Journal of Engineering Science and Technology
Vol. 17, No. 1 (2022) 0760 - 0780

TAMPER DETECTION AND LOCALIZATION SCHEME FOR COLOR MEDICAL IMAGES

RASHA THABIT

Computer Techniques Engineering Department, Al-Rasheed University College, P. O. B. 6068, Al Jamaa, 10001, Baghdad, Iraq
E-mail: rashathabit@yahoo.com

Abstract

A recent challenge in medical imaging systems is to provide an authentication scheme that is suitable for colour medical images because this type of images is increasingly used in this field. In this work, a new tamper detection and localization scheme is presented to safeguard the colour medical images which are stored or shared through open access networks. The proposed scheme ensures the safety of the region of interest (ROI), which is very important for the diagnosis process, by excluding it from the embedding process. The authentication data has been calculated from the ROI and embedded in the Slantlet transform coefficients of the remaining part of the image. The experiments that have been carried out confirmed the efficiency of the proposed technique which can detect and localize any tampering in the ROI. The experimental results and the general comparisons with the state-of-the-art schemes proved that there is a promising future for the proposed technique in the practical applications.

Keywords: Color medical image protection, Color medical image security, Tamper detection, Tamper localization.

1. Introduction

The computing field is rapidly growing day after another and with this swift growth many types of digital information (e.g., music, video, image, text, …) are distributed through different networks such as local networks and internet [1, 2]. The digital medical data in their different forms (e.g., medical images, electronic patient record (EPR), electronic health record (EHR), health surveys, clinical trials data, …) are widely used and distributed. One of the important medical data is the digital medical image which can be exchanged through internet for different purposes such as getting the diagnosis results from different hospitals or getting opinion of a specialist who is far away from the currently examined patient. Saving the medical images in their digital form or sending them through internet requires security and protection against any modifications which may cause wrong diagnosis process. Over the years, different tamper detection and localization methods have been presented based on image watermarking techniques [3-5]. Some medical image authentication (MIA) schemes can only detect tampering without providing any information about the tampered place [6-14] while others can also localize the region in which tampering has been conducted [15-18].

The watermarking process mainly based on modifying the pixels of the image in order to hide the data that is required for authentication. In some medical image authentication techniques (MIA), the whole image is used to embed the watermark [12, 15-18] while in others the medical image is divided into two regions [6-11, 13]. Since the diagnosis processes are relying on medical images, the watermarking techniques should ensure the intactness of the image either by using the reversible watermarking process or by excluding the region of interest (ROI) from the watermark embedding process. The limitation of the MIA schemes in [6-9, 12, 15, 17] is that they cannot ensure the intactness of the medical image because they used irreversible watermarking techniques to hide the watermark.

The watermark can be inserted in the image either in the spatial domain by modifying the pixels [19-23] or in the transform domain which require applying a transformation process before embedding the watermark [24-30]. It is known that the spatial domain-based watermarking techniques are fragile and any small modification in the image will destroy the watermark, therefore, most of the MIA schemes depends on this property for authentication process. However, the recent researches proved that the medical image watermarking techniques require robustness against unintentional attacks such as channel noise and image compression [31-37]. On the other hand, the previous MIA schemes focused on grayscale images because of their prevalence. Nowadays, the colour medical images (CMIs) are increasingly used in the medical imaging systems therefore the following research questions are raised:

- Are the available authentication schemes directly applicable to CMIs?
- Is it possible to present an authentication scheme that can exactly detect and localize the tampered region in CMIs?
- Is it possible to provide robustness against unintentional attacks while achieving the tamper detection and localization objectives?
- How to achieve the above-mentioned objectives without affecting the medical image diagnosis process?

The watermarking techniques for grayscale images are not directly applicable to colour medical images because of their nature as explained in [37-39]. Since this research gap has not been highlighted sufficiently, there are very rare researches related to this topic. On the other hand, the recent research interests in the medical image authentication field are directed towards obtaining robustness against unintentional attacks while achieving the tamper detection and localization capabilities [39]. Therefore, it is necessary to present a new authentication scheme suitable for CMIs which can meet these recent interests.

Based on the previously mentioned research gap and questions, the objective of this work has been directed towards presenting a new tamper detection and localization (TDL) scheme that is suitable for CMIs and at the same time it can withstand unintentional attacks. The transform domain-based watermarking is a better candidate for obtaining robustness against attacks which has been proved by many researches in this field [23, 36, 40-44], therefore, this domain will be adopted to carry the authentication data. The next section of this paper illustrates the details of the proposed scheme and its algorithms; then section 3 presents the experimental results and discussions; and section 4 contains the conclusions of this work.

2. The Proposed Scheme and Algorithms

The proposed tamper detection and localization scheme in this paper is region of interest (ROI) based. In order to ensure the intactness of the ROI it will be excluded from the data embedding process. The main idea of the proposed scheme is to calculate the authentication bits for TDL from the ROI and embed them in the region of non-interest (RONI) using robust watermarking technique. Figure 1 presents a general architecture of the medical imaging system in which the proposed scheme is included. The proposed scheme for tamper detection and localization is mainly consists of two sides: one side is for the data embedding and the other is for data extraction. The upcoming subsections illustrate the details of the proposed algorithms.

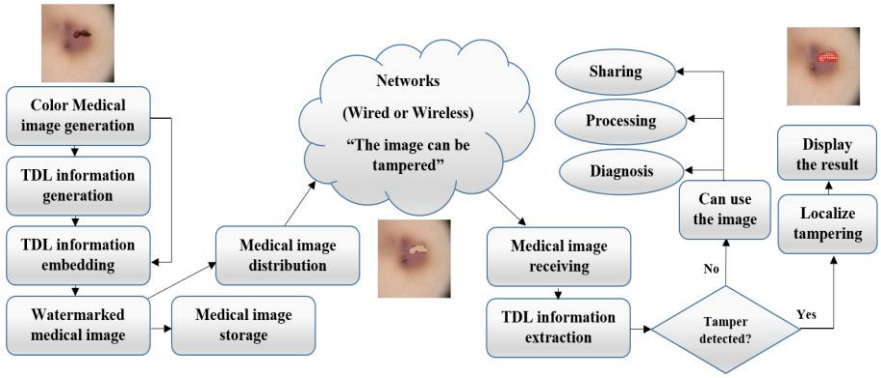

Fig. 1. General architecture of the medical imaging system including the proposed scheme.

2.1. The proposed data embedding scheme

In the proposed scheme, the tamper detection and localization data is generated from the image blocks that are related to the ROI for each channel in the colour

medical image. To ensure the robustness of the embedded data, it has been embedded in the transform domain by applying image transform. Since the Slantlet transform (SLT) proved its efficiency in many robust watermarking techniques, it will be adopted here. To facilitate the explanation of the data embedding scheme, the algorithms will be explained in three subsections that are the main embedding algorithm (*EmMain*), the embedding algorithm for a single channel from the colour medical image (*EmCh*), and the embedding algorithm for the RONI-blocks (*EmRONI*). Figure 2 illustrates the flow charts of the proposed algorithms for the data embedding scheme.

