Multimed Tools Appl (2016) 75:8381–8401
DOI 10.1007/s11042-015-2754-7

Hybrid technique for robust and imperceptible multiple watermarking using medical images

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

Received: 13 October 2014 / Revised: 22 April 2015 / Accepted: 15 June 2015 /
Published online: 16 July 2015

Abstract This paper presents a secure multiple watermarking method based on discrete wavelet transform (DWT), discrete cosine transforms (DCT) and singular value decomposition (SVD). For identity authentication purpose, the proposed method uses medical image as the image watermark, and the personal and medical record of the patient as the text watermark. In the embedding process, the cover medical image is decomposed up to second level of DWT coefficients. Low frequency band (LL) of the host medical image is transformed by DCT and SVD. The watermark medical image is also transformed by DCT and SVD. The singular value of watermark image is embedded in the singular value of the host image. Furthermore, the text watermark is embedding at the second level of the high frequency band (HH) of the host image. In order to enhance the security of the text watermark, encryption is applied to the ASCII representation of the text watermark before embedding. Results are obtained by varying the gain factor, size of the text watermark, and medical image modalities. Experimental results are provided to illustrate that the proposed method is able to withstand a variety of signal processing attacks such as JPEG, Gaussian, Salt-and-Pepper, Histogram equalization etc. The performance of the proposed technique is also evaluated by using the benchmark software Checkmark and the technique is found to be robust against the Checkmark attacks such as Collage, Trimmed Mean, Hard and Soft Thresholding, Wavelet Compression, Mid Point, Projective, and Wrap etc.

✉ Amit Kumar Singh
amit_245singh@yahoo.com

Mayank Dave
mdave67@gmail.com

Anand Mohan
profanandmohan@gmail.com

[1] Department of Computer Science & 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

Keywords Image watermark · Text watermark · Steganography · DWT · DCT · SVD · Encryption · Checkmark

1 Introduction

Information technology has eased the duplication, manipulation and distribution of digital data in recent times which has resulted in the demand for safe ownership of digital multimedia contents such as images, video and audio. The multimedia content-authentication and copyright protection has become an ongoing and constant requirement for protecting the media [6]. Recently, telemedicine applications play an important role in the development of the medical field. However, protect the transmission, storage and sharing of electronic patient record (EPR) data between two hospitals or via open channel are the most important issues in this field. Also, the digital imaging and communications in medicine (DICOM) is a basic criterion to communicate EPR data. A header is attached with the DICOM medical image files which contain important information about the patient, but it may be lost, attacked or disorder with other header file.

Digital watermarking is a technique which provides a best solution to these important issues [19]. The other advantages of the medical image watermarking are listed below [22]: 1) Storage space required for the image and the patient record is very voluminous. For small hospitals financial economy is an important decisive factor. Embedding the data in the corresponding images will save so much of the storage space. 2) Huge amount of bandwidth is required for the transmission of the image data for telemedicine purposes. The additional requirement of bandwidth for the transmission of the metadata can be avoided if the data is hidden in the image itself. Since the EPR and the image embedded into one, bandwidth for the transmission can be reduced in telemedicine applications. 3) Normally a patient does not like to expose his medical report to public; especially if the disease is of clandestine nature. The utmost confidentiality can be maintained by hiding the data in the image. When the patient data text and image are sent separately, if a tampering is done on the text or image, the after-effects may even cost a life due to wrong diagnosis. Most of the internet users are ignorant of the esoteric terms of watermarking techniques. When the patient data is hidden in medical image, such people will not try to tamper it. If tampered, it can be made out by using appropriate watermarking technique. Moreover, medical identity theft is a growing and dangerous crime as reported in various surveys [2, 25]. This demands development of secure medical data/image watermarking schemes.

The digital watermarking is a technique for inserting information into a cover massages (text, image, audio or video data) and later extracted or detected for variety of purposes including identification and authentication. Many wavelet based watermarking schemes were proposed for medical images [7, 10, 11, 18, 26, 35, 38, 40, 42]. Depending upon the type of data to be watermarked, the watermarking methods can be classified into four categories: text watermarking, image watermarking, audio watermarking, and video watermarking [32]. However, due to higher data embedding capacity of image covers, the present work focuses on watermarking using medical image as cover media. The image watermarking methods can be further classified as 'spatial domain' and 'transform domain' methods. Spatial domain methods are straight forward and computationally simple. LSB substitution, spread spectrum, and patchwork are the important spatial domain techniques. In spatial domain watermarking the watermark data is embedded directly by manipulating the pixel values, bit stream or code values of the host signal (cover media). However, spatial domain techniques are offer less robustness against attacks.

A spatial domain based digital image watermarking method is proposed by Lin et al. [12]. In this method, the host image is lossless and the watermark is robust to malicious attacks including geometric and non-geometric attacks. In the embedding process, the watermark logo is fused with noise bits first, and later XORed with the feature value of the image by $1/T$ rate forward error correction (FEC), where T is the times of data redundancy. During extraction process, the watermark bits are determined by majority voting. The experimental results have been shown that not only the image is lossless but also the proposed method can effectively resist the common malicious attacks. Also, the proposed method does not transfer the protected images to transform domain, and hence it can reduce the computation time of embedding and extraction process.

In the transform domain techniques the data is embedded by modulating the coefficients of a transform like discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD). The transform domain watermarking techniques are computationally complex but they provide greater robustness of watermarked data. Recently, the higher robustness of watermark has been achieved by using wavelet based watermarking are presented in [13–15]. 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 new image standard JPEG 2000. Further, performance improvement of the watermarking methods using hybrid watermarking has been proposed by some researchers [1, 4, 5, 8, 9, 16, 20, 23, 28–31, 34, 36, 39]

Rosiyadi et al. [28] proposed a hybrid watermarking method based on DCT and SVD for the copyright protection. In this embedding process, DCT is applied on the host image using the zigzag space-filling curve (SFC) for the DCT coefficients and subsequently the SVD is applied on the DCT coefficients. Finally, the host image is modified by the left singular vectors and the singular values of the DCT coefficients to embed the watermark image. In this method, Genetic Algorithm (GA) based technique is used to find the optimization scaling factor of the watermark image. They have experimentally shown that the proposed method is robust against several kinds of attacks. The comparison between the method based on DCT and SVD using GA and the hybrid method based on DCT-SVD has been presented by Rosiyadi et al. in [29]. It is shown that the robustness of the extracted watermark and the visual quality of the watermarked image of the method using GA technique is better than the hybrid method. Horng et al. [31] proposed a blind watermarking method based on DCT, SVD and GA. It is shown that this method is robust and offers high imperceptibility against several known attacks.

