Multimed Tools Appl (2016) 75:14381–14397
DOI 10.1007/s11042-016-3536-6

Iris based secure NROI multiple eye image watermarking for teleophthalmology

Richa Pandey[1] · Amit Kumar Singh[2] · Basant Kumar[1] · Anand Mohan[3]

Received: 23 December 2015 / Revised: 12 March 2016 / Accepted: 11 April 2016 /
Published online: 29 April 2016
© Springer Science+Business Media New York 2016

Abstract This paper presents a new secure multiple text and image watermarking scheme on cover eye image using fusion of discrete wavelet transforms (DWT) and singular value decomposition (SVD) for Teleophthalmology. Secure Hash Algorithm (SHA-512) is used for generating hash corresponding to iris part of the cover digital eye image and this unique hash parameter is used for enhancing the security feature of the proposed watermarking technique. Simultaneous embedding of four different watermarks (i.e. Signature, index, caption and reference watermark) in form of image and text using fusion of discrete wavelet transforms (DWT) and singular value decomposition (SVD) is achieved in this paper. The suggested technique initially divides the digital eye image into Region of interest (ROI) containing iris and Non-Region of interest (NROI) part where the text and image watermarks are embedded into the Non-Region of interest (NROI) part of the DWT cover image. The selection of DWT decomposition level for embedding the text and image watermarks depends on size, different characteristics and robustness requirements of medical watermark. The performance in terms of Normalized Correlation (NC) and bit error rate

✉ Amit Kumar Singh
amit_245singh@yahoo.com

Richa Pandey
richa8704@gmail.com

Basant Kumar
singhbasant@yahoo.com

Anand Mohan
profanandmohan@gmail.com

[1] Department of Electronics & Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad, India

[2] Department of Computer Sc. & Engineering, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, India

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

(BER) of the developed scheme is evaluated and analyzed against known signal processing attacks and ‘Checkmark’ attacks. The method is found to be robust against all the considered attacks. The proposed multilevel watermarking method correctly extracts the embedded watermarks without error and is robust against the all considered attacks without significant degradation of the medical image quality of the watermarked image. Therefore the proposed method may find potential application in secure and compact medical data transmission for teleophthalmology applications.

Keywords Electronic patient record (EPR) · Region of interest (ROI) and non-region of interest (NROI) · Discrete Wavelet Transform (DWT) · Singular value decomposition (SVD) · SHA-512 · Checkmark Attacks

1 Introduction

Recently, rapid advances in information and communication technology (ICT) have facilitated newer telemedicine services by supporting open channel communications for cost effective and speedy transmission of electronic patient record (EPR) to remote hospitals / medical consultation centres. However, such type of exchange of EPR for diagnostic applications faces the challenging risk of authenticity, confidentiality, and ownership identity due to attempts of malicious attacks or hacking of EPR either to alter / modify the original patient record or even to prevent its transfer to intended recipients. The authenticity of EPR and related medical images are generally ensured in telemedicine applications by embedding some kind of watermark(s). Therefore, authentication and preservation of originality of a patient’s record requires robust and secure embedding of the watermark(s) against attempts of unauthorized access or modification of medical data transmitted over open channels. In view of the above and considering wide applications of teleophthalmology as well as its related security concerns, the proposed method of medical watermarking attempts to provide guaranteed authenticity of transmitted medical information. The main advantages of the image watermarking for the medical applications are [31]:

a. Smaller storage space required for storing the medical image and the patient record together as the patient record is embedded inside the image.
b. Reduced bandwidth requirement as the additional requirement of bandwidth for the transmission of the medical data can be avoided if the data is hidden in the image itself.
c. Confidentiality of the patient data is maintained as this data is hidden in the medical image.
d. Protection against tampering as the after-effects of a tampered data may cost a life due to wrong diagnosis.

For teleophthalmology, tele-diagnosis and tele-consultancy services, medical images play a prominent role for instant diagnosis, understanding of crucial diseases as well as to avoid the misdiagnosis [28]. Currently, the combined methods of cryptography and watermarking have emerged to disseminate the security to the EPR medical data [22]. The main challenge for a good watermarking algorithm is robustness and security against the surviving attacks [35]. Any digital image consists of two important regions, region of interest (ROI) and non-region of interest (NROI) [30]. ROI is an area of image that has important data, so it cannot be allowed to be modified because most of the information is present in this area [40]. NROI is an area of image that does not have an important data i.e. background of image. The proper selection of an area of an image that does not have an important data for watermarking is crucial for example in medical images where the area under concern has to be the least required portion conveying any information [37]. It will give better protection if the data is embedded in NROI region of an image [21, 38]. According to working domain method, the watermarking techniques can be classified as 'spatial domain' and 'transform domain' techniques [29]. In spatial domain, image is represented in the form of pixels. In spatial domain watermarking watermark is embedded by modifying pixel values of cover image. The main advantage of this technique is that it is easier to embed watermark in spatial domain and its computing time is less than transform domain watermarking. Least Significant Method (LSB) and Spread Spectrum method comes under this category. Spatial domain watermarking technique is easy and high payload but it is not robust for attacks. To get robustness of watermarking technique transform domain watermarking is used. The reason of selecting transform domain is that it utilizes HVS features in a better way by spectral coefficients. The most commonly used transform techniques are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and singular value decomposition (SVD). Recently, the higher robustness of watermark has been achieved by using wavelet based watermarking are presented in [16–19, 24, 32–35]. The overall performance of the wavelet based watermarking technique depends greatly on embedding and extraction process.

