J Med Syst manuscript No.
(will be inserted by the editor)

Effective Management of Medical Information Through A Novel Blind Watermarking Technique

Sudeb Das · Malay Kumar Kundu

Received: 9 November 2011 / Accepted: 30 January 2012

Abstract Medical Data Management (MDM) domain consists of various issues of medical information like authentication, security, privacy, retrieval and storage etc. Medical Image Watermarking (MIW) techniques have recently emerged as a leading technology to solve the problems associated with MDM. This paper proposes a blind, Contourlet Transform (CNT) based MIW scheme, robust to high JPEG and JPEG2000 compression and simultaneously capable of addressing a range of MDM issues like medical information security, content authentication, safe archiving and controlled access retrieval etc. It also provides a way for effective data communication along with automated medical personnel teaching. The original medical image is first decomposed by CNT. The Low pass subband is used to embed the watermark in such a way that enables the proposed method to extract the embedded watermark in a blind manner. Inverse CNT is then applied to get the watermarked image. Extensive experiments were carried out and the performance of the proposed scheme is evaluated through both subjective and quantitative measures. The experimental results and comparisons, confirm the effectiveness and efficiency of the proposed technique in the MDM paradigm.

Keywords Digital Watermarking; Contourlet; Compression; Medical Imaging; EHR/PHR; DICOM.

Sudeb Das[1] and Malay Kumar Kundu[2]
Machine Intelligence Unit, Indian Statistical Institute
203 B.T.Road, Kolkata-108, India
Tel.: +91-33-2575-3100; Fax: +91-33-2578-3357
E-mail: [1]to.sudeb@gmail.com, [2]malay@isical.ac.in

1 Introduction

Due to its importance in clinical diagnosis, treatment, research and other commercial and non-commercial applications, both for private and government organizations, medical information is highly valuable and critical in nature. The rapid and significant advancements of information and communication technologies during the last few years have caused a sea change, both in concepts as well as in applications in MDM paradigm. The modern integrated health-care delivery systems (such as Hospital Management Systems (HISs), Picture Archiving and Communication Systems (PACS) etc.) provide easier access, effective manipulation and efficient distribution of medical information [1]. There are number of reasons for this medical information exchange, for example telemedicine applications (ranging from teleconsulting, telediagnosis and telesurgery etc.) to distant learning of medical personnel. Electronic Health Record (EHR)/ Personal Health Record (PHR) technology has replaced the inefficient paper records paradigm, and is available in various forms such as diagnostic reports, images and vital sign signals etc. It can also contain the health history information of a patient, such as demographic data, physical examination information, laboratory test results, treatment procedures, and prescriptions etc., which are highly confidential in nature [2].

On the other hand, these advances have introduced new risks for inappropriate use of medical information, given the ease with which digital form of data could be manipulated. Moreover, medical images have special characteristics and requirements. As well as, it is also concerned with legal and ethical issues, regarding the allowable operations and disclosures that can be undertaken on them, since any degradation of the quality of the images could result in misdiagnosis [3,4]. Therefore,

it is of paramount importance to prevent unauthorized access and manipulation of medical data, as well as to protect its confidentiality. As a result, there is a need to design a system for effective storage, controlled restriction of manipulation and access of medical information, keeping the authenticity, integrity and confidentiality requirements of medical data intact, for effective management purpose [3,5].

Digital watermarking (DWM), which imperceptibly embeds information (watermark) within a host signal (cover), such as image, audio or video, is an emerging research technique for multimedia data management [6]. Original motivation of this technique was to protect copyright, but it has also been applied to a wide range of other multimedia applications [7,28]. When it is applied to medical images, necessary steps are taken so that after watermark embedding, medical images can still conform to the DICOM format [8]. DWM has the potentiality of being a value-added tool for a wide range of issues related to medical data management [9,10].

As a subset of DWM, many MIW techniques have been proposed by various researchers. A spatial domain technique was proposed by Zain *et al.* [11] to improve the security of medical images by involving the ability to detect tamper and subsequently recover the images. A Region of Interest (ROI) lossless MIW technique with enhanced security and high payload embedding in the spatial domain was proposed by Kundu *et al.* in Ref. [12]. Chao *et al.*[13] proposed a DCT based data hiding scheme, capable of hiding EPR in the quantized DCT coefficients of an image. Wu *et al.*[14] proposed two schemes based on Modulo 256 and DCT, for tamper detection and recovery purpose. Recently few transform domain MIW methods have been proposed by various researchers based on Discrete Wavelet Transform (DWT) and Contourlet Transform (CNT) etc [15, 9,16,17]. Most of the existing MIW techniques are fragile and non-blind in nature. Moreover these existing methods lack the effective security measures required in the medical data management paradigm.

The very large number of medical images and related EHR/PHR data has created several problems regarding the effective management of medical information. The memory requirement to store these images and related data is ever increasing, so as the cost associated with it. Moreover, bandwidth is a valuable asset in network applications. The cost of transmission of this huge number of images and related EHR/PHR data is very high. Keeping these aforementioned issues in mind, in this paper we propose a novel blind MIW technique robust to high compression (both JPEG and JPEG2000). The proposed scheme can be used as an all-in-one solution tool to address various concerns like integrity, authenticity and confidentiality of the medical data management domain. It also conforms to the strict specifications and requirements regarding medical data handling by preserving their visual/information quality and diagnostic value. In the proposed method we hide EHR/PHR, Doctor's Identification Code (DIC), Indexing Keyword (INDX) and optionally ROI's information in the medical image. The confidentiality of the EHR/PHR is improved by embedding the data in the image. DIC works as a source authenticator and INDX serves as a querying keyword for use in medical image databases for effective image retrieval. If ROI's information is embedded in the image, then it works as a caption or annotation watermark which can be used for future reference, physician's guidance and/or teaching of medical personnel. In addition to that, both the storage and transmission bandwidth requirements as well as the possibility of EHR/PHR detachment are reduced.

The rest of the paper is organized as follows. In Section 2, we briefly describe the relevance of DWM techniques to medical data management paradigm. The contourlet transform is explained in Section 3. We outline in Section 4 the proposed watermark insertion and extraction algorithms. Experimental results and comparisons are presented in Section 5, and we draw conclusion in Section 6.

2 Digital Watermarking of Medical Images

DWM techniques have the potentiality of becoming an all-in-one solution tool, providing alternative and/or complementary solutions for a wide range of issues, related to medical information management and distribution. MIW is a subset of DWM, where medical information is embedded in medical images and/or videos.

