Multimed Tools Appl (2017) 76:8881–8900
DOI 10.1007/s11042-016-3514-z

Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images

Amit Kumar Singh [1]

Received: 26 September 2015 / Revised: 17 February 2016 / Accepted: 4 April 2016 /
Published online: 14 April 2016

Abstract This paper presents a new robust hybrid multiple watermarking technique using fusion of discrete wavelet transforms (DWT), discrete cosine transforms (DCT), and singular value decomposition (SVD) instead of applying DWT, DCT and SVD individually or combination of DWT-SVD / DCT-SVD. For identity authentication purposes, multiple watermarks are embedded into the same medical image / multimedia objects simultaneously, which provides extra level of security with acceptable performance in terms of robustness and imperceptibility. In the embedding process, the cover image is decomposed into first level discrete wavelet transforms where the A (approximation/lower frequency sub-band) is transformed by DCT and SVD. The watermark image is also transformed by DWT, DCT and SVD. The S vector of watermark information is embedded in the S component of the cover image. 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. Furthermore, the text watermark is embedding at the second level of the D (diagonal sub-band) of the cover image. The security of the text watermark considered as EPR (Electronic Patient Record) data is enhanced by using encryption method before embedding into the cover. The results are obtained by varying the gain factor, size of the text watermark, and cover medical images. The method has been extensively tested and analyzed against known attacks and is found to be giving superior performance for robustness, capacity and reduced storage and bandwidth requirements compared to reported techniques suggested by other authors.

Keywords Image and text watermarking · Steganography · Discrete wavelet transforms · Discrete cosine transforms · Singular value decomposition · Encryption · Robustness · Capacity · BER

✉ Amit Kumar Singh
amit_245singh@yahoo.com

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

1 Introduction

Digital document distribution over open channel using information and communication Technology (ICT) has proved an indispensible and cost effective technique for dissemination and distribution of digital media files. However, prevention of copyright violation, ownership identification, and identity theft have been challenging issues due to attempts of malicious attacks / hacking of open channel information. The prime motive behind attacks can be to alter, modify, or even delete the document watermark to illegally claim ownership or preventing the information transfer to intended recipients. Therefore, addressing these challenges has been an interesting problem for researchers in the field. The classic model for invisible communication was first proposed by Simmons in 1984 as the prisoner's problem [27], which is shown in Fig. 1. The two prisoners in Fig. 1 want to develop an escape plan, but unfortunately all communications between each other are arbitrated by a warden.

They are not allowed to communicate through encryption and if any suspicious communication is noticed, the two prisoners will be placed in solitary confinement and thus preventing any exchange of information. Therefore the prisoners must communicate invisibly in order not to arouse warden suspicion and they thought of hiding meaningful information in some cover message. To implement this, one of the prisoners created a picture of a blue cow lying on a green meadow and sent it to other prisoner. This way the Warden could not perceive that the colours of the objects in the picture are transmitting some information. This is an example of data hiding. As evident from the above example, the *data hiding* is a technique to hide data into a cover message without creating any perceptual distortion of the cover for identification, annotation and copyright. However, the constraints that affect the data hiding process [2] are: the quantity of data to be hidden, the need for invariance of these data under conditions where a cover (host) media is subjected to distortions like lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. Fundamentally, the data hiding techniques can be classified into two categories i.e. digital watermarking and steganography [12]. Digital watermarking is the process of embedding data (called a watermark) into digital multimedia cover objects in such a way that the watermark can be detected or extracted later to make an assertion about the authenticity and / or originality of the object [21]. The basic concept of digital watermarking is closely related to Steganography (also known as covered writing) which focuses on bandwidth of the hidden message while concealing a message, image, or file within another message, image, or file but in the case of watermarking, the watermark robustness is the key performance parameter.