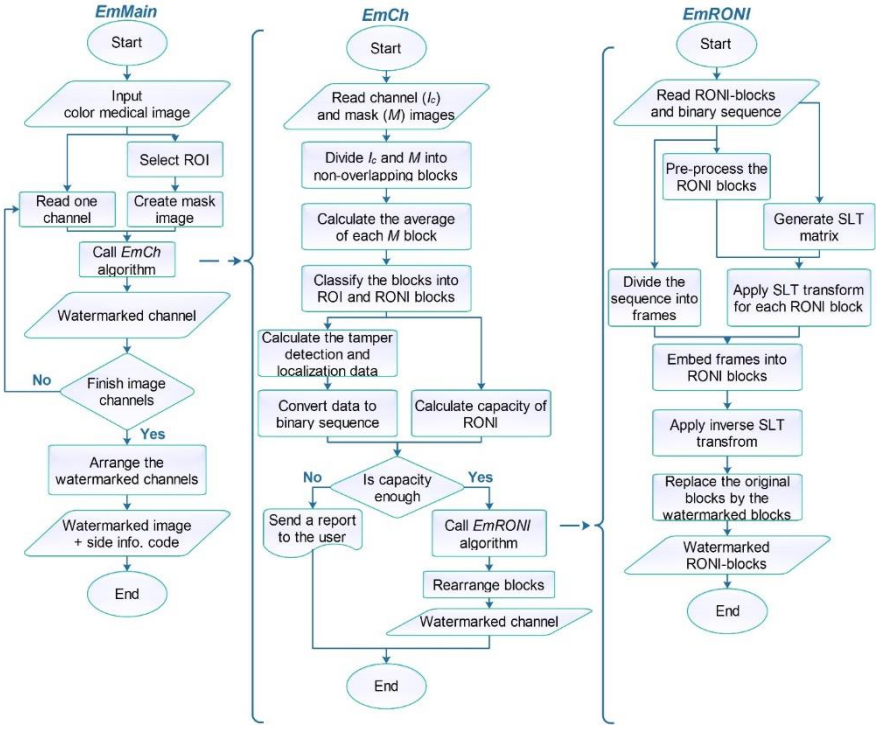

Fig. 2. Flow charts of the proposed algorithms for the data embedding scheme.

2.1.1. The main embedding algorithm (*EmMain*)

The main embedding algorithm (*EmMain*) which is shown in Fig. 2 starts by reading the colour medical image which consists of three channels that are the red, green, and blue (RGB). The three channels can be separated and each channel image can be processed as a grayscale image. The steps of *EmMain* algorithm can be explained as follows:

Input: Original colour medical image I.

Output: Watermarked colour medical image I_w and side information code (*SIC*).

Step 1: Read the original RGB colour medical image I of size $[H, W, 3]$.

Step 2: Display I and select the ROI using polygon. The positions of the selected points of the polygon are coded using Bose–Chaudhuri–Hocquenghem (BCH (15,11)) and saved as side information (*SIC*).

Step 3: Generate a logical mask image M of size $[H, W]$ as follows:

$$M(i,j) = \begin{cases} 0 & if\ I(i,j) \notin \text{ROI} \\ 1 & if\ I(i,j) \in \text{ROI} \end{cases}$$

where $I(i,j)\ and\ M(i,j)$ are pixels of the input image and the mask image, respectively, at the coordinates (i,j).

The mask image M is different according to the selected ROI as illustrated in Fig. 3.

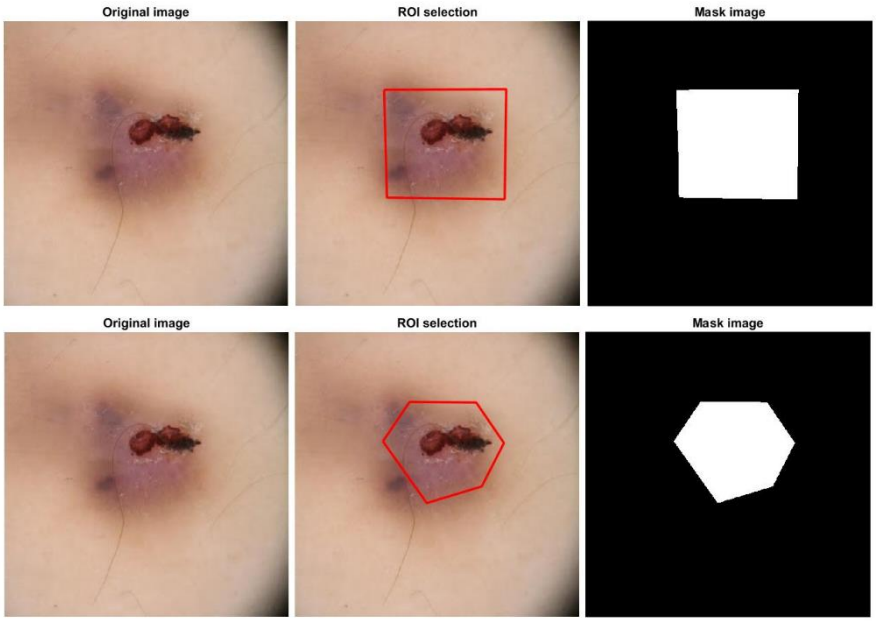

Fig. 3. Different mask images according to the selected *ROI*.

Step 4: Extract one channel (i.e., red, green, or blue) from the CMI and apply watermark embedding process by calling the *EmCh* algorithm (which will be explained in the next section) to obtain the watermarked channel. Repeat the process for the other two channels.

Step 5: Construct the watermarked colour medical image from the resultant watermarked channels. The watermarked colour medical image is sent with the side information code to the receiver side.

2.1.2. The embedding algorithm for a single channel (*EmCh*)

The embedding algorithm (*EmCh*) shown in Fig. 2 is applied to a single channel which is treated as a grayscale image. The *EmCh* algorithm can be illustrated as follows:

Input: the original channel image I_c and the mask image M

Output: the watermarked channel image I_{wc}

Step 1: Read the input channel I_c and mask image M.

Step 2: Divide I_c and M into non-overlapping blocks of size (16×16).

Step 3: Classify I_c blocks into $ROI - blocks$ and $RONI - blocks$.

The processes of dividing the images (I_c and M) and classifying the blocks of I_c are illustrated in Fig. 4 and the algorithm can be explained as follows:

Let the size of I_c is (H×W)
For $x = 1\ to\ H/16$
For $y = 1\ to\ W/16$
Select the block from the mask image M at the order (x, y)
Calculate average of the pixels in the selected block (AvM) in order to be used for classifying I_c blocks.
Classify the block of I_c according to the AvM value as follows:
If $AvM = 0$ then the block of I_c at the same position belongs to $RONI - blocks$
If $AvM \neq 0$ then the block of I_c at the same position belongs to $ROI - blocks$
Continue until finish all the image blocks.

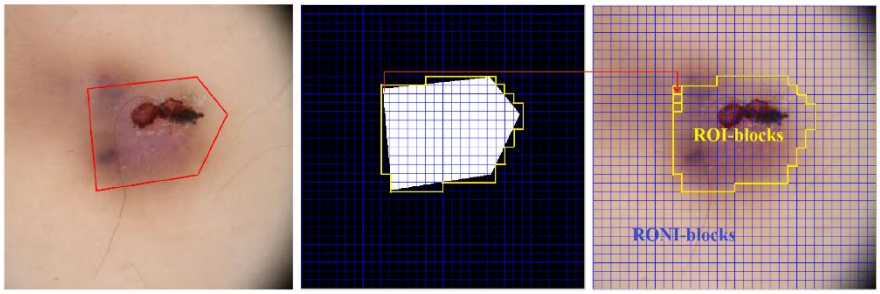

Fig. 4. Dividing images into non-overlapping blocks and classifying them.

Step 4: Calculate the tamper detection and localization data (*TDLD*) for each block in $ROI - blocks$ as follows:

$$TDLD\{B\} = \frac{1}{{B_s}^2} \sum_{i=1}^{B_s} \sum_{j=1}^{B_s} B(i,j)$$

where $TDLD\{B\}$ is the tamper detection and localization data for the block B from $ROI - blocks$. B_s is the side length of the block B, and $B(i,j)$ is the pixel value at the coordinates (i,j) in the block B.

