MF attacks in Tables 6, 7, 8 and 9. The NC and BER calculated between the generated and received watermarks for brain MRI and CT scan images are tabulated for SPN and GN attacks are listed in Tables 10–13. The NC and BER calculated between the generated and received watermarks for brain MRI and CT scan images are tabulated for CE, Quantization and JPEG compression attacks are listed in Table 15. The proposed scheme

Table 9. Correlation and BER values between the generated and received watermark against AF attack for different window sizes for CT images, where $Lo = 0, Hi = 1$.

	Average filtering					
	3×3		5×5		7×7	
CT Image	BER	NC	BER	NC	BER	NC
CT1	Lo	Hi	Lo	Hi	Lo	Hi
CT2	Lo	Hi	Lo	Hi	Lo	Hi
CT3	Lo	Hi	Lo	Hi	Lo	Hi
CT4	Lo	Hi	Lo	Hi	Lo	Hi

Table 10. Correlation and BER values between the generated and received watermark against SPN attack for CT images, where $Lo = 0, Hi = 1$.

	SPN					
	0.001		0.01		0.1	
MRI Image	BER	NC	BER	NC	BER	NC
MR1	Lo	Hi	Lo	Hi	Lo	Hi
MR2	Lo	Hi	Lo	Hi	Lo	Hi
MR3	Lo	Hi	Lo	Hi	Lo	Hi
MR4	Lo	Hi	Lo	Hi	Lo	Hi

Table 11. Correlation and BER values between the generated and received watermark against SPN attack for CT images, where $Lo = 0, Hi = 1$.

	SPN					
	0.001		0.01		0.1	
CT Image	BER	NC	BER	NC	BER	NC
CT1	Lo	Hi	Lo	Hi	Lo	Hi
CT2	Lo	Hi	Lo	Hi	Lo	Hi
CT3	Lo	Hi	Lo	Hi	Lo	Hi
CT4	Lo	Hi	Lo	Hi	Lo	Hi

Table 12. Correlation and BER values between the generated and received watermark against GN attack for MRI images, where $Lo = 0, Hi = 1$.

	GN					
	(0,1)		(0,2)		(0,3)	
MRI Image	BER	NC	BER	NC	BER	NC
MR1	Lo	Hi	Lo	Hi	Lo	Hi
MR2	Lo	Hi	Lo	Hi	Lo	Hi
MR3	Lo	Hi	Lo	Hi	Lo	Hi
MR4	Lo	Hi	Lo	Hi	Lo	Hi

Table 13. Correlation and BER values between the generated and received watermark against GN attack for CT images, where $Lo = 0, Hi = 1$.

	GN					
	(0,1)		(0,2)		(0,3)	
CT Image	BER	NC	BER	NC	BER	NC
CT1	Lo	Hi	Lo	Hi	Lo	Hi
CT2	Lo	Hi	Lo	Hi	Lo	Hi
CT3	Lo	Hi	Lo	Hi	Lo	Hi
CT4	Lo	Hi	Lo	Hi	Lo	Hi

Table 14. Processing time for sample images.

Image	Zero-watermark generation (s)	Zero-watermark verification (s)
CT1	0.4323	0.3549
CT2	0.4116	0.3316
CT3	0.4175	0.3332
MR1	0.4109	0.3286
MR2	0.4159	0.3281
MR3	0.4105	0.3265

performs better for both the MIs and general images for privacy protection for the listed attacks. This is because the schemes operate on the means of wavelet coefficients of high entropy segmented blocks.

The processing run time for sample CT and MR images is given in Table 14 for zero-watermark generation and verification. PSNR can't be used because there is no embedding or degradation to the original image. As the quality of the original image is maintained, then there is no need to verify the quality of the image.

Table 15. Correlation and BER values between the generated and received watermark against CE, quantization and JPEG compression attack for MRI and CT images, where $Lo = 0, Hi = 1$.