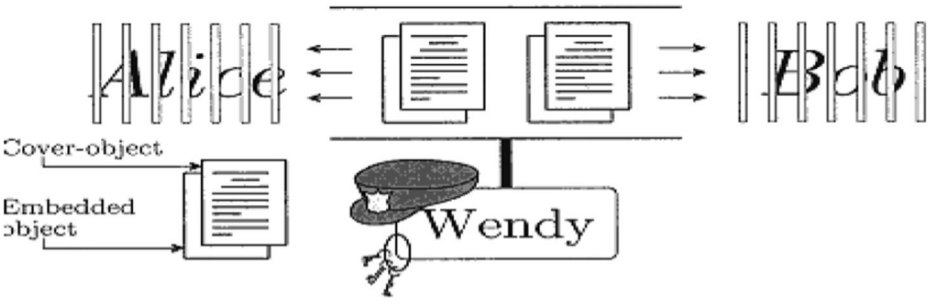

Fig. 1 The prisoners' problem [4]

1.1 Recent applications of digital watermark

In recent years, watermarking techniques develops very fast and applies to many applications, such as military, communication, privacy protection, identification, media file archiving, broadcast monitoring, Remote Education and Insurance Companies, Secured E-Voting Systems, fingerprinting, Secure Driver licenses and so on. Digital cinema is also considered as a practical application, where the information can be embedded as a watermark in every frame. Some of the important and latest applications are given below [7, 9, 29]:

a. Fingerprinting: It is the mechanism in which the watermarked content/documents contain the intended recipient's identification information in order to trace back the source of illegal distribution.
b. Broadcast Monitoring: Broadcast monitoring is an application which enables content owners to automatically verify where, when and how long their content was broadcast via terrestrial, cable or satellite television. Also, E-commerce has become a huge business and a driving factor in the development of the Internet. In addition, online shopping services and online delivery of digital media, is very popular today and will become an increasingly important part of e-commerce and mobile e-commerce. Digital watermarking play an important role to protect intellectual property in e-governance, e-commerce applications, copy control, media identification and tracking.
c. Copyright Protection: Providing copyright protection to digital data by hiding secret information is main goal of digital watermarking. Many content owners to embed digital watermarks in images as a means to communicate and protect image copyrights. This ensures that image users or licensees are acting in compliance with guidelines and allows legal departments to effectively communicate and enforce image copyrights.
d. Digital Signatures: A mechanism employed in public-key cryptosystems (PKCS) that enables the originator of an information object to generate a signature, by encipherment (using a private key) of a compressed string derived from the object. The digital signature can provide a recipient with proof of the authenticity of the object's originator.
e. Indexing: Video mail can be indexed, where comments can be embedded in the video content; movies and news items can also be, where markers and comments can be inserted that can be used by search engine.
f. Source Tracking: A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known.
g. Secured E-Voting Systems: With rapid growth of computer network, Internet has reached to common villagers of country and worldwide as well. Due to widespread use of the Internet with information and communication technologies in order to get their inevitable benefits like accuracy, speed, cost saving etc. more secure transactions such as shopping, banking, submitting tax returns are done online. Obviously, electronic voting is a possible alternative for conducting elections by maintaining security in election process. For the election commission of India and other countries to conduct free and fair polls is always be challenging task. Current research focuses on designing and building 'voting protocols' that can support the voting process, while implementing the security mechanisms required for preventing fraud and protecting voters' privacy. So we need a highly secured e-voting system is required. Digital watermarking provides a valuable solution to these problems.

h. Remote Education and Insurance Companies: Due to the shortage of teachers and other problems in rural areas in, distance education is gaining popularity of developing any diverse countries. So there is a strong need for intelligent technologies to create a deployable remote education solution. However, dissemination of valuable content and teacher-student interaction are some of the major challenges in the distance education solution. The secured transmission of data is part of distant learning. Digital watermarking may provide one of the important solutions for the remote education. Also, different insurance companies such as health and vehicle nowadays use image processing application. Health insurance companies are storing the scanned copies of the medical data of their clients. The database may require processing and transmitting to central administrative offices. The car companies' image databases are referred for insurance-related decision making in case of damage to vehicles during accidents. The digital image watermarking protection is provided to such image database.
i. Secure Driver licenses: Digital watermarks are also used to protect state driver licenses by providing covert and machine readable layer of security to fight against various issues such as digital counterfeiting, fraud, identity theft etc. (http://www.digitalwatermarkingalliance.org/faqs.asp)