Step 5: Convert the $TDLD$ values to binary sequence and apply BCH (15,11) encoding to improve the robustness.

Step 6: Calculate the length of the resultant sequence, if the length is not a multiple of 64 bits then extend the length of the sequence by zeros. The resultant binary sequence is saved as follows:

$$Seq = \{S_1, S_2, \dots, S_{Lseq}\ (where\ Lseq\ is\ the\ length\ of\ the\ binary\ sequence)\}.$$

Step 7: Calculate the capacity of the $RONI$ as follows:

$$C_{RONI} = Total\ number\ of\ RONI - blocks * 64\ (bits)$$

Step 8: Compare $Lseq$ and C_{RONI} to ensure there is an enough space to embed the binary sequence. If the $C_{RONI} < Lseq$ then a report is sent which clarifies that that the algorithm cannot continue because the selected ROI is large which will give an option to select a smaller ROI. If the $C_{RONI} \geq Lseq$ then continue to the next step.

Step 9: Call the embedding algorithm for $RONI - blocks$ ($EmRONI$) (which is explained in the next section). The inputs of the algorithm are $RONI - blocks$ and Seq. The outputs of the algorithm are the watermarked $RONI - blocks$.
Step 10: Construct the resultant watermarked channel image I_{wc} by replacing the original $RONI - blocks$ by the watermarked $RONI - blocks$.

2.1.3. The embedding algorithm for RONI-blocks (*EmRONI*)

The embedding algorithm for RONI blocks (*EmRONI*) which is shown in Fig. 2 can be explained as follows:

Input: The set of RONI blocks $B_m = \{B_1, B_2, \dots, B_L\}$ and the binary sequence $Seq_n = \{S_1, S_2, \dots, S_{Lseq}\}$

Output: The watermarked RONI blocks $B_{wm} = \{B_{w1}, B_{w2}, \dots, B_{wL}\}$

Step 1: Pre-process B to avoid overflow/underflow of the pixels as follows:
For $m = 1\ to\ L$ (where L is the total number of RONI blocks)
Block=B_m;

$$B_{am}(i,j) = \begin{cases} 3 & if\ B_m(i,j) \le 2 \\ 252 & if\ B_m(i,j) \ge 253 \end{cases}$$

End for
The resultant adjusted blocks are saved in $B_{am} = \{B_{a1}, B_{a2}, \dots, B_{aL}\}$
Step 2: Generate the Slantlet matrix (SLT) for the same size of B_{am} block, and set the threshold value $Thr = 3$.

Step 3: Divide the Seq into frames $F_d = \{F_1, F_2, \dots, F_{nf}\}$ each of length (64 bits). The reason of dividing the sequence into frames is to prepare the binary bits that will be embedded in each block from *RONI* where each B_{am} block can carry 64 bits as illustrated in Fig. 5.

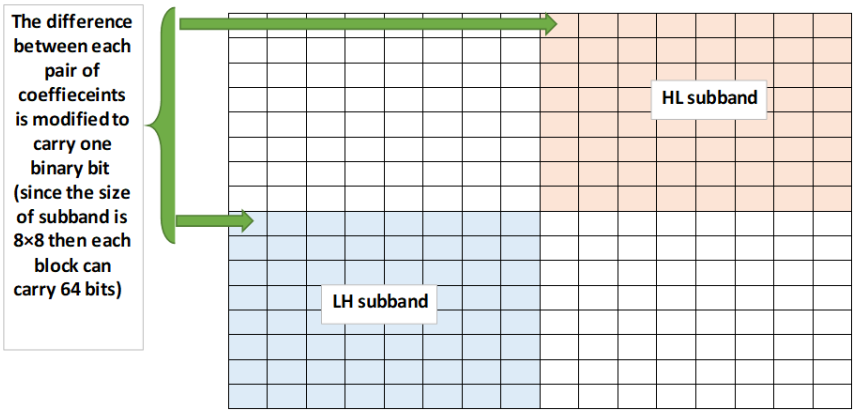

Fig. 5. Illustration for the number of bits that can be embedded in each block from the *RONI*.

Step 4: Embed each frame from F_d in a block from B_{am} as follows:
$F = fram\ from\ F_d$ (64 bits); $B = Block\ from\ B_{am}$;
Transform B using SLT matrix [36] as follows: $B_T = SLT * B * SLT'$
Divide the block B_T into four subbands as follows:

$LL = B_T\left(1{:}\frac{N}{2}, 1{:}\frac{N}{2}\right); LH = B_T\left(\frac{N}{2}+1{:}N, 1{:}\frac{N}{2}\right);$
$HL = B_T\left(1{:}\frac{N}{2}, \frac{N}{2}+1{:}N\right); HH = B_T\left(\frac{N}{2}+1{:}N, \frac{N}{2}+1{:}N\right);$
Take one bit from F and modify the difference between HL and LH coefficients according to the bit value as follows:
If the bit is 1 and $D_1 = HL(x,y) - LH(x,y)$ is less than or equal to Thr then increase HL and decrease LH by $(\frac{Thr-D1}{2})$.
If the bit is 0 and $D_2 = LH(x,y) - HL(x,y)$ is less than Thr then increase LH and decrease HL by $(\frac{Thr-D2}{2})$.
Repeat until finish all 64 bits of the frame F.
Replace the original HL and LH by the adjusted HL and LH subbands then apply inverse SLT [36] to obtain the watermarked blocks as follows:
$B_W = SLT' * B_T * SLT$
Save the watermarked blocks to obtain the output $B_{wm} = \{B_{w1}, B_{w2}, \dots, B_{wL}\}$

2.2. The proposed data extraction scheme

The algorithms for the data extraction will be explained in three subsections that are the main extraction algorithm (*ExMain*), the extraction algorithm for a single channel from the colour medical image (*ExCh*), and the extraction algorithm for the *RONI*-blocks (*ExRONI*). The flow charts of the proposed data extraction algorithms are shown in Fig. 6.

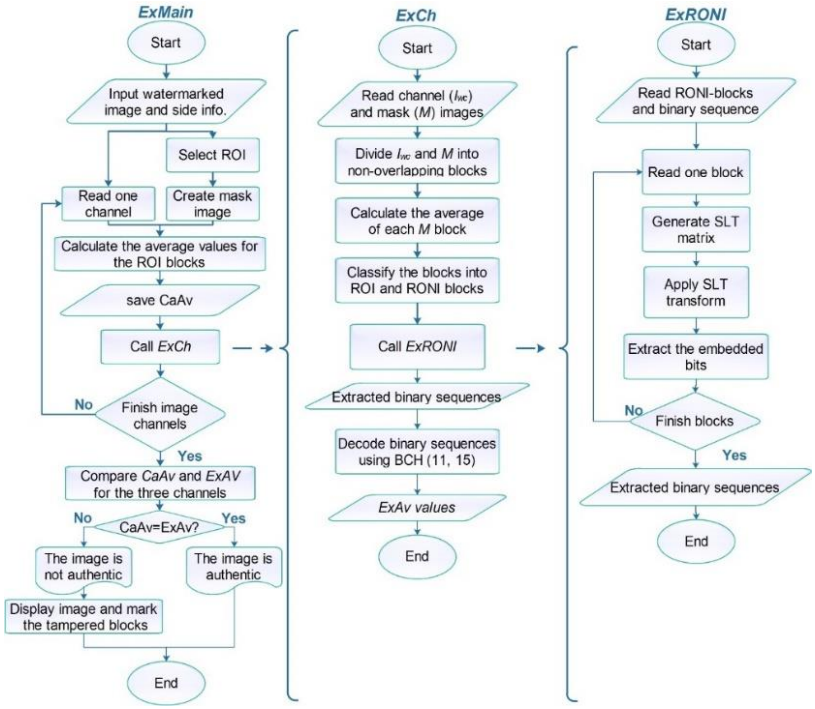

Fig. 6. Flow charts for the proposed algorithms for the data extraction scheme.

