Effective Management of Medical Information through ROI-Lossless Fragile Image Watermarking Technique

Sudeb Das[1], Malay Kumar Kundu

Machine Intelligence Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata-108

Abstract:

In this article, we have proposed a blind, fragile and Region of Interest (ROI) lossless medical image watermarking (MIW) technique, providing an all-in-one solution tool to various medical data distribution and management issues like security, content authentication, safe archiving, controlled access retrieval and captioning etc. The proposed scheme combines lossless data compression and encryption technique to embed electronic health record (EHR)/DICOM metadata, image hash, indexing keyword, doctor identification code and tamper localization information in the medical images. Extensive experiments (both subjective and objective) were carried out to evaluate performance of the proposed MIW technique. The findings offer suggestive evidence that the proposed MIW scheme is an effective all-in-one solution tool to various issues of medical information management domain. Moreover, given its relative simplicity, the proposed scheme can be applied to the medical images to serve in many medical applications concerned with privacy protection, safety, and management etc.

Keywords:

Electronic Health Record, Personal Health Record, DICOM, Security, Privacy, Watermarking

[1] Corresponding author.
E-mail addresses: to.sudeb@gmail.com (S. Das), malay@isical.ac.in (M. K. Kundu)

1. Introduction

Medical information is highly valuable and critical due to its importance in clinical diagnosis, treatment, research, education and other commercial/non-commercial applications, both for private and government organizations. During the last few years, due to the rapid and significant advancements of information and communication technologies medical data distribution and management systems have undergone a significant change, both in concepts as well as in applications. Hospital Information System (HIS) and Picture Archiving and Communication Systems (PACS) based on The Digital Imaging and Communications in Medicine (DICOM) standard (as advised by National Electrical Manufacturers Association (NEMA)), form the base of the modern integrated and sophisticated health-care delivery systems [1]. These systems provide easier access, effective manipulation and efficient distribution of medical information between hospitals. There are number of reasons for this medical information exchange, for example telemedicine applications (ranging from tele-consulting, tele-diagnosis and tele-surgery etc.) to distant learning of medical personnel [2]. Electronic health record (EHR) 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 [3].

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 [4, 5]. Therefore, it is of paramount importance to prevent unauthorized access and manipulation of medical data, as well as to protect its confidentiality. These result in 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 [4-7].

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 [8]. Original motivation of this technique was to protect copyright, but it has also been applied to a wide range of multimedia applications [9, 10]. 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 [11]. DWM techniques have the potentiality of becoming an all-in-one solution tool providing alternative and/or complementary solutions for a wide number of issues related to medical information management and distribution [4-7].

Many medical image watermarking schemes were proposed during the last few years [11-29]. In [13] Chao et al. have proposed a secure data-hiding technique based on the bipolar multiple-base conversion to allow a variety of EHR data to be hidden within the same mark image. This is different from the conventional encryption methods in which information or digital signatures are appended to the message separately. Two schemes of interleaving patient information (text and graphical signal) in medical images were proposed by Acharya et al. [14, 16]. In [14], the authors have showed that reliability of transmission and storage of medical images interleaved with patient information by least significant bit (LSB) plane replacement scheme, over noisy channel can be enhanced using suitable error correction techniques. The other technique proposed by Acharya et al. in [16] is based on interleaving the texts and graphical signals in the last bits of discrete cosine transform (DCT) coefficients from the middle frequency

range onwards. The blind MIW method described in [17] by Zain et al., is reversible and is used for authentication of DICOM images with good imperceptibility. This scheme is based on Region of Interest (ROI) and works in spatial domain. Woo et al. have proposed a multiple watermark method for privacy control and tamper detection in medical images with good imperceptibility [18]. In this scheme, an annotation watermark consisting encrypted patient information and a digital signature of the medical practitioner is embedded into the border pixels of images by discrete wavelet transform (DWT) based robust watermarking method. For integrity checking and tamper detection a tiled fragile binary watermark pattern is embedded in the LSB plane. In [21], Wu et al. have proposed two block based schemes for tamper detection and recovery using an adaptive robust watermarking technique with the modulo operation. Guo et al. have proposed a region based lossless MIW method for security enhancement and authentication using difference expansion of adjacent pixel values in [22]. This scheme does not introduce any embedding-induced distortion in ROI. In [23], Guo et al. have incorporated tamper localization capability to their previous method of [22] by partitioning an image into certain non-overlapping regions and appending the associated local authentication information directly into the watermark payload. A contextual based transform domain MIW technique is proposed in [25] by Nambakhsh et al. to embed electrocardiograph (ECG) and demographic text data as double watermark in PET images. Extensive review on different MIW schemes can be found in [6,7,29].

The present paper aims to reveal the potentials of digital watermarking in medical data management issues and proposes a novel method to enforce integrity, authenticity and confidentiality of the medical information, by embedding two different fragile watermarks in the last two least significant bit-planes of the medical image. Even though, there exist several medical image watermarking techniques, but most of them have several disadvantages: some of them are task and modality specific, whereas others suffer from the problem of low security, imperceptibility, payload capacity and without tamper localization capability etc. A comparative analysis of the advantages/disadvantages of the proposed technique over several state-of-the-art MIW schemes is given in Section 4 of this article. The proposed MIW method is modality and task independent, having high imperceptibility and payload capacity. The proposed scheme is highly secure having several layers of security mechanisms. Watermarking by combining lossless data compression and encryption techniques, scattered embedding of the watermark bits in the embedding region, use of binary location map for the novel tamper localization method, all these aspects make the proposed scheme an effective novel MIW technique. Moreover, the proposed scheme can be used as an all-in-one solution tool, which makes it a novel technique in the medical image management domain. The proposed method conforms to the strict specifications and requirements regarding medical data handling by preserving their visual/information quality and diagnostic value.

1.1. Medical Image Watermarking: 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: confidentiality, reliability and availability [4].

- 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 that 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. The strict specifications and requirements regarding the quality of the medical images could be met by lossless (reversible, invertible, distortion free, erasable etc.) watermarking, which has the capability to recover the exact original content from a watermarked image [24, 30, 31]. Selective regions watermarking by the selection of regions of interest (ROIs) is another alternative procedure. Here ROIs are left intact by the embedding procedure and the rest of the image - the regions of non-interest (RONIs) are used for watermark embedding. Of course, the watermarked image is not distortion free, but the distorted image is used only as a carrier for data to be embedded and not for diagnosis. The losslessly recovered image is the final one for diagnosis [12, 15, 22, 24]. We have followed a similar approach in this paper, where the whole image including ROI and RONI is used to embed the watermark. If there is no modification in the watermarked image then the method can completely recover the ROI of the image to their original form.

1.2 Medical Image Watermarking: Applications

A brief outline of MIW applications in medical data management domain is as follows [4, 6, 19]

1.2.1 Saving Memory

At present, medical images and the corresponding medical information related to the patient (EHR) are stored separately. Memory space requirement for the image and the patient record is very voluptuous and rapidly increasing. Embedding the data in the corresponding images will save a lot of memory, as the image and the data become a single entity after watermarking.

1.2.2 Avoid Detachment

As the medical images and related medical records are stored separately, the chances of corruption of these records or their detachment from the images are 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.

1.2.3 Saving Bandwidth

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

1.2.4 Confidentiality and Security

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

1.2.5 Controlling Integrity

Fragile watermark is used for integrity verification and tamper localization [32]. 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 [20].

1.2.6 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 [11, 13].