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 [29]. However, due to higher data embedding capacity of image, the present work focuses on watermarking using image as cover media. The image watermarking techniques can be classified as 'spatial domain' and 'transform domain' techniques [29]. The spatial domain techniques are straight forward and computationally simple. LSB substitutions, correlation-based and spread-spectrum 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, the spatial domain techniques offer less robustness against the signal processing attacks. 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.

The wavelet transforms provides excellent spatial-frequency localization properties as discussed detail in [29, 30]. Recently, the higher robustness of watermark has been achieved by using wavelet based watermarking are presented in [15–18, 24, 31, 32]. 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, 6, 8, 10, 11, 13, 14, 19, 22, 23, 25, 26, 33, 34, 36].

In this paper, a new robust hybrid multiple 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 proposed method can embed multiple watermark (text and image both) simultaneously, which provide extra level of security with the acceptable performance in

terms of robustness and imperceptibility. 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 healthcare applications such as teleophthalmology, telemedicine, tele-diagnosis and tele-consultancy applications. In addition, the major advantages of medical image watermarking are data compactness, reduced bandwidth requirement, confidentiality of the patient data, protection against tampering [31] etc.

In the embedding process, the cover image is decomposed into first level discrete wavelet transforms where the A (approximation/lower frequency sub-band) is transformed by DCT and SVD. The watermark image is also transformed by DWT, DCT and SVD. The S vector of watermark information is embedded in the S component of the cover image. 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. Furthermore, the text watermark is embedding at the second level of the D (diagonal sub-band) of the cover image. The security of the text watermark considered as electronic patient records (EPR) data is enhanced by using encryption method [31] before embedding into the cover.

1.2 Concepts of electronic patient records (EPR)

Wherever (and whenever) a patient is treated, there is a record of that treatment. Using information and communication technologies (ICT), these records can be made safer and available for other health professionals. These organizational records will become the *Electronic Patient Records* (EPRs), and a subset of them will contribute to a lifelong record of a patient's health and healthcare - the *Electronic Health Record* (EHR) [5].

EPR as text watermarks are broadly classified in the proposed method as follows [32]:

a. Patient image/health centre logo watermark is embedded in the first level of the DWT image for the purpose of data integrity control.
b. Patient's medical records/identity/reference watermark contains the physician's identification code, keywords and patient's personal and examination data. The physician's identification code for the purpose of origin authentication. The keywords such as diagnostic codes, the insertion of indices image, acquisition characteristics, which facilitates image retrieval by database querying mechanisms. The efficient indexing and archiving of digital medical data in hospital information systems, which eliminates storage and transmission bandwidth requirements.

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 [31]. Hence, a brief description of these concepts is included in the given below sections.

2.1 Discrete wavelet transform (DWT)

Wavelet is a finite energy function i.e. $\psi \in L^2$ (finite energy function) with zero mean and is normalized ($\|\psi\| = 1$) [3]. A family of wavelets can be obtained by scaling ψ by s and translating it by u.

$$\Psi_{u,s}(t) = s^{-1/2} \ \Psi \ \left(\frac{t-u}{s}\right) \tag{1}$$

The continuous wavelet transform (CWT) of finite energy which is the sum over all time of scaled and shifted versions of the mother wavelet ψ for a 1-D signal $f(t)$ is given by:

$$f(u,s) = \int_{-\infty}^{+\infty} (t) \ s^{-1/2} \Psi^* \left(\frac{t-u}{s}\right) dt \tag{2}$$