The main advantages of wavelet transform techniques for watermarking applications are: space frequency localization, multi-resolution representation, multi-scale analysis, adaptability and linear complexity. The wavelet based watermarking is also compatible with the image standard JPEG 2000 [29]. The main idea behind DWT results from multi-resolution analysis, which involves decomposition of an image in frequency channels of constant bandwidth on a logarithmic scale. It has advantages such as similarity of data structure with respect to the resolution and available decomposition at any level [31]. DWT separates an image into a set of four non- overlapping multi-resolution sub bands denoted as lower resolution approximation image (LL1) as well as horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. The process can then be repeated to compute multiple scale wavelet decomposition. Since human eyes are much more sensitive to the low-frequency part (LL1 sub-band), the watermark can be embedded into the other three sub-bands (HL1, LH1 and HH1 sub-band) to maintain better image quality. 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 sub-bands [33]. Figure 1 shows four level wavelet decomposed pyramid structure by DWT.

1.1 Related work

Many watermarking schemes based on discrete wavelet transform (DWT) and singular value decomposition (SVD) has been proposed in the literature [7, 16, 20, 33]. For a detailed description on these combined approaches, interested readers may directly refer to them. Kundu et al. [15] proposed a fragile watermarking technique with enhanced security and high payload embedding in spatial domain. A polygonal ROI is used to define diagnostic important part of image. EPR is encrypted by Advanced Encryption Standard (AES) method by using secret key. After this the watermarked data is generated by compressing the payload data, which is defined by concatenating number of vertices in polygonal, vertex co-ordinates of ROI, hash of ROI generated by SHA-256, encrypted data and bits of ROI as binary string. Guo et al. [10] proposed a false positive free SVD based image watermarking scheme. It watermarked cover image by

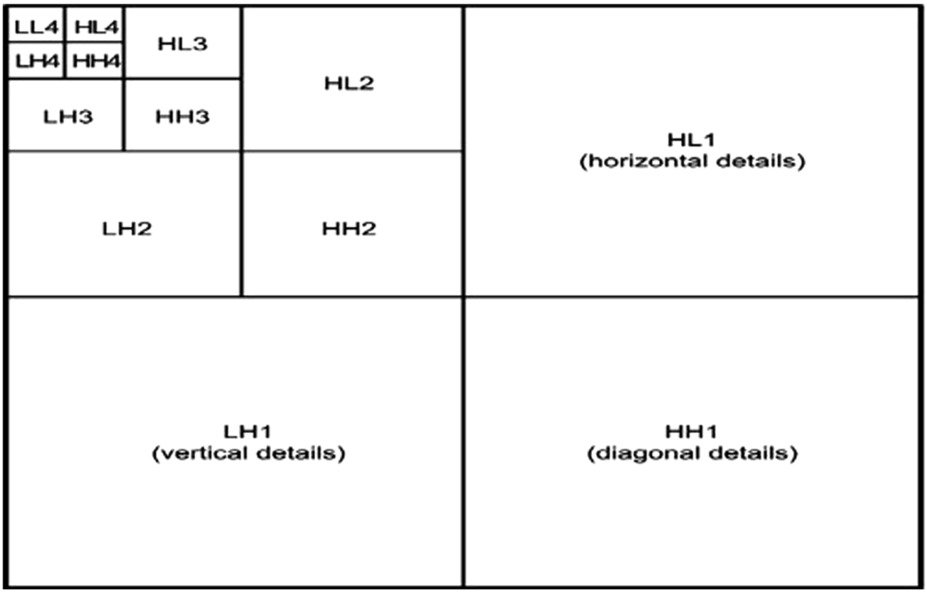


Fig. 1 Four level wavelet decomposed pyramid structure

embedding the principal component of a watermark into the host image in block based manner using spread spectrum concept. Shuffled Singular Value Decomposition (SSVD) is used in place of SVD to remove false positive problem with wavelet transform domain to embed watermarks. Eswaraiah et al. [8] proposed a method of RONI watermarking with exact recovery of ROI using SHA-1. To authenticate ROI, Hash code of ROI is calculated using SHA-1 technique. After this it divided ROI and RONI in blocks considering that ROI has lesser number of pixels than RONI. The recovery data of each ROI block is embedded into LSBs of pixels inside the corresponding mapped RONI block. Hajjaji et al. [11] 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. [14] focused on the issue of the security for medical images and proposed an encryption based image watermarking method in frequency and spatial domain. The 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 AES, RSA and RC4 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. [3] presented 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-non-interest (RONI) part of the cover image in order to avoid any compromise on its diagnostic value. 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 & pepper attacks. Badshah et al. [4] proposed a watermarking method based on Lempel-Ziv-Welch (LZW) compression technique using ultrasound medical images. In this method, the watermark is the combination of region of interest (ROI) and a secret key. The compression ratio has been compared with other compression techniques. Lu et al. [12] proposed a medical image watermarking algorithm using image and tag information as different watermarks. The image watermark is embedded in the ROI and the private tag information is embedded in the RONI part of the cover medical image. The watermark in the ROI is used to detect image tampering, and the watermark in the RONI is robust to different signal processing attacks.