2.2.1. The main extraction algorithm (*ExMain*)

The main extraction algorithm (*ExMain*) which is shown in Fig. 6 starts by reading the input image and *SIC* and ends at a verification message and tamper localization result when the watermarked image is tampered. The steps of the algorithm can be explained as follows:

Input: The watermarked colour medical image I_w and side information code *SIC*.

Output: Verification message and tamper localization result for the tampered image.

Step 1: Read I_w and *SIC*.

Step 2: Select the ROI using the side information code which contains the locations of the points that have been selected to specify the ROI.

Step 3: Generate the mask image according to the selected ROI as illustrated in (Section 2.1.1).

Step 4: Calculate the average values of the ROI blocks in each channel as follows:

For $i = 1\ to\ 3$ (the steps are repeated for the three channels)
$Channel = Ch_i; Mask = M;$
Divide Ch_i and M into non-overlapping blocks
Calculate the average of each M block and classify Ch_i blocks into ROI-blocks and RONI-blocks as illustrated in (section 2.1.1).
Calculate average of ROI-blocks using:

$$CaAv\{B\} = \frac{1}{B_s{}^2}\sum_{i=1}^{B_s}\sum_{j=1}^{B_s} B(i,j)$$

Where $CaAv\{B\}$ is the calculated average value for the block B, and B_s is the side length of the block. $B(i,j)$ is the pixel value at the coordinates (i,j) in the block B.
Save the outputs of the algorithm in $CaAv_i$
End for

Step 5: Extract *TDLD* information from the RONI-blocks in each channel of the CMI as follows:

For $i = 1\ to\ 3$ (the steps are repeated for the three channels)
$Channel = Ch_i; Mask = M;$
Call the extract from channel algorithm (*ExCh*) for the inputs Ch_i and M
Save the outputs of the algorithm in $ExAv_i$
End for

Step 6: Compare the $CaAv_i$ and $ExAv_i$ for the three channels to detect any tampering in the medical image as follows:

For $i = 1\ to\ 3$ (the steps are repeated for the three channels)
If $CaAv_i = ExAv_i$ then the channel is authentic (there is no tampering)
Else the channel is not authentic (tampering has been detected)
End for
If the three channels are authentic, then a message can be displayed such as "The colour medical image is authentic" as a verification message and the algorithm is turned off at this step.
If tampering has been detected, then a message can be displayed such as "The colour medical image is not authentic" as a verification message and the algorithm is continued to the next step.

Step 7: Localize the tampered region using the following steps:

Display the watermarked colour medical image
For $i = 1\ to\ 3$ (the steps are repeated for the three channels)
If $CaAv_i \neq ExAv_i$ then localize the tampered blocks by displaying a border around the tampered blocks in the image.
End for

2.2.2. The extraction algorithm from a single channel (*ExCh*)

The data embedded in the *RONI*-blocks can be extracted using extraction algorithm for a single channel (*ExCh*) which is shown in Fig. 6. The steps of the algorithm are as follows:

Input: The watermarked channel image I_{wc} and the mask image M

Output: The extracted average values $ExAv$

Step 1: Read I_{wc} and M.

Step 2: Divide I_{wc} and M into non-overlapping blocks of size (16×16).

Step 3: Calculate average value for each block in M (AvM) then classify the blocks of I_{wc} into two types ($ROI - blocks$ and $RONI - blocks$) according to the AvM values as explained in (section 2.1.2).

Step 4: Call the $ExRONI$ algorithm where its inputs are $RONI - blocks$. The output of the algorithm is the extracted average sequences from the RONI.

Step 5: Decode the extracted average sequences from the RONI using *BCH* (11,15) then convert the binary sequence to average values to obtain $ExAv$.

2.2.3. The extraction algorithm from RONI-blocks (*ExRONI*)

The embedded bits in the RONI-blocks can be extracted using the extraction from the RONI algorithm (*ExRONI*) which is shown in Fig. 6. The steps of the algorithm can be explained as follows:

Input: The set of RONI blocks $B_m = \{B_1, B_2, \dots, B_L\}$

Output: The extracted binary sequences $ExSeq$

Step 1: Generate the Slantlet matrix (SLT) for the same size of B_m block.

Step 2: Extract the embedded bits from each block B_m as follows:

For $m = 1\ to\ L$ (where L is the total number of RONI blocks)
Block=B_m;
Transform B using SLT matrix as follows: $B_T = SLT * B * SLT'$
Divide the block B_T into four subbands.
Extract the 64 bits from the block using:
For $a = 1\ to\ 64$

$$Bit(a) = \begin{cases} 1 & if\ HL(x,y) \geq LH(x,y) \\ 0 & if\ LH(x,y) < HL(x,y) \end{cases}$$

End for
The extracted binary sequences are saved in $ExSeq_m$
End for

Step 3: Save the extracted binary sequences in $ExSeq$

3. Experimental results and discussion

Several experiments have been conducted for different CMIs from [45, 46] in order to evaluate the proposed TDL scheme. The following subsections introduce some results that have been obtained from the experimental tests. A general comparison with state-of-the-art schemes from [6-18] is presented in the final subsection.

3.1. TDL test

The performance of the proposed TDL scheme has been evaluated for two different tampering processes in the ROI. The first tampering process that has been imposed on the watermarked CMI is the (copy & paste) process in which some pixels of the image are copied and used to replace some other pixels in the ROI. The second tampering process is erasing some pixels in the ROI. Samples of the experimental results that have been obtained from this test are shown in Figs. 7 and 8. This test proved the ability of the proposed TDL scheme to detect and localize any tampering in the ROI of the CMIs. The accuracy of the scheme is 100% and there is no false detection even for very small, tampered region.

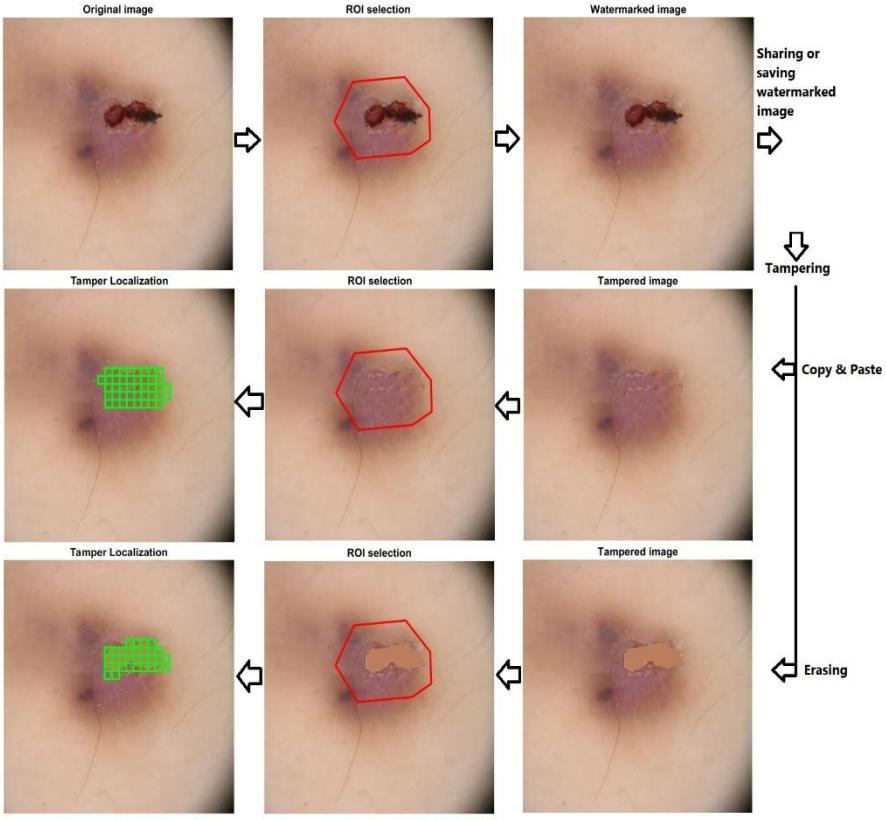

Fig. 7. Tamper detection and localization results for colour medical image 1.