Horng et al. [30] proposed an adaptive watermarking method based on DCT, SVD and GA. In this embedding process, the host image luminance masking is used and the mask of each sub-band area is transformed into frequency domain. Subsequently, the watermark image is embedded by modifying the singular values of DCT-transformed host image with singular values of mask coefficients of host image and the control parameter of DCT-transformed watermark image using GA. It is shown that this method is robust against several known attacks.

Consequently, many other image watermarking techniques combining three transform methods have been proposed [1, 4, 5, 8, 9, 16, 20, 23, 34, 36, 39]. For a detailed description on these combined approaches, interested readers may directly refer to them.

Singh et al. [32] proposed a robust hybrid watermarking technique using fusion of DWT, DCT, and SVD instead of applying DWT, DCT and SVD individually or combination of DWT-SVD / DCT-SVD. The suggested technique initially decomposes the host image into first level DWT followed by transformation of Low frequency band (LL) and watermark image using DCT and SVD. Then the S vector of watermark image is embedded in the S component of the host image and the watermarked image is generated by inverse SVD on modified S vector and original U, V vectors followed by inverse DCT and inverse DWT. The watermark is extracted using an extraction algorithm. The proposed method has been extensively tested and analyzed against known attacks.

Terzija et al. [37] have proposed a method for improving efficiency and robustness of the watermarks using three different error correction codes namely, (15,7)-BCH, (7,4)-Hamming Code and (15-7)-Reed-Solomon code. These codes are applied to the ASCII representation of the text which is used as watermark. The watermark is embedded into the original cover image by first decomposing the cover up to second level using discrete wavelet transform (DWT) with the pyramidal structure and then the watermark is added to the largest DWT coefficients that represent high and middle frequencies of the cover image. It is shown that Reed-Solomon code performs better due to its excellent ability to correct errors, however, the ECCs considered are not able to deal with bit error rates (BER) greater than 10–20 %.

In this paper, we are using Singh method to embed the image watermark and Terzija method to embed text watermark. Results are obtained by varying the gain factor, size of watermark, and medical image modalities. Experimental results are provided to illustrate that the proposed method is able to withstand a known attacks.

The following observation are apparent:

1) Capacity of embedding multiple watermark: The method proposed in [1, 4, 5, 8, 9, 16, 20, 23, 34, 36, 39] has been embedded only one watermark. However, in the proposed method multiple watermarks (text and image) are embedded simultaneously, which provides extra level of security with acceptable performance in terms of robustness and imperceptibility. 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 telemedicine and tele-diagnosis applications. The simultaneous multiple watermarking embedding method has fewer constraints than the other multiple watermarks embedding methods [33].
2) Improved robustness performance: In Table 5, The robustness of proposed method is compared with other reported techniques [29, 34, 36] and it is found that the proposed method offers superior performance
3) Enhance 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.
4) 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.

Therefore the proposed method may find potential application in prevention of patient identity theft in telemedicine applications

2 Theoretical background

The proposed multiple watermarking method based on DWT, DCT and SVD. The watermark image will be discrete Cosine transformed at first. The DCT information of the watermark image contains low frequency information and as long as such information is not lost or lost a little, the watermarking image can be extracted well. One of important 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 quality of the watermarked image and robustness of the extracted watermark. Hence, a brief description of these concepts is included in the given below sections.

2.1 Discrete wavelet transform (DWT)

The DWT has received considerable attention in various signal processing applications, including image watermarking. 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 [11]. DWT separates an image into a set of four non- overlapping multi-resolution sub bands denoted as lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) 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 (LL sub-band), the watermark can be embedded into the other three sub-bands (HL, LH and HH 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 [3].

2.2 Discrete cosine transform (DCT)

The discrete cosine transform (DCT) works by separating image into parts of different frequencies, low, high and middle frequency coefficients [32], makes it much easier to embed the watermark information into middle frequency band that give additional resistance to the lossy compression techniques, while avoiding significant modification of the cover image. The DCT has a very good energy compaction property. For an input image, I, of size N x N the DCT coefficients for the transformed output image, D, are computed according to Eq. (1). I (x,y) is the intensity of the pixel in row x and column y of the image, and D (i, j) is the DCT coefficient in row i and column j of the DCT matrix.

$$\begin{gathered} D\,(i,j) \;=\; \frac{1}{\sqrt{2N}} C\,(i)\,C\,(j) \sum\nolimits_{x=0}^{N-1} \sum\nolimits_{y=0}^{N-1} I\,(x,y)\; cos\,\frac{(2x+1)i\pi}{2N} cos\,\frac{(2y+1)i\pi}{2N} \\ \mathrm{C(i), C(j)} = \frac{1}{\sqrt{\mathrm{N}}}\ \text{ for i,}\quad \mathrm{j}=0 \quad \text{and} \quad \mathrm{C(i), C(j)} = \sqrt{\frac{2}{\mathrm{N}}}\ \text{for i, j} = 1, 2, \ldots\ldots.\mathrm{N}-1 \end{gathered} \tag{1}$$

2.3 Singular value decomposition (SVD)

The singular value decomposition of a rectangular matrix R_m is a decomposition of the form

$$R_m = USV^T \tag{2}$$

Where R_m is an M × N matrix, U and V are orthonormal matrices, S is a diagonal matrix comprised of singular values of R_m. The singular values s1≥s2≥………≥sn≥0 appear in descending order along the main diagonal of S. These singular value are obtained by taking the square root of the Eigen values of $R_m R_m^T$ and $R_m^T R_m$. The singular values are unique; however the matrices U and V are not unique [32].

2.4 Encryption and decryption process of EPR data

For providing additional security, text watermark (EPR data) may be encrypted before watermarking. However, the delay encountered during embedding and extraction of the watermark is also an important factor in telemedicine applications. Therefore, watermarking methods using encryption techniques should be simple to save execution time [41]. The text watermark in the proposed method is encrypted using the equation

$$\text{Encrypted text watermark} = (\text{text watermark}^{r}) - d \tag{3}$$

where r and d are constants. Here, r can have a value in the range 1.000 to 1.143 and d can be between 0.0 and 10.0. The first level of security lies in this encryption process [21].