1.2 Main contribution of work

In this research work, simultaneous embedding of four different watermarks (i.e. Signature, index, caption and reference watermark) in form of image and text has been carried out using fusion of discrete wavelet transforms (DWT) and singular value decomposition (SVD) on cover digital eye image. Experimental results illustrate that the proposed method is able to withstand 'Checkmark' attacks (http://watermarking.unige.ch/Checkmark/) [27]. The following observations are apparent:

- The main advantages of wavelet transform techniques for watermarking applications are: space frequency localization, multi-resolution representation, multi-scale analysis, adaptability and linear complexity. The wavelet based watermarking is also compatible with the image standard JPEG 2000. Due to its excellent spatio-frequency localization properties, the DWT is also very suitable to determine the embedding areas in the cover image where a watermark can be imperceptibly embedded. One of attractive mathematical properties of SVD is that slight variations of singular values do not affect the visual perception of the cover image, which motivates the watermark embedding procedure to achieve better performance in terms of imperceptibility, robustness and capacity as compared to DWT and SVD applied individually. However, the main drawback of the SVD-based image watermarking is its false positive problem of which a specific watermark is detected in a watermarked image that actually was not embedded in it [10]. The false positive problem present in SVD can be removed by using shuffled SVD (SSVD) [10]. Shuffled SVD improves the reconstructed image quality by breaking an image into set of ensemble images. The Shuffled SVD can be viewed as a pre-processing from SVD by permuting the original image with the data-independent permutation. In the proposed method, shuffled SVD can be used in place of SVD to remove false positive problem.
- Improved performance: The robustness of proposed method is compared with other reported techniques [33] and it is found that the proposed method offers superior performance. In addition, the method proposed by Singh et al.[33] has been embedded 812 bits only. However, proposed method can embed 5145 bits with acceptable visual quality of the watermarked image (determined by PSNR values).
- Enhance security: Security of the medical watermarks may be enhanced by using secure Hash Algorithm (SHA-512) [5, 23, 36]. MD5 (Message digest) and SHA-512 both are the hashing algorithm. In this research, the security of the watermark is the prime objective of the work. Table 1 [13] show that SHA 512 is more secure than the MD5. However, the computational speed of the MD5 algorithm is faster than the SHA-512. In addition, the important differences between these two hashing algorithms are given below in Table 1.

- For identity authentication purposes, multiple watermarks are embedded instead of single watermark into the same medical image / multimedia objects simultaneously, which offer superior performance in teleophthalmology, telemedicine and tele-diagnosis applications. In addition, simultaneous embedding of different watermarks on cover Iris image while addressing the management of EPR data also.
- Reduced storage and bandwidth requirements: The medical image files / electronic patient record (EPR) contain important patient data. Further, in order to conserve the transmission bandwidth or storage space the patient's details may be embedded inside the medical image.

2 Performance measures

The performance of the watermarking algorithm can be evaluated on the basis of its robustness and imperceptibility. A larger Peak Signal to Noise Ratio (PSNR) indicates that the watermarked image more closely resembles the original image meaning that the watermark is more imperceptible. Generally, watermarked image with PSNR value greater than 28 dB is acceptable [31]. The PSNR is defined as

$$\mathrm{PSNR} = 10\log\frac{(\mathrm{Bmax})^2}{\mathrm{MSE}} \tag{1}$$

Where Bmax is maximum pixel value of the image, the Mean Square Error (MSE) is defined as

$$\mathrm{MSE} = \frac{1}{\mathrm{X}\times\mathrm{Y}}\sum_{\mathrm{i}=1}^{\mathrm{X}}\sum_{\mathrm{j}=1}^{\mathrm{Y}}\left(\mathrm{I}_{\mathrm{ij}}-\mathrm{W}_{\mathrm{ij}}\right)^2 \tag{2}$$

where I_{ij} is a pixel of the original image of size XXY and W_{ij} is a pixel of the watermarked image of size XXY. The robustness of the algorithm determined in term of correlation factor. The similarity and differences between original 'watermark and extracted watermark is measured by the Normalized Correlation (NC). Its value is generally 0 to 1. Ideally it should be 1 but the value 0.7 is acceptable [31].

$$\mathrm{NC} = \sum_{\mathrm{i}=1}^{\mathrm{X}}\sum_{\mathrm{j}=1}^{\mathrm{Y}}\left(\mathrm{W}_{\mathrm{originalij}}\times\mathrm{W}_{\mathrm{recoveredij}}\right)/\sum_{\mathrm{i}=1}^{\mathrm{X}}\sum_{\mathrm{j}=1}^{\mathrm{Y}}\mathrm{W}^2_{\mathrm{originalij}} \tag{3}$$

Table 1 Comparison between two important hashing algorithms

Key points for comparison	MD5	SHA 512
Message-digest length in bits	128	512
Attack to try and find the original message given in message digest	Require 2^128 operations to break in	require 2^512 operations to break in, therefore more secure
Attack to try and find two message producing the same message digest	require 2^64 operations to break in	require 2^80 operations to break in
Speed	Faster (64 iterations, and 128-bit buffer)	Slower (80 iterations, and 512-bit buffer)
Software implementation	Simple	Simple

where $W_{originalij}$ is a pixel of the original watermark of size X × Y and $W_{recoveredij}$ is a pixel of the recovered watermark of size X × Y.

The bit error rate (BER) [31] 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.

$$\text{BER} = (\text{Number of incorrectly decoded bits})/(\text{Total number of bits}) \tag{4}$$

3 Proposed method

The proposed secure watermarking method provides a way of securing EPR data in cover eye image without affecting diagnostic important region (ROI). The selection of DWT decomposition level for embedding watermarks depends on size and desired robustness of watermark which is shown in Table 2. The embedding of text and image watermarks is embedding in NROI part of the cover image. A medical image may contain several regions of interest but this proposed watermarking algorithm uses a single one. There are several ways of choosing ROI part of any medical image such as forming a square or polygonal [1, 39], defining a threshold [6], defining seeds [9, 25] etc. The proposed algorithm defines ROI part by forming a rectangular boundary. The wavelet domain ROI map is produced based on the spatial self similarity between sub-bands [26]. The ROI part of the cover Iris image is used for modifying text watermarks using SHA-512 which will enhance security feature of this medical image watermarking scheme [2].