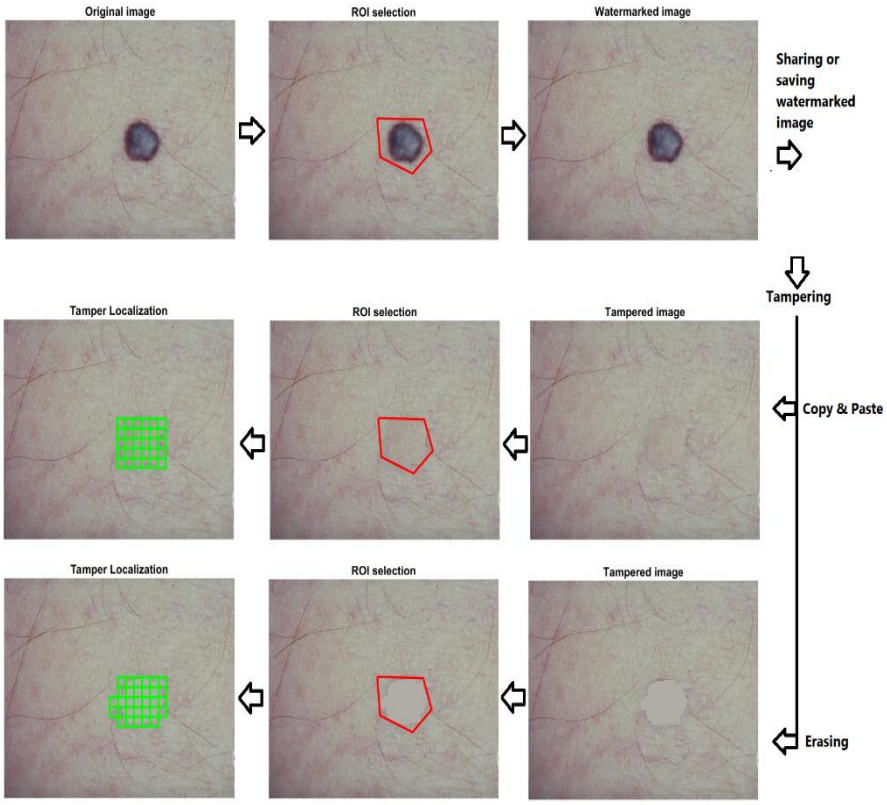

Fig. 8. Tamper detection and localization results for colour medical image 2.

3.2. Capacity and payload test

The embedding capacity of the proposed TDL scheme refers to the total number of bits that can be embedded in the *RONI* while the payload refers to the total number of bits that are generated as tamper detection and localization information for the selected *ROI*.

To test the capacity and payload of the proposed scheme, different *ROI* areas have been selected from different colour medical images as shown in Fig. 9. The sizes of the test images are as follows: (image 1 (512×512×3), image 2 (1043×1640×3), image 3 (336×453×3), and image 4 (356×455×3)).

The results from the capacity test are shown in Fig. 10 which proved that for the same medical image when the size of the selected *ROI* is increased the capacity is decreased because the number of the *RONI*-blocks is decreased. The results from the payload test are shown in Fig. 11 which proved that the larger the *ROI*, the higher the payload because of generating more tamper detection and localization bits. Thus one can conclude that the embedding capacity and payload for the same medical image depend on the size of the selected *ROI*. Note that the names of the images have been abbreviated in the Figs. 10 and 11 as follows: (Im1 for image 1, Im2 for image 2, Im3 for image 3, and Im4 for image 4).

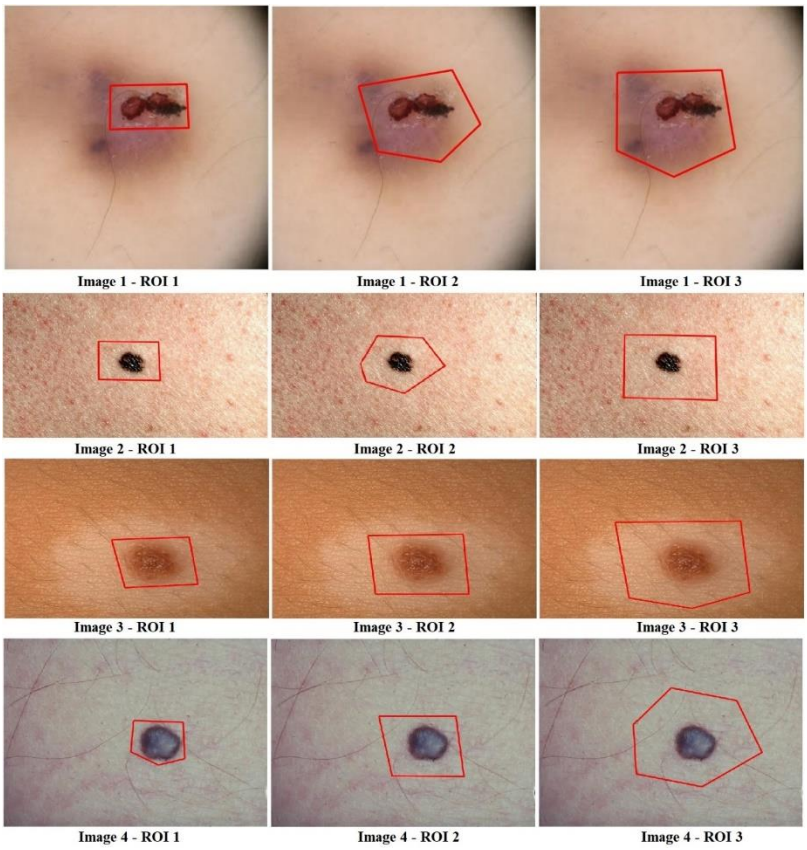

Fig. 9. Samples of the colour medical images with different ROI areas.

Fig. 10. Capacity test results.