1.2.7 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

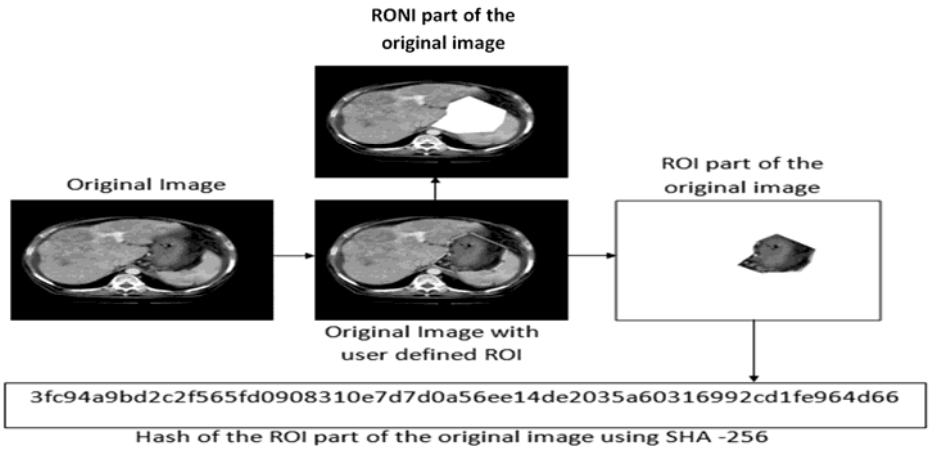

Fig. 1 – Hash of the ROI using SHA-256.

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.

1.2.8 Controlling Access

In MIW, EHR/DICOM metadata are embedded in the image in such a way that 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 [4, 33].

1.2.9 Captioning

Caption or annotation watermarks can be used for providing additional valuable information about the patient's report. ROIs in a medical image can 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 novel MIW system with the potentialities and maintaining the strict requirements mentioned above is described next.

2. Methods

We have used some standard tools, like SHA-256, Advanced Encryption Standard (AES) and arithmetic coding in our proposed scheme. SHA-256 is used to compute the hash of the ROI of the medical image. This hash is used as a message digest to verify the integrity of the medical image. In our algorithm, AES cryptographic method is used to encrypt/decrypt the EHR/DICOM metadata part to achieve better security. To reduce the payload's size we losslessly compressed the watermark using arithmetic coding.

2.1 Hash of the Region of Interest (ROI)

The ROI is the most important part in a medical image. It contains the most valuable information of the medical image and should not undergo any modification. There can be several disjoint ROIs in a medical image and several ways exist to define the ROI in a medical image: manual, automatic and semi-automatic. In the standard DICOM format if the ROI is present then its description is embedded in a tag of the DICOM header. In the proposed scheme, a polygonal ROI can be defined by the user (physician, clinician etc.) interactively. The reason of choosing polygonal ROI is that in most of the cases ROI in a medical image is irregularly shaped. A polygonal ROI, can be completely characterized by the number of vertices n_v and their coordinates v(x, y). Although, we only have concentrated on single ROI, the proposed method can also work on multiple ROIs. After the selection of the ROI, the hash of the ROI is computed using the SHA-256 cryptographic hash function, which produces a 64 character (256 bits) message digest as shown in Fig. 1.

0	0	40	10	0	50	20	0	0	30
0	0	27	0	0	37	7	0	47	17
0	44	14	0	0	24	0	0	34	4
0	31	1	0	41	11	0	0	21	0
48	18	0	0	28	0	0	38	8	0
35	5	0	45	15	0	0	25	0	0
22	0	0	32	2	0	42	12	0	0
9	0	49	19	0	0	29	0	0	39
0	0	36	6	0	46	16	0	0	26
0	0	23	0	0	33	3	0	43	13

Fig. 2 – Dispersion of the watermark bits for k = 23, n = 100 and h = 50.

2.2 Dispersion of the Watermark Bits

To increase the security of the proposed scheme, we take the help of a one-to-one mapping function, which depends on a secret prime key and disperses the bit values of the watermark payload into the embedding region. For example, one function that may be used for this purpose is given below:

$$f(x) = (kx \bmod n) + 1 \quad (1)$$

where, for an image of size $P \times Q$ and watermark payload of h bits,

$n = P \times Q$;

k = prime number ϵ [1, n];

x = bit position in the watermark payload and $x \epsilon$ [1, h].

As an example, if we take $k = 23$, $n = 100$ (say 10 × 10 pixels image) and $h = 50$, then the dispersion of the bits of the watermark in the image is going to be like Fig. 2.

2.3 Tamper Localization

We have used a novel image content dependent block based tamper localization method in the proposed MIW technique. Considering Bp as the LSB plane of the image, after embedding the first watermark in the penultimate LSB plane (say Bp+1), the LSB plane Bp of the watermarked image is filled with 0s. The modified watermarked image of size P × Q is then divided into 3 × 3 blocks in a non-overlapping manner. If the image size is not a multiple of 3, then some more rows and/or columns with all values 0 are added to the image to get an extended image. A binary location map (BLM) of the same size as the image or the extended image is formed for tamper localization purpose. For every 3 × 3 image block a 9 bits block identification code (BIC) is calculated using a cryptographic hash function. For example if we use SHA-256, for a block we will get a BIC of 256 bits. Among these 256 bits, 9 bits are selected. The selection of 9 bits among 256 bits is same for both the watermark insertion and extraction procedures. This selection of 9 bits also provides a level of security. The BLM constructed by all the block's BICs, is embedded in the LSB plane Bp of the modified watermarked image. Considering, a 3 × 3 image block as an example, Fig. 3, describes this method. In this example, we have used SHA-256 to compute the BIC of the block. We have chosen the 1st, 28th, 56th, 84th, 112th, 140th, 168th, 196th and 224th bits as the selected 9 bits out of the 256 bits to construct the BIC. The Block 1 in the Fig. 3 is the image after embedding the first watermark in the Bp+1 bitplane of the original image. After setting the LSB (Bp) plane of the Block 1 to 0, the Block 2 will always contains only even numbers. In this case, only the odd numbers of the Block 1 will be reduced to next lower even numbers. SHA-256 hashing is used on Block 2 to get the 256 bits unique hash code as shown in the Fig. 3. Among these 256 bits only 9 bits are selected to form the BIC (Block 3 in Fig. 3). The selected bits are shown in red colour in the Fig. 3. This BIC is used to construct the BLM. The BP plane of the Block 2 (which only contains 0) is replaced by this BIC (BLM for the whole image) to get the final watermarked image (Block 4 in Fig. 3.). Replacing the Bp plane of Block 2 by the BIC (Block 3) bits will change the pixel values of Block 2 in the following manner: if the bit at the (i, j)th position of BIC (Block 3) is 1 then

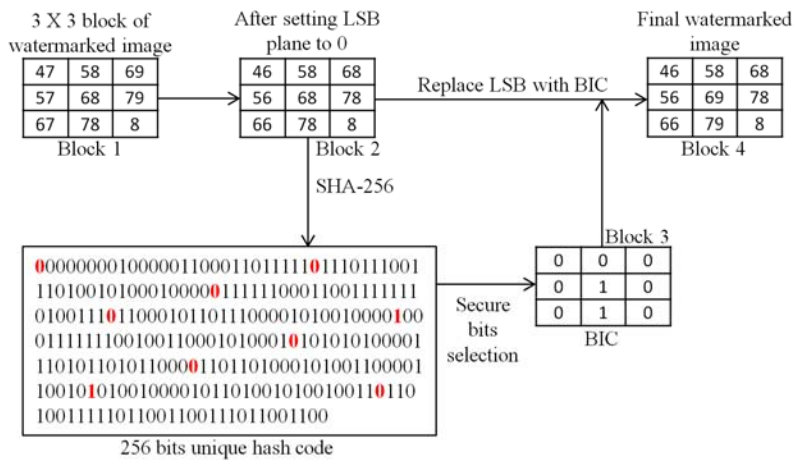

Fig. 3 – Embedding of the tamper localization information. (For interpretation of the references to color in text, the reader is referred to the web version of this article.)