The technique has four parts, the image watermark embedding and extraction processes, and the text watermark embedding and extraction processes. The details of the four algorithms are given in separate subsections:

3.1 Watermark embedding algorithm

Embedding of watermark can be divided in two parts: text watermark and image watermark. The cover image (*I*) is first divided into two part ROI and NROI part. The DWT is applied on the NROI part of the cover image and now SVD is applied on the selected sub-band of the DWT cover. In addition, the hash value of the ROI part of the cover image is calculated by using the RSA hashing algorithm. The logical XOR operation has been applied on the ASCII value of the text watermark and the hash value of the ROI part of the cover which contain the encoded text watermark. Finally, the image and encoded text watermark is embedded into the

Table 2 Allocation of watermarks according to robustness and capacity criteria at different DWT sub-band

Sub-band used	Embedded watermark			Description of the considered watermarks
	Watermark types	Robustness requirements	Watermark size(bits)	
HL1	Reference	Low	512 × 512	Image watermark. To check the robustness against attacks.
HL2	Caption	High	4480 bits	This watermark contains most of the part of patient information
HL3	Index	High	483 bits	It provides an index for each type of disease
LL4	Signature	Very High	182 bits	Smallest watermark. It contains physician's signature which is used for authentication purpose

NROI part of the cover image. The detail description of the embedding algorithm for the text and image is given in Section 3.1.1 to 3.1.2 respectively. The extraction algorithm for the text and image is given in section 3.2.1 to 3.2.2 respectively.

The steps of embedding these watermarks are given below:

1. Read the cover Iris image I of size ($M \times N$).
2. Select iris by drawing a rectangular ROI for eye image and segment it,
3. Transform the image using "Haar" wavelet transform and get coefficients up to fourth level.
4. Apply SVD to selected sub-bands LL4, HL3, HL2 and HL1 which are used for embedding watermark.

3.1.1 Embedding algorithm for text watermark

1. Read the message to be hidden and convert it into binary sequence.
2. Compute hash of ROI by using SHA-512 algorithm and convert it into binary sequence.
3. Perform a logical XOR operation between hash of ROI and binary sequence of watermark. This will give embedding watermark w.
4. Repeat above mentioned steps for generating encoded signature watermark w_s, index watermark w_i and caption watermark w_c.
5. Select singular values which belong to RONI randomly of subbands LL4, HL3 and HL2 according to the size of w_s, w_i and w_c respectively.
6. Replace these singular values by generated watermarks.
7. Generate respective subbands using these modified singular values and singular vectors of respective sub-bands.

3.1.2 Embedding algorithm for image watermark

1. Read the image watermark w_{im} of size equal to size of sub band HL1.
2. Apply SVD to HL1 and w_{im} to compute singular values of them. Let singular values for HL1 and w_{im} are λ_c and λ_w respectively.
3. Modify singular value of HL1 by following equation:

$$\lambda_{cw} = \lambda_c + (\alpha \times \lambda_w) \tag{5}$$

   Where α is a scale factor.
4. Generate HL1 with this modified singular value.
5. Take inverse DWT to generate watermarked image.
6. Add ROI part to the watermarked image.

3.2 Watermark extraction algorithm

For extracting watermarks, we used the same hash of ROI and embedding key to extract watermark. To generate original watermarks cover image and original reference image is also required to get singular value. Following steps are applied to extract the watermark:

3.2.1 Extraction algorithm for text watermark

1. Transform watermarked image using “Haar” wavelet transform and get coefficients up to fourth level.
2. Apply SVD to 4^{th} level approximation coefficients a_4, 3^{rd} level horizontal coefficients b_3 and 2^{nd} level horizontal coefficients b_2.
3. Using same random pattern of selection of singular value generate the embedded watermarks bit by following equation for each above mentioned levels:

$$t_{ext} = \lambda_{wm} - \lambda_o \tag{6}$$

   Here λ_{wm} and λ_o are singular values of watermarked subbands and cover image subbands respectively.
4. Perform logical XOR operation between t_{ext} and hash of ROI which gives binary sequence of extracted watermark.
5. Convert these extracted binary sequences to character to generate original text watermark.

3.2.2 Extraction algorithm for image watermark

1. Apply SVD to 1^{st} level horizontal coefficients b_1.
2. Compute singular value for extracted image watermark by following equation:

$$\lambda_{ext} = (\lambda_{cw} - \lambda_c)/\alpha \tag{7}$$

3. Generate extracted image watermark using this singular value λ_{ext} and singular vectors of original reference image watermark which will give extracted reference watermark.

4 Experimental results & analysis

The performance of the proposed multiple watermarking technique is based on DWT, SVD and secure Hash Algorithm (SHA-512) is investigated. The text watermarks are extracted successfully from watermarked image using embedding key and hash of ROI of eye image. In the proposed method cover image of size 1024 × 1024, the image watermark of size 512 × 512 considered as a reference watermark and the text watermark of varying size are used for testing. The robustness of the image and text watermarks is evaluated by determining NC and BER respectively. The quality of the watermarked image is evaluated by PSNR. It is quite apparent that size of the watermark affects quality of the watermarked image. The size of the watermark is sum total of bits occupied by all watermarks in the case of multiple watermarking. However, degradation in quality of the watermarked image will not be observable if the size of watermark (total size in case of multiple watermarking) is small. Figure 2a and b shows the cover and watermarked image respectively. Figure 3 show the extracted signature, index and caption watermarks. Figure 4a and b shows original and extracted reference watermarks respectively.