2.1 Requirements

Due to the special characteristics, derived from strict ethics, legislative and diagnostic implications - integrity protection, confidentiality and prevention of unauthorized manipulation of medical information is very important. The risks are increased, when dealing with an open environment like the internet. This imposes three mandatory characteristics [3]:

- Confidentiality imposes that only the entitled users, in the normally scheduled conditions, have access to the information.
- Reliability has two different aspects :
  - Integrity : the information has not been modified by non-authorized persons, and

- Authentications : a proof that the information belongs indeed to the correct patient and is issued from the correct sources.
- Availability is the ability of an information system to be used by the entitled users in the normal scheduled conditions of access and exercise.

Another key requirement is that, the medical image should not undergo any degradation, which will affect the diagnosis from the image. Generally, medical images are required to remain intact to achieve this, with no visible alteration to their original form.

2.2 Applications

A brief outline of MIW applications in medical data management is as follows [9,18,3]:

2.2.1 Avoid Detachment

As the medical images and related EHR/PHR data are stored separately, the chance of corruption of these records or their detachment from the images is very high. Misplacing a data from its corresponding medical image may lead to a fiasco. Applying watermarking, this separate data can be embedded into the corresponding medical image, thus reducing the risk of detachment.

2.2.2 Saving Bandwidth

Transmission bandwidth is a valuable asset in network application. Since the EHR/PHR and the medical image is integrated into one by MIW, bandwidth for the transmission can be reduced in telemedicine applications.

2.2.3 Confidentiality and Security

Confidentiality and security of patient record, is of utmost importance in medical data management and distribution paradigm. Imperceptibility and key dependency of MIW with advanced encryption techniques, can provide solutions to these problems.

2.2.4 Controlling Integrity

Fragile watermark is used for integrity verification and tamper localization. As the integrity of medical data (images, records) is of paramount importance, fragile watermarking technique can be used in this scenario. Fragile MIW techniques, allow us to evaluate the extent of tampering, localization of the modified regions, and help us to determine whether the data are trustworthy for use or not [11].

2.2.5 Authentication

Combined with cryptographic techniques, MIW provides a means of identity authentication, by embedding the encrypted version of the physician's or clinician's digital signature (DS) or identification code, in the medical image. To obtain the original data, knowledge of both encryption technique and watermark keys are required, which provides more complete protection [13].

2.2.6 Indexing

Watermark can also play the role of keywords or indices (e.g., USG-LA), based on which effective archiving and retrieval from querying mechanism could take place. PACS nowadays retrieve images through indexing. Patient demographics, image acquisition characteristics, diagnostic codes etc. can be used as the indices or keywords. This can also eliminate the extra storage and transmission bandwidth requirements [19].

2.2.7 Controlling Access

In MIW, EHR/PHR/DICOM metadata are embedded in the image in such a way, which gives permanency and more protection than in the case of simple metadata. This is because; access to them is only possible through the use of proper key. In this way, MIW has the potential of becoming an alternative access control mechanism, since different keys might reveal different information [3].

2.2.8 Captioning

Caption or annotation watermarks can also be used for providing additional valuable information about the patient's report. ROIs in an medical image can also be highlighted through descriptive watermarks for future reference, physicians' guidance or teaching of medical personnel.

The above discussion shows the potentialities of MIW as an all-in-one solution tool, and also describes the strict requirements of the medical image management paradigm. A MIW technique addressing the aforementioned issues is described in this paper.

3 Contourlet Transform (CNT)

The major drawback of DWT in two dimensions is their limited ability in capturing directional information. In light of this, Do and Vetterli [20] developed the CNT, based on an efficient two-dimensional multiscale and directional filter bank (DBF). CNT not only possess

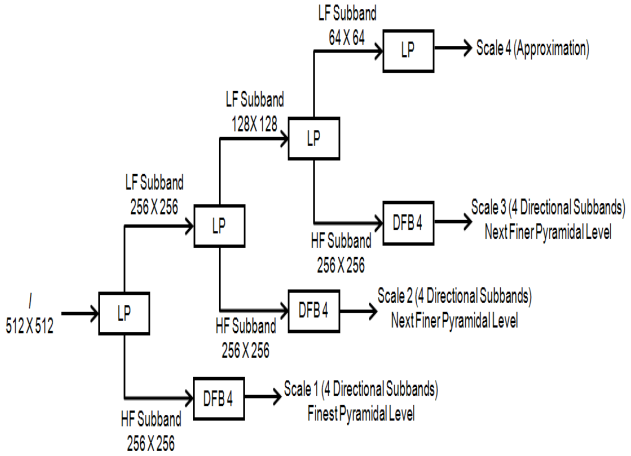


Fig. 1 Flowchart of contourlet transform for a 512 × 512 image.

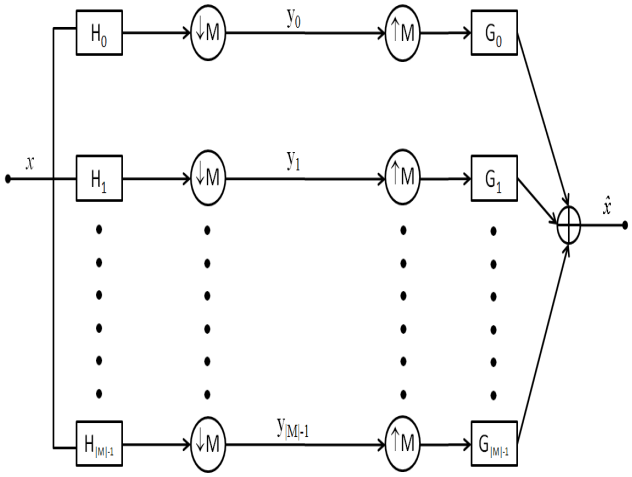


Fig. 3 Construction of DBF.

the main features of DWT, but also offer a high degree of directionality and anisotropy. It allows for different and flexible number of directions at each scale, while achieving nearly critical sampling. In addition, CNT uses iterated filter banks, which makes it computationally efficient ($O(N)$ operations for an N-pixels image).

