Wireless Pers Commun (2015) 83:2133–2150
DOI 10.1007/s11277-015-2505-0

Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain

Amit Kumar Singh[1] · Mayank Dave[2] · Anand Mohan[3]

Published online: 10 March 2015

Abstract This paper presents a secure multilevel watermarking scheme in which the encrypted text acts as a watermark. The algorithm is based on secure spread-spectrum technique for digital images in discrete wavelet transform (DWT) domain. Potential application of the proposed watermarking scheme is successfully demonstrated for embedding various medical watermarks in text format at different subband decomposition levels depending upon their performance requirements. In the embedding process, the cover CT Scan image is decomposed up to third level of DWT coefficients. Different text watermarks such as personal and medical record of the patient, diagnostic/image codes and doctor code/signature are embedded into the selective coefficients of the second and third level DWT for potential telemedicine applications. Selection of DWT coefficients for embedding is done by column wise thresholding of coefficients values. Also, encryption is applied to the ASCII representation of the text and the encoded text watermark is embedded. The algorithm correctly extracts the embedded watermarks without error and is robust against numerous known attacks without much degradation of the medical image quality of the watermarked image.

Keywords Text watermark · Spread-spectrum · DWT · Encryption · BER · EPR

✉ Amit Kumar Singh
amts.juit@gmail.com

Mayank Dave
mdave67@gmail.com

Anand Mohan
profanandmohan@gmail.com

[1] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India

[2] Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India

[3] Department of Electronics Engineering, Indian Institute of Technology BHU, Varanasi, Uttar Pradesh, India

1 Introduction

Advancements in information and communication technologies (ICT) has opened up newer opportunities for telemedicine by facilitating medical data transmission across geographical boundaries through Internet, mobile networks, and other wireless/wired communication channels and thus covering rural/remote areas, accident sites, ambulance, and hospitals. However, the transmission of medical data over an open communication channel poses different possibilities of threat that can severely affect its authenticity, integrity, and confidentiality. This calls for implementing some kind of medical watermarking scheme to avoid prompting attention and preventing access by an unintended recipient. Digital watermarking of medical image providing a best solution to these issues [1]. Despite the broad literature on various application fields, little work has been done towards the exploitation of health-oriented perspectives of watermarking [2–7]. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Confidentiality, authentication, integrity and availability are important security requirements with electronic patient record (EPR) data exchange through open channels [8]. All these security requirements can be fulfilled using suitable watermarks. General watermarking method needs to keep the three factors like, imperceptibility, robustness, capacity and security reasonably very high. These requirements are hindering each other. There must be some trade off among these requirements according to the applications. The watermarks are classified into four categories according to the type of data to be watermarked. These categories are text watermarking, image watermarking, audio watermarking and video watermarking [9].

The image watermarking techniques are distinguished on the basis of two domain methods [10]: spatial domain method and Transform domain method. In the spatial domain methods [11–12] (LSB substitution, spread spectrum and patchwork), the data is embedded directly by manipulating the pixel values, bit stream or code values of the host signal. Spatial domain techniques are less complex but are less robust against attacks whereas the transform domain watermarking techniques are more robust. In this method the data is embedded by modulating the coefficients in transform domain like discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) etc. The main advantages of wavelet transform domain for watermarking applications are: (1) space frequency localization, (2) multiresolution representation, (3) adaptability, (4) multi-scale analysis and (5) linear complexity. The Wavelet transform provides both spatial and frequency resolutions [13–15]. The wavelet transform also allows localized watermarking of image. Watermarking technique can also be further classified as reversible and irreversible [16, 17].

Recently, telemedicine applications in teleconsulting, telediagnosis, telesurgery and remote medical education play a vital role in the evolution of the healthcare domain [18]. Medical identity theft has been a serious security concern in telemedicine [19]. Robert Siciliano, CEO of IDTheftSecurity.com, an identity theft expert, says, that would be a big fat yes. It’s almost like the perfect crime as far as medical identity theft is concerned. The long-distance nature of this type of treatment fuels the anonymity of it all [20]. Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery [21] and identity theft resource center produced a survey showing that medical-related identity theft accounted for nearly half of all identity thefts reported in the United States in 2013, *USA Today* reports said. These demand development of secure medical data/image watermarking schemes. Many wavelet based watermarking schemes were proposed for medical images [22–29]. Digital watermarking studies have always been driven by the improvement of robustness. On the contrary, security has received little attention in the watermarking community. The first difficulty is that security and robustness are neighboring concepts, which are hardly perceived as different. Security deals with intentional attacks whereas robustness is observed as degradation in data fidelity due to common signal processing operations. Also, digital watermarking may not be secure despite its robustness [30]. Therefore, security of the watermark becomes a critical issue in many applications. The problem of watermark security can be solved using spread-spectrum scheme [8, 22, 31–34]. Spread-spectrum is a military communication scheme was designed to be good at combating interference due to jamming, hiding a signal by transmitting it at low power, and achieving secrecy. These properties make spread-spectrum very popular in present-day digital watermarking.

A brief review of recent watermarking methods is presented below:

D-Ferrer and Sebé [35] proposed a spread spectrum based invertible watermarking method for image authentication purpose in lossless format. The method is robust and highly imperceptible. Das et al. [36] proposed a watermarking method based on spread spectrum technique. The method is designed from the analytical study of state transition behavior of non-group cellular automata (CA) and the basic cryptography/encryption scheme to provide the data authenticity and security. Multiple messages have been embedded using complimentary modulation function with *M*–ary modulation. Experimental results shown that the method is robust against various signal processing attacks. Interleaving and interference cancellation methods are applied to improve the performance of the method as compared to conventional matched filter detection. Basant et al. [8] proposed secure spread-spectrum based watermarking algorithms for embedding sensitive medical information such as doctor signature and hospital logo into radiological image for identity authentication purposes. These watermarking schemes used watermarks in binary image format only. In this method, different watermark messages are hidden in the same transform coefficients of the cover image using PN code. Performance of the method has been analyzed by varying the gain factor, subband decomposition levels, size of watermarks, wavelet filters and medical image modalities. Simulation results shown that the proposed method achieved higher security and robustness against JPEG attacks. Also, they proposed another algorithm [22] based on spread-spectrum technique in which, two different pseudo noise (PN sequence) vectors of size identical to the size of each subband column are generated for each watermark message bit. So, this algorithm enhanced the watermarking capacity when compared with previous algorithm as proposed in [8].