Table 3 shows the PSNR, BER and NC performance of the proposed method at different scale factor. It is found that larger gain factor results in stronger robustness of the extracted watermark whereas smaller gain factor provides better PSNR values between original and watermarked medical images. The maximum PSNR value is 35.84 dB and BER = 0 against at gain factor = 0.01. Here, the NC value is 0.87. However, the maximum NC value is 0.99 at gain factor = 0.2. Here, the PSNR value is 39.97 dB. For all the considered text watermark BER value is Zero. It is found that larger the gain factor results stronger robustness of extracting watermark whereas smaller the gain factor provides better visual quality of the watermarked image.

In this work, JPEG attacks with different quality factors are considered as signal a processing attack which is shown in Table 4. However, the other attacks are considered as Checkmark attacks which is shown in Table 5. Table 4 shows BER and NC performance of the proposed method for JPEG attacks at different quality factors (QF) at gain = 0.09. The highest NC value of 0.98 has been obtained against JPEG Compression with quality factor = 95. However, the minimum NC value of 0.957 has been obtained against JPEG Compression with quality factor = 55. For all the considered text watermark BER value is Zero. Table 5 shows the BER and NC performance of the proposed method for 'Checkmark' attacks. The maximum BER value of 8.514 has been obtained against Gaussian Noise (Mean =0, Variance = 0.05) for the caption watermark, where the NC value is 0.792. However, the maximum NC value of 0.99 has been obtained against Flip, where the BER value is '0' for the entire chosen text watermark.

In Table 6, the visual quality (determined by PSNR values) of the watermarked image robustness performance (determined NC values) of the proposed method is compared with other methods [33] at different gain factors. It is observed that the proposed method offers higher visual quality and robustness at all considered gain as compared to the other reported method. Referring this table, the maximum NC value with proposed method has been obtained as 0.984 against 0.9697 obtained by Singh et al. in [33] method at gain factor = 0.1. However, the minimum NC value with proposed method has been obtained as 0.87 against 0.5247 obtained by Singh et al. in [33] method at gain factor = 0.01. The maximum PSNR value has been obtained with Singh et al. in [33] is 28.17. However, the maximum PSNR value has been obtained by the proposed method is 54.26 dB at gain factor = 0.01. However, the minimum PSNR value has been obtained with Singh et al. in [33] is 26.85 dB. However, the minimum

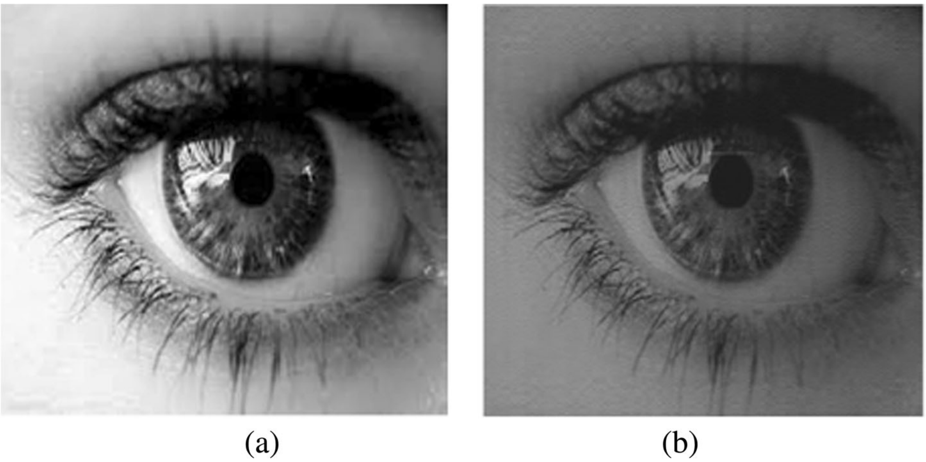
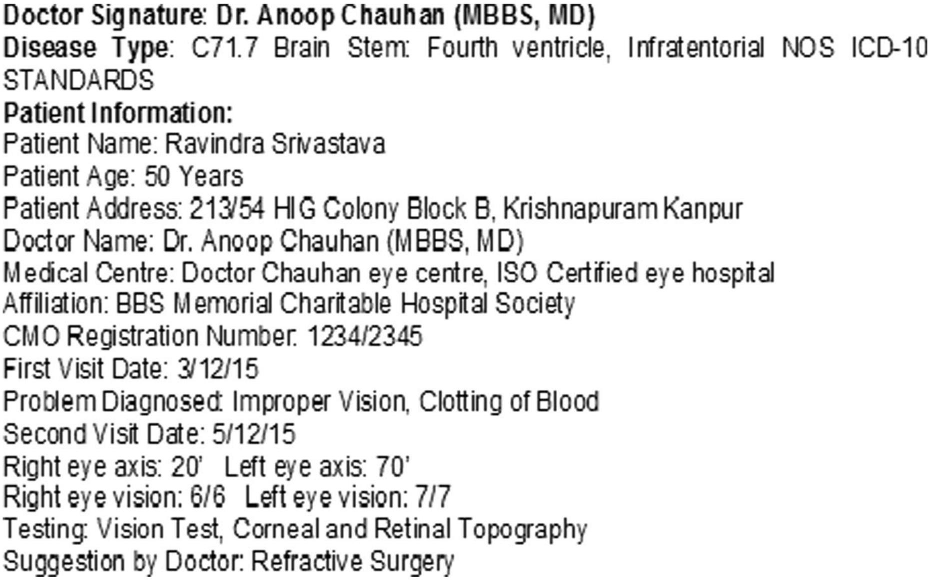