	MRI image		CT image	
Attack	NC	BER	NC	BER
CE	Hi	Lo	Hi	Lo
Quantization	Hi	Lo	Hi	Lo
JPEG (QF = 0.9)	Hi	Lo	Hi	Lo
JPEG (QF = 0.8)	Hi	Lo	Hi	Lo
JPEG (QF = 0.7)	Hi	Lo	Hi	Lo
JPEG (QF = 0.5)	0.999	0.001	0.997	0.001
JPEG (QF = 0.3)	0.986	0.001	0.994	0.002
JPEG (QF = 0.1	0.983	0.002	0.993	0.002

6. Conclusion and future work

In this article, a robust zero-watermarking scheme for medical images has been proposed using SLIC segmentation, DWT and PPLU decomposition. In the zero-watermarking schemes, the quality of the medical images will be preserved as there is no embedding of the watermark (patient information). This is an advantage of using the zero-watermarking scheme compared to the embedded watermarking because in embedded watermarking the patient information is embedded into the original image which modifies the content of the original image. In the proposed method, the high entropy segments are selected after applying SLIC to the original image and processed DWT on them. A zero watermark is generated from the product matrix of the PPLU decomposition on wavelet coefficients. The proposed technique has been implemented on UCID dataset images and the proposed technique tolerates a set of attacks such as SPN, GN, AF, MF and CE. To exchange the medical images and electronic patient records in distant locations, the proposed zero-watermarking scheme is preferable as the original data are not disturbed which preserves the original content. In future, the real-time hardware solution of the proposed work can be implemented with low computational complexity and costs.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Ayesha Shaik http://orcid.org/0000-0002-9804-8031

References

[1] Hosny KM, Darwish MM. New geometrically invariant multiple zero-watermarking algorithm for color medical images. Biomed Signal Process Control. 2021;70: 103007.

[2] Briassouli A, Tsakalides P, Stouraitis A. Hidden messages in heavy-tails: dct-domain watermark detection using alpha-stable models. IEEE Trans Multimedia. 2005;7(4):700–715.

[3] Langelaar GC, Setyawan I, Lagendijk RL. Watermarking digital image and video data. A state-of-the-art overview. IEEE Sig Process Mag. 2000;17(5):20–46.

[4] Rahman SM, Ahmad MO, Swamy M. A new statistical detector for dwt-based additive image watermarking using the gauss–hermite expansion. IEEE Trans Image Process. 2009;18(8):1782–1796.

[5] Zheng P, Huang J. Walsh–Hadamard transform in the homomorphic encrypted domain and its application in image watermarking. In: Information Hiding: 14th International Conference, IH, 2012. p. 240–254. 2012 Lecture Notes in Computer Science, vol 7692. Springer, Berlin, Heidelberg. 2012. https://doi.org/10.1007/978-3-642-36373-3_16

[6] Rahimi F, Rabbani H. A dual adaptive watermarking scheme in contourlet domain for dicom images. Biomed Eng Online. 2011;10(1):1.

[7] Sun T, Quan W, Wang S. Zero-watermark watermarking for image authentication. Proc Signal Image Process. 2002:503–508.

[8] Tsai SM. A robust zero-watermarking algorithm for audio based on IPCC. In: 2013 International Conference on Orange Technologies (ICOT), IEEE; 2013. p. 63–66.

[9] Yu Y, Min L, Mingzhi C, et al. An audio zero-watermark scheme based on energy comparing. China Commun. 2014;11(7):110–116.

[10] Yu Y, Lei M, Liu X, et al. Novel zero-watermarking scheme based on dwt-dct. China Commun. 2016;13(7):122–126.

[11] Xuesong C, Guanglong B, Haotian L, et al. A video zero-watermark algorithm based on the contourlet transform. In: 3rd International Conference on Multimedia Technology (ICMT-13). Atlantis Press; 2013.

[12] Li D, Qiao L, Kim J. A video zero-watermarking algorithm based on lpm. Multimed Tools Appl. 2016;75 (21):13093–13106.

[13] Zhao C, Liu W. Block compressive sensing based image semi-fragile zero-watermarking algorithm. Acta Autom Sinica. 2012;38(4):609–617.

[14] Tang X, Ma Z, Niu X, et al. Compressive sensing-based audio semi-fragile zero-watermarking algorithm. Chinese J Electron. 2015;24(3):492–497.

[15] Dhar PK, Khan MI, Kim JM. A new audio watermarking system using discrete Fourier transform for copyright protection. Int J Computer Sci Netw Security. 2010;10(6):35–40.