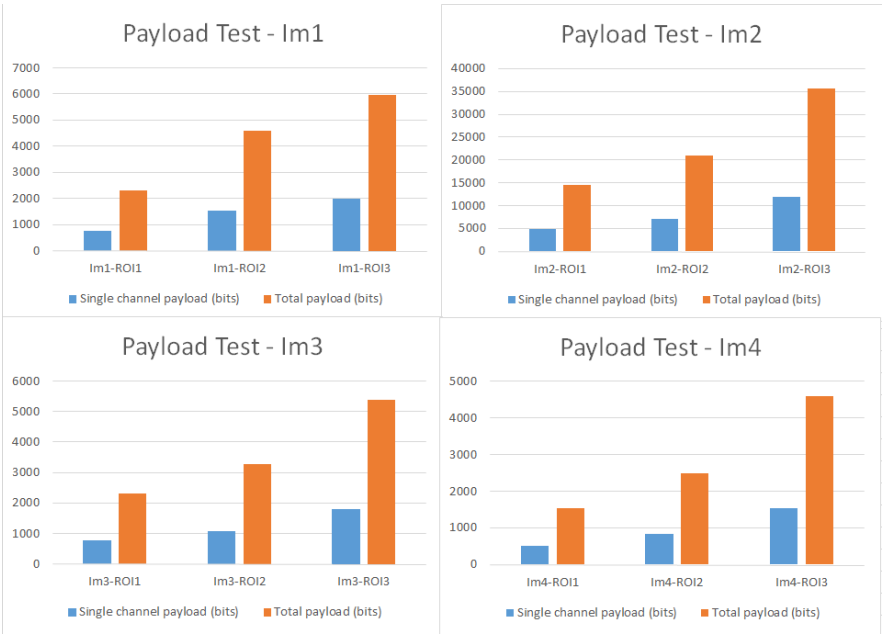

Fig. 11. Payload test results.

3.3. Invisibility test

To provide security, it is necessary to obtain watermarked CMIs with high visual quality. To evaluate the performance of the proposed scheme in terms of visual quality, two evaluation tests have been conducted which are subjective and objective evaluation methods. For subjective evaluation, the watermarked CMIs are displayed to be checked if there are any visible distortions in the image. Samples of the CMIs are shown in Fig. 12 which proved that the difference between the original CMIs and the watermarked CMIs is imperceptible. For objective evaluation, the peak signal-to-noise ratio for colour images (*PSNRc*) and the mean square error (*MSEc*) have been calculated [37].

The *PSNRc* results for the same test images that have been used in section (3.2) are shown in Fig. 13 which proved that the larger the size of the *ROI*, the lower the visual quality of the watermarked image because more modifications are performed to embed the binary data. The *MSEc* results for the same test images are shown in Fig. 14 which proved that the errors are increased when larger *ROI* is selected. On the other hand, the results proved that when the size of the medical image is small, the value of the *MSEc* is high for the same payload as shown in the results of Im1-ROI1 and Im3-ROI1 and the reason of this behaviour is that the *MSEc* is inversely proportional to the total number of pixels in the image.

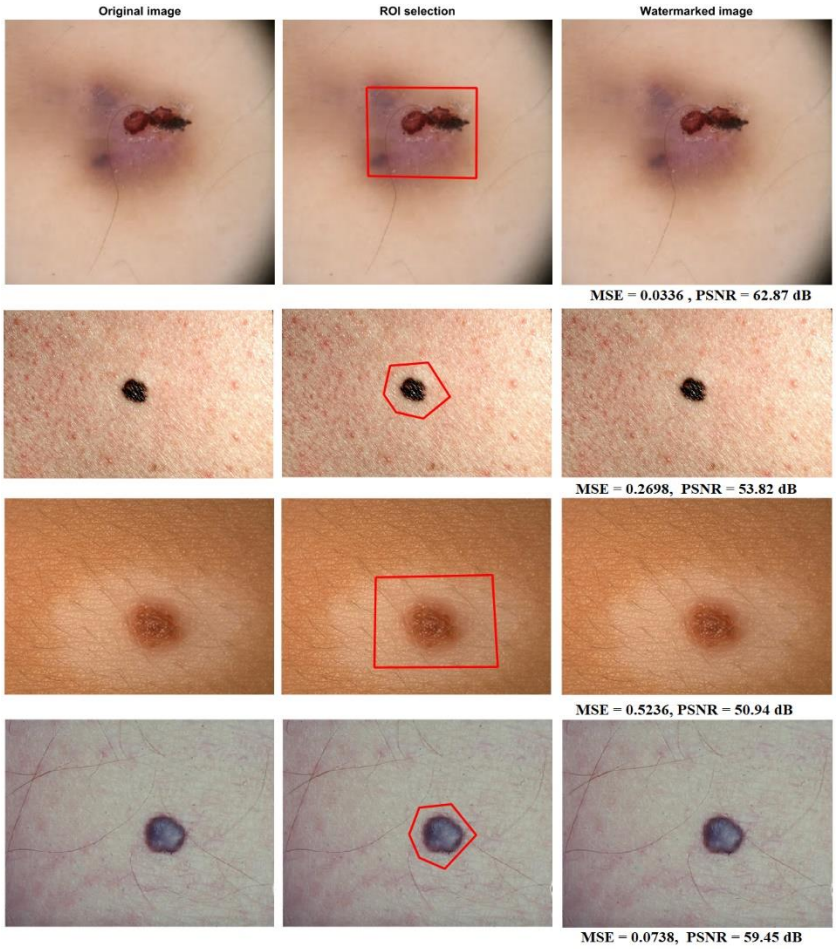

Fig. 12. Samples of the watermarked colour medical images.

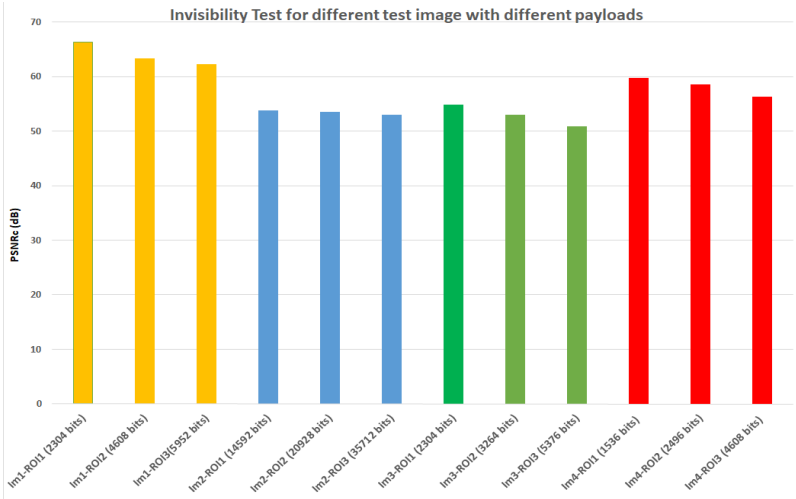

Fig. 13. *PSNRc* test results for different CMIs.

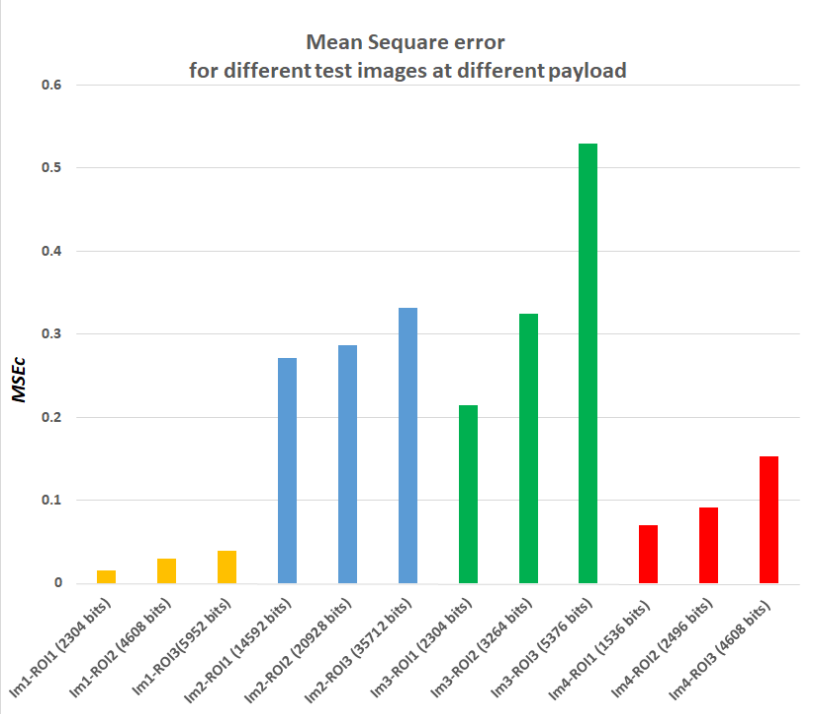

Fig. 14. *MSEc* test results for different CMIs.