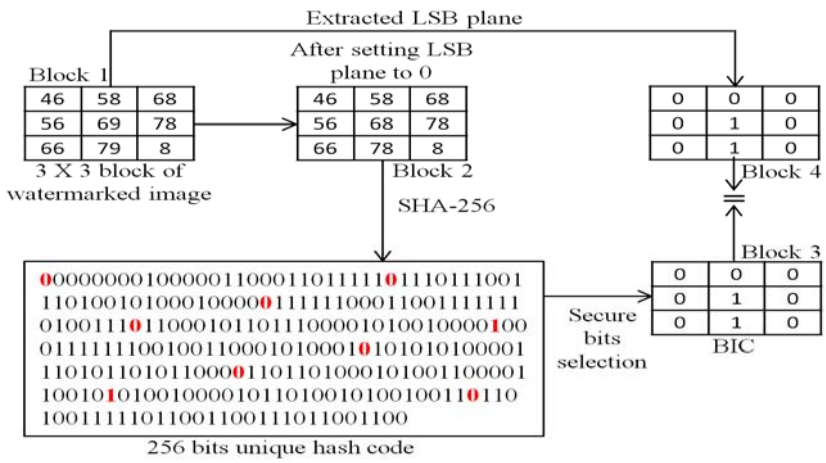

Fig. 4 – Tamper localization in case of no tampering.

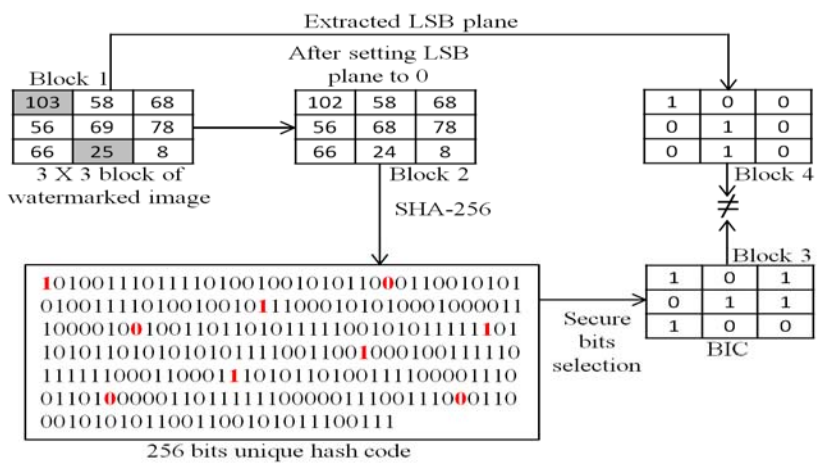

Fig. 5 – Tamper localization in case of tampering (shaded pixels).

increase the (i, j)th pixel value of Block 2 by 1 to the next higher odd value. For example, the BIC (Block 3) shown in Fig. 3, contains 1 bit at (2,2) and (3,2) positions. Therefore, only the pixel values 68 and 78 at the corresponding positions (2,2) and (3,2) of Block 2 are increased by 1 to the next higher odd values 69 and 79, respectively.

During watermark extraction procedure, the LSB plane Bp (Block 4 in Figs. 4-5) from the watermarked image (Block 1 in Figs. 4-5) is extracted. Following the same procedure as

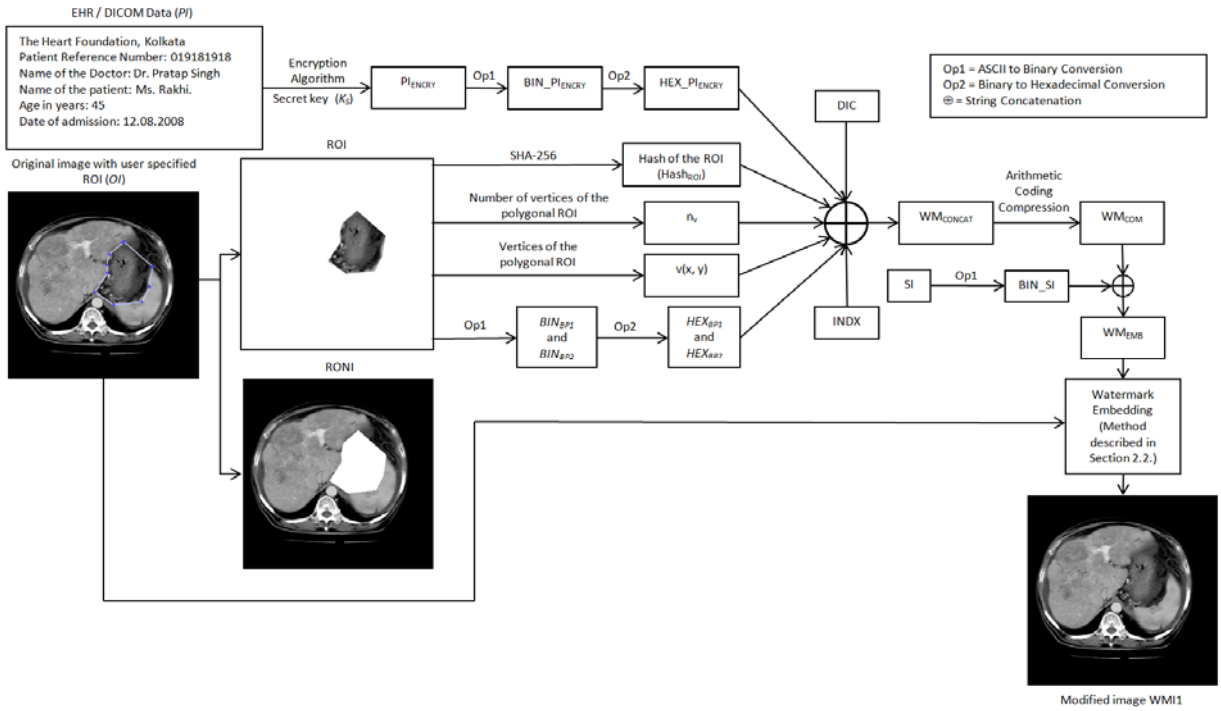

Fig. 6 – First watermark WM_{EMB} generation and insertion.

described above, a BIC/BLM is formed (Block 3 in Figs. 4-5). If there is no tampering to the watermarked image (Block 1 in Fig. 4), then the extracted bit-plane (Block 4 in Fig. 4) and the BIC/BLM (Block 3 in Fig. 4) are going to be same as shown in the Fig. 4. Fig. 5 shows that for any modification in the watermarked image (shaded pixels are the modified pixels of Block 1 in Fig. 5), the extracted bit-plane (Block 4 in Fig. 5) and the BIC/BLM (Block 3 in Fig. 5) is not going to be same. The difference between the extracted bit-plane and the BLM, will give the tampered locations.

2.4 Watermark Generation and Insertion

Two different watermarks are embedded in the medical images in our proposed method. The first watermark is used to insert the encrypted EHR/DICOM metadata, indexing keywords, Doctor's identification code, ROI information and the side information used during the watermark extraction procedure. The ROI information consists of the number of vertices n_v and their corresponding coordinates v(x, y) of the polygonal ROI. It also contains the bits of the LSB planes Bp and Bp+1 of the ROI.