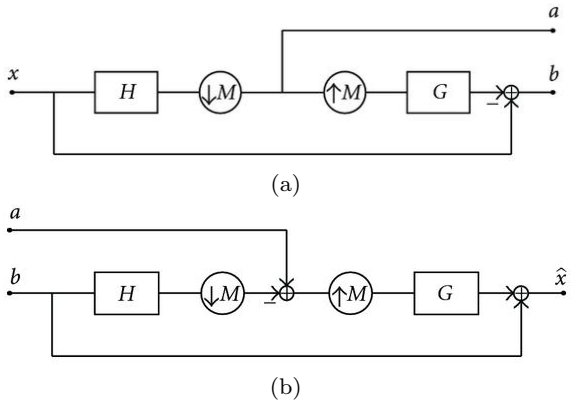


Fig. 2 Laplacian pyramid scheme: (a) Analysis and (b) Synthesis.

CNT gives a multiresolution, local and directional expansion of image using Pyramidal Directional Filter Bank (PDFB). The PDFB combines Laplacian Pyramid (LP) which captures the point discontinuities, with a DFB which links these discontinuities into linear structures. Figure 1, shows the flowchart of CNT for a 512 × 512 image. As shown in Figure 1, first stage of CNT is LP decomposition and DFB is the second stage.

LP scheme is shown in Figure 2. Here, the input image x is first lowpass filtered by analysis filter H and then downsampled to produce a coarse approximation a. It is then interpolated and passed through the synthesis filter G. The resulting image is subtracted from the original image x to obtain the bandpass image b. This process can be iterated repeatedly on the coarser version of the image a. LP is a multiscale decomposition of $L^2(R^2)$ into series of increasing resolution subspaces which are orthogonal complements of each other as follows [21]:

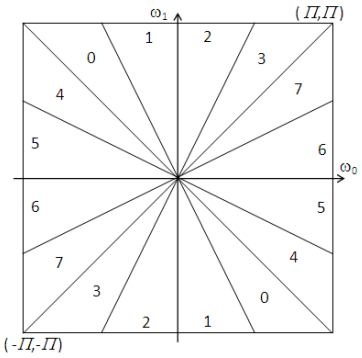
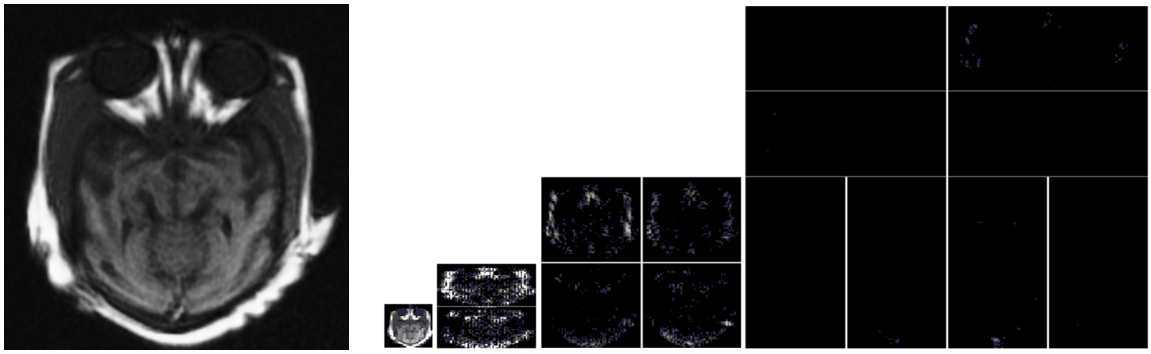


Fig. 4 Frequency partition of contourlet transform.

$$L^2(R^2) = V_{j_0} \oplus \left(\bigoplus_{j=J_0}^{-\infty} W_j\right) \tag{1}$$

where V_{j_0} is the approximation subspace at the scale 2^{j_0}, W_j is the detail in the finer scale 2^{j-1}. In the LP, each subspace W_j is spanned by a frame $\mu_{j,n}(t)_{n\epsilon Z^2}$ that utilizes a uniform grid on R^2 of intervals $2^{j-1} \times 2^{j-1}$.

In 1992, Bamberger and Smith constructed a 2D DFB that can be maximally decimated while achieving perfect reconstruction [22]. It is used in the second stage of CNT to link the edge points into linear structures,



(a) (b)

Fig. 5 Contourlet Transform : (a) Original Image and (b) Subbands after decomposition.

which involves modulating the input image and using quincunx filter banks (QFB) with diamond-shaped filters. A l-level tree-structured DFB is equivalent to a 2^l parallel channel filter bank with equivalent filters and overall sampling matrices as shown in Figure 3. As shown in Figure 3, corresponding to the subbands indexed, the equivalent analysis and synthesis filters are denoted using H_k and G_k, $0 \leq k < 2^m$.

A l-level DFB generates a perfect directional basis for discrete signal in $l^2(Z^2)$ that is composed of the impulse responses of 2^l directional synthesis filters and their shift. They can be represented as follows:

$$g_k^{(l)}[n - S_k^{(l)} n]_{0 \leq k < 2^l, n \epsilon Z^2} \tag{2}$$

$$g[n] = \frac{2\Pi}{n_1}[\psi(\frac{n_1(l+1)}{N} + n_2) - \psi(\frac{n_1 l}{N} + n_2)] \tag{3}$$

where $N = 2^{n-2}$ and $\psi(x)$ is similar to the common *sin* function.

$$\psi(x) = \frac{1 - cos(\pi x)}{\pi x} \tag{4}$$

In CNT, applying a l_j-level DBF to the detail subspace W_j results in a decomposition with 2^{l_j} directional subspaces as follows:

$$W_j = \bigoplus_{k=0}^{2^{l_j - 1}} W_{j,k}^{l_j} \tag{5}$$

A DFB is designed to capture the high frequency content like smooth contours and directional edges. Figure 4, shows the frequency partition of CNT, and Figure 5(a)-(b), presents an image along with its subbands after decomposition by CNT.

4 Proposed Scheme

The watermark insertion and extraction algorithms are described in this section. Block diagrams of both the insertion and extraction methods are also given to clarify these schemes.

4.1 Watermark Insertion

As mentioned earlier, that we can embed EHR/PHR (refereed in this paper as EPR), DIC, INDX and optionally ROI's information in the medical image. If the user wants to embed ROI's information, then the user first manually draw a polygonal ROI in the medical image. We use a polygonal ROI because in most of the cases the ROI is irregular in shapes. A polygon can be fully described by its number of vertices (V_n) and their coordinates $\{v_i(x, y) : v_i$ is the i-th vertex at coordinate (x, y) and $i = 1, 2, ..., V_n\}$. So ROI's information contains these V_n and $\{v_i(x, y) : v_i$ is the i-th vertex at coordinate (x, y) and $i = 1, 2, ..., V_n\}$. The salient steps of the insertion process are as follows:

Inputs: Original Medical Image (OI) of size $M \times N$, EPR, DIC, IDX, Secret Key (K_S) and optionally ROI's Information (ROI_{INFO}).