3.4. Comparison with the state-of-the-art

The main aim of the proposed TDL scheme is to be suitable for the CMIs. The previous authentication techniques that have been presented for grayscale medical images are not directly comparable with the proposed technique in terms of experimental results, therefore, only general comparisons are valid here.

This section presents a general comparison between the proposed scheme and the tamper detection schemes in [6-14] and the tamper detection and localization schemes in [15-18] to prove the superiority of the proposed TDL scheme. Table 1 illustrates the comparison in terms of tamper detection and localization capabilities, intactness of the image or the ROI, the domain of watermark embedding, and the type of the medical images.

The comparison can be summarized as follows:

- The proposed TDL scheme outperforms the schemes in [6-14] because it can not only detect tampering but also localize the tampered region.
- The proposed TDL scheme outperforms the schemes in [6-9, 12, 15, 17] in terms of preserving the intactness of the ROI.
- The proposed TDL scheme outperforms the spatial-domain based schemes [6, 10-16, 18] in terms of robustness against unintentional attacks because the spatial-domain based schemes are fragile. On the other hand, the proposed TDL scheme is better than the DWT based schemes in [7-9, 17] because the SLT based watermarking performs better in terms of visual quality and robustness against attacks which has been proved in many researches [35-37, 39, 44, 47].

- The scheme is suitable for colour medical images which makes it a better candidate for the colour medical imaging systems.

Table 1. General comparison between the proposed scheme and the state-of-the-art schemes.

Scheme	ROI-based	TD	TL	I-ROI	Domain	Image type
[6]	✓	✓	×	×	Spatial-LSBs	Grayscale
[7]	✓	✓	×	×	Transform-DWT	Grayscale
[8]	✓	✓	×	×	Transform-DWT	Grayscale
[9]	✓	✓	×	×	Transform-DWT	Grayscale
[10]	✓	✓	×	✓	Spatial-LSBs	Grayscale
[11]	✓	✓	×	✓	Spatial-chaotic key	Grayscale
[12]	×	✓	×	×	Spatial-LSBs	Grayscale
[13]	✓	✓	×	✓	Spatial-LSBs	Grayscale
[14]	✓	✓	×	✓	Spatial -DE	Grayscale
[15]	×	✓	✓	×	Spatial-LSBs	Grayscale
[16]	×	✓	✓	✓	Spatial-Pixels modification	Grayscale
[17]	×	✓	✓	×	Transform-DWT	Grayscale
[18]	×	✓	✓	✓	Spatial-Pixels modification	Grayscale
Proposed	✓	✓	✓	✓	Transform-SLT	Color

* TD: Tamper detection , TL: Tamper localization, I-ROI: Intactness of the region of interest

4. Conclusions

In this work, a new tamper detection and localization scheme for CMIs is presented. To prevent distortions in the ROI which may be generated because of hiding the data bits in the image, the scheme has been implemented to exclude the ROI from the watermark embedding process. The authentication bits have been generated from the ROI and embedded in the SLT coefficients of the RONI. To assess the performance of the proposed TDL scheme different experimental tests have been performed. The results provide that the scheme can detect and localize any tampering in the ROI. The watermarked images obtained good visual quality results and the embedded data is imperceptible. The capacity and payload has been tested for different ROI areas and the results proved that the smaller the ROI, the higher the capacity, the lower the payload and vice versa. The scheme has been successfully used for CMIs and it can be adopted for other colour images in practical applications.

Nomenclatures

AvM	Average of the mask image block
B	Block from the ROI
B_{am}	Adjusted B_m block
B_m	Block from the region of non-interest
B_s	Side length of the block B
B_T	Transformed B block

B_w	Watermarked B_{am} block
CaAv	Average of ROI blocks
Ch	The channel image
C_{RONI}	Capacity of the region of non-interest
ExAv	Extracted average values
ExSeq	Extracted binary sequence
F_d	Frame (64 bits) from the binary sequence (*Seq*)
H	Height of original colour medical image
HH	High-high subband
HL	High-low subband
I	Original colour medical image
I_c	Original channel image
I_w	Watermarked colour medical image
I_{wc}	Watermarked channel image
L	Total number of RONI blocks
LH	Low-high subband
LL	Low-low subband
L_{seq}	Length of the binary sequence
M	Mask image
MSE_c	Mean Sequer Error for Color image
$PSNR_c$	Peak Signal to Noise Ratio for colour image
Seq	The binary sequence
SIC	Side Information Code
TDLD	Tamper detection and localization data
Thr	Threshold value
W	Width of original colour medical image

Abbreviations

CMI	Color medical image
CMIs	Color medical images
EHR	Electronic health record
EmCh	Embedding algorithm for a single channel from the image
EmMain	Main embedding algorithm
EmRONI	Embedding algorithm for region of non-interest blocks
EPR	Electronic patient record
ExCh	Extraction algorithm for a single channel from the colour medical image
ExMain	Main extraction algorithm
ExRONI	the extraction algorithm for region of non-interest blocks
Im1	Sample colour medical image 1
Im2	Sample colour medical image 2
Im3	Sample colour medical image 3
Im4	Sample colour medical image 4
MIA	Medical image authentication
RGB	Red, Green, and Blue
ROI	Region of interest
RONI	Region of non-interest
SLT	Slantlet transform
TDL	Tamper detection and localization

References

1. Elbaşi, E. (2010). Robust multimedia watermarking: Hidden Markov model approach for video sequences. *Turkish Journal of Electrical Engineering and Computer Sciences*, 18(2), 159-170.
2. Yadav, J.; and Sehra, K. (2018). Large scale dual tree complex wavelet transform based robust features in PCA and SVD subspace for digital image watermarking. *Procedia Computer Science*, 132, 863-872.
3. Mousavi, S.M.; Naghsh, A.; and Abu-Bakar, S.A.R. (2014). Watermarking Techniques used in Medical Images: a Survey. *Journal of Digital Imaging*, 27(6), 714-729.
4. Nyeem, H.; Boles, W.; and Boyd, C. (2013). A review of medical image watermarking requirements for teleradiology. *Journal of Digital Imaging*, 26(2), 326-343.
5. Allaf, A.H.; and Kbir, M.A. (2019). A review of digital watermarking applications for medical image exchange security. *In the Proceedings of the Third International Conference on Smart City Applications*, Tetouan, Morocco, 472-480.
6. Memon, A.N. (2010). *Watermarking of medical images for content authentication and copyright protection* (PhD. Thesis). GIK Institute of Engineering Sciences and Technology.
7. Giakoumaki, A.; Pavlopoulos, S.; and Koutsouris, D. (2005). Multiple digital watermarking applied to medical imaging. *Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society*. New York, NY, USA, 3444-3447.
8. Giakoumaki, A.; Pavlopoulos, S.; and Koutsouris, D. (2006). Multiple image watermarking applied to health information management. *IEEE Transactions on Information Technology in Biomedicine*, 10(4), 722-732.
9. Giakoumaki, A.; Pavlopoulos, S.; and Koutsouris, D. (2006). Secure and efficient health data management through multiple watermarking on medical images. *Medical and Biological Engineering and Computing*, 44(8), 619-631.
10. Guo, X.; and Zhuang, T.G. (2009). A region-based lossless watermarking scheme for enhancing security of medical data. *Journal of Digital Imaging*, 22(1), 53-64.
11. Naseem, M.T.; Qureshi, I.M.; and Cheema, T.A. (2013). Hash based medical image authentication and recovery using chaos and residue number system. *Journal of Basic Applied Scientific Research*, 3(6), 488-495.
12. Woo, C.-S.; Du, J.; and Pham, B. (2005). Multiple watermark method for privacy control and tamper detection in medical images. *APRS Workshop on Digital Image Computing* (*WDIC*). University of Queensland, 43-48.
13. Zain, J.M.; and Clarke, M. (2007). Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. *International Journal of Computer Science and Network Security*, 7(9), 19-28.
14. Qasim, A.F.; Aspin, R.; Meziane, F.; and Hogg, P. (2019). ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. *Multimedia Tools and Applications*, 78(12), 16433-16463.