The second watermark consists of the binary location map, used for tamper localization. During embedding the first 524 bits of the first watermark is used as the side information. The watermark insertion procedure is described as follows:

Inputs: Original Image (*OI*) of size $P \times Q$, EHR/DICOM metadata (*PI*), Secret Key (K_S), n_v, $v(x, y)$, Index (*IDX*), Doctor's Identification Code (DIC) and Side Information (*SI*).

Outputs: Watermarked image (*WMI*).

Steps:

1. Separate *OI*, into *ROI* and *RONI*.
2. Compute the message digest $HASH_{ROI}$ of *ROI*, using SHA-256.
3. Assuming, *BP*1_*ROI* and *BP*2_*ROI* represents the bit-planes of the ROI, numbered *Bp* and *Bp* + 1 respectively. Represent the pixels of *BP*1_*ROI* and *BP*2_*ROI*, as binary strings BIN_{BP1} and BIN_{BP2} respectively.
4. Change BIN_{BP1} and BIN_{BP2} to their hexadecimal representations as HEX_{BP1} and HEX_{BP2}.
5. Encrypt *PI* using K_S by Advanced Encryption Standard (AES) method to get PI_{ENCRY}.
6. Create the binary string representation of PI_{ENCRY} as BIN_PI_{ENCRY}.

7. Represent BIN_PI_{ENCRY} to its equivalent hexadecimal form as HEX_PI_{ENCRY}.
8. Concatenate n_v, $v(x, y)$, IDX, DIC, $HASH_{ROI}$, HEX_{BP1}, HEX_{BP2} and HEX_PI_{ENCRY} to get WM_{CONCAT}.
9. Compress WM_{CONCAT} losslessly to WM_{COM} using arithmetic coding compression technique.
10. Concatenate WM_{COM} and the binary representation of side information SI to WM_{EMB}, which is the first watermarked to be embedded in the $Bp + 1$ bit-plane.
11. Embed the bits of WM_{EMB} in the $Bp + 1$ bit-plane of OI using the method described in Section 2.2, to get the modified image $WMI1$.
12. If the size of $WMI1$ is not a multiple of 3, then modify it as described in Section 2.3, and set all the bits of the LSB plane Bp of $WMI1$ to zero to get a modified image $WMI1_{MOD}$.
13. Divide $WMI1_{MOD}$ into B number of 3×3 non-overlapping blocks:

    $BLOCK\_IM_b = \{block\_im_b(i, j),\ 1 \le i, j \le 3\}$,

    where, $block\_im_b(i, j) \in 0, 1, 2, ..., 2^L - 1$,
14. For each block $BLOCK\_IM_b$, compute its block identification code :

    $BIC_b = \mathrm{BIT}\_SEL(HASH(BLOCK\_IM_b))$,

    where, $b \in 1, 2, 3, ..., B$; $HASH(\cdot)$ represents the cryptographic hash function used, and $BIT\_SEL(\cdot)$ indicates the 9 bits selection procedure out of 256 bits.

    Create the final binary location map (BLM) using the method described as follows:

    $BLM = \{BIC_b, b \in 1, 2, 3, ..., B\}$
15. Obtain the final watermarked image WMI, by replacing the LSB plane Bp of $WMI1_{MOD}$ by BLM. If the size of $WMI1$ is increased to get $WMI1_{MOD}$ during watermark embedding, then reduce the size of WMI to the original image size by deleting the added rows and/or columns from WMI.

Fig. 6, describes the generation procedure of WM_{EMB}.

2.5 Watermark Extraction and Verification

The salient steps of the extraction and verification process can be enumerated as follows:

Inputs: Watermarked and possibly attacked image (WMI') of size $P \times Q$, Secret Key K_S.

Outputs: Authenticity result ($AUTH_{RES}$) and/or Watermark extracted image (WMI_{EXI}), PI, IDX, DIC.

Steps:

1. Using the same function (as Equ. (1)) used for watermark insertion, with proper key k, extract the bit string representation of the embedded watermark, from the bit-plane $Bp + 1$ of WMI'. Let it be denoted by WM_{EXT}.
2. Divide WM_{EXT} into two parts. One as the side information SI (first 524 bits from WM_{EXT}) and the rest as WM_{COM}.
3. Decompress WM_{COM} using arithmetic coding with the help of SI to WM_{CONCAT}.
4. Separate n_v, $v(x, y)$, IDX, DIC, $HASH_{ROI}$, HEX_{BP1}, HEX_{BP2} and HEX_PI_{ENCRY} from WM_{CONCAT}.
5. Using n_v and coordinates $v(x, y)$ information, the proposed scheme automatically specify the ROI in WMI'.
6. Convert HEX_{BP1}, HEX_{BP2} to their bit string representations as BIN_{BP1} and BIN_{BP2}, respectively.
7. Replace the bits of the Bp and $Bp + 1$ bit-planes in the ROI of WMI' by the bits of BIN_{BP1} and BIN_{BP2}, respectively.
8. Calculate the hash $Hash_{ROI\_EXT}$ of the ROI of WMI' using SHA-256.
9. Extract the Bp bit-plane of WMI' as BLM_{EXT}.

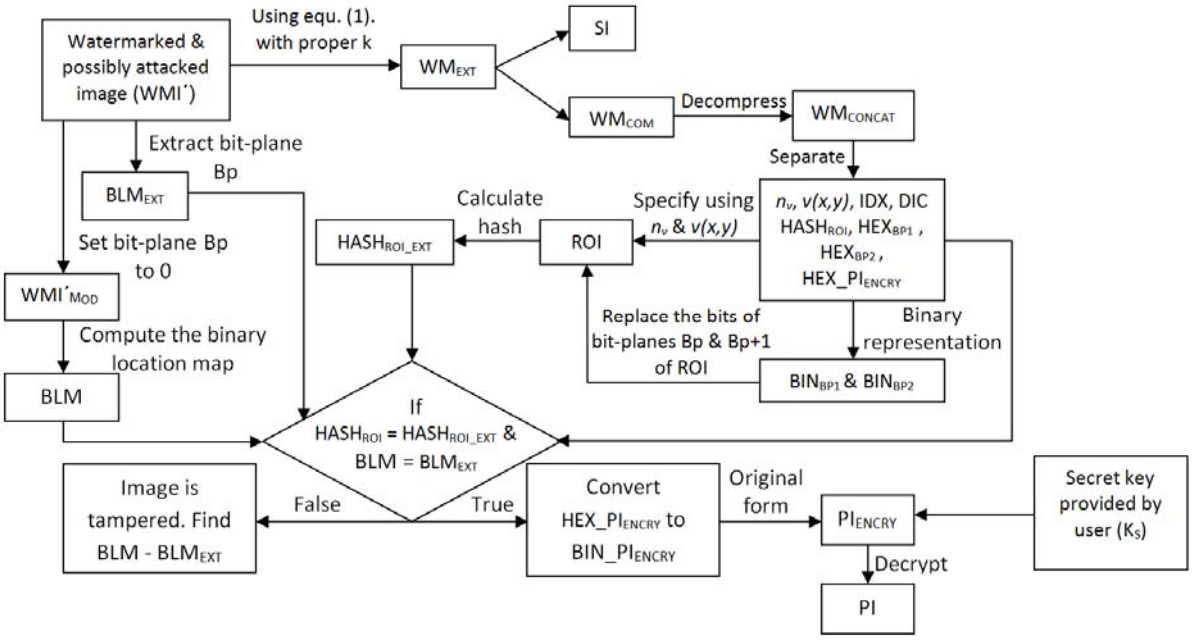

Fig. 7 – Watermark extraction and verification.