Performance of the spread-spectrum based watermarking algorithm [22] has been tested for text watermark in [37]. The algorithm is applied for embedding text file represented in binary arrays using ASCII code into host digital radiological image for potential telemedicine applications. In order to enhance the robustness of text watermarks like patient identity code, BCH (Bose, Ray-Chaudhuri, Hocquenghem) error correcting code (ECC) is applied to the ASCII representation of the text watermark before embedding. Robustness and performance of the scheme was tested against some known signal processing attacks like compression, filtering, channel noise, sharpening, and histogram equalization. Singh et al. [38] presents a robust and secure digital watermarking scheme for its potential application in Telemedicine. The algorithm embeds different medical text watermarks into selected sub-band DWT coefficients of the cover medical image using spread-spectrum technique. In the embedding process, the cover image is decomposed up to third level DWT coefficients. Three different text watermarks are embedded into the selected horizontal and vertical sub band DWT coefficients of the first, second and third level respectively. Selection of these coefficients for embedding purpose is based on threshold criteria. Robustness of the proposed watermarking scheme is further enhanced by applying BCH ECC to the ASCII representation of the text watermark and the encoded text watermark is finally embedded into the cover medical image. The proposed scheme correctly extracts the embedded watermarks without error and provides high degree robustness against numerous known attacks while maintaining the imperceptibility of watermarked image. The method is compared with other reported techniques and has been found to be giving superior performance for robustness and imperceptibility suggested by other authors [37].

Singh et al. [39, 40] proposed two hybrid watermarking method based on DWT, DCT and SVD. The proposed hybrid method combines the advantages and removes the disadvantages of these most popular transforms. The important difference between these two methods is: DWT is applied on watermark image in the first method whereas; DCT is applied on watermark image in second method. The DCT information of the watermark image contains the low frequency information as long as this information does not suffer. These watermarking methods achieved high robustness and good imperceptibility against various signal processing attacks. Wioletta [41] proposed a biometric (iris) based medical image watermarking method using DWT. The iris biometric data as a binary watermark which contains the high uniqueness property is embedded into the cover medical image. Before embedding the watermark, the medical image has been decomposed by DWT. The method achieved high robustness in lower frequency component of DWT cover image against signal processing attacks. Also, the combination of biometric and watermarking contains the security solution for the medical image.

Mangaiyarkarasi et al. [42] proposed a medical image watermarking method based on DWT and independent component analysis (ICA). For the embedding process, second level DWT applied on the cover image then the binary logo is embedded into the selected suband of the cover image. Before the embedding process, noise visibility function (NVF) has been calculated for the selected subband. Fast ICA is used for the watermark extraction process. The proposed method achieved high robustness and good image quality against signal processing attacks. Also, the method can be applied for color images. Priya et al. [43] proposed a medical image watermarking method based on spatial (LSB) and frequency domain (DWT, DCT and DFT) techniques and compared them. After transformed the image, read the image in zig-zag manner. Based on the experimental results, DWT provides better performance in term of robustness and imperceptibility. Hajjaji et al. [44] proposed a medical image watermarking method based on DWT and K–L transform. The K–L transform applied only on details subbands of the second level DWT cover image. The visibility factor is determined by the fuzzy inference system. A binary signature owned by the hospital center is generated by SHA-1 hash function and the rest of patient record in a binary sequence concatenated with the binary signature. Before embedding the patient record into the cover image, it has been coded by the serial Turbo code. The method achieved high robustness and good imperceptibility against signal processing attacks.

Kannammal et al. [45] proposed an encryption based image watermarking method in frequency and spatial domain. The proposed method using medical image as watermark and it is embedded in each block of cover image by altering the wavelet coefficients of chosen DWT subband. For the watermark embedding least significant bit (LSB) method is used. After the embedding process, the watermarked image is encrypted by advanced encryption standard (AES), Rivest-Shamir-Adleman (RSA) and Rivest Cipher (RC) 4 algorithm and compared them. Based on the experimental results, RC4 encryption algorithm performs better than other two encryption algorithm. Also, the method achieved high robustness and security against signal processing attacks.

Al-Haj et al. [46] proposed a region based watermarking algorithm for medical images. The method used multiple watermarks in spatial (LSB) and frequency domain (DWT and SVD). With frequency domain techniques, robust watermarks embedded in region-of-noninterest (RONI) part of the cover image. However, fragile watermarks embed into region-of-interest (ROI) part of the image by using the spatial domain technique. The method achieved high robustness against JPEG and salt and pepper attacks. Wang et al. [47] proposed a semi blind and adaptive watermarking method based on DWT. For the watermark embedding purpose, selected third level DWT coefficients categorized into Set Partitioning in Hierarchical Trees (SPIHT). Those trees are further decomposed into the set of bitplanes. Now, the binary watermark is embedded into the selected bitplanes with adaptive watermark embedding strength. The proposed method is robust and imperceptible against signal processing attacks. Also, the method has good computational efficiency for practical applications. Gao et al. [48] proposed a hybrid medical image watermarking based on redundancy discrete wavelet transform (RDWT) and singular value decomposition (SVD). In the embedding process, first level RDWT applied on the cover image which decomposed the image into four subbands. Then SVD applied on each suband and the cover image itself is used as watermark to embed in each sub-band by directly modify the singular values. The proposed method achieved and good robustness without significant degradation of the image quality against rotation attack. Moreover, the proposed watermarking method has the ability of rotation correction function and high embedding capacity. Yu et al. [49] focused on the security problems of the digital signature scheme, RSA, and proposed an efficient forward-secure group certificate digital signature method based on Shamir's threshold method and Schnorr's digital signature method to manage electronic medical records (EMR's) security issues. Experimental results shown that the method is robust against attacks. However, proposed signature method is not compatible with HIS. Singh et al. [50] proposed a wavelet based spread-spectrum multiple watermarking scheme considering medical watermarks in the form of text and image both. Experimental results were obtained by varying watermark size, gain factor. Performance of the developed scheme was tested against various attacks like compression, filtering, channel noise, sharpening, and histogram equalization. Robustness of the text watermark was enhanced by using BCH code.

According to our recent literature review, medical image watermarking approaches have focused achieving secure and bandwidth efficient transmission of medical data for telemedicine applications. Multilevel watermarking of medical images aims to simultaneously embed various types of medical watermarks such as patient ID, doctor's signature/code, EPR etc. on cover medical image addressing the health data management issues of data security, data compaction, unauthorized access and temper proofing. This paper applies watermarking algorithm proposed in Ref. [50] for text file watermark only where each character is represented in binary format using ASCII codes. Encrypted text medical watermarks such as personal and medical record of the patient, identification code/signature of the doctor and patient's diagnostic/image codes are embedded into column wise selected DWT coefficients in different subband decomposition levels using PN sequences. In each selected subband, the complete coefficient range is grouped in ten equally spaced bins. The bin having the maximum number of coefficients is chosen for embedding. The following observation are apparent:

(1) Capacity of embedding large data: The method proposed by Basant et al. [37] and Singh et al. [38] has been embedded 196 and 381 bits respectively. However, in our proposed method we can embed 728 bits (116 character) with the acceptable performance in terms of robustness and imperceptibility.