[16] Datta K, Sengupta I. A redundant audio watermarking technique using discrete wavelet transformation. In: Second International Conference on Communication Software and Networks, ICCSN'10. IEEE; 2010. p. 27–31.

[17] Zhou X, Huang H, Lou SL. Authenticity and integrity of digital mammography images. IEEE Trans Med Imaging. 2001;20(8):784–791.

[18] Zain JM, Baldwin L, Clarke M. Reversible watermarking for authentication of dicom images. In: The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 2, IEEE; 2004. p. 3237–3240.

[19] Guo X, Zhuang TG. A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging. 2009;22(1):53–64.

[20] Kundu MK, Das S. Lossless ROI medical image watermarking technique with enhanced security and high payload embedding. In: 20th International Conference on Pattern Recognition. IEEE; 2010. p. 1457–1460.

[21] Chao H-M, Hsu C-M, Miaou S-G. A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed. 2002;6(1):46–53.

[22] Acharya R, Niranjan U, Iyengar SS, et al. Simultaneous storage of patient information with medical images in the frequency domain. Comput Methods Programs Biomed. 2004;76(1):13–19.

[23] Lee H-K, Kim H-J, Kwon K-R, et al. Digital watermarking of medical image using ROI information. In: Proceedings of 7th International Workshop on Enterprise Networking and Computing in Healthcare Industry, HEALTHCOM. IEEE; 2005. p. 404–407.

[24] Navas K, Thampy SA, Sasikumar M. Epr hiding in medical images for telemedicine. Int J Biomed Sci. 2008;3(1):44–47.

[25] Maity HK, Maity SP. Joint robust and reversible watermarking for medical images. Procedia Technol. 2012;6:275–282.

[26] Soualmi A, Alti A, Laouamer L. A novel blind watermarking approach for medical image authentication using mineigen value features. Multimed Tools Appl. 2021;80(2):2279–2293.

[27] Soualmi A, Alti A, Laouamer L, et al. A blind fragile based medical image authentication using Schur decomposition. In: International Conference on Advanced Machine Learning Technologies and Applications. Springer; 2019. p. 623–632.

[28] Soualmi A, Alti A, Laouamer L. A new blind medical image watermarking based on weber descriptors and arnold chaotic map. Arabian J Sci Eng. 2018; 43(12).

[29] Benssalah M, Rhaskali Y, Drouiche K. An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. Multimed Tools Appl. 2021;80(2):2081–2107.

[30] Xia Z, Wang X, Wang C, et al. Local quaternion polar harmonic Fourier moments-based multiple zero-watermarking scheme for color medical images. Knowl Based Syst. 2021;216:106568.

[31] Shaik A, Masilamani V. A novel digital watermarking scheme using dragonfly optimizer in transform domain. Comput Electr Eng. 2021;90:106923.

[32] Yang C, Li J, Bhatti UA, et al. Robust zero watermarking algorithm for medical images based on Zernike-DCT. Security Commun Netw. 2021;2021.

[33] Gong C, Li J, Bhatti UA, et al. Robust and secure zero-watermarking algorithm for medical images based on harris-surf-dct and chaotic map. Security Commun Netw. 2021;2021.

[34] Muhammad N, Bibi N. Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. IET Image Process. 2015;9(9):795–803.

[35] Ren X, Malik J. Learning a classification model for segmentation. In: ICCV, Vol. 1, 2003. p. 10–17.

[36] Achanta R, Shaji A, Smith K, et al. Slic superpixels. Tech. Rep., 2010.

[37] Levinshtein A, Sminchisescu C, Dickinson S. Multiscale symmetric part detection and grouping. Int J Comput Vis. 2013;104(2):117–134.

[38] Felzenszwalb PF, Huttenlocher DP. Efficient graph-based image segmentation. Int J Comput Vis. 2004;59 (2):167–181.

[39] Shi J, Malik J. Normalized cuts and image segmentation. IEEE Trans Pattern Anal Mach Intell. 2000;22(8):888–905.

[40] Vedaldi A, Soatto S. Quick shift and kernel methods for mode seeking. In: Computer Vision–ECCV 2008, 2008. p. 705–718.

[41] Connolly C, Fleiss T. A study of efficiency and accuracy in the transformation from RGB to cielab color space. IEEE Trans Image Process. 1997;6(7):1046–1048.