10. Set all the bits of the *Bp* bit-plane of *WMI´* to 0 to get a modified image as WMI'_{MOD}.
11. Compute the binary location map (*BLM*) from the WMI'_{MOD} using the steps 12 to 15 described in Section 2.4.
12. To get the authenticity result ($AUTH_{RES}$) follow the next procedure:

    if $HASH_{ROI} = Hash_{ROI\_EXT}$ **and** $BLM = BLM_{EXT}$ **then**

    $AUTH_{RES} = True$

    Do steps 13 to 15

    else

    $AUTH_{RES} = False$

    Do step 16

    end if
13. Convert HEX_PI_{ENCRY} to its equivalent binary string representation as BIN_PI_{ENCRY}.
14. Change BIN_PI_{ENCRY} to its original representation as PI_{ENCRY}.
15. Decrypt PI_{ENCRY} using K_S by AES method to get *PI*.
16. Find the difference between *BLM* and BLM_{EXT} to get the tampered regions.

The block diagram of the watermark extraction and verification process is shown in Fig. 7.

3. Results

We implemented the proposed MIW technique in MATLAB. Experiments were done on a PC with 2.66 GHz CPU and 4 GB RAM. 430 medical images of 7 different modalities (CT, MRI, USG, X-ray, Barium Study, Mammogram etc.), various sizes, file formats (BMP, TIF, GIF, DICOM), and bit-depths (8, 12, 16) were used to test our proposed scheme. Among these 430 images, 140 images were of size 128 × 128 pixels, 140 images were of size 256 × 256 pixels and 140 images were of size 512 × 512 pixels. Each of the 7 different modalities had 60 images individually. So, each modality of medical images consisted of 20 images of size 128 × 128, 256 × 256 and 512 × 512 pixels separately. The rest 10 images were DICOM images having different sizes and bit-depths. EHR of different sizes were used in the experiments. Fig. 8 shows an example of the EHR used in the experiment.

To show the effectiveness of the proposed technique, 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. Higher value of PSNR and WPSNR indicates less

The Heart Foundation, Kolkata
Patient Reference Number: 019181918
Name of the Doctor: Dr. Pratap Singh
Name of the patient: Ms. Rakhi
Age in years: 45
Residential address: #44, 5th F.G. Road, I Block, E phase, Kolkata - 109
Date of admission: 12.08.2008
Case History: Dyspnea on exertion NYHA Class IV. Chest pain.
Pain radiating to the left side of the neck and mastoid.
Patient had h/o a similar attack 4 months ago.
Test performed: Lead II E.C.G.
Results: T wave inversion.
Diagnosis: Suspected myocardial infarction.
Treatment: Sublingual Nitroglycerin.
Required tests: Balloon angioplasty
Referred to: Dr. M. Pathak, Future Hospital, Kolkata

Fig. 8 – An example of HER used in the experiment.

distortion in the watermarked image. Mean Structural SIMilarity index (MSSIM) was used to measure the similarity between the original image and the watermarked image [34]. 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 [35]. Lower the value of TPE the better the result.

An expert clinician was asked to subjectively evaluate the effectiveness of the proposed MIW method. Some of the medical images used in the experiment are shown in the Fig. 9, with their corresponding intensity histograms. It also shows the corresponding watermarked and watermark extracted medical images. Table 1, shows the result of watermark insertion in terms of the used quantitative measures in average. The results given in the Table 1, denotes the average results obtained by watermarking the 60 test images for that particular modality of image. Table 2, shows the results for 3 DICOM images among the 10 different test DICOM images with different modality, size and bit-depth. The graph of the Fig 10, shows that relationship between ROI data size and watermarking payload. The performance of the proposed MIW scheme was compared with several state-of-the-art existing MIW techniques and the findings are given in the Table 3. The Fig. 11, describes the tamper localization capability of the proposed MIW technique.

4. Discussion

During the subjective evaluation of the performance of the proposed MIW scheme, original, watermarked and watermark extracted images obtained by the proposed method were shown to an expert clinician. He was asked to classify the images shown to them into different category: original, watermarked and watermark extracted. He agreed with our claim that it was impossible to distinguish the original, watermarked and watermark extracted images. He found no significant visual difference between the original, watermarked and watermark extracted medical images, which suggests that there was no noticeable visual and/or informational degradation in the watermarked and watermark extracted images. The clinician was also asked to evaluate the proposed MIW scheme for its usability. He confirmed that the proposed MIW system is easy to use and described the system as a quality product, which satisfies the strict ethical and legislative requirements of medical information paradigm. The images of the Fig. 9, indicates that the visual degradation caused by watermark insertion and extraction cannot be identified easily. The intensity histograms of Fig. 9, also supports the low visual degradation caused by the proposed technique, as the intensity histograms of the watermarked and watermark extracted images, are very similar to the intensity histograms of the original images.