(2) Include the security: security of the medical text watermark may be enhanced by using simple encryption method to save execution time. For telediagnosis, the encryption and decryption speed has become an important factor if the situation demands.

(3) Reduced bandwidth requirements: huge amount of bandwidth is required for the transmission of the image data for telemedicine purposes. The addition requirement of bandwidth for the transmission of the metadata can be avoided if the data is hidden in the image itself. Since the EPR data and the image embedded into one (cover), bandwidth for the transmission can be reduced in telemedicine applications.

(4) Our multilevel watermarking method attempted to simultaneously address the health data management issues such as data security, data compaction, unauthorized access and temper proofing, having different characteristics and requirements. Also, the proposed method achieved two level of protection mechanism that uses both cryptography and robust watermarking simultaneously which provide effective protection mechanism for telemedicine security problem of patient identity theft.

The rest of the paper is organized as follows. Section 2 provides a brief overview of wavelet based spread-spectrum watermarking, encryption/decryption method and the proposed method. Performance of the new algorithm has been analyzed and experimental results are explained in Sect. 3. Conclusion of overall work is explained in Sect. 4.

2 Methods

The proposed work based on spread-spectrum technique in wavelet transform domain which requires certain theoretical considerations related to their application in image processing. Hence, a brief description of these concepts is discussed as follows:

Due to its ability to provide excellent multi-resolution analysis, space-frequency localization and superior HVS modeling, wavelet-based watermarking has recently gained great attention [51]. DWT separates an image into four different sub bands denoted as LL1 (approximation sub band), LH1 (horizontal sub-band), HL1 (vertical sub-band) and HH1 (diagonal sub-band), where LH1, HL1, and HH1 subband represent the finest scale wavelet coefficients and LL1 subband stands for the coarse-level coefficients. The process can be repeated to obtain multiple scale wavelet decomposition. This domain offers added benefits like increased robustness, tolerance to various compression algorithms and filtering as it allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH1, HL1, HH1). The watermarks are inserted in different decomposition levels and subbands depending on their type, and in locations specified by a random key; thus, they can be independently embedded and retrieved, without any interference among them. It is evident that the energy of an image is concentrated in the high decomposition levels corresponding to the perceptually significant low frequency coefficients; the low decomposition levels accumulate a minor energy proportion, thus being vulnerable to image alterations. Therefore, watermarks containing crucial medical information such as doctor's reference, patient identification code, image codes etc. requiring great robustness are embedded in higher level subbands.

In general most of the image energy is concentrated at the lower frequency coefficient sets LL and therefore embedding watermarks in these coefficient sets may degrade the image significantly. Embedding in the low frequency coefficient sets, however, could increase robustness significantly. On the other hand, the high frequency coefficient sets HH include the edges and textures of the image and the human eye is not generally sensitive to changes in such coefficient sets. This allows the watermark to be embedded without being perceived by the human eye. The agreement adopted by many DWT-based watermarking methods, is to embed the watermark in the middle frequency coefficient sets HL and LH is better in perspective of imperceptibility and robustness [50].

In spread-spectrum watermarking technique [8], the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: the location of the watermark is not obvious and frequency regions should be selected in a fashion that ensures sufficiently small energy in any single coefficient. A watermark that is well placed in the frequency domain of an image will be practically impossible to see. Hence, the string watermarked in the image becomes highly imperceptible.

2.1 Encryption and Decryption Process of EPR Data

For security issues, encrypting EPR data before watermarking has become unavoidable, but the delay encountered during embedding and extraction of the watermark is also an important factor in telemedicine applications. Therefore, watermark constitution by using encryption methods should be simple to save execution time. For telediagnosis, the speed has become an important factor if the situation demands [52].

The EPR is first encrypted for extra security using the equation

$$Encrypted\ text = \left(input\ text^{r}\right) - d \tag{1}$$

where *r* and *d* are constants. The value of *r is* carried out from 1 to 1.143 and *d* can be between 0.0 and 10.0. The first level of security lies in this encryption process [53].

The extracted encrypted text is decrypted using the relation

$$Decrypted\ text = (Encrypted\ text + d)^{\frac{1}{r}} \tag{2}$$

2.2 Medical Watermarks and Their Performance Measures

To enhance medical data confidentiality protection and to allow efficient data management, retrieval and integrity control, various medical watermarks may be inserted into cover radiological image. Medical watermarks are broadly classified as follows:

Signature/Identification code watermark—comprises physician's digital signature or identification code for the purpose of origin authentication.

Patient's diagnostic/image codes watermark—contains keywords such as diagnostic codes, image acquisition characteristics etc., which facilitates image retrieval by database querying mechanisms. The insertion of indices into the images provides an alternative for efficient indexing and archiving of digital medical data in hospital information systems, which eliminates storage and transmission bandwidth requirements.

Patient's medical records watermark—contains patient's personal and examination data such as health history, diagnostic reports etc., which grants a permanent link between the patient and the medical data, and provides extra level of protection.

Patient's personal record watermark—is embedded throughout the image for the purpose of data integrity control.

According to robustness requirement of the EPR data which is shown in Table 1 [6], the personal and medical record of the patient is embedded into selected subbands of the second level. However, identification code/signature of the doctor and patient's diagnostic/image codes of the patient are embedded into selected subbands of the third level.

The performance of the watermarking algorithm can be evaluated on the basis of its robustness and imperceptibility. Larger peak signal-to-noise ratio (PSNR) between cover and watermarked image indicates that the watermarked image more closely resembles the cover image resulting into imperceptible watermarking. Generally, watermarked image with PSNR value >27 dB is acceptable [23]. PSNR is defined as

$$PSNR = 10\log\frac{(255)^2}{MSE} \tag{3}$$

where the mean square error (*MSE*) is defined as

$$MSE = \frac{1}{X \times Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}(I_{ij} - W_{ij})^2 \tag{4}$$

where I_{ij} a pixel of the original is image of size $X \times Y$ and W_{ij} is a pixel of the watermarked image of size $X \times Y$.