The extracted encrypted text is decrypted at the receiving end using the relation

$$\text{Decrypted text watermark} = (\text{Encrypted text watermark} + d)^{\frac{1}{r}} \tag{4}$$

3 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 27 is acceptable [32]. The PSNR is defined as

$$\text{PSNR} = 10\log\frac{(\text{Bmax})^2}{\text{MSE}} \tag{5}$$

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

$$\text{MSE} = \frac{1}{X \times Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}\left(I_{ij} - W_{ij}\right)^2 \tag{6}$$

where I_{ij} is a pixel of the original image of size X × Y and W_{ij} is a pixel of the watermarked image of size X × Y. 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 [32].

$$\mathrm{NC} = \sum\nolimits_{\mathrm{i}=1}^{\mathrm{X}}\sum\nolimits_{\mathrm{j}=1}^{\mathrm{Y}}\left(\mathrm{W}_{\mathrm{originalij}} \times \mathrm{W}_{\mathrm{recoveredij}}\right) / \sum\nolimits_{\mathrm{i}=1}^{\mathrm{X}}\sum\nolimits_{\mathrm{j}=1}^{\mathrm{Y}}\mathrm{W}^{2}_{\mathrm{originalij}} \tag{7}$$

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

The bit error rate (BER) [33] 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.

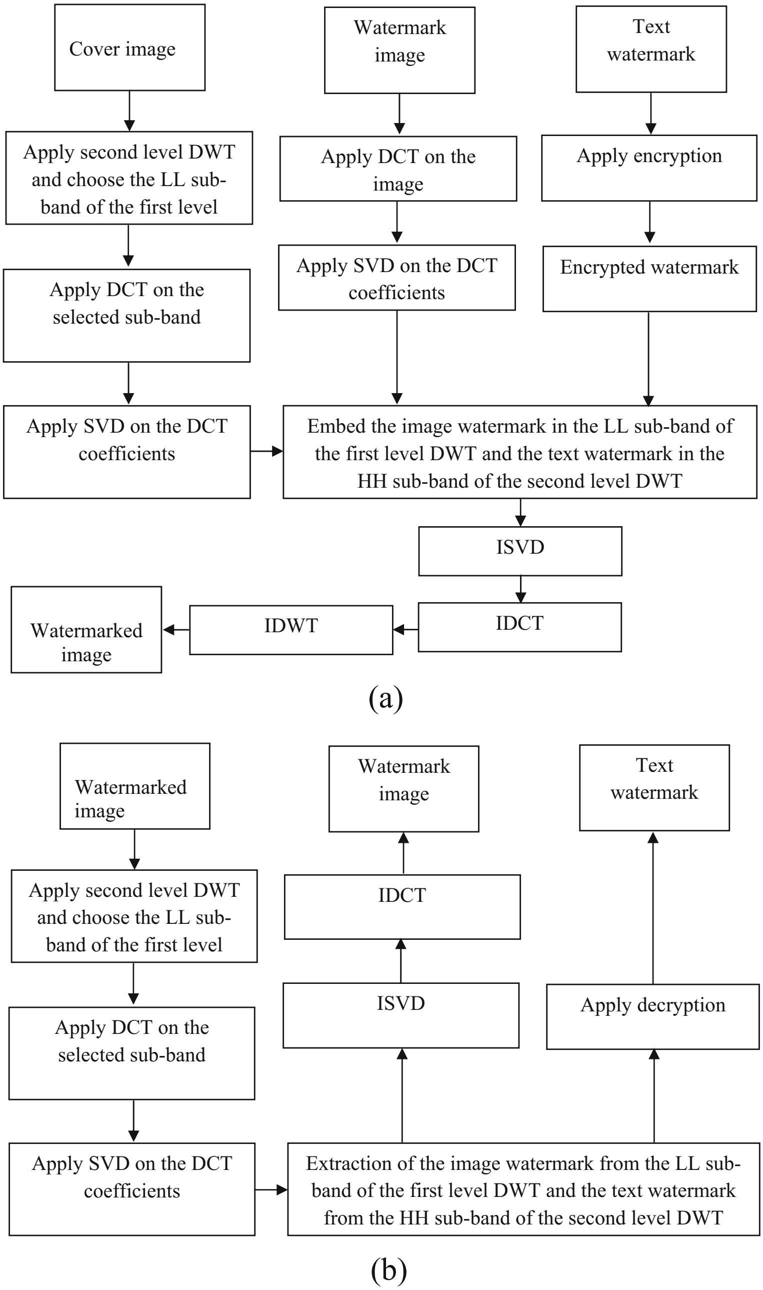
$$\mathrm{BER} = \ (\text{Number of incorrectly decoded bits})/(\text{Total number of bits}) \tag{8}$$

4 Proposed method

The method proposed is a combined DWT, DCT and SVD based process. The proposed method increases the robustness without significant degradation of image quality against the signal processing attacks. Figure 1a and b illustrates the multiple watermark embedding and extraction process respectively. The algorithmic steps are discussed below:

4.1 Embedding algorithm for image watermark

```
start:
  STEP 1: Variable Declaration
  Barbara Image: cover image
  Medical Image (Thorax): watermark image
  C_w: read the cover image
  W_w: read the watermark image
  α: gain factor
  DWT, DCT and SVD: Transform Domain Techniques
  Wavelet filters: Haar
  $LL_c$, $LH_c$, $HL_c$, and $HH_c$: First level DWT coefficients for cover image
  D: DCT coefficients of watermark image
  $D_c^1$: DCT coefficients matrix for $HH_c$
  $U_c$ and $V_c^T$: orthonormal matrices for $D_c^1$
  $S_c$: diagonal matrix for $D_c^1$
  $U_w$ and $V_w^T$: orthonormal matrices for D
  $S_w$: diagonal matrix for D
  $W_w^k$: modified value of $S_c$
  $U_{ww}$ and $V_{ww}^T$: orthonormal matrices for $W_w^k$
  $S_{ww}$: diagonal matrix for $W_w^k$
  $W_{modi}$: Modified DWT coefficient
  $W_{idct}$: InverseDCT coefficients matrix
  $W_d$: Watermarked Image
```


Cover image
Watermark image
Text watermark
Apply second level DWT and choose the LL sub-band of the first level
Apply DCT on the image
Apply encryption
Apply DCT on the selected sub-band
Apply SVD on the DCT coefficients
Encrypted watermark
Apply SVD on the DCT coefficients
Embed the image watermark in the LL sub-band of the first level DWT and the text watermark in the HH sub-band of the second level DWT
ISVD
IDCT
IDWT
Watermarked image
Watermarked image
Watermark image
Text watermark
Apply second level DWT and choose the LL sub-band of the first level
IDCT
ISVD
Apply decryption
Apply DCT on the selected sub-band
Apply SVD on the DCT coefficients
Extraction of the image watermark from the LL sub-band of the first level DWT and the text watermark from the HH sub-band of the second level DWT

(a)

(b)