We also evaluated the proposed MIW scheme to measure its watermark capacity. As

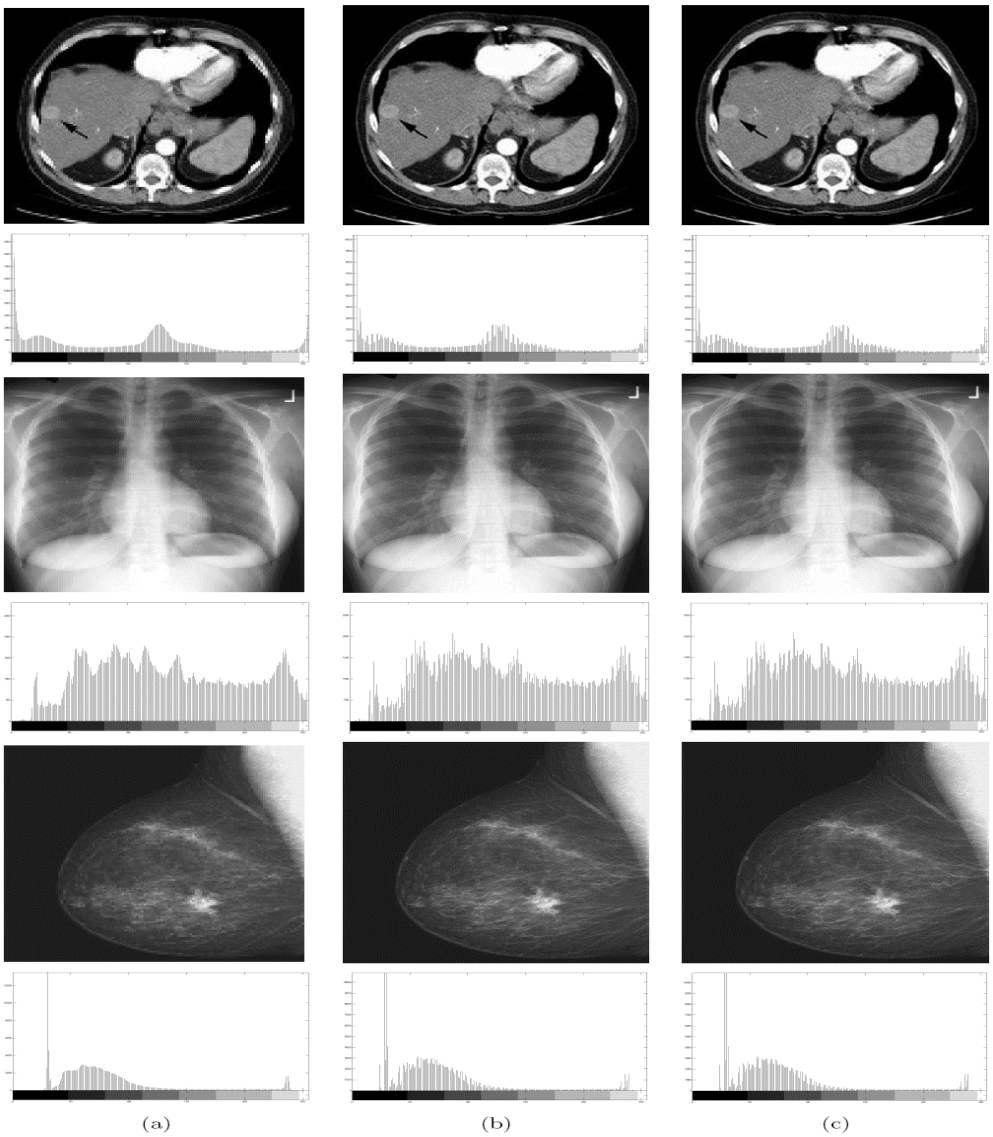

Fig. 9 – Sample medical images used in the experiment (a) original images, (b) watermarked images, (c) watermark extracted images.

mentioned earlier, the second watermark is the binary location map, having the same size of the corresponding image. Since the second watermark is solely used for tamper localization purpose, it should not be included in the computation of watermark payload. Only the first watermark can be of different sizes. The fixed 524 bits needed for SI were also not considered in the watermark payload computation. In this experiment we considered different sizes ROIs (5% to 30% of the original image's pixels). The bits needed for two bitplanes (Bp and Bp+1) of ROI were excluded in the watermark payload calculation. Then we calculated how much other information (EPR, Hash of ROI, DIC etc.) can be embedded in the medical image keeping in mind the imperceptibility requirement of MIW. Considering an image of size P x Q pixels and a ROI of size Y% of the whole image, the watermarking capacity is approximately (PQ(100-2Y)-52400)/100PQ bpp[2]. In other words, the results given in the Table 1, indicates the highest visual degradation considering the maximum possible watermarking payload. The results shown in Table 1 are of the watermark

[2] Number of bits needed for 2 bitplanes of ROI = 2PQY/100 bits,
Number of bits available for information (EPR, HASH, DIC etc.) insertion = PQ - 524 - (2PQY/100) bits,
Watermarking payload capacity = {PQ(100 - 2Y) - 52400}/(100PQ) bpp

Table 1 - Performance of the proposed MIW scheme.

Image Modality	Average PSNR	Average WPSNR	Average MSSIM	Average TPE
Abdomen CT	43.5219	45.2290	0.9527	0.0635
Barium Study	44.8029	45.8453	0.9786	0.0322
Brain MRI	43.6067	45.5822	0.9486	0.0649
Chest X-ray	44.3848	45.4122	0.9891	0.0250
Head CT	44.0263	45.6086	0.9635	0.0542
Mammogram	43.0897	43.6464	0.8707	0.0923
USG	43.8484	45.4997	0.9751	0.0419

extracted images. It is clear from the Table 1 that the proposed method works well for all the different modalities of medical images. Furthermore, it is referred in [36], medical image distortion should be maintained in the range of 40 to 50 dB (PSNR value). The PSNR and WPSNR values in Table 1, are well over 40 dB, which indicates that the distortion in the watermark extracted images is low, considering the maximum possible watermark payload. The average MSSIM values for all the modalities of medical images are near about 1. This indicates that the perceived change in structural information in the watermark extracted images is insignificant, and that these are similar to the original un-watermarked images. The low average TPE values show that the proposed MIW scheme causes low visual degradation in the watermark extracted images.

Table 2 - Performance of the proposed scheme for DICOM images.

Image Modality	Size & Bit-depths	Average PSNR	Average WPSNR	Average MSSIM	Average TPE
MR-Shoulder	1024 X 1024, 12	43.0234	44.2318	0.9192	0.0619
CT-Abdomen	512 X 512, 8	42.1649	43.1469	0.8096	0.0634
MR-Knee	253 X 256, 16	43.9823	44.0346	0.9904	0.0102

As DICOM (Digital Imaging and Communications in Medicine) is the international standard for handling, storing, printing, and transmitting information in medical imaging, we also experimented with several DICOM images of different modalities, having different size and bit-depths. In those experiments we first extracted the metadata part of the DICOM data and then embedded this information into the medical images. Table 2, shows the performance of the proposed MIW scheme in watermarking DICOM images. The results given in the Table 2, shows the performance of the watermark extracted images. In this experiment, the same experimental setup was used as of for the non-DICOM images. It is obvious from the results of Table 2 that our proposed method also performs efficiently for DICOM images.

The graph of the Fig. 10, shows there exists an inverse relationship between ROI size and watermarking payload. We can see from the given graph of Fig. 10, that for low ROI size (5% of original image's pixels), the proposed MIW scheme have achieved watermarking

payload of approximately 0.89 bpp, and that of for 30% ROI is approximately 0.39 bpp. The watermarking payload decreases approximately 10% with 5% increase in the ROI size. For example, for a 512 x 512 medical image (today's digital medical images often have high resolution) considering a ROI with 30% of total image pixels, the proposed technique can embed approximately 12kb information (near about 14500 characters considering 7 bits ASCII characters). Decreasing the ROI size to 5% of the total image pixels, the amount of embedded information increase to approximately 28kb. This amount of information is enough for modern EHR data. It should also be noted that in most of the cases in real life, the size of the watermark payload is much less than the maximum available embedding payload capacity. Therefore, in those cases we will have much better visual results using our scheme. Moreover, the proposed MIW scheme

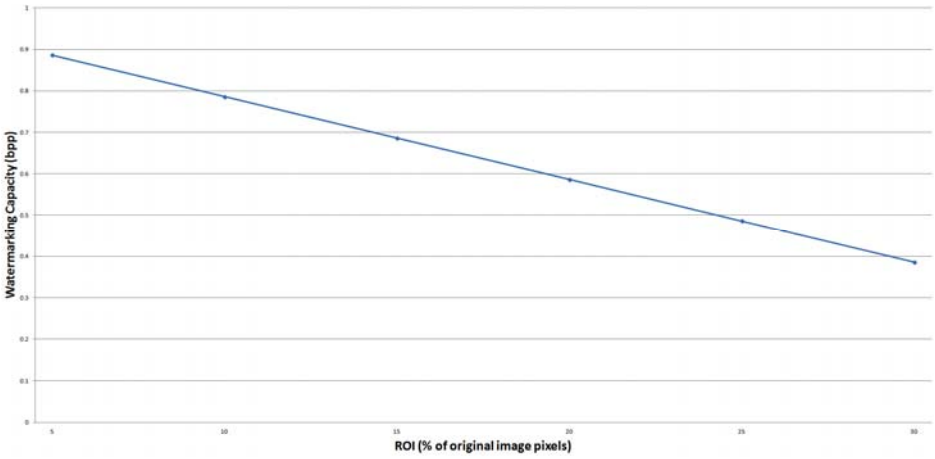

Fig. 10 – Performance in terms of watermark capacity versus ROI size (% original image pixels).

uses lossless compression technique to compress the information to be embedded in the medical image. The amount of compression that can be achieved is different for different ROIs and EHR. Therefore, the results given in Table 1, Table 2 and Fig. 10 are without using the compression technique. In this regard, it should also be noted that if we consider the compression scheme, the watermarking payload of the proposed scheme will be higher.