Performance of text/string watermarks is evaluated in terms of bit error rate (BER), where each string character is represented in the form of bits. BER is defined as ratio between number of incorrectly decoded bits and total number of bits. It is suitable for random binary sequence watermark. Ideally it should be zero.

$$BER = (\text{Number of incorrectly decoded bits})/(\text{Total number of bits}) \tag{5}$$

2.3 Proposed Algorithm

This paper proposes a new DWT based spread-spectrum watermarking algorithm for embedding text watermarks using medical images as cover. Dyadic sub-band decomposition is performed on the cover image using Haar wavelet transform. Text watermarks like

Table 1 Allocation of watermarks according to robustness and capacity criteria at different subband

DWT subband	Capacity (embeddable coefficients)	Embedded watermark	
		EPR data	Robustness requirements
LH3	4096	Identification code/signature of the doctor and patient's diagnostic/image codes	Very high
HL3	4096	Identification code/signature of the doctor and patient's diagnostic/image codes	Very high
LH2	16,384	Patient's medical and personal records	High
HL2	16,384	Patient's medical records	High

doctor's identification code/signature and radiological image/diagnostic code are embedded into third level HL3 and LH3 subbands, while patient record is embedded into HL2 and LH2 subbands of second level. Also, encryption is applied to the ASCII representation of the text watermark and the encrypted text watermark is then embedded. So, the extra level of security and save execution time lies in this encryption process. In the embedding process, subband decomposition of the cover medical image is performed to obtain third level DWT coefficients. Different watermarks bits are hidden in the same transform coefficients of the cover image using uncorrelated codes, i.e. low cross correlation value (orthogonal/near orthogonal) among codes. For each string data bit, two different pseudo noise (PN) sequence vectors namely of size identical to the size of DWT column vector, are generated. A PN sequence is a sequence of binary numbers which appears to be random, but is in fact perfectly deterministic. The sequence appears to be random in the sense that the binary values and groups or runs of the same binary value occur in the sequence in the same proportion. PN sequences are a good tool for watermarking because of the following reasons [54]:

- PN sequence is having correlation properties, noise like characteristics and resistance to interference.
- PN generator produces periodic sequences that appear to be random.
- PN sequences are generated by an algorithm that uses an initial seed.
- The PN sequence generated is actually not statically random but will pass many test of randomness.
- Unless the algorithm and seed are known, the sequence is impractical to predict.

Pseudo noise (PN) sequences can be extended further to improve the correlation and security in the watermarking applications. These sequences include random sequence, maximal length sequence, gold sequence and Kasami sequence. Since the security level of the watermarking algorithm depends on the strength of its secret key, a grey scale image of size 1 × 35 is used as a strong key for generating pseudorandom sequences. Based on the value of the bit of the message vector, the respective two PN sequence pairs are then added/subtracted to/from selective columns of wavelet coefficient. This selection is done by thresholding the coefficient values present in that column. The complete coefficient range is grouped in ten equally spaced bins. The bin having the maximum number of coefficients is chosen for embedding. Proposed algorithm procedure is described in Fig. 1. The column wise DWT coefficients of second level horizontal and vertical subbands are taken. In each column, the coefficients under the threshold criteria are used for embedding and rest of coefficients remains unchanged. Example embedding process illustrated in Fig. 1 shows that of coefficients S_2 and S_3 are changed after watermarking as these value lie inside the threshold range while values of coefficient S_1 and S_4 lying outside the threshold criteria are remains same. The wavelet coefficients of cover image are divided into b_w number of *bins* having equal width for desired level. From this b_w number of *bins*, *max_bin*, having maximum number of coefficients is selected. In medical images the coefficients are mostly concentrated toward the origin. Thus, *max_bin* has coefficients concentrated toward origin.

$$\text{Width of each bin} = \frac{\text{maximum coefficient} - \text{minimum coefficient}}{\mathrm{b_w}}$$

b_1 *and* b_2 are the minimum and maximum values within *max_bin.* In each column, the coefficients under the threshold criteria are used for embedding the data bit as follows:

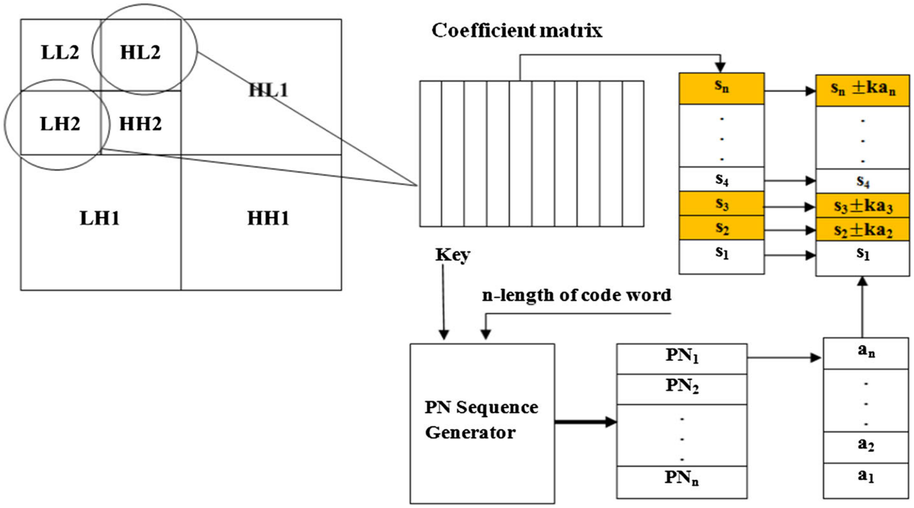

Fig. 1 Embedding procedure of PN sequence in the proposed method

$$W = V + kX \quad \text{if } b = 0$$

$$W = V - kX \quad \text{if } b = 1$$

where *V* is embeddable wavelet coefficient column vector of the cover image, W is the wavelet coefficient vector after watermark embedding, *k* is the gain factor, X is the PN sequence vector and *b* is the message bit that has to be embedded. The corresponding column of the wavelet coefficient, to which the generated sequence has to be added/subtracted, is decided by the following relation:

$$p = \begin{cases} \text{modulo}\left(d, \frac{N}{2^{\ell}}\right) & \text{if modulo}\left(d, \frac{N}{2^{\ell}}\right) \neq 0 \\ \frac{N}{2^{\ell}}, & \text{else} \end{cases}$$

where *p* is the column in which sequence has to be added, $N/2^{\ell}$ is the number of columns in coefficient matrix and ℓ represents one of three subbands. Generation of a pair of PN sequences for embedding each bit enhances the security of the watermarking algorithm. Following steps are applied in data embedding process:

2.3.1 Text Embedding Process

(1) Read the Cover image I(M,N) of size M × N.