Fig. 1 Multiple watermarks **a** embedding process and **b** extraction process

```
STEP 2: Read the Images
C_w←MRI.bmp (Cover image of size 512*512)
W_w←Thorax.bmp (Watermark image of size 256*256)
```

```
  STEP 3: Perform DWT on Cover and DCT on Watermark image
  Apply first level DWT on cover image
  [$LL_c$, $LH_c$, $HL_c$, $HH_c$]←DWT(C_w, wavelet filter);
  D=DCT(W_w);
  STEP 4: Choice of subands in Cover and obtain the DCT coefficients for the same
  //Choose sub-band $LL_c$ from cover image
  if (DCT on $LL_c$) then
  $D_c^1$← DCT ($LL_c$);
  endif;
  STEP 5: Compute the singular values of DCT coefficients for Cover and Watermark image
  if (SVD on $D_c^1$) then
  $U_c S_c V_c^T \leftarrow SVD(D_c^1)$
  endif;
  if (SVD on D) then
  $U_w S_w V_w^T \leftarrow SVD(D)$
  endif;
  STEP 6: Watermark Embedding
  for  ←0.1:0.9
  $S_c$+  $S_w$=$W_w^k$;
  end;
  STEP 7: Compute the singular values for $W_w^k$ and obtain the modified DWT coefficients
  if (SVD on $W_w^k$) then
  $U_{ww} S_{ww} V_{ww}^T \leftarrow SVD(W_w^k)$
  endif;
  //modified DWT coefficient
  $W_{modi} \leftarrow U_c S_{ww} V_C^T$
  Step 8: Obtain the Watermarked Image.
  $W_{idct}$←inverse($W_{modi}$);
  //Apply InverseDWT to $LL_c$, $LH_c$, $HL_c$ and $HH_c$ with modified coefficient
  $W_d$←InverseDWT ($W_{idct}$, $LH_c$, $HL_c$, $HH_c$ wavelet filter);
  end:
```

4.2 Extraction algorithm for image watermark

```
start:
  STEP 1: Variable Declaration
  α scale factor
  $LL_c$, $LH_c$, $HL_c$, $HH_c$: sub-bands for watermarked image
  $D_w^*$: DCT coefficients matrix for $HH_c$
  $U_w^*$ and $V_w^{*T}$: orthonormal matrices for $D_w^*$
  $S_w^*$: diagonal matrix for $D_w^*$
  $S^{*k}$: modified values
  $U_w^{*1}$ and $V_w^{*1T}$: orthonormal matrices for $S^{*k}$
  $S_w^{*1}$: diagonal matrix for $S^{*k}$
  $I_{cc}^{*}$: modified DWT coefficients
  $W_{EW}$: Extracted watermark image
  STEP 2: Perform DWT on Watermarked image (possibly distorted)
  [$LL_c$, $LH_c$, $HL_c$, $HH_c$]←DWT ($W_d$, wavelet filter);
  STEP 3: Obtain the DCT coefficients for $HH_c$
  if (DCT on $LL_c$) then
  $D_w^*$← DCT ($LL_c$);
  endif;
  STEP 4: Compute the singular values for $D_w^*$
  $U_w^* S_w^* V_w^{*T} \leftarrow SVD(D_w^*)$
  end;
  STEP 5: Perform the operation and then apply SVD
  for $\alpha$ =0.1:0.9
  $S^{*k} = \frac{S_w^* - S_c}{\alpha}$
  end;
  $U_w^{*1} S_w^{*1} V_w^{*1T} \leftarrow SVD(S^{*k})$
  STEP 6: Compute modified DWT coefficients
  $I_{cc}^* \leftarrow U_w S_w^{*1} V_w^T$
  STEP 7: Extract the watermark image.
  $W_{EW}$←InverseDCT ($I_{cc}^*$);
  end:
```

4.3 Embedding algorithm for text watermark

```
start:
  STEP 1: Variable Declaration
  Medical Image(MRI): cover image
  Leena: watermark image
  C_w: read the cover image
  W_w: read the text watermark
  α: scale factor
  DWT: discrete wavelet transforms
  Wavelet filters: Haar
  $LL_c$, $HL_c$, $LH_c$ and $HH_c$: First level DWT coefficients for cover image
  $LL_{c1}$, $HL_{c1}$, $LH_{c1}$ and $HH_{c1}$: Second level DWT coefficients for cover image
  STEP 2: Read the Images
  M_w ← MRI.bmp (Cover image of size 512*512)
  STEP 3: Perform DWT on Cover image
  //Apply second level DWT on cover image
  [$LL_c$, $HL_c$, $LH_c$ and $HH_c$]← DWT (M_w, wavelet filter);
  [$LL_{c1}$, $HL_{c1}$, $LH_{c1}$ and $HH_{c1}$]← DWT ($HH_c$, wavelet filter);
  STEP 4: Encrypt the watermark text by using Eq. (3)
  STEP 5: Convert encrypted watermarking text to Binary bits
  // converting text watermark into binary bits
  Wtxt←binary(Text Watermark);
```

```
STEP 6: Replace '(0,1)' by '(-1,1)' in the watermarking bits
// bit stream is transformed into a sequence w(1) w(2)....w(L) by replacing the 0 by -1 and 1 by 1, L is the length of string
-1←0 and 1←1;
STEP 8: Embedding the text watermark
// text watermark is embeds into $HH_{c1}$ sub-band
for $\propto \leftarrow 0.01:0.1$
    $f'(x,y)=f(x,y)(1+\propto \times Wb)$; $f(x,y)$ and $f'(x,y)$ is DWT coefficients before and after embedding process
end;
STEP 9: Obtain the Watermarked Image $W_d$
//Apply Inverse DWT to $LL_c$, $HL_c$, $LH_c$ and $HH_c$ with modified and un-modified DWT coefficients
$W_{mg} = inverse\ DWT(LL_{c1},\ HL_{c1},\ LH_{c1}\ and\ HH_{c1},\ wavelet\ filter)$;
$W_d \leftarrow inverse\ DWT(LL_c,\ HL_c,\ LH_c\ and\ W_{mg},\ wavelet\ filter)$;
end:
```

4.4 Extraction algorithm for text watermark

In the watermark extraction procedure, both the received image and the cover image are decomposed into the two levels. It is assumed that the cover image is available for extraction process

```
start:
STEP 1: Variable Declaration
Medical Image (MRI): cover image
Leena: watermark image
C_w: read the cover image
α: scale factor
DWT: discrete wavelet transforms
Wavelet filters: Haar
$LL_c$, $HL_c$, $LH_c$ and $HH_c$: First level DWT coefficients for cover image
$LL_{c1}$, $HL_{c1}$, $LH_{c1}$ and $HH_{c1}$: Second level DWT coefficients for cover image
STEP 2: Perform DWT on Watermarked image (possibly distorted)
// original image is also available for extraction process
[$LL_c$, $HL_c$, $LH_c$ and $HH_c$, wavelet filter] ← DWT ($W_d$, wavelet filter);
STEP 3: Watermark extraction
$W_r b = \frac{(f_r'(x,y)-f(x,y)}{\alpha f(x,y)}$; $f_r'(x,y)$ are the DWT coefficients of the received image.
//finally extracted watermark taken as sign (either positive or negative)
$W_e b \leftarrow$ positive or negative sign($W_r b$);
STEP 4: Convert the watermark bits into text to get the characters
STEP 5: Decrypt the characters by using Eq. (4) to get the original watermark
end:
```