Outputs: Watermarked image (WI), Modified secret key (K_S').

Steps:

1. Apply CNT on the original image OI to get low pass subband (OI_{LPS}) and high pass subbands (OI_{HPSs}). Let the size of OI_{LPS} be $S \times T$.
2. Encrypt the EPR by Advanced Encryption Standard (AES) method using a secret key K_S to get EPR_{ENCRY} (the EPR is encrypted to increase the security of the proposed scheme).
3. If $V_n > 2$, then concatenate ROI_{INFO}, DIC, $INDX$, EPR_{ENCRY} to WM_{CON} and represent WM_{CON} to its binary form as WM_{BIN} and set $ROI = 1$. If

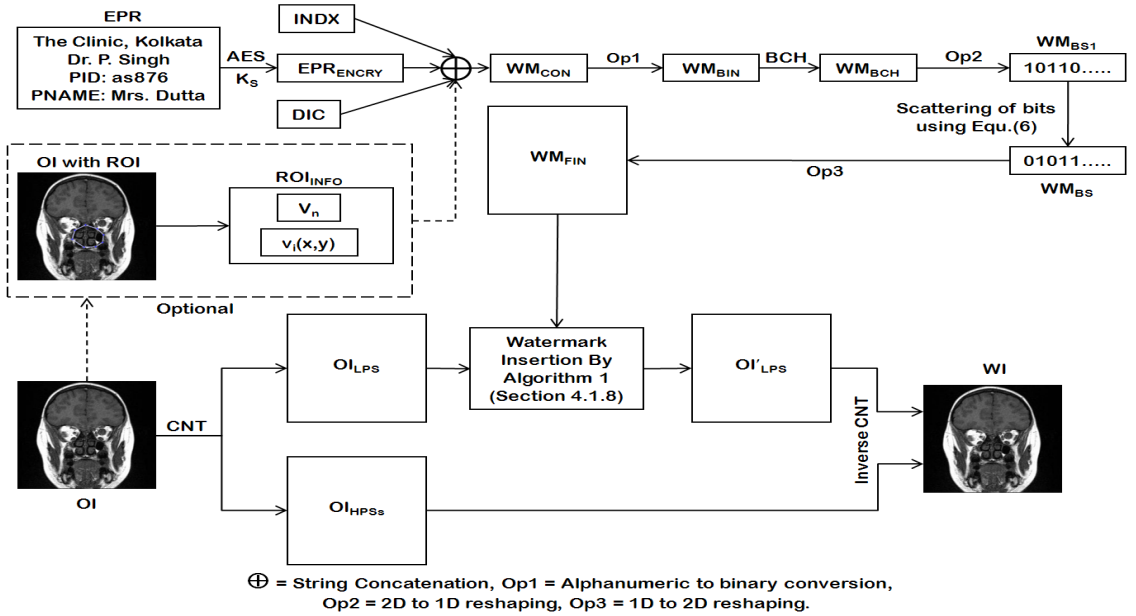


Fig. 6 Watermark Insertion.

no ROI's information is present or $V_n \leq 2$, then construct WM_{BIN} from DIC, $INDX$ and EPR_{ENCRY} and set $ROI = 0$.

4. If $ROI = 1$, then modify the secret key K_S to K'_S by concatenating 1 to K_S. Otherwise, if $ROI = 0$ (i.e., no ROI), then concatenate 0 with K_S to get K'_S. (As an example, if K_S = 'xxxxxxxx' and $ROI = 1$ then K'_S = 'xxxxxxxx1', otherwise K'_S = 'xxxxxxxx0'.)
5. Apply Bose, Chaudhuri and Hocquenghem (BCH) error correcting code to WM_{BIN} to get WM_{BCH}.
6. Reshape WM_{BCH} as a 1D-binary string (WM_{BS1}) and scatter the bits of WM_{BS1} using the function given below to get (WM_{BS}) :

$$f(x) = px \ mod \ n + 1 \tag{6}$$

where,
n = size of the subband $OI_{LPS} (= S \times T)$;
p = secret prime number ϵ $[1, n]$;
x = bit position in WM_{BS1} and
$x \ \epsilon \ [1, length(WM_{BS1})]$;
(This scattering of bits improves the security of the proposed scheme, as to correctly extract the watermark bits, one should have knowledge about the used scattering function (Equation 6), as well as the value of p.)

7. Reshape the resultant string in a matrix of equal size as OI_{LPS} (i.e., $S \times T$) to get the final watermark payload WM_{FIN}.
8. Modify the coefficients of OI_{LPS} using the algorithm given below:

Algorithm 1 : Modifying the coefficients of OI_{LPS}

```
for i = 1 to S do
  for j = 1 to T do
    r(i,j) = round(OI_LPS(i,j) / α)
    if mod((r(i,j) + WM_FIN(i,j)), 2) = 1 then
      OI'_LPS(i,j) = [r(i,j) + 1] * α
    else
      OI'_LPS(i,j) = OI_LPS(i,j)
    end if
  end for
end for
```

where,
OI'_{LPS} = modified low pass subband,
(i, j) = co-ordinates of the coefficients,
$round(\bullet)$ = rounding operation, and
α = watermarking strength factor. The robustness as well as the imperceptibility of the proposed MIW scheme depends on α. If it is high, the robustness is high, however, the image quality is worse and the vice versa.

9. Finally to get the watermarked image WI, apply Inverse CNT on the OI'_{LPS}, along with other non-modified directional subbands (OI_{HPSs}).

The block diagram of the proposed watermark insertion method is given in Figure 6. The dashed lines in the Figure 6, indicates that these activities are optional.