(2) Read the text watermark to be hidden and convert it into binary sequences D_d (d = 1 to n).

(3) Apply encryption on the binary representation of text watermark using Eq. (1).

(4) Transform the host image using "*Haar*" wavelet transform and get first, second and third level subband coefficients.

(5) Generate *n* different PN sequence pairs (PN_h and PN_v) each of $M/2^{\ell} \times 1$ using a secret key to reset the random number generator for each level $\ell = 1$ to 3.

(6) For $\mathrm{d} = 1$ to n, and $\ell = 1$ to 3

$$\mathrm{p} = \begin{cases} \mathrm{modulo}\left(\mathrm{d}, \dfrac{\mathrm{N}}{2^{\ell}}\right) & \text{if modulo}\left(\mathrm{d}, \dfrac{\mathrm{N}}{2^{\ell}}\right) \neq 0 \\ \dfrac{\mathrm{N}}{2^{\ell}}, & \text{else} \end{cases}$$

Case 1: when message vector bit = 0
Hence $1 \leq p \leq (\mathrm{N}/2^{\ell})$, For $\mathrm{i} = 1$ to $(\mathrm{M}/2^{\ell})$.

$$\mathrm{cH}^{\ell}(\mathrm{i},\mathrm{p}) = \begin{cases} \mathrm{cH}^{\ell}(\mathrm{i},\mathrm{p}) + \mathrm{k} \times \mathrm{PN\_h}(\mathrm{i},\mathrm{d}) & \text{if } \mathrm{b1} < cH1^{\ell}(i,p) < b2 \\ \mathrm{cH}^{\ell}(\mathrm{i},\mathrm{p}) & \text{otherwise} \end{cases}$$

$$\mathrm{cV}^{\ell}(\mathrm{i},\mathrm{p}) = \begin{cases} \mathrm{cV}^{\ell}(\mathrm{i},\mathrm{p}) + k \times \mathrm{PN\_v}(\mathrm{i},\mathrm{d}) & \text{if } \mathrm{b1} < cV1^{\ell}(i,p) < b2 \\ \mathrm{cV}^{\ell}(\mathrm{i},\mathrm{p}) & \text{otherwise} \end{cases}$$

Case 2: when message vector bit = 1
Hence $1 \leq p \leq (\mathrm{N}/2^{\ell})$, For $\mathrm{i} = 1$ to $(\mathrm{M}/2^{\ell})$

$$\mathrm{cH}^{\ell}(\mathrm{i},\mathrm{p}) = \begin{cases} \mathrm{cH}^{\ell}(\mathrm{i},\mathrm{p}) + \mathrm{k} \times \mathrm{PN\_h}(\mathrm{i},\mathrm{d}) & \text{if } \mathrm{b1} < cH1^{\ell}(i,p) < b2 \\ \mathrm{cH}^{\ell}(\mathrm{i},\mathrm{p}) & \text{otherwise} \end{cases}$$

$$\mathrm{cV}^{\ell}(\mathrm{i},\mathrm{p}) = \begin{cases} \mathrm{cV}^{\ell}(\mathrm{i},\mathrm{p}) + \mathrm{k} \times \mathrm{PN\_v}(\mathrm{i},\mathrm{d}) & \text{if } \mathrm{b1} < cV1^{\ell}(i,p) < b2 \\ \mathrm{cV}^{\ell}(\mathrm{i},\mathrm{p}) & \text{otherwise} \end{cases}$$

where *k* is the gain factor used to specify the strength of the embedded data.

(7) Apply inverse "Haar" Wavelet transform to get the final watermarked image $I_w(M, N)$.

2.3.2 Text Extraction Process

The DWT coefficients of watermarked image are divided into k number of bins having equal width for desired level. From this k number of bins, max_bin, having maximum number of coefficients is selected. To detect the watermark we generate the same PN sequence vectors used during insertion of watermark by using same state key and determine their correlation with the corresponding selected column's detail subbands DWT coefficients. Average of n correlation coefficients corresponding to each PN sequence vector is obtained for both LH and HL subbands. Mean of the average correlation values are taken as threshold T for message extraction. During detection, if the average correlation exceeds T for a particular sequence a "0" is recovered; otherwise a "1". The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered. For extracting the watermark, following steps are applied to the watermarked image:

(1) Read the watermarked image $I_w(M, N)$.

(2) Transform the stego image using "Haar" Wavelet transform and get first, second and third level subband coefficients.

(3) Generate one's sequences (*msg*) equal to message vector (from 1 to n).

(4) Generate n different PN sequence pairs ($PN^{\ell}h1$ and $PN^{\ell}v1$) each of size $M/2^{\ell} \times 1$ using same secret key to reset the random number generator for each level $\ell = 1$ to 3.

(5) For $d = 1$ to n, generate $PN^{\ell}h2(d)$ and $PN^{\ell}v2(d)$ as
For $i = 1$ to (M/2^{ℓ})

$$PN^{\ell}h2(i,d) = \begin{cases} PN^{\ell}h1(i,d) & \text{if b1} < cH1^{\ell}(i,p) < b2 \\ 0 & \text{else} \end{cases}$$

$$PN^{\ell}v2(i,d) = \begin{cases} PN^{\ell}v1(i,d) & \text{if b1} < cV1^{\ell}(i,p) < b2 \\ 0 & \text{else} \end{cases}$$

Calculate the correlations between the values $cH1^{\ell}$ and $PN^{\ell}h2$ and store in *corr_H (d)* and $cV1^{\ell}$ and $PN^{\ell}v2$ and store in *corr_V (d).*
corr_H (d) = correlation between $PN^{\ell}h2$ (d) and $cH1^{\ell}$ (pth column)
corr_V (d) = correlation between $PN^{\ell}v2$ (d) and $PN^{\ell}v2$ (pth column)

$$\mathrm{p} = \begin{cases} \mathrm{modulo}\left(\mathrm{d}, \dfrac{\mathrm{N}}{2^{\ell}}\right) & \text{if modulo}\left(d, \dfrac{\mathrm{N}}{2^{\ell}}\right) \neq 0 \\ \dfrac{\mathrm{N}}{2^{\ell}}, & \text{else} \end{cases}$$

Hence $1 \leq p \leq N/4$

(6) Calculate average correlation avg_corr (d) = (corr_H (d) + corr_V(d))/2 at each level.

(7) Calculate the corr (mean) = mean of all the values stored in avg_corr (d) at each level.