Where ψ^* (.) is the complex conjugate of $\psi(.)$. Equation (2) can be viewed as convolution of the signal with dilated band-pass filters. In order for the wavelet transforms to be calculated using computers the data must be discretized. A continuous signal can be sampled so that a value is recorded after a discrete time interval. If the sampling of the signal is carried out at the Nyquist rate, no information would be lost. After sampling the discrete wavelet series could be used. However, this can still be very slow to compute. The reason is that the information available through evaluation of wavelet series is still highly redundant and the solution requires a large amount of computation time. In order to make the wavelet computationally simple, a discrete algorithm is needed. The DWT provides sufficient information both for analysis and synthesis of the original signal with a significant reduction in the computation time. In addition, DWT is considerably easier to implement in comparison to the CWT (Continuous wavelet transform). DWT is one of the well-known techniques for sub-band image coding.

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 [12]. The DWT is decomposes a 2-D signal such as image into a set of four sub-bands that are non-overlapping multi-resolution [20], A (approximation/lower frequency sub-band), H (horizontal sub-band), V (vertical sub-band) and D (diagonal sub-band) as shown in Fig. 2. The process can be repeated to obtain multiple scale wavelet decomposition.

Human eyes are much more sensitive to the approximation/lower frequency sub-band, the watermark can be embedded into the other three sub-bands to maintain better perceptual quality of an image.

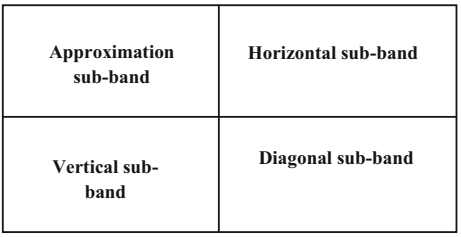

Fig. 2 The sub-bands of discrete wavelet transform

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 [31], makes it much easier to embed the watermark information into middle frequency band that provide an 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 the input image, I, of size N x N the DCT coefficients for the transformed output image, D, are computed using Eq. (1). The intensity of image is denoted as I (x, y), where the pixel in row x and column y of the image. The DCT coefficient denoted as D (i, j) where i and j represent the row and column of the DCT matrix.

$$\begin{aligned} &D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} I(x,y) cos \frac{(2x+1)i\pi}{2N} cos \frac{(2y+1)i\pi}{2N} \\ &C(i), C(j) = \frac{1}{\sqrt{2}} \; for \; i,j = 0 \\ &C(i), C(j) = 1 \; for \; i,j > 0 \end{aligned} \tag{3}$$

The DCT matrix can be define by using Eq. (3)

$$\begin{aligned} &M_{i,j} = \frac{1}{\sqrt{N}} \; for \; i = 0 \\ &M_{i,j} = \sqrt{\frac{2}{N}} \, cos \left(\frac{(2j+1)i\pi}{2N} \right) for \; i > 0 \end{aligned}$$

2.3 Singular value decomposition (SVD)

The singular value decomposition of a rectangular matrix A is as follows [28]:

$$A = USV^T \tag{4}$$

where A is an $M \times N$ matrix, U and V are the orthonormal matrices. S is a diagonal matrix consists of singular values of A. The singular values $s_1 \geq s_2 \geq \ldots s_n \geq 0$ appear in the descending order along with the main diagonal of S. However, these singular values have been obtained by taking the square root of the eigen values of AA^T and A^TA. These singular values are unique, however the matrices U and V are not unique. The relation between SVD and eigen values are:

$$\begin{aligned} &A = USV^T \\ &\text{Now } AA^T = USV^T \left(USV^T\right)^T = US^2U^T \\ &Also, A^TA = \left(USV^T\right)^T USV^T = VS^2V^T \end{aligned}$$

Thus, U and V are calculated as the eigen vectors of AA^T and A^TA, respectively. If the matrix A is real, then the singular values are always real numbers, and U and V are also real. The SVD has two main properties from the viewpoint of image processing applications are: 1) the singular values of an image have very good stability, when a small perturbation is added to an image, its singular values do not change significantly, and 2) singular values represent the intrinsic algebraic image properties [28].