4.2 Watermark Extraction

Blind watermarking is very useful for real-life application, as often access to the original un-watermarked

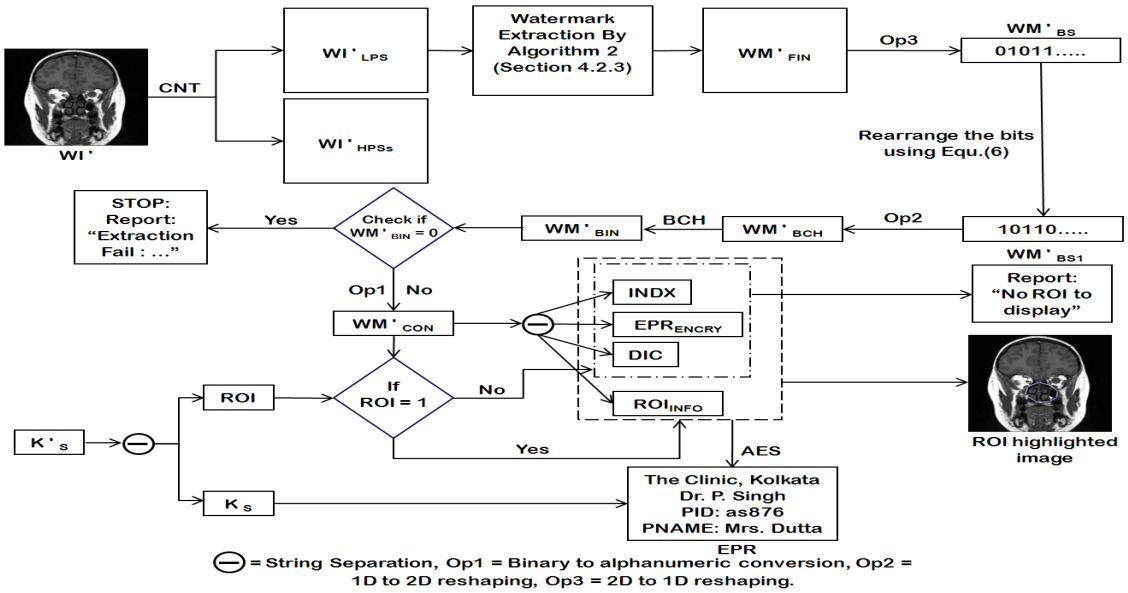


Fig. 7 Watermark Extraction.

image is restricted to maintain the privacy, security, integrity etc. Keeping this in mind, we have tried to make our proposed MIW technique blind, which means we do not need the original image during the extraction process. The steps of the extraction process are as follows:

Inputs: Watermarked (and possibly attacked) Medical Image (WI') of size $M \times N$ and Secret Key (K'_S).

Outputs: Extraction Report, EPR, DIC, INDX, and ROI highlighted medical image (optional).

Steps:

1. Separate K'_S to two parts, K_S and ROI.
2. Apply CNT on WI' with the same decomposition configuration of the embedding process, to get the low pass subband (WI'_{LPS}) of size $S \times T$ and high pass subbands (WI'_{HPSs}).
3. Extract the watermark WM'_{FIN} using the following rules:

Algorithm 2 : Extraction of watermark WM'_{FIN}

```
for i = 1 to S do
  for j = 1 to T do
    r(i,j) = round(WI'_LPS(i,j) / α)
    if mod((r(i,j),2)) = 1 then
      WM'_FIN(i,j) = 1
    else
      WM'_FIN(i,j) = 0
    end if
  end for
end for
```

4. Reshape WM'_{FIN} as a binary string WM'_{BS} and rearrange the bits to their original positions using the Equation 6, to get WM'_{BS1}.
5. Reshape WM'_{BS1} to WM'_{BCH} and apply BCH error correcting procedure on WM'_{BCH}, to get WM'_{BIN}. Now if WI' is the original watermarked image (i.e., $WI' = WI$) or, WI' is a modified watermarked image where modification level is such that, the BCH error correcting procedure can correctly rectify the errors due to this modification, then the output of BCH error correcting process will be $WM'_{BIN} = WM_{BIN}$. Otherwise, BCH will not be able to rectify the errors correctly and will provide output as $WM'_{BIN} = 0$.
6. If $WM'_{BIN} = 0$, then stop the process and report the result: "Extraction Fail: Un-watermarked image or modification level exceed maximum acceptable level". Otherwise, transform WM'_{BIN} to its original format WM_{CON} and go to step 6.
7. Now check if $ROI = 1$, then separate WM_{CON} to ROI_{INFO}, DIC, $INDX$, and EPR_{ENCRY}, otherwise, if $ROI = 0$, then separate WM_{CON} to DIC, INDX, and EPR_{ENCRY}.
8. Decrypt EPR_{ENCRY} using the same secret key K_S to get the original EPR.
9. If $ROI = 0$, then report "No ROI to display". Otherwise if, $ROI = 1$, then the algorithm automatically draws the polygonal ROI using the ROI_{INFO}.

Figure 7, shows the block diagram of the proposed MIW extraction procedure.

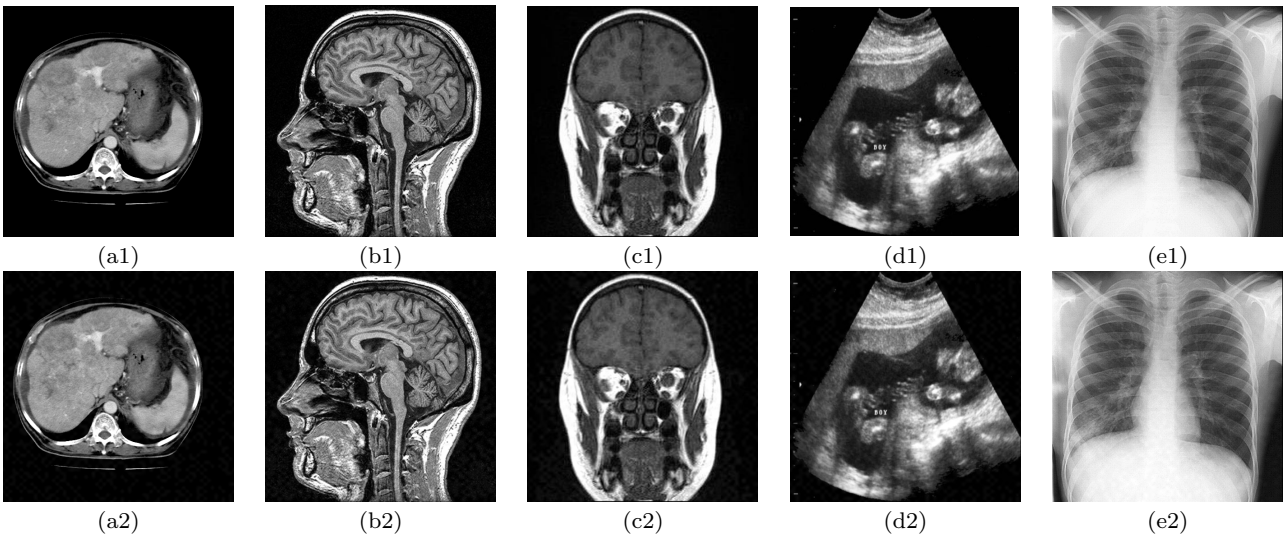


Fig. 8 Original images (above ((a1)-(e1)) and their corresponding watermarked images (below ((a2)-(e2)).