(8) Extract the watermark bit stream, using the relationship given below
for $d = 1$ to n
if avg_corr (d) > corr (mean)
Msg (d) = 0.

(9) Decrypt the extracted watermark using Eq. (2).

(10) Convert the decrypted watermark into bit sequence.

(11) Convert bit sequence to text watermark to get the recovered watermark.

3 Experimental Results

Performance of the proposed watermarking algorithm was tested for encrypted text medical watermark considering gray-level medical images of size 512 × 512 [55] as cover image. Two text namely watermarks doctor's identification code of ten characters and radiological image/diagnostic code of five characters are embedded into third level HL3 and LH3 subbands, while patient record varying size is embedded into HL2 and LH2 subbands of second level. Encryption is applied to the ASCII representation of these text watermarks and the encrypted text watermarks are then embedded providing the extra level of security in this embedding process. Strength of watermark is varied by varying the gain factor in the watermarking algorithm. For testing the robustness and quality of the watermarked image of the

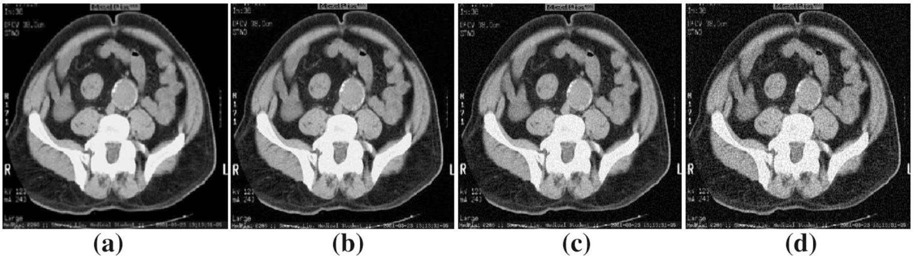

Fig. 2 Original and watermarked CT scan images **a** original image and watermarked images with gain factor; **b** 5; **c** 15 and **d** 40

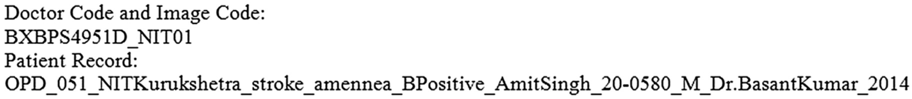
Doctor Code and Image Code:
BXBPS4951D_NIT01
Patient Record:
OPD_051_NITKurukshetra_stroke_amennea_BPositive_AmitSingh_20-0580_M_Dr.BasantKumar_2014

Fig. 3 EPR data as watermark

Table 2 Effect of gain factor against size of watermark

Gain factor (α)	With encryption				Without encryption			
	104 characters		60 characters		104 characters		60 characters	
	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)
5	40.02	0.1538	42.49	0.0961	40.06	0.1923	42.53	0.1250
10	34.24	0.0576	36.71	0.0288	34.27	0.0769	36.8	0.0480
15	31.05	0	33.29	0	31.08	0.0192	33.32	0.0096

proposed scheme MATLAB 7.0 is used. Also, evaluate the quality of watermarked image (as shown in Fig. 2) by the parameter PSNR and robustness of the proposed algorithm by BER.

Figure 2 shows the cover CT scan image and watermarked images obtained at different gain factors. Figure 3 shows the EPR data using as a text watermark. In the experiment, values of PSNR and BER are illustrated in Tables 2, 3 and 4 for varying gain factor (α) in the range of 5.0–15.0. In Table 2, performance of the proposed method against different size of watermark has been evaluated without any noise attack. With the encryption, maximum PSNR value is 40.02 dB and BER = 0.1538 against maximum size of watermark at gain factor = 5. However, PSNR value is 31.05 dB and BER = 0 at gain factor = 15. It is found that larger the gain factor results stronger robustness of extracting watermark whereas smaller the gain factor provides better PSNR between original and watermarked CT scan images.

Table 3 shows the performance of the proposed watermarking method against different attacks. The highest BER value of 0.3846 has been obtained against JPEG Compression with quality factor (QF) = 10 with encryption which is slightly better than the BER performance without encryption (BER = 0.4326).

Table 3 Performance of proposed method against different attacks at gain = 15

Attack	With encryption BER (%) for 104 characters	Without encryption BER (%) for 104 characters
JPEG compression (QF-10)	0.3846	0.4326
JPEG compression (QF-50)	0.0096	0.0288
JPEG compression (QF-90)	0	0.0192
Sharpening mask with threshold = 0.2 and 0.1	0.0192 and 0	0.0288
Median filtering [3 3] and [2 2]	0.0480 and 0	0.0769 and 0.0288
Scaling factor 2.5,1.5 and 0.5	0.0769, 0.0576 and 0	0.1057, 0.0673 and 0.0288
Motion blur (len = 2 and theta = 9)	0.0192	0.0192
Motion blur (len = 1 and theta = 9)	0	0.0192
Disk (radius = 1)	0.0288	0.0480
Disk (radius = 0.5)	0	0.0192
Gaussian LPF with standard deviation = 0.2, 0.5 and 0.9	0, 0.0096 and 0.0673	0.0192, 0.0192 and 0.0865
Gaussian noise with mean = 0, Var-0.05	0.0769	0.1057
Gaussian noise with mean = 0, Var-0.01	0.0288	0.0480
Gaussian noise with mean = 0, Var-0.005	0	0.0192
Salt and pepper noise with (density = 0.05)	0.0961	0.1153
Salt and pepper noise with (density = 0.01)	0.0288	0.0384
Salt and pepper noise with density = 0.005	0	0.0192
Histogram equalization	0.0961	0.1250

Table 4 Effect of cover image at gain = 15

Image type	With encryption	
	PSNR (dB)	BER (%)
CT scan	31.03	0
Ultrasound	30.37	0
MRI	31.23	0.0480

Table 4 shows the effect of cover image as proposed algorithm was tested for other types of medical images like MRI and ultrasound. The highest BER and PSNR were obtained with MRI image.

4 Conclusions

This paper proposed a new wavelet based spread-spectrum multilevel watermarking scheme considering medical watermarks in the form of text. Experimental results were obtained by varying watermark size, and gain factor. Performance of the developed scheme was tested against various attacks like compression, filtering, sharpening, and histogram equalization. Security and robustness of the text watermarks such as personal and medical record of the patient, diagnostic/image codes and doctor code/signature may be enhanced by using spread-spectrum along with encryption technique. The proposed method achieved two level of security which may provide a potential solution to existing telemedicine security problem of patient identity theft. Correlation and security of the method can be improved further by using other extended PN sequences such as random sequence, maximal length sequence, gold sequence and Kasami sequence.