We also tested our proposed method for security analysis. The key used to encrypt the EHR data, is the first level of security in our proposed scheme. Without the proper encryption key the unintelligible EHR cannot be decrypted correctly. The secret prime key (integer) and the dispersion function used for dispersing the watermark bits in the embedding region, is the second security measure used in the method. As the watermark bits are not embedded sequentially in the medical image, so for correct watermark extraction the proper dispersion function and the secret prime key is needed. Even if an attacker correctly guesses the bitplane numbers, where the watermarks have been embedded, he/she cannot do much with that information. Assuming, an attacker correctly have guessed the bitplane numbers Bp+1 for inserting the first watermark and Bp for inserting the second watermark, respectively. The first watermark consists of encrypted EHR/DICOM metadata part, ROI information, Side information, INDX and DIC etc. The attacker has to know the proper order of in which these data are concatenated. Even if he/she knows the proper order of concatenation, the attacker has to know the key for encryption/decryption and the dispersion function along with the secret prime number used to scatter the watermark's bits. If the attacker changes one or more bits in the Bp and/or Bp+1 bit-planes, the extraction and verification algorithm can correctly detect it. If the attacker removes the whole bitplane Bp and/or Bp+1, the algorithm can detect it correctly. Furthermore, the proposed tamper localization procedure is based on selecting 9 bits out of available 256 bits, generated by

SHA-256 scheme. This selection of 9 bits makes the tamper localization technique secure in the sense, that the attacker has to know which 9 bits out of 256 bits are used.

As mentioned earlier, our proposed method is fragile in nature. Therefore, any kind of alteration in the watermarked image, would destroy the hidden watermark and the proposed tamper localization scheme, would identify the tampered locations. Moreover, the proposed MIW scheme is secured against common fragile watermarking attacks, such as the copy or the collage attack. Two different watermarks are inserted in the medical images using the proposed method. Both of these two watermarks are image content dependent. As a result, for each different image different watermarks are embedded. The first watermark consists of the image content dependent image hash and the second watermark contains the image content dependent binary location map. Both the image hash and binary location map is different for different images. Hence, the proposed method is secured against the common fragile watermark attacks.

Fig. 11 – Tamper localization (a) original watermarked image, (b) tampered watermarked image, (c) tampered region. (For interpretation of the references to color in text, the reader is referred to the web version of this article.)

To demonstrate the efficiency of the novel tamper localization scheme, we changed the values of some pixels in an USG image. Fig. 11 shows the result of the tamper localization experiment. The USG image shown in Fig. 11(a) was watermarked with the proposed MIW technique. Fig. 11(b) shows the tampered watermarked image, in which the region containing a text ("BOY") was tampered. The tampered region was successfully detected as shown in Fig. 11(c). The proposed scheme marks the tampered regions with red colour.

We have compared our proposed scheme with some of the state-of-the-art MIW techniques. The advantages/disadvantages of the compared method are tabulated in Table 3. The problem with the method proposed in [13] is that it embeds data in a mark image which is an image of hospital's mark (used to identify the origin of an EHR). No medical image is used in the scheme. Depending on the size of the mark image and the amount of data embedded, the proposed technique produces hidden image with low visual quality (PSNR 33.57 dB). Acharya et al. have used the technique of [16] to interleave EHR and graphical signal (ECG) in the medical images. As mentioned in the Table 3, this method is of low watermark capacity, without reversibility and tamper localization capabilities. Even though the scheme uses encryption of EHR and graphical signals before interleaving, the system lacks the modern digital data security concerns. In [17], only the hash (SHA-256) of the whole image is embedded in the RONI part of the image. The method depends on the size ROI. Moreover, the authors claim that their method is lossless, with the assumption that all the pixels in the RONI of all medical images are zeros. This assumption is not true for all the medical images and so the claim of the reversibility of the technique. Furthermore,

the method is not secured. The MIW scheme of [18] lacks the security measures needed in modern digital data management domain. The tamper detection procedure can easily be forged. The method of [21] uses a pre-processing step for changing the pixel value of the original from the range 0 - 255 to 3 - 252. This pre-processing step makes the scheme a near-lossless technique. During tamper detection, the proposed scheme gives a block of size 256 x 256 as the tampered block. This limits the tamper localization accuracy. Moreover, the method is tested only for mammogram images. Its effect on other modalities of medical images is not experimented. The method proposed by Guo et al. in [22], is based on region of embedding (ROE) selection automatically or semi-automatically. The watermark is embedded in ROE only. This restricts the watermark capacity. Moreover, two essential requirements of the proposed scheme are that the ROE should not intersect the ROI, and ROE should be in the smooth region (mostly background) of the image. This also reduces the applicability of the method. In [23] Guo et

al. proposed an improved version of the method described in [22] with tamper localization capability. Apart from the shortcomings of the technique [22], the tamper localization procedure of [23] will fail if the tampering occurs in the ROE. The MIW scheme proposed by Nambakhsh et al. in [25] is based on secret key >= 13 bytes and tested on PET image only. This key needs to be stored separately and securely. It uses ECG signal and text image as watermarks. In the reconstructed 1D image, some characters are not completely extracted but are visually recognizable. Increase in the size of ECG also decreases the visual quality drastically (for 512 bytes PSNR 50dB and for 4 kb PSNR 27db). It is clear from the above mentioned discussion that most of the compared methods are task specific with low hiding capacity or imperceptibility etc. Moreover, most of the methods shown in the Table 3, lack one or more useful properties that are very much needed for a modern MIW system. In comparison to these compared MIW schemes, the advantages of our proposed technique can be listed as follows:

1. The proposed method can be used as an all-in-one solution tool having various applicability mentioned in Section 1.2.

2. It works equally well for different modalities of medical images having different image format, bit-depths etc.

3. Even though, we have used several tools such that SHA-256 for hashing, AES for encryption and arithmetic coding for lossless compression, it should be noted that these tools can easily be replaced by other advanced ones, without or with little modification to the proposed scheme.

4. As the proposed technique is based on spatial domain, the time requirements of watermark insertion and watermark extraction/verification phases are very low.

5. The proposed method has superior tamper localization capability of 3×3.

6. The security concerns of the existing MIW scheme is overcome in the proposed technique through several layers of effective security measures.

7. The proposed scheme has relatively higher embedding capacity and imperceptibility.

The limitations of the proposed MIW technique are: the watermark payload is dependent on the size of the ROI. The proposed scheme is only ROI lossless. Moreover, the use of two separate bitplanes for watermark embedding, results in slightly higher degradation in the watermarked image (even though, the degradation is not visually significant). Moreover, the proposed scheme is not tested on colour medical images.

5 Conclusions

Digital watermarking has the potentiality of becoming an all-in-one solution tool to address various issues regarding effective medical information management and distribution. We have presented a blind, fragile watermarking scheme applied to medical images with good imperceptibility, high payload and enhanced security. Our scheme can be used for different modalities of medical images. It can be applied to a variety of digital medical images with different size, format, and bit-depth. The tamper localization

Table 3 - Performance comparison.