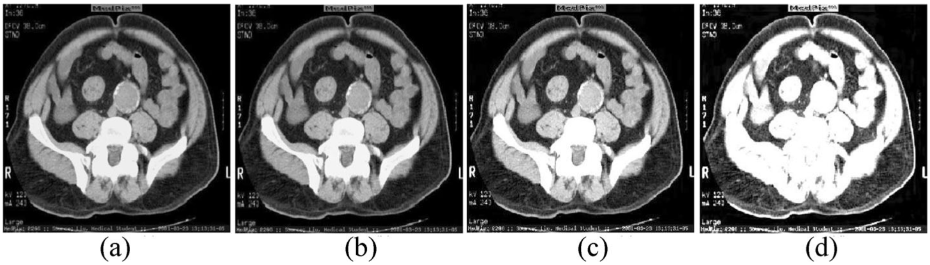


Fig. 2 Original and watermarked CT scan images **a** original image and watermarked images with gain factor; **b** 0.05; **c** 0.5 and **d** 1.0

5 Experimental results and analysis

The performance of the proposed watermarking method by applying encryption on patient data before embedding the text watermark has been investigated. For testing the robustness and quality of the watermarked image MATLAB is used. In the proposed method cover image of size 512×512 [17], the image watermark of size 256×256 and the text watermark of size 50 characters 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.

The image watermark (Thorax image) embedding method is based on DWT, DCT and SVD. In order to enhance the security of the text watermark, encryption is applied to the ASCII representation of the text watermark before embedding. 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. However, overall performance of the proposed method highly depends on the size of the watermarks, gain factor and the noise variation.

Figure 2a shows the CT Scan cover image and Fig. 2b–d show watermarked images at different gain factors 0.05, 0.5 and 1.0 respectively. Figure 3a shows the original image watermark (Thorax image). The text watermark is the patient data as shown in Fig. 3b. In the experiment, values of PSNR, NC and BER are illustrated in Table 1 to Table 3 for varying gain factor (α) in the range of 0.01 to 0.5. Furthermore, we have tested the robustness of the

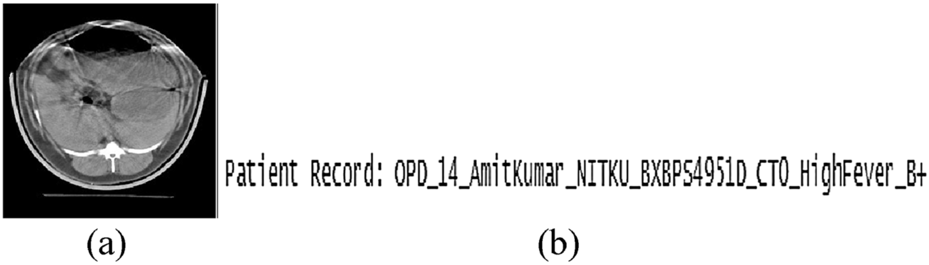

Patient Record: OPD_14_AmitKumar_NITKU_BXBPS4951D_CTO_HighFever_B+

Fig. 3 Original **a** image and **b** text watermark

Table 1 Performance of proposed method at different gain factor

Gain factor (α)	Without encryption						With encryption					
	50 characters			30 characters			50 characters			30 characters		
	PSNR (dB)	NC Values	BER (%)	PSNR (dB)	NC Values	BER (%)	PSNR (dB)	NC Values	BER (%)	PSNR (dB)	NC Values	BER (%)
0.01	35.84	0.9808	0.08	36.19	0.9808	0.02	35.84	0.9802	0	36.19	0.9801	0
0.05	34.64	0.9986	0.08	34.9	0.9989	0.02	34.64	0.9985	0	34.9	0.9988	0
0.1	32.19	0.9992	0.08	32.34	0.9993	0	32.19	0.9992	0	32.34	0.9993	0

image watermark with checkmark benchmarking software (http://watermarking.unige.ch/Checkmark/) [27] which is shown in Table 4.

In Table 1, performance of the proposed method against different size of watermark has been evaluated without any noise attack. With the encryption, maximum PSNR value is 35.84 dB and BER=0 against maximum size of watermark at gain factor=0.01. Here, the NC value is 0.9802. However, the maximum NC value is 0.9992 at gain factor=0.1. Table 2 shows the performance of the proposed watermarking method against different attacks. With encryption, the highest BER value of 0.96 has been obtained against JPEG Compression with quality factor=10. Figure 4 shows the performance of the proposed method against known attacks.

Table 3 shows the effect of cover image as proposed method was tested for other types of cover images like Brain CT Scan, ultrasound, Barbara and Lena images. The highest PSNR were obtained with ultrasound image at $\alpha=0.05$. Here, the NC and BER value is 0.9983 and 0.6 respectively. However, the maximum NC and BER were obtained with Lena and MRI

Table 2 Performance of proposed method against different attacks at gain=0.05

Attacks	Proposed method with encryption	
	Image watermark (NC value)	Text watermark (BER value in %)
JPEG compression (QF-10)	0.9905	0.96
JPEG compression (QF-50)	0.9785	0.62
JPEG compression (QF-90)	0.9982	0
Median filtering [1 1] and [2 2]	0.9985, 0.9752	0, 0.93
Scaling factor 2	0.7375	0.44
Scaling factor 1.5	0.8086	0.26
Scaling factor 1.1	0.8964	0
Gaussian LPF with standard Deviation=0.6 and 0.4	0.9343, 0.9913	0.36, 0
Gaussian noise with Mean=0, Var-0.01	0.7267	0.5
Gaussian noise with Mean=0, Var-0.001	0.9365	0
Salt & pepper noise with (Density=0.01)	0.7552	0.14
Salt & pepper noise with (Density=0.05)	0.6069	0.48
Salt & pepper noise with Density=0.001	0.9843	0
Histogram equalization	0.569	0.14