References

1. Mostafa, S. A. K., El- sheimy, N., Tolba, A. S., Abdelkader, F. M., & Elhindy, H. M. (2010). Wavelet packets-based blind watermarking for medical image management. *The Open Biomedical Engineering Journal, 4*, 93–98.
2. Chao, H. M., Hsu, C. M., & Miaou, S. G. (2002). A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Transactions on Information Technology in Biomedicine, 6*(1), 46–53.
3. Acharya, U. R., Anand, D., Bhat, P. S., & Niranjan, U. C. (2001). Compact storage of medical images with patient information. *IEEE Transactions on Information Technology in Biomedicine, 5*(4), 320–323.
4. Coatrieux, G., Lecornu, L., Roux, Ch., & Sankur, B. (2006). A review of image watermarking applications in healthcare. *IEEE Engineering in Medicine and Biology Society, 1*, 4691–4694.
5. Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D. (2004). A medical image watermarking scheme based on wavelet transform. In *Proceedings 25th Annual International Conference of IEEE-EMBS, San Francisco* (pp. 1541–1544).
6. Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D. (2006). Secure and efficient health data management through multiple watermarking on medical images. *Medical & Biological Engineering & Computing, 44*, 619–631.
7. Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D. (2006). Multiple image watermarking applied to health information management. *IEEE Transactions on Information Technology in Biomedicine, 10*(4), 722–732.
8. Kumar, B., Singh, H. V., Singh, S. P., & Mohan, A. (2011). Secure spread-spectrum watermarking for telemedicine applications. *Journal of Information Security, 2*, 91–98.
9. Mohanty, S. P. (1999). Watermarking of digital images. In M.S. Thesis, Indian Institute of Science, India.
10. Wolak, M. C. (2000). *Digital watermarking*. United States: Preliminary Proposal, Nova Southeastern University.
11. Nikolaidis, N., & Pitas, I. (1999). Digital image watermarking: An overview. In *IEEE International Conference on Multimedia Computing and Systems* (Vol. 1, pp. 1–6).
12. Cox, I. J., & Miller, M. L. (2002). The first 50 years of electronic watermarking (EURASIP). *Journal on Applied Signal Processing, 2*, 126–132.
13. Meerwald, P., & Uhl, A. (2001). A survey of wavelet-domain watermarking algorithms. In *Proceedings of the SPIE Security and Watermarking of Multimedia Contents, San Jose* (pp. 516–505).
14. Hajjara, S., Abdallah, M., & Hudaib, A. (2009). Digital image watermarking using localized biorthogonal wavelets. *European Journal of Scientific Research, 26*(4), 594–608.
15. Paquet, A. H., & Ward, R. K. (2002). Wavelet-based digital watermarking for image authentication. In *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, Winnipeg 2002* (Vol. 2, pp. 884–879).
16. Feng, J. B., Lin, I. C., Tsai, C. S., & Chu, Y. P. (2006). Reversible watermarking: Current and key issues. *International Journal of Network Security, 2*(3), 161–170.
17. Lee, S., Chang, C. D., & Kalker, T. (2007). Reversible image watermarking based on integer-to-integer wavelet transform. *IEEE Transaction on Information Forensics and Security, 2*(3), 321–330.
18. Youngberry, K. (2004). Telemedicine research. *Journal of Telemedicine and Telecare, 10*(2), 121–123.
19. Terry, M. (2009). Medical identity theft and telemedicine security. *Telemedicine and e-Health, 15*(10), 928–932.
20. Bowman, D. (2012). http://www.fiercehealthit.com/story/researchers-use-digital-watermarks-protect-medical-images.
21. Ollove, M. (2014). www.usatoday.com/story/…/stateline-identity-thefts-medical…/5279351.
22. Kumar, B., Anand, A., Singh, S. P., & Mohan, A. (2011). High capacity spread-spectrum watermarking for telemedicine applications. *World Academy of Science, Engineering and Technology, 5*, 62–66.

23. Umaamaheshvari, A., & Thanushkodi, K. (2012). High performance and effective watermarking scheme for medical images. *European Journal of Scientific Research, 67*, 283–293.
24. Soliman, M. M., Hassanien, A. E., Ghali, N. I., & Onsi, H. M. (2012). An adaptive watermarking approach for medical imaging using swarm intelligence. *International Journal of Smart Home, 6*, 37–50.
25. Kannamma, A., Pavithra, K., & Subha Rani, S. (2012). Double watermarking of DICOM medical images using wavelet decomposition technique. *European Journal of Scientific Research, 70*, 46–55.
26. Pal, K., Ghosh, G., & Bhattacharya, M. (2012). Biomedical image watermarking in wavelet domain for data integrity using bit majority algorithm and multiple copies of hidden information. *American Journal of Biomedical Engineering, 2*, 29–37.
27. Zhang, L., & Zhou, P.-P. (2010). Localized affine transform resistant watermarking in region-of-interest. *Telecommunication Systems, 44*, 205–220.
28. Zain, J., & Clarke, M. (2005). Security in telemedicine: Issue in watermarking medical images. In *International Conference: Science of Electronic, Technologies of Information and Telecommunications*.
29. Memon, N. A., & Gilani, S. A. M. (2008). NROI watermarking of medical images for content authentication. In *Proceedings of 12th IEEE International Multitopic Conference, Karachi, Pakistan* (pp. 106–110).
30. Singh, A. K., Dave, M., & Mohan, A. (2014). Wavelet based image watermarking: Futuristic concepts in information security. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, *84*(3), 345–359. doi:10.1007/s40010-014-0140-x.
31. Cox, I. J., Kilian, J., Thomson, L. F., & Talal, Shamoon. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing, 6*(12), 1673–1687.
32. Malvar, H. S., & Florencio, D. A. F. (2003). Improved spread spectrum: A new modilation technique for robust watermarking. *IEEE Transactions on Signal Processing, 51*(4), 898–905.
33. Perez-Freire, L., & Perez-Gonzalez, F. (2009). Spread-spectrum watermarking security. *IEEE Transactions on Information Forensics and Security, 4*(1), 2–24.
34. Xuan, G., Yang, C., Zheng, Y., Shi, Y. Q., & Ni, Z. (2004). Reversible data hiding based on wavelet spread spectrum. In *IEEE International workshop on multimedia signal processing (MMSP2004), Siena, Italy* (pp. 211–214).
35. Domingo-Ferrer, J., & Sebé, F. (2002). Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images. In *Proceedings of the International Conference on Information Technology: Coding and Computing* (pp. 1–6).
36. Das, T. S., Mankar, V. H., & Sarkar, S. K. (2007). Spread spectrum based robust image watermark authentication. In *International Conference, Madurai, India* (pp. 673–676).
37. Kumar, B., Kumar, S. B., & Chauhan, D. S. (2014). Wavelet based imperceptible medical image watermarking using spread-spectrum. In *37th International Conference on telecommunications and signal processing, Berlin Germany* (pp. 660–664).
38. Singh, A. K., Kumar, B., Dave, M., & Mohan, A. (2015). Robust and imperceptible spread-spectrum watermarking for telemedicine applications. *Proceedings of the National Academy of Sciences, India, Section A: Physical Sciences,*. doi:10.1007/s40010-014-0197-6.
39. Singh, A. K., Dave, M., & Mohan, A. (2013). A hybrid algorithm for image watermarking against signal processing attack. In S. Ramanna et al. (Eds.), *Proceedings of 7th Multi-Disciplinary International Workshop in Artificial Intelligence, Krabi-Thailand, Lecture Notes in Computer Science (LNCS)* (Vol. 8271, pp. 235–246).
40. Singh, A. K., Dave, M., & Mohan, A. (2013). Hybrid technique for robust and imperceptible image watermarking in DWT-DCT-SVD domain. *National Academy Science Letters,*. doi:10.1007/s40009-014-0241-8.
41. Wójtowicz, W. (2013). *Biometric watermarking for medical images-example of iris code* (pp. 409–416). Technical Transactions. doi:10.4467/2353737XCT.14.051.1977.
42. Mangaiyarkarasi, P., & Arulselvi, S. (2013). Medical image watermarking based on DWT and ICA for copyright protection. In R. Malathi & J. Krishnan (Eds.), *Recent Advancements in System Modelling Applications, Lecture Notes in Electrical Engineering* (Vol. 188, pp. 21–33).
43. Priya, S., Santhi, B., & Swaminathan, P. (2014). Study on medical image watermarking techniques. *Journal of applied science, 14*(14), 1638–1642.
44. Hajjaji, M. A., El-Bay, Bourennane, Abdelali, A. B., & Mtibaa, A. (2014). Combining Haar wavelet and Karhunen loeve transforms for medical images watermarking. *BioMed Research International, 2014*, 1–15.
45. Kannammal, A., & Subha Rani, S. (2014). Two level security for medical images using watermarking/encryption algorithms. *International Journal of Imaging Systems and Technology*, *24*(1), 111–120.