Fig. 2 **a** Original cover image and **b** watermarked image



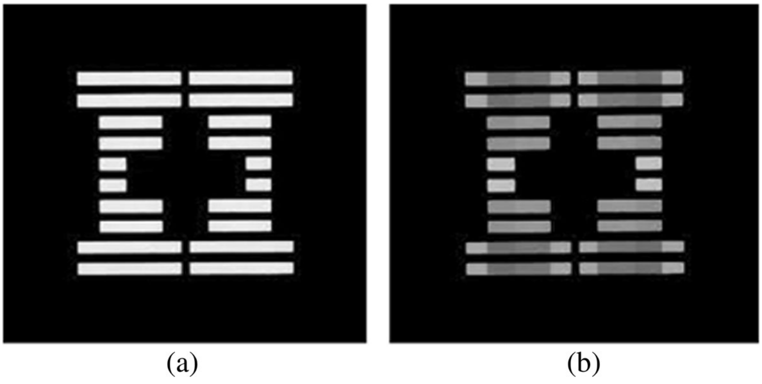
Doctor Signature: Dr. Anoop Chauhan (MBBS, MD)
Disease Type: C71.7 Brain Stem: Fourth ventricle, Infratentorial NOS ICD-10 STANDARDS
Patient Information:
Patient Name: Ravindra Srivastava
Patient Age: 50 Years
Patient Address: 213/54 HIG Colony Block B, Krishnapuram Kanpur
Doctor Name: Dr. Anoop Chauhan (MBBS, MD)
Medical Centre: Doctor Chauhan eye centre, ISO Certified eye hospital
Affiliation: BBS Memorial Charitable Hospital Society
CMO Registration Number: 1234/2345
First Visit Date: 3/12/15
Problem Diagnosed: Improper Vision, Clotting of Blood
Second Visit Date: 5/12/15
Right eye axis: 20' Left eye axis: 70'
Right eye vision: 6/6 Left eye vision: 7/7
Testing: Vision Test, Corneal and Retinal Topography
Suggestion by Doctor: Refractive Surgery

Fig. 3 Extracted signature, index and caption watermark

PSNR value has been obtained by the proposed method is 39.58 dB at gain factor = 0.1. In addition, the method proposed by Singh et al.[33] has been embedded 812 bits only. However, in our proposed method, we can embed 5145 bits with the acceptable PSNR performance. Overall, the performance of the proposed method is better than the other reported technique [33] in terms of robustness, capacity and security. Finally, the overall PSNR, NC and BER performance of the proposed method highly depends on the size of the watermarks (image and text), gain factor and the noise variation.

5 Conclusion and future directions

The proposed algorithm provided a new watermarking technique for eye care centers dealing with eye image transmission by hiding information about patient and doctor in a



(a) (b)

Fig. 4 Reference watermark **a** original **b** extracted

Table 3 PSNR, BER and NC performance at different scale factor

Scale factor (α)	PSNR (dB)	BER values for text watermark			NC values for Image watermark
		Signature watermark	Index watermark	Caption watermark	
0.01	54.26	0	0	0	0.87
0.03	51.79	0	0	0	0.91
0.05	48.42	0	0	0	0.93
0.07	45.82	0	0	0	0.96
0.09	42.68	0	0	0	0.98
0.2	39.97	0	0	0	0.99

secure way using cryptographic hash function of the iris pattern. Each embedded watermarks has different characteristics in terms of capacity, type and size of information, robustness and application. The described watermarking technique is robust to compression and ‘Checkmark’ attacks. Use of SVD along with DWT increased the robustness of algorithm. As the hash encoded watermarks were embedded randomly in singular values hence without knowledge of embedding key, data could not be extracted which enhanced the security of watermarking system. In this research, the gray scale images have been considered. However, the watermark embedding into color image provides greater space against the watermark embedding into gray scale image. This space will hide more watermark information (capacity will improve). The choice of color space and selection of embedding color channel is important ‘RGB’ model and watermarking in blue plane is not suitable due to poor robustness against compression attacks. This is because the blue channel is heavily quantized during JPEG compression. However, blue channel is able to give better imperceptibility. The ‘YCbCr’ model gives advantage of robustness against compression attacks if watermark is embedded in ‘Y’ channel because ‘Y’ channel is less quantized as compared to chrominance channels (‘Cb’ and ‘Cr’) in JPEG compression process. However, ‘Y’ channel (Luminance) is more sensitive to human eyes. Therefore, even small modifications in the wavelet coefficients of this channel may lead to poor imperceptibility which limits the embedding capacity of ‘Y’ channel. The major findings of this work can be identified as follows:

Table 4 BER and NC performance for JPEG attacks at different quality factors(QF)

JPEG attacks	BER values for text watermark			NC values for Image watermark
	Signature watermark	Index watermark	Caption watermark	
QF = 95	0	0	0	0.98
QF = 85	0	0	0	0.975
QF = 75	0	0	0	0.964
QF = 65	0	0	0	0.96
QF = 55	0	0	0	0.957