Scheme	Objectives	Hiding Capacity	ROI Based	Tamper Localization	Lossless	Blind
Chao et al. [13]	Authentication, integration and confidentiality of EHR.	Relatively low	No	No	No	No
Acharya et al. [16]	EHR/graphic signal hiding	Low, approximately 0.125 bpp - 0.25 bpp	No	No	No	Yes
Zain et al. [17]	Authentication and integrity of DICOM images	Only authentication data, no EPR	Yes	No	Near-lossless	Yes
Woo et al. [18]	Authentication, data hiding	Very low, only the border of the image is used for EHR hiding.	No	Yes	No	Yes
Wu et al. [21]	Authentication	Low, only authentication data, no EPR.	Yes	Yes	Near-lossless	Yes
Guo et al. [22]	Authentication, data hiding	Theoretically 0.75 bpp. However, the authors did not use the scheme for EPR hiding	Yes	No	Yes	Yes
Guo et al. [23]	Authentication, data hiding	Theoretically 0.75 bpp. However, the authors did not use the scheme for EPR hiding.	Yes	Yes	ROI lossless	Yes
Nambakhsh et al. [25]	Authentication, EHR hiding (as image)	Low, approximately 0.25 bpp	No	No	No	Yes
Our method	Authentication, integrity, data hiding	0.89 bpp to 0.39 bpp for ROI size of 5% to 30%	Yes	Yes	ROI lossless	Yes

capability can successfully locate even a single tampered pixel and gives the corresponding 3 × 3 block as the tampered region. 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 privacy protection, safety, effective archiving, efficient controlled access retrieval and management.

6 Mode of availability of software

The program is freely available (demo source code, test image files etc.) on request from the author.

Acknowledgements

We would 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 (Medicare Images, Asansol-4, West Bengal) for the subjective evaluation of the watermarked images.

References

1. E. L. Siegel, R. M. Kolodner, Filmless Radiology. Springer, New York, 1999.
2. H. Munch, U. Engelmann, A. Schroeter, H. P. Meinzer, Web-based distribution of radiological images from PACS to EHR, International Congress Series 1256 (2003) 873-879.
3. S. Kaihara, Realisation of the computerised patient record; relevance and unsolved problems, International Journal of Medical Informatics 49(1) (1998) 1-8.
4. G. Coatrieux G, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, Relevance of Watermarking in Medical Imaging, in: Proc. of International Conference on IEEE EMBS Information Technology Applications in Biomedicine, Paris, France, 2000, pp. 250-255.
5. G. Coatrieux, H. Maitre, B. Sankur, Strict integrity control of biomedical images, in: Proc. of SPIE Security Watermarking Multimedia Contents III, San Jose, CA, 2001 January, pp. 229-240.
6. K. A. Navas, M. Sasikumar, Survey of Medical Image Watermarking Algorithms, in: Proc. of 4th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, Tunisia, 2007 March, pp. 1-6.
7. H. Nyeem, W. Boles, C. Boyd, A Review of Medical Image Watermarking Requirements for Teleradiology, Journal of Digital Imaging 26(2) (2013) 326-343.
8. F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, Information hiding - a survey, in: Proc. of IEEE Special issue on protection of multimedia content, 87(7), 1999 July, pp. 1062-1078.
9. J. Cox, M. L. Miller, The first 50 years of electronic watermarking, EURASIP Journal of Applied Signal Processing 2002(2) (2002) 126-132.
10. N. Nikolaidis, I. Pitas, Digital image watermarking: An overview, in: Proc. of IEEE International Conference on Multimedia Computing and Systems, 1, 1999 June, pp. 1-6.
11. U. R. Acharya, A. Deepthi, P. S. Bhat, U. C. Niranjan, Compact storage of medical images with patient information, IEEE Trans. on Information Technology in Biomedicine 5(4) (2001) 320-323.
12. A. Wakatani, Digital watermarking for ROI medical images by using compressed signature image, in Proc. Annual Hawaii Int. Conf. System Sciences, 6, 2002 January, pp. 157-163.
13. H. M. Chao, C. M. Hsu, 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) 46-53.
14. U. R. Acharya, P. S. Bhat, S. Kumar, L. C. Min, Transmission and storage of medical images with patient information, Computers in Biology and Medicine 33 (4) (2003) 303-310.
15. L. Xuanwen, C. Qiang, J. Tan, A lossless data embedding scheme for medical images in application of e-diagnosis, in Proc. 25th Annual Int. Conf. of the IEEE EMBS, 2003 September, pp. 852-855.
16. U. R. Acharya, U. C. Niranjan, S. S. Iyengar, N. Kannathal, L. C. Min, Simultaneous storage of patient information with medical images in the frequency domain, Computer Methods and Programs in Biomedicine 76 (2004) 13–19.
17. J. M. Zain, L. P. Baldwin, M. Clarke, Reversible watermarking for authentication of DICOM images, in Proc. 26th Annual Int. Conf. IEEE EMBS, 2004 September, pp. 3237-3240.
18. C.-S. Woo, J. Du, B. Pham, Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images,

in Proc. APRS workshop on digital image computing pattern recognition and imaging for medical applications (2005).

19. A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Multiple image watermarking applied to health information management, IEEE Transactions on Information Technology in Biomedicine 10(4) (2006) 722-732.

20. J. M. Zain, A. M. Fauzi, Medical Image Watermarking with Tamper Detection and Recovery, in Proc. The 28th IEEE EMBS Annual Int. Conf., 2006, pp. 3270-3273.

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

22. X. Guo, T. Zhuang, A region-based lossless watermarking scheme for enhancing security of medical data, Journal of Digital Imaging 22(1) (2009) 53-64.

23. X. Guo, T. Zhuang, Lossless watermarking for verifying the integrity of medical images with tamper localization, Journal of Digital Imaging 22 (6) (2009) 620 – 628.

24. M. K. Kundu, S. Das, Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding, in Proc. IEEE Int. Conf. on Patter Recognition, 2010 August, pp. 1457-1460.

25. M. S. Nambakhsh, A. Ahmadian, H. Zaidi, A contextual based double watermarking of PET images by patient ID and ECG signal, Computer Methods and Programs in Biomedicine 104(3) (2011) 418-425.

26. O. M. A.-Wershi, B. E. Khoo, Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images, Journal of Digital Imaging 24(1) (2011) 114-125.

27. S. Das, M. K. Kundu, Hybrid Contourlet-DCT Based Robust Image Watermarking Technique Applied to Medical Data Management, in: Proc. Of 4th International Conference on Pattern Recognition and Machine Intelligence, 2011, pp. 286-292.

28. D. Bouslimi, G. Coatrieux, C. Roux, A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images, Computer Methods and Programs in Biomedicine 106 (1) (2012) 47-54.

29. A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Secure efficient health data management through multiple watermarking on medical images, Med. Biol. Eng. Comput. 44 (2006) 619–631.

30. J. Fridrich, M. Goljan, R. Du, Lossless data embedding for all image formats, in Proc. SPIE Photonics West Electronic Imaging Security and Watermarking of Multimedia Contents, 4675, 2002 January, pp. 572-520.

31. J. Tian, High capacity reversible data embedding and content authentication, in Proc. Int. Conf. Acoustics, Speech, and Signal Processing, 3, 2003 April, pp. 517-520.

32. E. T. Lin, E. J. Delp, A review of fragile image watermarks, in Proc. ACM Multimedia Security Workshop, 1999 October, pp. 47-51.

33. F. Hartung, M. Kutter, Multimedia watermarking techniques. In Proc. IEEE 87(7) (2006) 1079-1107.

34. W. Zhou, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE Transactions on Image Processing 13(4) (2004) 600-612.

35. A. B. Watson, DCT quantization matrices visually optimized for individual images, in Proc. SPIE Human Vision, Visual Processing and Digital Display IV, 1913, 1993 September, pp. 202-216.

36. K. Chen, T.V. Ramabadran, Near-lossless compression of medical images through entropy coded DPCM, IEEE Transactions on Medical Imaging 13 (3) (1994) 538–548.