46. Ali, Al-Haj, & Amer, A. (2014). Secured telemedicine using region-based watermarking with tamper localization. *Journal of Digital Imaging,*. doi:10.1007/s10278-014-9709-9.
47. Wang, S., Zheng, D., & Zhao, J. (2014). Adaptive watermarking and tree structure based image quality estimation. *IEEE Transactions on Multimedia, 16*(2), 311–325.
48. Gao, L., Gao, T., Sheng, G., & Zhang, S. (2014). Robust medical image watermarking scheme with rotation correction. In J. -S. Pan et al. (Eds.), *Intelligent Data Analysis and Its Applications, Volume 2, Advances in Intelligent Systems and Computing* (Vol. 298, pp. 283–292).
49. Yu, Y. C., & Hou, T. W. (2014). An efficient forward-secure group certificate digital signature scheme to enhance EMR authentication process. *Medical & Biological Engineering & Computing, 52*, 449–457.
50. Singh, A. K., Kumar, B., Dave, M., & Mohan, A. (2015). Multiple watermarking on medical images using selective DWT coefficients. *Journal of Medical Imaging and Health Informatics, 5*, 1–8. doi:10.1166/jmihi.2015.1432.USA.
51. Khademi April and Krishnan Sridhar. (2007). Shift-invariant discrete wavelet transform analysis for retinal image classification. *Medical & Biological Engineering & Computing, 45*, 1211–1222.
52. Zaz, Y., & Fadil, L. E. (2010). Protecting EPR data using cryptography and digital watermarking. In *International Conference on Models of Information and Communication Systems, Rabat, November 2010.*
53. Navas, K. A., Nithya, S., Rakhi, R., & Sasikumar, M. (2007). Lossless watermarking in JPEG2000 for EPR data hiding. In *Proceedings of IEEE-EIT 2007, Chicago, USA* (pp. 697–702).
54. Shivani Garg and Ranjit Singh. (2012). An efficient method for digital image watermarking based on PN sequences. *International Journal on Computer Science and Engineering (IJCSE), 4*(09), 1550–1561.
55. MedPix^{TM} Medical image database http://rad.usuhs.mil/medpix/medpix.html.

Amit Kumar Singh working as Assistant Professor in the Department of Computer Science & Engineering, Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh-India. Mr. Singh obtained his B.Tech. in Computer Science & Engineering from Institute of Engineering and Technology, Purvanchal University Jaunpur, Uttar Pradesh-India in 2005. M.Tech. in Computer Science & Engineering from Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh in 2010. Pursuing Ph.D. from Department of Computer Engineering, NIT, Kurukshetra from 2012. His research interests include Information Security, Biometrics and Image processing.

Mayank Dave working as Professor in the Department of Computer Engineering, NIT, Kurukshetra, Haryana-India. Dr. Dave obtained his Ph.D. (Computer Engineering) and M.Tech. (Computer Engineering) from IIT Roorkee and he has 25 years rich experience of serving both academia and industry in various capacities. He has also written a book on Computer Networks published by Cengage Learning India. His research interests include Computer Networks, Mobile / Vehicular Adhoc and Sensor Networks and Database Systems. He is a member of many Professional Bodies like IEEE, IEEE (Computer Society), IETE, Institutions of Engineers (India), ISTE etc. He has also chaired many sessions in the various International / National Conf.s of repute.

Anand Mohan is a Professor of Electronics Engineering at Institute of Technology, Banaras Hindu University where he has held as several important administrative positions namely Member of Executive Council, Head of the Department of Electronics Engineering, Coordinator, Centre for Research in Microprocessor Applications (established by MHRD), and In charge, University Science Instrumentation Centre. Prof. Mohan has 35 years rich experience of serving both academia and industry in various capacities. *Prof. Mohan* obtained Ph.D., PG and UG degrees in Electronics Engineering from Banaras Hindu University in 1994, 1977 and 1973 respectively. He has made notable contributions to the academic and research development in Electronics Engineering at Banaras Hindu University by creating dedicated research groups of eminent academic experts from the country and abroad. He conducted high quality research in the emerging areas like *fault tolerant/survivable system design*, *information security*, and *embedded systems.*