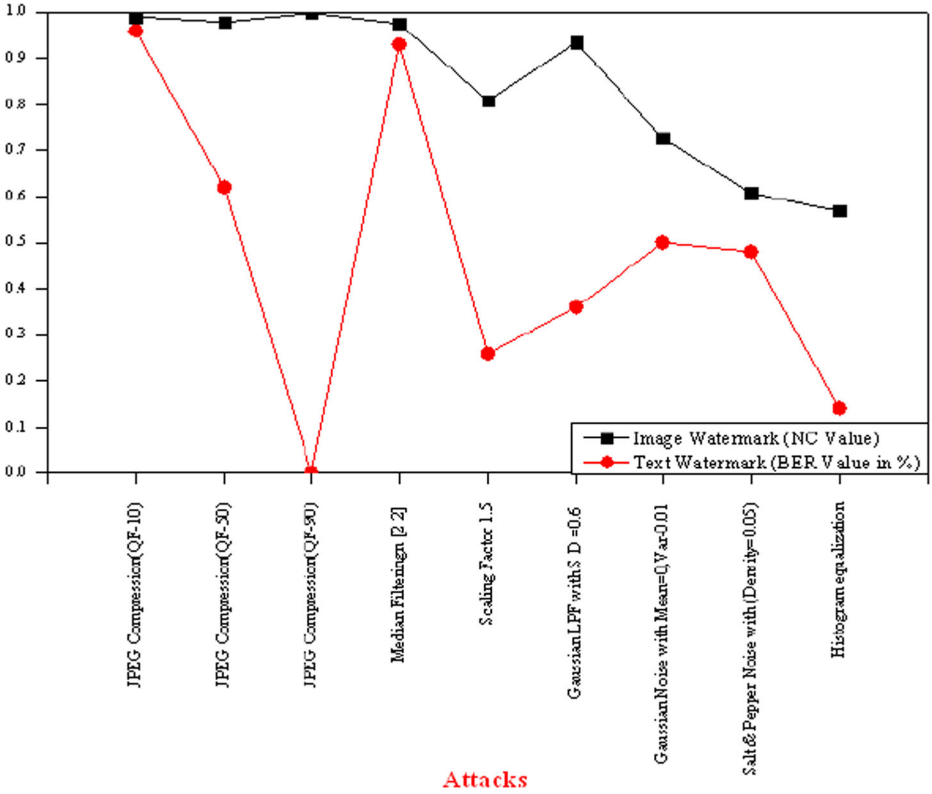


Fig. 4 Performance of the proposed method against different signal processing attacks

image respectively. Figure 5 shows the effect of the cover image on the parameter PSNR, BER and NC values.

Table 4 shows the performance of the proposed method against checkmark attacks. The maximum NC values of the extracted watermark under different attacks is shown at α=0.09. In this table, the maximum NC value of 0.9774 has been obtained by the proposed method against projective attack. However, the minimum NC value is 0.6189 against rows and columns removal attack. Here, all the NC values have been accepted except the rows and

Table 3 Effect of cover image at gain=0.05

Image type	With encryption		
	PSNR (dB)	NC Value	BER
Brain	35.61	0.9743	0.5
CT scan	34.64	0.9985	0
Ultrasound	37.62	0.9983	0.6
MRI	35.78	0.9960	0.64
Lena	37.23	0.9998	0.02
Barbara	28.35	0.9997	0

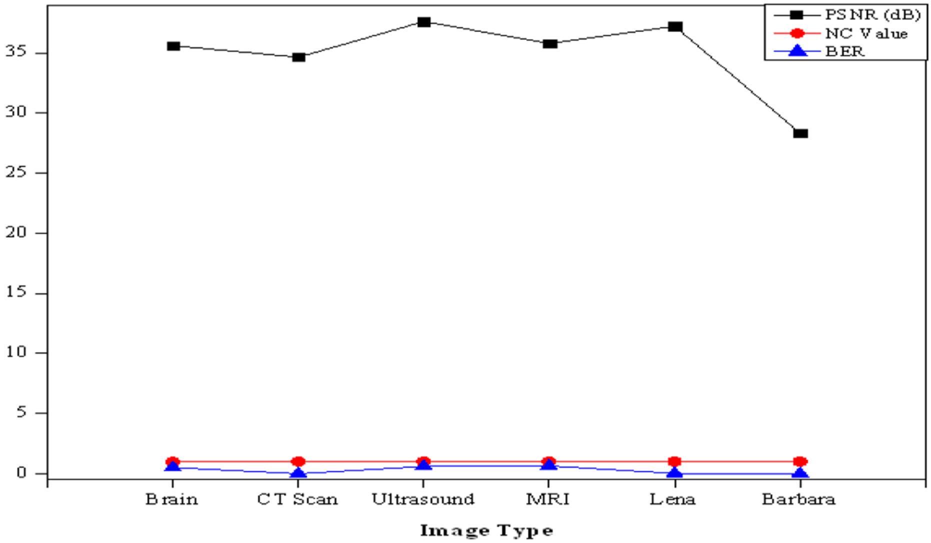


Fig. 5 Performance of the proposed method against different cover images

Table 4 Performance measure for checkmark attacks at gain=0.09

Checkmark attacks	Maximum NC values for image watermark
Collage	0.9003
Template remove	0.823
Rows and columns removal	0.6189
Denoising followed by perceptual remodulation (DPR)	0.7102
DPR_Corr attack	0.7266
Scale	0.8753
Trimmed mean	0.643
Cropping	0.9829
Gaussian	0.8653
Hard thresholding	0.7777
Soft thresholding	0.7243
JPEG compression	0.7503
Wavelet compression	0.7146
Medium filter	0.8663
Mid point	0.689
Projective	0.9774
Linear	0.8816
Ratio	0.7912
Rotation scale	0.8224
Rotation	0.7547
Shearing	0.8787
Warp	0.8247
Wiener	0.7936
Sample down up	0.756