2.4 Encryption and decryption process of text watermark

For providing additional security, text watermark is encrypted before embedding into the cover image. 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 [31]. The text watermark in the proposed method is encrypted using the equation

$$\text{Encrypted text watermark} = (\text{text watermark}^{r}) - d \tag{5}$$

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 [31].

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

$$\text{Decrypted text watermark} = (\text{Encrypted text watermark} + d)^{\frac{1}{r}} \tag{6}$$

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 dB is acceptable [31]. The PSNR is defined as

$$\text{PSNR} = 10\log\frac{(\text{Pmax})^2}{\text{MSE}} \tag{7}$$

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

$$\text{MSE} = \frac{1}{X \times Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}\left(I_{ij} - W_{ij}\right)^2 \tag{8}$$

where I_{ij} is a pixel of the original image of size XY and W_{ij} is a pixel of the watermarked image of size $X \times Y$. 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 [31].

$$\text{NC} = \sum_{i=1}^{X}\sum_{j=1}^{Y}\left(W_{\text{originalij}} \times W_{\text{recoveredij}}\right) / \sum_{i=1}^{X}\sum_{j=1}^{Y} W^2_{\text{originalij}} \tag{9}$$

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

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.

$$\text{BER} = (\text{Number of incorrectly decoded bits}) / (\text{Total number of bits}) \tag{10}$$

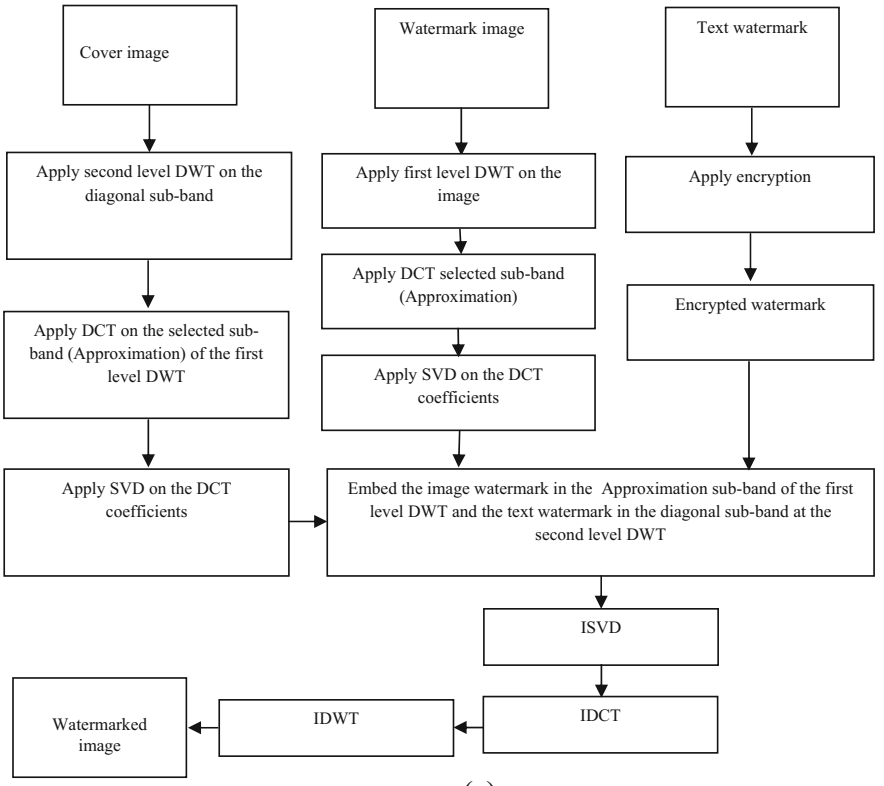

Fig. 3 Multiple watermarks (**a**) embedding process and (**b**) extraction process

4 Proposed algorithm

The proposed algorithm is the combination of DWT, DCT and SVD based process, which enhanced the robustness without significant degradation of the image quality against the signal processing attacks. The proposed algorithm has two parts, one is the image watermark embedding and other is image watermark extraction method as follows. Figure 3a and b shows the multiple watermarks embedding and extraction process respectively. However, the proposed method is using text watermark embedding and extraction algorithm as discussed detail in [35]. However, the summary of the text watermark embedding and extraction algorithm are given in section 4.3 and section 4.4 respectively.