5 Experimental Results and Comparisons

To evaluate the performance effectiveness of the proposed MIW method, extensive experiments were carried out on various modalities (CT, MRI, USG, X-Ray etc.) of grayscale (8 bpp) medical images of size 512×512. The DIC and $INDX$ consisted of 20 ($20 \times 7 = 140$ bits) and 15 ($15 \times 7 = 105$ bits) characters respectively. EHRs/PHRs of different sizes (128 and 144 characters) were used in the experiments, along with two different configurations for BCH error correcting process. EHR/PHR of size 128 characters with BCH(255,115,21) was used in case when ROI's information was specified, and in case of no ROI, EHR/PHR of size 144 characters with BCH(255,139,15) was used. After three level CNT (2,4,8) decomposition of the image with '9-7' pyramid filter and 'pkva' directional filter, the size of the low pass subband was 64×64. We used $p = 23$ in the Equation 6. The value of α was set to 55 after lots of experiments. We implemented the proposed technique in MATLAB, and experiments were carried out on a PC with 2.66 GHz CPU and 4 GB RAM.

To show the effectiveness of the proposed MIW technique both subjective as well as quantitative analysis were carried out. We used Peak Signal-to-Noise Ration (PSNR) and Weighted PSNR (WPSNR) to measure the distortion produced after watermark embedding. The higher the value of PSNR and WPSNR, the lower the distortion. Mean Structural SIMilarity index (MSSIM) was used to measure the similarity between the original image and the watermarked image [23]. MSSIM value 1 indicates that the images are similar. Visual degradation was quantitatively measured using the Total Perceptual Error (TPE) measurement calculated from the Watson Metric [24]. Lower the value of TPE, better the result. The conventional measures used for authentication of the extracted watermark like Normalized Correlation (NC), Bit Error Rate (BER) etc., are not applicable to our proposed method. The proposed scheme, can successfully extract the embedded watermark without any error, from the original watermarked image or a modified watermarked image, where the modification level is below a maximum acceptable modification amount. Otherwise, if an un-watermarked image or a modified watermarked image, where the modification level exceed the maximum acceptable modification amount, is used during the extraction process, then the proposed scheme will give output: "Extraction Fail: Un-watermarked image or modification level exceed maximum acceptable level". Therefore, NC and/or BER are not suitable to evaluate the performance of the proposed technique.

An expert clinician was asked to subjectively evaluate the effectiveness of the proposed MIW method. After careful manual inspection, the clinician conformed to the effectiveness of the proposed scheme. He found no significant visual difference between the original and the watermarked medical images, which suggests that there is no noticeable visual and/or informational degradation in the watermarked images.

Figure 8, shows the visual effect of watermark insertion in some of the test medical images used in the experiments. The results show that there is no significant visual difference between the original and the watermarked images.

Table 1, shows the PSNR, WPSNR, MSSIM and TPE values, when no ROI was specified. The PSNR

and WPSNR values of the different test medical images show that, the visual differences between the original and the watermarked images are very low. Acquired values for MSSIM indicate that the original and the watermarked images are very much similar. The low values for TPE suggests that, the visual degradation caused by the proposed method is also very low.

Table 1 Performance when no ROI is specified

Image	PSNR	WPSNR	MSSIM	Watson's Metric (TPE)
abdomeCT	34.8498	35.952	0.7887	0.19
cthead	34.3799	35.982	0.9054	0.10
mriBrain	34.0404	37.159	0.9344	0.08
usg	34.6249	36.412	0.8932	0.14

Performance of the proposed scheme in case when ROI was specified is shown in Table 2, for the same set of test images, which were used to produce the results of Table 1. During this performance evaluation, a polygonal ROI having 10 vertices were used for all the test images. From Table 1 and Table 2, we can see that the values of PSNR, WPSNR, MSSIM and TPE differs very slightly, which indicates that the proposed method perform equally well in both the cases when ROI is specified or not.

Table 2 Performance when ROI is specified

Image	PSNR	WPSNR	MSSIM	Watson's Metric (TPE)
abdomeCT	34.5594	35.583	0.7703	0.20
cthead	34.3763	35.970	0.9007	0.11
mriBrain	34.0338	37.117	0.9343	0.08
usg	34.5218	36.214	0.8838	0.14

In the proposed MIW scheme the watermark is embedded in the low pass subband (LPS) of the medical images, after 3 level of contourlet decomposition. The size of the original image and LPS is 512×512 and 64×64 respectively. So the maximum payload capacity of the proposed method is $(64 \times 64)/(512 \times 512) = 0.0156$ bpp. But if we embed this maximum amount of watermark payload in the image by our proposed medical image watermarking technique, the watermarked image would be unacceptably distorted. The watermark to be embedded consists of DIC, INDX, EHR/PHR and optionally ROI Information. If ROI is specified then the size of the embedded watermark is 1369 bits and incase when ROI is not specified, then the size of the embedded watermark is 1253 bits. So the hiding capacity of the proposed scheme considering acceptable distortion is 0.0052 bpp (with ROI) or 0.0047 bpp (without ROI).

As mentioned previously that the value of α determines the robustness and imperceptibility of the proposed MIW scheme. The higher the value of α, the more robust the method is, and the imperceptibility becomes low. The reverse is also true. The graph of the Figure 9, shows the variation of image quality (in terms of PSNR in dB) with respect to watermarking strength factor α of the proposed technique for a particular test medical image (abdomenCT Figure 8(a1)). Similar results have been found for other test images used in the experiments.