15. Gull, S.; Loan, N.A.; Parah, S.A.; Sheikh, J.A.; and Bhat, G.M. (2020). An efficient watermarking technique for tamper detection and localization of medical images. *Journal of Ambient Intelligence and Humanized Computing*, 11(5), 1799-1808.
16. Dou, W.; Poh, C.L.; and Guan, Y.L. (2012). An improved tamper detection and localization scheme for volumetric DICOM images. *Journal of Digital Imaging*, 25(6), 751-763.
17. Saju, G.; and Sreenimol, K.R. (2019). An effective method for detection and localization of tampering. *International Journal of Information Systems and Computer Sciences*, 8(2), 152-154.
18. Guo, X.; and Zhuang, T.-g. (2009). Lossless watermarking for verifying the integrity of medical images with tamper localization. *Journal of Digital Imaging*, 22(6), 620-628.
19. Abraham, J.; and Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University - Computer and Information Sciences*, 31(1), 125-133.
20. Li, L.-D.; and Guo, B.-L. (2009). Localized image watermarking in spatial domain resistant to geometric attacks. *AEU - International Journal of Electronics and Communications*, 63(2), 123-131.
21. Wenyin, Z.; and Shih, F.Y. (2011). Semi-fragile spatial watermarking based on local binary pattern operators. *Optics Communications*, 284(16), 3904-3912.
22. Su, Q.; Niu, Y.; Wang, Q.; and Sheng, G. (2013). A blind color image watermarking based on DC component in the spatial domain. *Optik*, 124(23), 6255-6260.
23. Alotaibi, R.A.; and Elrefaei, L.A. (2019). Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). *Applied Computing and Informatics*, 15(2), 191-202.
24. Yadav, J.; and Sehra, K. (2018). Large scale dual tree complex wavelet transform based robust features in PCA and SVD subspace for digital image watermarking. *Procedia Computer Science*, 132, 863-872.
25. Shaik, A.; and Masilamani, V. (2018). Zero-watermarking in transform domain and quadtree decomposition for under water images captured by robot. *Procedia Computer Science*, 133, 385-392.
26. Kang, X.; Zhao, F.; Chen, Y.; Lin, G.; and Jing, C. (2020). Combining polar harmonic transforms and 2D compound chaotic map for distinguishable and robust color image zero-watermarking algorithm. *Journal of Visual Communication and Image Representation*, 70, 102804.
27. Yuan, Z.; Liu, D.; Zhang, X.; and Su, Q. (2020). New image blind watermarking method based on two-dimensional discrete cosine transform. *Optik*, 204, 164152.
28. Senapati, R.K.; Srivastava, S.; and Mankar, P. (2020). RST invariant blind image watermarking schemes based on discrete Tchebichef transform and singular value decomposition. *Arabian Journal for Science and Engineering*, 45, 3331-3353.
29. Fares, K.; Amine, K.; and Salah, E. (2020). A robust blind color image watermarking based on Fourier transform domain. *Optik*, 208, 164562.

30. Kishore, R.R. (2020). A novel and efficient blind image watermarking in transform domain. *Procedia Computer Science*, 167, 1505-1514.
31. An, L.; Gao, X.; Deng, C.; and Ji, F. (2010). Robust lossless data hiding: Analysis and evaluation. *Proceedings of the* 2010 *International Conference on High Performance Computing and Simulation* (*HPCS* 2010), Caen, France, 512-516.
32. An, L.; Gao, X.; Li, X.; Tao, D.; Deng, C.; and Le, J. (2012). Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Transactions on Image Processing*, 21(8), 3598-3611.
33. An, L.; Gao, X.; Yuan, Y.; and Tao, D. (2012). Robust lossless data hiding using clustering and statistical quantity histogram. *Neurocomputing*, 77(1), 1-11.
34. An, L.; Gao, X.; and Deng, C. (2010). Reliable embedding for robust reversible watermarking. *Proceedings of the* 2*nd International Conference on Internet Multimedia Computing and Service* (*ICIMCS'*10), Harbin, China, 57-60.
35. Thabit, R.; and Khoo, B.E. (2014a). Capacity improved robust lossless image watermarking. *IET Image Processing*, 8(11), 662-670.
36. Thabit, R.; and Khoo, B.E. (2014b). Robust reversible watermarking scheme using Slantlet transform matrix. *Journal of Systems and Software*, 88(1), 74-86.
37. Thabit, R.; and Khoo, B.E. (2015). A new robust lossless data hiding scheme and its application to color medical images. *Digital Signal Processing: A Review Journal*, 38, 77-94.
38. Celebi, M.E.; and Schaefer, G. (2013). Color medical image analysis. *Lecture Notes in Computational Vision and Biomechanics*. Springer Netherlands.
39. Thabit, R. (2021). Review of medical image authentication techniques and their recent trends. *Multimedia Tools and Applications*, 80, 13439–13473.
40. Kasmani, S.A.; and Naghsh-Nilchi, A.R. (2009). Robust Digital image watermarking based on joint DWT-DCT. *International Journal of Digital Content Technology and its Applications* (*JDCTA*), 3(2), 42-54.
41. Gunjal, B.L.; and Manthalkar, R.R. (2010). An overview of transform domain robust digital image watermarking algorithms. *Journal of Emerging Trends in Computing and Information Sciences*, 2(1), 37-42.
42. Mohammed, R.T.; and Khoo, B.E. (2012). Image watermarking using slantlet transform. 2012 *IEEE Symposium on Industrial Electronics and Applications, Bandung, Indonesia*, 285-290.
43. Dabas, P.; and Khanna, K. (2013). A study on spatial and transform domain watermarking techniques. *International Journal of Computer Applications*, 71(14), 38-41.
44. Thabit, R. (2019). Improved steganography techniques for different types of secret data. *Advances in Systems Science and Applications*, 19(3), 38-51.
45. EHRSAM, E. (2016). Dermoscopy. Retrieved August 1, 2020, from http://dermoscopic.blogspot.com/
46. Waterloo, U. (2019). Vision and image processing lab. Retrieved August 1, 2020, from https://uwaterloo.ca/vision-image-processing-lab/research-demos/skin-cancer-detection.
47. Thabit, R.; and Khoo, B.E. (2014c). A new robust reversible watermarking method in the transform domain. *Lecture Notes in Electrical Engineering*, 291, 161-168.