4.1 Image watermark embedding algorithm

start:

STEP 1: Variable Declaration

Barbara Image: cover image of Size 512*512

Leena Image: watermark image of size 512*512

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

A_c, H_c, V_c, and D_c: First level DWT coefficients for cover image

A_{c1}, H_{c1}, V_{c1}, and D_{c1}: Second level DWT coefficients for cover image

A_w, H_w, V_w, and D_w: First level DWT coefficients for watermark image

D_c^1: DCT coefficients matrix for A_c

H_w^1: DCT coefficients matrix for H_w

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 H_w^1

S_w: diagonal matrix for H_w^1

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

Wmodi: Modified DWT coefficient

Widct: InverseDCT coefficients matrix

W_d: Watermarked Image

STEP 2: Read the Images

C_w ←Barbara.bmp (Cover image of size 512*512)

W_w ← Leena.bmp (Watermark image of size 512*512)

STEP 3: Perform DWT on Cover and Watermark image

Apply second level DWT on cover image and first level DWT on Watermark image

[A_c, H_c, V_c, and D_c] ←DWT (C_w, Haar);

[A_{c1}, H_{c1}, V_{c1}, and D_{c1}] ←DWT (D_c, Haar);

[A_w, H_w, V_w, and D_w] ← DWT (W_w, Haar);

// D_c is the first level diagonal sub-band of the cover image and D_{c1} is the second level DWT coefficients of the diagonal sub-band (D_c) of the cover.

STEP 4: Choice of subands in Cover and Watermark image and obtain the DCT coefficients for the same

//Choose subband A_c from cover image and A_w from watermark image

if (DCT on A_c)**then**

D_c^1← DCT (A_c);

// D_c^1 is the DCT coefficients matrix for the first level approximation sub-band of the cover image.

endif;

if (DCT on A_w)**then**

H_w^1←DCT (A_w);

STEP 5: Compute the singular values of DCT coefficients for Cover and Watermark image

if (SVD on D_c^1)**then**

$U_c S_c V_c^T$← SVD (D_c^1)

endif;

if (SVD on H_w^1)**then**

$U_w S_w V_w^T$ ← SVD (H_w^1)

endif;

STEP 6: Watermark Embedding

for ←*0.01:0.1*

S_c+ S_w =W_w^k;

// W_w^k is the modified singular value (after the embedding watermark information).

end;

STEP 7: Compute the singular values for W_w^k **and obtain the modified DWT coefficients**

if (SVD on W_w^k)**then**

[$U_{ww} S_{ww} V_{ww}^T$]←SVD(W_w^k)

// When SVD is applied on an image, only singular values of the diagonal matrix are retained in a vector. The singular values are arranged in descending order on the diagonally and that first singular value contains the greatest amount of information and subsequent singular values contain decreasing amounts of image information. Thus, the lower singular values containing negligible or less important information can be discarded without significant image distortion. The concepts can be understand by a example as under

Let us consider 3*3 matrices as an image. When, SVD applied on the image which contains the diagonal elements as singular values in the form of s1≥s2≥s3≥0 of size 3*1. However, SVD is again applied on the obtained singular values (s1≥s2≥s3≥0) which contains only one value. This small singular value has the sufficient amount of image information.