Table 5 BER and NC performance for 'checkmark' attacks

Checkmark attacks	BER values for text watermark			NC values for image watermark
	Signature watermark	Index watermark	Caption watermark	
Sharpening	0	0	0	0.918
Gaussian Noise (Mean =0, Variance = 0.01)	0	0	0	0.8325
Gaussian Noise (Mean =0, Variance = 0.05)	0	1.62	8.514	0.792
Frequency mode LR Attack	0	0	0	0.6628
Flip	0	0	0	0.99
Median Filtering [2 2] and [3 3]	0	0	0	0.9077 and 0.8560
Hard threshold	0	0	0	0.9834
Rotation (20°)	0	0	0	0.9255
Dither	0	0	0	0.7058
Scaling by 2.5	0	1.01	6.45	0.695
Warping (wf = 5)	0	0	0	0.624
Wiener Filtering [2 2] and [3 3]	0	0	0	0.9125 and 0.862

- With excellent spatio-frequency localization properties, the DWT is also very suitable to determine the embedding areas in the cover image where a watermark can be imperceptibly embedded. One of attractive mathematical properties of SVD is that slight variations of singular values do not affect the visual perception of the cover image, which motivates the watermark embedding procedure to achieve better performance in terms of imperceptibility, robustness and capacity as compared to DWT and SVD applied individually.
- For identity authentication purposes, multiple watermarks are embedded instead of single watermark into the same medical image / multimedia objects simultaneously, which offer superior performance in various applications.
- The PSNR and NC performance of the proposed method is compared with other reported techniques and it is found that the proposed method offers superior

Table 6 Comparison of PSNR and NC values with other reported method

Gain factor	Singh et al.[33]		Proposed method	
	PSNR(dB)	NC	PSNR (dB)	NC
0.01	28.17	0.5247	54.26	0.87
0.05	28.02	0.9288	48.42	0.93
0.09	27.17	0.9668	42.68	0.98
0.1	26.85	0.9697	39.58	0.984

performance. In addition, the capacity of embedding text watermarks is better than the other reported technique.

- Security of the medical watermarks is enhanced by using secure Hash Algorithm (SHA-512) for generating hash of ROI part (iris) of the cover eye image, which provides 256 bits of hash.
- The medical image files / electronic patient record (EPR) contain important patient data. Further, in order to conserve the transmission bandwidth or storage space the patient's details may be embedded inside the medical image.
- The proposed multilevel watermarking approach aims to simultaneously embed different types of watermarks on cover eye image while addressing the management of EPR data also.

This method may provide a potential solution to existing teleophthalmology security problem of patient identity theft. The inclusions of many techniques were combined to improve the robustness, high capacity (in form of multiple watermarks) and include the security of the watermarks with the acceptable quality of the watermarked image for the Teleophthalmology application which is the prime objective of the research. However, it may have increased the computational complexity to some extent which needs to be investigated separately.

We would like to further improve the performance in terms of robustness, visual quality of the watermarked image, additional security of watermark, capacity of the cover multimedia object, false positive problem of the SVD and poor directionality information of DWT, which will be reported in future communication.

References

1. Aggeliki G, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Med Biol Eng Comput 44(8):619–631
2. Ahmed F, Siyal MY, Abbas VU (2010) A secure and robust hash-based scheme for image authentication. Signal Process 90(5):1456–1470
3. Al-Haj A, Amer A (2014) Secured telemedicine using region-based watermarking with tamper localization. J Digit Imaging 27(6):737–750
4. Badshah G, Liew S-C, Zain JM, Ali M (2015) Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique, J Digit Imaging:1–10
5. Bouslimi D, Coatrieux G, Cozic M, Roux C (2012) A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans Inf Technol Biomed 16:891–899
6. Das S, Kundu MK (2013) Effective management of medical information through ROI-lossless fragile image watermarking technique". Comput Methods Prog Biomed 111(3):662–675
7. Dhanalakshmi R, Thaiyalnayaki K (2010) Dual watermarking scheme with encryption. Int J Comput Sci Inf Secur 7(1):248–253
8. Eswaraiah R, Sreenivasa Reddy E (2014) Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. Int J Telemed Appl 2014(2014):1–10
9. Gunjal BL, Mali SN (2012) ROI based embedded watermarking of medical images for secured communication in telemedicine". Int J Comput Commun Eng 6(48):293–298
10. Guo J-M, Prasetyo H (2014) False-positive-free SVD-based image watermarking. Journal of Visual Communication and Image Representation 25(5):1149–1163
11. Hajjaji MA, Bourennane E-B, Abdelali AB, Mtibaa A (2014) Combining Haar wavelet and Karhunen Loeve transforms for medical images watermarking. BioMed Res Int 2014:1-15
12. Jianfeng L, Meng W, Junping D, Qianru H, Li L, Chin-Chen C (2015) Multiple watermark scheme based on DWT-DCT quantization for medical images. J Inf Hiding Multimedia Signal Process Ubiquit Int 6(3):458–472
13. Kahate A (2013) Cryptography and network security, TMH 2nd edition. Mcgraw Hill Education, India