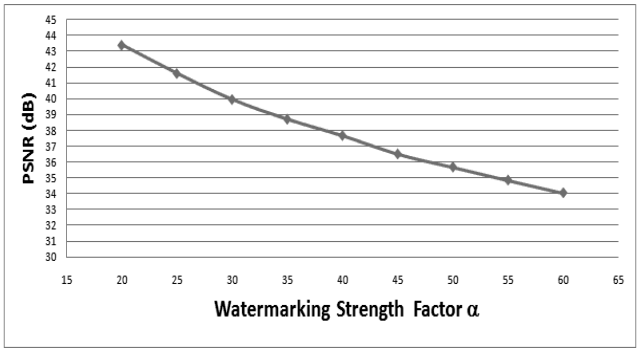


Fig. 9 Watermarking strength factor α vs PSNR (dB).

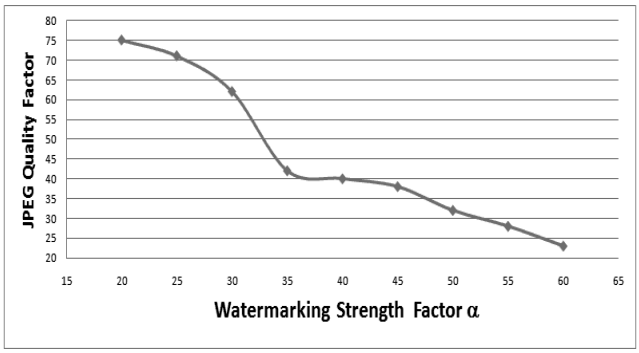


Fig. 10 Watermarking strength factor α vs JPEG Quality Factor.

To evaluate the effectiveness of the proposed MIW method against JPEG compression, different watermarking strength factors α were used and the watermarked images were JPEG compressed with different quality factors (high quality factor indicates low compression and better image quality and low quality factor means high compression and worse image quality). The graph of the Figure 10, indicates the effectiveness of the proposed MIW scheme for a particular test medical image (abdomenCT Figure 8(a1)). In the graph of the Figure 10, the JPEG quality factor at a certain α denotes the highest JPEG compression, that can be achieved

Table 3 Attacks where the proposed method successfully extracted the watermark

Attack	Parameters
Copy Attack	——
Gaussian Filtering1	3×3 window
Gaussian Filtering2	5×5 window
Mean Filtering	3×3 window
Median Filtering	3×3 window
Trimmed Mean Filtering	7×7 window, 2 samples trimmed
Wiener Filtering	3×3 window
Hard Thresholding	3×3 window
Sample Down Up1	Downsample factor 0.75, Upsample factor 1.333
Sample Down Up2	Downsample factor 0.50, Upsample factor 2.000
Template Removal	——
Salt & Pepper Noise	Noise Density = 0.002
Speckle Noise	Mean = 0, Var = 0.004

with that α, without any error in the extracted watermark. For the other test images used in the experiments, similar results have been obtained.

We used Checkmark benchmark software [25], to evaluate the performance of the proposed MIW method in case of JPEG2000 compression. The watermarked images were compressed with varying bitrates using JPEG2000 wavelet compression (the JASPER compression program) as mentioned in the Checkmark benchmark. We compressed the watermarked images using bit rates [8,3.5,1.5,0.8,0.6,0.5,0.4,0.3,0.2]. It has been found that the proposed method can successfully extract the embedded watermark in all the cases.

Even though, the main motivation of the proposed MIW scheme is to resists high compression attacks (both JPEG and JPEG2000), we also tested the robustness of the proposed method against other watermark attacks (mostly using Checkmark benchmark software and some others). The performance of the proposed scheme is given in Table 3, which shows only the attacks (with parameters) where the proposed method successfully extracted the inserted watermark.

Comparison with Ref.[16] reveals that, the method is more imperceptible (in terms of PSNR), but less robust than our scheme. In Ref.[16] only the ROI of the image can be embedded, but no EHR/PHR or DIC or INDX. If the method of Ref.[16] is used to insert EHR/PHR, DIC and INDX, it will not be able to extract the watermark without error, even with a small JPEG compression. Comparison with Ref.[15] shows that, our method is more imperceptible (in terms of PSNR) and also more robust. The MIW methods described in Refs.[15, 16] are non-blind, that means the original un-watermarked medical image is needed for correct extraction of the watermark. Whereas, our proposed scheme is blind, which makes it suitable for real-life applications. The watermarking technique described in Ref. [26] is less secured and needs a reference image of size 128×128 for blind extraction of the embedded watermark. Whereas, in our proposed scheme we only need the secret key during watermark extraction. The hiding capacity of our proposed method (0.0052 bpp (with ROI) or 0.0047 bpp (without ROI)) is higher than the hiding capacity (0.0036 bpp) of the scheme described in Ref. [26]. Moreover, the MIW technique of Ref. [26], is less robust against JPEG compression attack (up to quality factor $80\% - 75\%$) and no result is given against JPEG2000 compression. Comparison with the method of Ref. [27] shows that both the hiding capacity (0.0077 bpp) and imperceptibility in terms of PSNR (60 dB) is higher than our proposed method. But, the scheme of Ref. [27] is less robust against various watermarking attacks than our proposed scheme. Also, the scheme of Ref. [27] is not robust against JPEG and JPEG2000 compression. Our proposed MIW technique is also much more secure than the methods described above. The use of EHR/PHR encryption by AES with a secret key makes the EHR/PHR secured, which is very much required, as EHR/PHR is highly confidential, critical as well as sensitive in nature. Also the scattering of watermark bits in the embedding region makes the proposed scheme safe and protected.

6 Conclusion and Discussion

To address various issues regarding effective management of digital medical images and related EHR/PHR data, MIW methods have recently emerged as an effective tool. In this paper, we have presented a blind, robust watermarking scheme applied to medical images with good imperceptibility and enhanced security, which can be used as an all-in-one solution tool. The proposed method is not only robust against both high JPEG and JPEG2000 compression, but also can resists a large number of other attacks. Our scheme can be

used for different medical image modalities. The experimental results indicate that the proposed scheme is feasible and given its relative simplicity, it can be applied to the medical images at the time of acquisition to serve in many medical applications concerned with authenticity, integrity and confidentiality. Some of the future scopes of the proposed scheme are listed below:

1. As mentioned earlier, that the value of α plays a vital role in performance of the proposed method. The value of α was experimentally set in the proposed scheme. It would be better if the value of α can be set adaptively and automatically.
2. Other transforms like curvelet, bandlet, ripplet etc. can be tested to improve the result.
3. Different insertion and extraction rules can be used to improve the imperceptibility as well as robustness of the proposed technique.

We are trying to incorporate all these above mentioned aspects to our proposed scheme to improve the performance.