In order to maintaining large number of singular value only few singular values can be stored.

endif;

//modified DWT coefficient

$Wmodi$← $U_c S_{ww} V_c^T$

Step 8: Obtain the Watermarked Image.
$Widct \leftarrow$ iDCT ($Wmodi$);
//Apply iDWT to A_{c1}, H_{c1}, V_{c1}, and D_{c1} with modified coefficient
$H_c \leftarrow$ iDWT(A_{c1}, H_{c1}, V_{c1}, and D_{c1}, 'Haar');
//Apply iDWT to A_c, H_c, V_c, and D_c with modified coefficient
$W_d \leftarrow$ iDWT($Widct$, H_c, V_c, D_c, 'Haar');
end:

4.2 Image watermark extraction algorithm

start:
STEP 1: Variable Declaration
α : scale factor
A_c, H_c, V_c, D_c: subbands for watermarked image
D_w^*: DCT coefficients matrix for H_c
U_w^* and V_w^{*T}: orthonormal matrices for D_w^*
S_w^*: diagonal matrix for D_w^*
S_c^k: diagonal matrix for DCT coefficients of cover image
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
I_{Wcc}^*: InverseDCT coefficients matrix
W_{EW}: Extracted watermark image
STEP 2: Perform DWT on Watermarked image (possibly distorted)
[A_c, H_c, V_c, D_c] $\leftarrow$ DWT (W_d, 'Haar');
STEP 3: obtain the DCT coefficients for A_c
if (DCT on A_c)**then**
$D_w^* \leftarrow$ DCT (A_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 ∝=0.01:0.1
$S^{*k} = \frac{S_w^* - S_c}{\propto}$
//S_w^* is the singular values of the DCT coefficients for possibly distorted image (watermarked image), S_c is the singular values of DCT coefficients for cover image and '∝' is denoted as gain factors.
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.
$I_{Wcc}^* \leftarrow$ InverseDCT (I_{cc}^*);
$W_{EW} \leftarrow$ InverseDWT (I_{Wcc}^*, H_w, V_w, D_w , 'Haar');
end:

4.3 Text watermark embedding algorithm

For embedding, text watermark is converted into a bit stream and then transformed into a sequence w*(1)*...w*(L)* by replacing the 0 by −1, where 'L' is the length of the bit stream and w(k) ε {−1,1} (k=1,…,L). The watermark is added to the largest DWT coefficients in second level diagonal sub-band which represent the high frequencies of the cover image. Let f (m, n) denote the DWT coefficients which are not located at the approximation band (A) of the cover image. The embedding procedure is performed according to the following formula [35]:

$$f'(m,n) = f(m,n) + \alpha f(m,n)w(k) \tag{11}$$

Where 'α' is the strength/gain of the watermark controlling the level of the watermark *w(1)...w(L)*. The watermarked image is obtained by applying the inverse discrete wavelet transform (IDWT). Before embedding the text watermark, encryption is applied to the text watermark by Eq. (5).

4.4 Extraction process for text watermark

In the watermark extraction procedure both the received image and the original/cover image are decomposed into the two levels. It is assumed that the original image is known for extraction. The extraction procedure is described by the formula:

$$w_r(k) = \left(f'(m,n) - f(m,n)\right)/(\alpha f(m,n)) \tag{12}$$

Due to noise, extracted sequence contains both '+ve' & '-ve' values, so extracted watermark is given by formula:

$$\mathrm{w_e(k)} = \mathrm{sgn(w_r(k)}$$

After extraction of the watermark, the bit stream is reconstructed according to the replacement rule. The decryption is applied to the encrypted text watermark by using the Eq. (6).

5 Experimental results and analysis

The performance of the proposed hybrid watermarking method by applying encryption on patient data before embedding into the cover has been investigated. For testing the robustness, capacity and visual quality of the watermarked image, MATLAB is used. In the proposed method, cover image and the image watermark of size 512 × 512 and the text watermark of size up to 185 characters are used for testing. The robustness of the image and text watermarks is evaluated by determining NC and BER respectively. The visual 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 (Lena 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. Figure 4a shows the

Fig. 4 (**a**) Cover image and (**b**) Watermarked Barbara images at gain factor = 0.05, (**c**) 0.1 and (**d**) 0.9

Barbara cover image and Fig. 4b–d show watermarked images at different gain factors 0.05, 0.1 and 0.9 respectively.