14. Kannammal A, Subha Rani S (2014) Two Level Security for Medical Images Using Watermarking/Encryption Algorithms. Int J Imaging Syst Technol 24:111–120
15. Kundu MK, Das S (2010). Lossless ROI medical image watermarking technique with enhanced security and high payload embedding. 20th International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, pp. 1457–1460, August 2010
16. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
17. Lin W-H, Horng S-J, Kao T-W, Fan P, Lee C-L, Pan Y (2008) An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans Multimed 10(5):746–757
18. Lin W-H, Wang Y-R, Horng S-J, Kao T-W, Pan Y (2009) A blind watermarking method using maximum wavelet coefficient quantization. Expert Syst Appl 36(9):11509–11516
19. Lin W-H, Wang Y-R, Horng S-J (2009) A wavelet-tree-based watermarking method using distance vector of binary cluster. Expert Syst Appl 36(6):9869–9878
20. Mahajan LH, Patil SA (2013) Image watermarking scheme using SVD. Int J Adv Res Sci Eng 2(6): 69–77
21. Memon NA, Gilani SAM (2008) NROI watermarking of medical images for content authentication, In: Proceedings of 12th IEEE international multi topic conference, Karachi, Pakistan, pp. 106–110, 2008
22. Mousavi SM, Naghsh A, Abu-Bakar SAR (2014) Watermarking techniques used in medical images: a survey. J Digit Imaging 27(6):714–729
23. Paar C, Pelzl J (2009) Understanding cryptography: a textbook for students and practitioners,3rd edition, Springer, pp.29-53
24. 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. Am J Biomed Eng 2(2):29–37
25. Pal K, Mankar VH, Das TS, Sarkar SK (2010) Contour detection and recovery through bio-medical watermarking for telediagnosis. Int J Tomogr Simul™ 14(S10):109–119
26. PC Su, Wang HJ, Kuo CCJ (1999) Digital image watermarking in regions of interest, Proceedings of 1999 PICS 52nd annual conference Savannah, Georgia, pp. 295–300, 1999
27. Pereira S, Voloshynovskiy S, Madueño M, Marchand-Maillet S, Pun T (2001) Second generation benchmarking and application oriented evaluation, In information hiding workshop III, Pittsburgh, PA, USA, pp. 340–353, 2001
28. Rey C, Dugelay JL (2002) A survey of watermarking algorithm for image authentication. EURASIP J Appl Signal Process 2002(1):613–621
29. Singh AK (2015) Some new techniques of improved wavelet domain watermarking for medical images, PhD Thesis, National Institute of Technology Kurukshetra, Haryana, India, 2015
30. Singh AK, Dave M, Mohan A (2014) Wavelet based image watermarking: futuristic concepts in information security. Proc Natl Acad Sci India Sect A: Phys Sci 84(3):345–359
31. Singh AK, Dave M, Mohan A (2015) Hybrid technique for robust and imperceptible multiple watermarking using medical images. J Multimedia Tools Appl. doi:10.1007/s11042-015-2754-7
32. Singh AK, Dave M, Mohan A (2015) Multilevel encrypted text watermarking on medical images using spread-spectrum in DWT domain. Wirel Pers Commun: Int J 83(3):2133–2150
33. Singh AK, Dave M, Mohan A (2015) Robust and secure multiple watermarking in wavelet domain, a special issue on Advanced Signal Processing Technologies and Systems for Healthcare Applications(ASPTSHA). J Med Imaging Health Inform 5(2):406–414
34. Singh AK, Dave M, Mohan A (2015) Multiple watermarking on medical images using selective DWT coefficients. J Med Imaging Health Inform 5(3):607–614
35. Singh AK, Kumar B, Dave M, Mohan A (2015) Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun 80(4):1415–1433
36. Wong PW, Memon N (2001) Secret and public key image watermarking scheme for image authentication and ownership verification. IEEE Trans Image Process 10(10):1593–1601
37. Yang C-Y, Hu W-C (2010) Reversible data hiding in the spatial and frequency domains. Int J Image Process 3(6):373–384
38. Zain J, Clarke M (2005) Security in telemedicine: issue in watermarking medical images. In: Proceedings of 3rd International conference on science of electronic, technologies of information and telecommunications, TUNISIA, March 27–31, 2005
39. Zain JM, Clarke M (2007) Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. Int J ComputSci Netw Secur 7(9):19–28
40. Zhang L, Zhou P-P (2010) Localized affine transform resistant watermarking in region-of-interest. Telecommun Syst 44(3):205–220

Richa Pandey received M.Tech in Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad in 2015. Her research interests include Data Hiding & Cryptography.

Dr. Amit Kumar Singh is currently working as Assistant Professor in the Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT) Waknaghat, Solan, Himachal Pradesh-India since April 2008. He was previously associated with Purvanchal University (U.P. State University), Jaunpur as Lecturer and prior to that he was Investigator-I in Rajbhasha Information Technology Application Promotion Programme (RITAP) Project, funded by Information Ministry, Department of Computer Science & Engineering, Indian Institute of Technology BHU Varanasi-India. He has completed his PhD degree from the Department of Computer Engineering, NIT Kurukshetra, Haryana in 2015. He obtained his M. Tech degree in Computer Science and Engineering from JUIT Waknaghat, Solan, Himachal Pradesh in 2010. He obtained his B. Tech degree in Computer Science and Engineering from Institute of Engineering and Technology, Purvanchal University Jaunpur, Uttar Pradesh in 2005. He has presented and published over 40 research papers in reputed journals and various national and international conferences. His important research contributions includes to develop watermarking methods that offer a good trade-off between major parameters i.e. perceptual quality, robustness, embedding capacity and the security of the watermark embedding into the cover digital images. His research interests include Data Hiding, Biometrics & Cryptography.

Dr. Basant Kumar is currently working as Assistant Professor in Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad. He has more than 13 years of teaching and research experience. He obtained his B.Tech. degree in Electronics and Instrumentation Engineering from Bundelkhand Institute of Engineering and Technology, Jhansi, Uttar Pradesh, and M.E. degree in Communication Engineering from Birla Institute of Technology and Science, Pilani, in 1999 and 2002 respectively. He received Ph.D. in Electronics Engineering from Indian Institute of Technology, Banaras Hindu University, Varanasi, India (IIT-BHU) in 2011. His area of research includes telemedicine, data compression, data hiding, multimedia communication and medical image processing. He has published more than 30 research papers in reputed international journals/conferences.

Prof. 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*