Acknowledgements The authors thank the editor and the anonymous reviewers for their careful work and valuable suggestions.We would also like to thank Machine Intelligence Unit, Indian Statistical Institute, Kolkata-108 (Internal Academic Project) for providing facilities to carry out this work. We are grateful to Dr. Pradip Kumar Das (Dept. of Radiology, Sonoscan Healthcare (P) Limited, Malda, West Bengal) for the subjective evaluation of the watermarked images.

References

[1] E. L. Siegel and R. M. Kolodner, *Filmless Radiology*, Springer, New York, (1999).

[2] S. Kaihara, *Realization of the computerized patient record; relevance and unsolved problems*, International Journal of Medical Informatics, 1:49 (1998), pp. 1–8.

[3] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, *Relevance of Watermarking in Medical Imaging*, in Proc. IEEE EMBS Information Technology Applications in Biomedicine, (2000), pp. 250–255.

[4] G. Coatrieux, H. Maitre and B. Sankur, *Strict integrity control of biomedical images*, in Proc. SPIE Security Watermarking Multimedia Contents III, 4314 (2001), pp. 229–240.

[5] N. V. Rao and V. Meena Kumari, *Watermarking in Medical Imaging for Security and Authentication*, Information Security Journal: A Global Perspective, 20:3 (2011), pp. 148–155.

[6] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, *Information hiding - a survey*, in Proc. IEEE Special issue on protection of multimedia content, 87:7 (1999), pp. 1062–1078.

[7] I. J. Cox and M. L. Miller, *The first 50 years of electronic watermarking*, EURASIP Journal on Applied Signal Processing - Emerging applications of multimedia data hiding, 2002:2 (2002), pp. 126–132.

[8] X. Guo and TG. Zhuang, *A Region-Based Lossless Watermarking Scheme for Enhancing Security of Medical Data*, Journal of Digital Imaging, 22:1 (2009), pp. 53–64.

[9] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris, *Multiple image watermarking applied to health information management*, IEEE Trans Inf Technol Biomed., 10:4 (2006), pp. 722–732.

[10] M. Nergui, U. S. Acharya, R. Acharya U and W. Yu, *Reliable and Robust Transmission and Storage Techniques for Medical Images with Patient Information*, Journal of Medical Systems, 34:6 (2010), pp. 1129–1139.

[11] J. M. Zain and A. R. M. Fauzi, *Medical Image Watermarking with Tamper Detection and Recovery*, in Proc. of the 28th IEEE EMBS Annual International Conference, (2006), pp. 3270–3273.

[12] M. K. Kundu and S. Das, *Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding*, in Proc. International Conference on Patter Recognition, (2010), pp. 1457–1460.

[13] H. M. Chao, C. M. Hsu and S. G. Miaou, *A data-hiding technique with authentication, integration, and confidentiality for electronic patient records*, IEEE Trans. on Information Technology in Biomedicine, 6:1 (2002), pp. 46–53.

[14] J. H. Wu, R. F. Chang, C. J. Chen, C. L. Wang, T. H. Kuo, W. K. Moon and D.-R. Chen, *Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique*, Journal of Digital Imaging, 21:1 (2008), pp. 59–76.

[15] T. Manasrah and A. Al-Haj, *Management of medical images using wavelets-based multi-watermarking algorithm*, in Proc. International Conference on Innovations in Information Technology, (2008), pp. 697–701.

[16] H.-K. Lee and H.-J. Kim and K.-R. Kwon and J.-K. Lee, *ROI Medical Image Watermarking Using DWT and Bit-plane*, in Proc. Asia-Pacific Conf. Communica., (2005), pp. 512–515.

[17] Sudeb Das and Malay Kumar Kundu, *Hybrid Contourlet-DCT Based Robust Image Watermarking Technique Applied to Medical Data Management*, in Proc. 4th International Conference on Pattern Recognition and Machine Intelligence, (2011), pp. 286–292.

[18] K. A. Navas and M. Sasikumar, *Survey of Medical Image Watermarking Algorithms*, in Proc. Internation Conf. Sciences of Electronics, Technologies of Information and Telecommunications, (2007), pp. 25–29.

[19] G. P. Robinson, H. D. Tagare, J. S. Duncan, and C. C. Jaffe, *Medical image collection indexing: Shape-based retrieval using KD-trees*, Comut. Med. Image. Graph., 20:4 (1996), pp. 209–217.

[20] M. N. Do and M. Vetterli, *The Contourlet Transform: An Efficient Directional Multiresolution Image Representation*, IEEE Transactions on Image Processing, 14:12 (2005), 2091–2106.

[21] P. J.Burt and E. H. Adelson, *The Laplacian pyramid as a compact image code*, IEEE Transactions on Communications, 31:4 (1983), pp. 532–540.

[22] R. H. Bamberger and M. J. T. Smith, *A filter bank for the directional decomposition of images: theory and design*, IEEE Transactions on Signal Processing, 40:4 (1992), pp. 882–893.

[23] Zhou Wang and Alan C. Bovik and Hamid R. Sheikh and Eero P. Simoncelli, *Image Quality Assessment: From Error Visibility to Structural Similarity*, IEEE Transactions on Image Processing, 13:4 (2004), pp. 600–612.

[24] Andrew B. Watson, *DCT quantization matrices visually optimized for individual images*, in Proc. SPIE : Human Vision, Visual Processing and Digital Display IV, 1913 (1993), pp. 202–216.

[25] S. Pereira, S. Voloshynovskiy, M. Madueno, S. M.-Maillet and T. Pun, *Second Generation Benchmarking and Application Oriented Evaluation*, in Proc. of the 4th International Workshop on Information Hiding, IHW '01 (2001), pp. 340–353.

[26] S. A. K. Mostafa, N. E. El-sheimy, A. S. Tolba, F. M. Abdelkader and H. M. Elhindy, *Wavelet Packets-Based Blind Watermarking for Medical Image Management*, Open Biomed Eng. J., 4 (2010), pp. 93–98.

[27] F. Rahimi and H. Rabbani, *A dual adaptive watermarking scheme in contourlet domain for DICOM images*, BioMedical Engineering OnLine, 10:53 (2011), pp. 1–18.

[28] W.-T. Huang, S.-Y. Tan, Y.-J. Chang and C.-H. Chen, *A Robust Watermarking Technique for Copyright Protection Using Discrete Wavelet Transform*, Journal of WSEAS Transactions on Computers, 9:5 (2010), pp. 485–495.