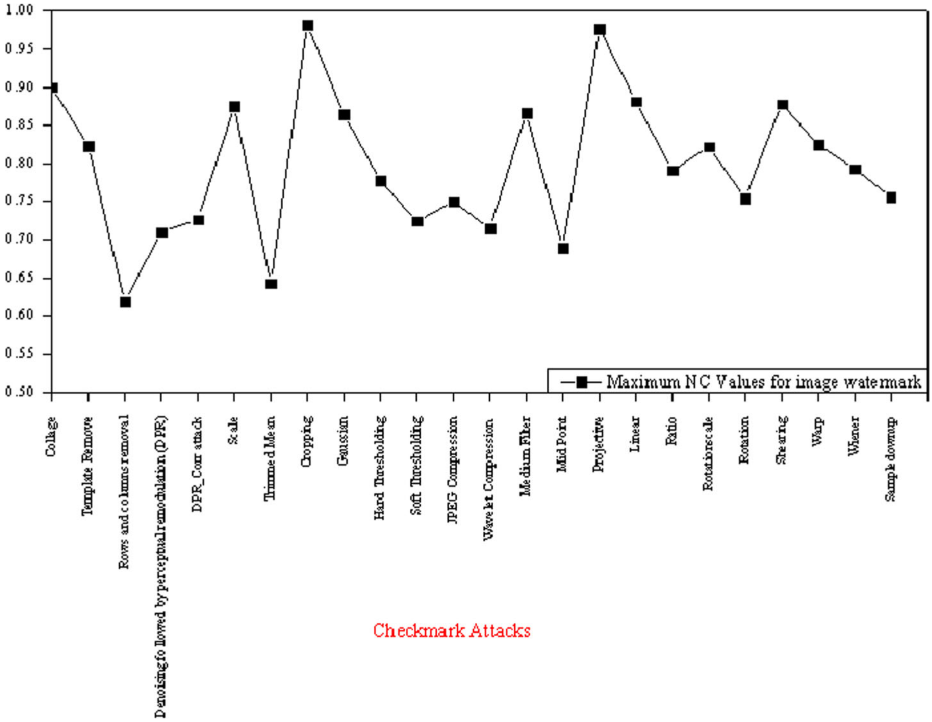


Fig. 6 Performance of the proposed method against checkmark attacks

columns removal, trimmed mean and mid point attack which are less than 0.7. Figure 6 shows the robustness performance of the proposed method against checkmark attacks.

Table 5 shows the performance comparison of the proposed method with other reported techniques. In this table, the NC value with proposed method has been obtained as 0.9994, 0.9752 and 0.6565 against JPEG, Median Filtering, and Gaussian Noise (Var-0.5) attacks

Table 5 Performance comparison results under NC value

Attacks	Rosiyadi et al. [29]	Singh and Tayal [34]	Srivastav et al. [36]	Proposed method
JPEG compression (QF=50)	−0.1863	Not found	Not found	0.9994
Median filtering [2 2]	0.4585	Not found	0.6019	0.9752
Gaussian LPF	Not found	0.9956	Not found	0.9956
Gaussian noise with mean=0, Var-0.5	0.5012	Not found	Not found	0.6565
Gaussian noise with mean=0, Var-0.01	Not found	0.8893	0.632	0.9754
Salt & pepper noise with (Density=0.08)	Not found	0.7809	Not found	0.8856
Histogram	Not found	0.9941	0.9123	0.9208
Salt & pepper noise with Density=0.01	Not found	0.9636	Not found	0.9952

respectively. However, the NC value obtained with Rosiyadi et al. [29] method is −0.1863, 0.4585 and 0.5012 against the same attacks respectively. The NC value with Singh and Tayal method [34] has been obtained as 0.9956, 0.8893, 0.7809 and 0.9636 against Gaussian LPF, Gaussian Noise (Var-0.01), Salt & Pepper Noise (Density=0.08) and Histogram attacks respectively. However, the NC value obtained with proposed method is 0.99560.9754, 0.8856 and 0.9208 against the same attacks respectively. The NC value with Srivastav et al. [36] has been obtained as 0.6019, 0.632 and 0.9123 against Median Filtering, Gaussian Noise (Var-0.01) and Histogram attacks respectively. However, the NC value obtained with proposed method is 0.9752, 0.9754 and 0.9208 against the same attacks respectively.

Overall, the performance of the proposed method is better than the other reported technique [29, 34, 36] in terms of robustness, capacity and security. Finally, quality of the watermarked image has been measured by the subjective method [24]. Humans are involved to check and vote for the quality of the watermarked data. Table 6 reports their combined suggestion. It may be observed that the reported visual quality of the watermarked images is acceptable for diagnosis at all chosen gain factors except the gain factor (α)=1.0 and 5.0, which indicate the poor quality. It may be concluded from the subjective measure test that smaller gain factor provides acceptable quality of the watermarked image for diagnosis.

6 Conclusions

In this paper, a hybrid image-watermarking technique based on DWT, DCT and SVD has been presented, where the watermark is embedded on the singular values of the cover image DWT sub bands. The main properties of this work can be identified as follows:

1) Proposed algorithm combines the advantages and removes the disadvantages of these three most popular transforms namely DWT, DCT and SVD. These are the novel techniques used for watermarking so their fusion makes a very attractive watermarking technique. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify areas in the cover image where a watermark can be imperceptibly embedded. The DCT information of the watermark image contains low frequency information and as long as such information is not lost or lost a little, the watermarking image can be extracted well. 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

Table 6 Subjective measure of the watermarked image quality at different gain factor

Gain factors	Quality of the watermarked image
0.001	Excellent quality
0.01	Very good quality
0.05	Good quality
0.5	Average quality
1	Poor quality
5	Very poor quality

terms of imperceptibility, robustness and capacity as compared to DWT, DCT and SVD applied individually or combination of DWT-SVD or DCT-SVD.

2) For identity authentication purposes, multiple watermarks have been embedded instead of single watermark into the same medical image / multimedia objects simultaneously, which offer superior performance in telemedicine and tele-diagnosis applications.
3) In the proposed method, we have embedded two watermarks simultaneously. This technique has fewer constraints than the other two dual watermarks embedding methods.
4) Security of the text watermark is enhanced by using encryption method. However, 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. The encryption /decryption method used in the proposed technique is very simple.

Overall, the proposed method is better than the other reported technique in terms of robustness and security. This may provide a potential solution to existing telemedicine security problem of patient identity theft.

The inclusions of many techniques were combined to improve the robustness of the watermarks and the quality of the watermarked image 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 also need to investigate approaches that will simultaneously improve the performance such as robustness, imperceptibility, security and capacity.

We would like to further improve the performance, which will be reported in future communication.

Acknowledgments The Author's are sincerely thankful to the potential/ anonymous reviewer's for their critical comments and suggestions to improve the quality of the paper.

We are also thankful to Dr. V. K. Agarwal, MD (Med.), D.M. (Neuro.) G. B. Pant Hospital, New Delhi for their valuable comments to evaluate the quality of the watermarked image for the diagnosis purpose.

I am grateful to Prof. S P Ghrera, Head of the Department, Department of CSE, Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh-India for their willingness to share their bright thoughts with me are very fruitful for shaping up my ideas and the quality of the paper.

References

1. Awasthi M, Lodhi H (2013) Robust image watermarking based on discrete wavelet transform, discrete cosine transform & singular value decomposition. Adv Electr Electron Eng 3(8):971–976
2. Bowman D (2012) http://www.fiercehealthit.com/story/researchers-use-digital-watermarks-protect-medical-images
3. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Med Biol Eng Comput 44:619–631
4. Golshan F, Mohammadi K (2013) A hybrid intelligent SVD-based perceptual shaping of a digital image watermark in DCT and DWT domain. Imag Sci J 61(1):35–46
5. Harish NJ, Kumar BBS, Kusagur A (2013) Hybrid robust watermarking techniques based on DWT, DCT, and SVD. Int J Adv Electr Electron Eng 2(5):137–143
6. Horng S-J, Farfoura ME, Fan P, Wang X, Li T, Guo J-M (2014) A low cost fragile watermarking scheme in H.264/AVC compressed domain. Multimed Tools Appl 72(3):2469–2495
7. Kannamma A, Pavithra K, Subha Rani S (2012) Double watermarking of DICOM medical images using wavelet decomposition technique. Eur J Sci Res 70:46–55

8. Kelkar V, Shaikh H, Khan MI (2013) Analysis of robustness of hybrid digital image watermarking technique under various attacks. Int J Comput Sci Mob Comput 2(3):137–143
9. Khan MI, Rahman MM, Sarker MIH (2013) Digital watermarking for image authentication based on combined DCT, DWT, and SVD transformation. Int J Comput Sci Issues 10(5):223–230
10. Kumar B, Anand A, Singh SP, Mohan A (2011) High capacity spread-spectrum watermarking for telemedicine applications. World Acad Sci Eng Technol 5:62–66
11. Lai C-C, Tsai C-C (2014) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
12. Lin W-H, Horng S-J, Kao T-W, Chen R-J, Chen Y-H, Lee C-L, Terano T (2009) Image copyright protection with forward error correction. Expert Syst Appl 36(9):11888–11894
13. 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 Multimedia 10(5):746–757
14. 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
15. 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
16. Madhesiya S, Ahmed S (2013) Advanced technique of digital watermarking based on SVD-DWT-DCT and Arnold transform. Int J Adv Res Comput Sci Eng Technol 2(5):1918–1923
17. MedPix^{TM}Medical Image Database available at http://rad.usuhs.mil/medpix/medpix.html.
18. Memon NA, Gilani SAM (2008) NROI watermarking of medical images for content authentication. Proceedings of 12th IEEE International Multitopic Conference, Karachi, Pakistan, p 106–110
19. Mostafa SAK, El- Sheimy N, Tolba AS, Abdelkader FM, Elhindy HM (2010) Wavelet packets-based blind watermarking for medical image management. Open Biomed Eng J 4:93–98
20. Navas KA, Cheriyan AM, Lekshmi M, Archana Tampy S, Sasikumar M (2008) DWT-DCT-SVD Based Watermarking, Third International conference on Communication Systems Software and Middleware and Workshops, COMSWARE, p 271–274
21. Navas KA, Nithya S, Rakhi R, Sasikumar M (2007) Lossless watermarking in JPEG2000 for EPR data hiding. Proc. IEEE-EIT 2007, Chicago, USA, p 697–702
22. Navas KA, Sasikumar M (2007) Survey of medical image watermarking algorithms, 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, p 1–6, March 25–29, TUNISIA
23. Nidhi HD, Jani NN (2012) Image watermarking algorithm using DCT, DWT and SVD. Int J Comput Appl 13–16
24. Nisha, Kumar S (2013) Image quality assessment techniques. Int J Adv Res Comput Sci Softw Eng 3(7):636–640
25. Ollove M (2014) www.usatoday.com/story/…/stateline-identity-thefts-medical…/5279351
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. Am J Biomed Eng 2:29–37
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, p 340–353
28. Rosiyadi D, Horng S-J, Fan P, Wang X (2012) Copyright protection for e-government document images. IEEE MultiMedia 19(3):62–73
29. Rosiyadi D, Horng S-J, Suryana N, Masthurah N (2012) A comparison between the hybrid using genetic algorithm and the pure hybrid watermarking scheme. Int J Comp Theory Eng (IJCTE) 4(3):329–331
30. Shi-Jinn H, Rosiyadi D, Fan P, Wang X, Khan MK (2014) An adaptive watermarking scheme for e-government document images. Multimed Tools Appl 72(3):3085–3103
31. Shi-Jinn H, Rosiyadi D, Li T, Takao T, Guo M, Khan MK (2013) A blind image copyright protection scheme for e-government. J Vis Commun Image Represent 24(7):1099–1105
32. Singh AK, Dave M, Mohan A (2014) Hybrid technique for robust and imperceptible image watermarking in DWT- DCT-SVD domain. Natl Acad Sci Lett 37(4):351–358
33. Singh AK, Kumar B, Dave M, Mohan A (2014) Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun 80(4):1415–1433
34. Singh A, Tayal A (2012) Choice of wavelet from wavelet families for DWT-DCT-SVD image watermarking. Int J Comput Appl 48(17):9–14
35. Soliman MM, Hassanien AE, Ghali NI, Onsi HM (2012) An adaptive watermarking approach for medical imaging using swarm intelligence. Int J Smart Home 6:37–50
36. Srivastava A, Saxena P (2013) DWT-DCT-SVD based semiblind image watermarking using middle frequency band. IOSR J Comput Eng 12(2):63–66
37. Terzjia N, Repges M, Luck K, Geisselhardt W (2002) Digital image watermarking using discrete wavelet transform: performance comparison of error correction codes. International Association of Science and Technology for Development

38. Umaamaheshvari A, Thanushkodi K (2012) High performance and effective watermarking scheme for medical images. Eur J Sci Res 67:283–293
39. Wang B, Ding J, Wen Q, Liao X, Liu C (2009) An Image Watermarking Algorithm based on DWT DCT and SVD, IEEE International Conference on Network Infrastructure and Digital Content, p 6–8
40. Zain J, Clarke M (2005) Security in telemedicine: issue in watermarking medical images. International Conference: Science of Electronic, Technologies of Information and Telecommunications
41. Zaz Y, El Fadil L (2010) Protecting EPR data using cryptography and digital watermarking, International Conference on Models of Information and Communication Systems, Rabat
42. Zhang L, Zhou P-P (2010) Localized affine transform resistant watermarking in region-of-interest. Telecommun Syst 44:205–220

Amit Kumar Singh Received B. Tech. in Computer Science and Engineering from Institute of Engineering and Technology, Purvanchal University Jaunpur, Uttar Pradesh in 2005. M. Tech in Computer Science and 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. He is with Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh since April 2008. His research interests include information security, Biometrics and Cryptography.

Dr. 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 22 years rich experience of serving both academia and industry in various capacities. His research interests include Computer Networks, Mobile/Vehicular Adhoc and Sensor Networks, Database Systems and information security, wireless sensor network and distributed computing.

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*