Figure 5a shows the original image watermark (Lena image). The text watermark is the patient data as shown in Fig. 5b. In the experiment, values of PSNR, NC and BER are illustrated in Tables 1, 2, 3 and 4 at varying gain factor (α) in the range of 0.01 to 0.1. In addition, the performance (PSNR, NC and BER) of the proposed method has been compared in Tables 1, 2 and 3.

In Table 1, PSNR, NC and BER performance of the proposed hybrid method for different size of watermark has been evaluated without any noise attack. With the encryption, maximum PSNR value is 28.51 dB and BER= 0 against maximum size of watermark at gain factor = 0.01. Here, the NC value is 0.9930. However, the maximum NC value is 1.0 at gain factor = 0.1. In addition, this table also shows the PSNR, NC and BER performance comparison of the proposed method with other reported techniques [31]. Here, the maximum NC value with proposed method has been obtained as 0. 9930, 0.9990 and 1.0 at gain factor 0.01, 0.05 and 0.1 respectively with acceptable PSNR values. However, the maximum NC value obtained with Singh et al. [31] method is 0.9802, 0.9995 and 0.9992 at the same gain factors respectively. The BER value is zero in all the cases.

The maximum PSNR value have been obtained with Singh et al. [31] is 35.84 dB at gain = 0.01 using the image watermark of size 256*256. However, the maximum PSNR value has been obtained by the proposed method is 28.51 dB at the same gain using the image watermark of size 512*512. The degradation in the PSNR value will be high if the size of image watermark (512*512) and the text watermark (50 Characters = 350 bits) is small.

(a)

Electronic Patient's record:
OPD_15_AmitKumar_JUITW_BXBPS4951D_CT0_HighFever_B
+

(b)

Fig. 5 Original (**a**) Cover image and (**b**) Text watermark of size 50 characters

Table 1 Performance of proposed method at different gain factor

Gain factor(α)	Using encryption [31]						Proposed method using 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	0.9802	0	36.19	0.9801	0	28.51	0.993	0	29.65	0.9937	0
0.05	34.64	0.9985	0	34.9	0.9988	0	28.12	0.999	0	29.43	0.9995	0
0.1	32.19	0.9992	0	32.34	0.9993	0	27.87	1	0	27.03	0.9998	0

Table 2 shows the NC and BER performance of the proposed hybrid watermarking method for different attacks at gain factor = 0.05. With encryption, the maximum NC value of 0.9993 has been obtained against Median Filtering and Motion Blur attacks. However, minimum NC value of 0.5919 has been obtained against Salt & Pepper Noise (Density=0.05). The maximum BER value of 0.94 has been obtained against Median Filtering attacks. In addition, Table 2 shows the performance comparison of the proposed method with other reported techniques [31]. In this table, the maximum NC value with proposed method has been obtained as 0.9993, 0.9993, 0.9959, 0.9591, 0.9938, 0.8157, 0.6341, 0.993 against JPEG(QF = 90), Median Filtering, Gaussian low pass filter (standard Deviation = 0.4), Gaussian Noise (Var-0.001), Salt & Pepper Noise (Density=0.001), Histogram equalization, Unsharp contrast enhancement filter (ALPHA = 0.5) and Motion Blur (len=1 and theta =0) attacks respectively. However, the maximum NC value obtained with Singh et al. [31] method is 0.9982, 0.9985, 0.9913, 0.9365, 0.9843 and 0.569 against JPEG (QF = 90), Median Filtering, Gaussian low pass filter (standard Deviation = 0.4), Gaussian Noise (Var-0.001), Salt & Pepper Noise (Density=0.001), Histogram equalization attacks respectively. The BER value with proposed method is always zero except for JPEG Compression (QF-10), Median Filtering (2 2) and Motion Blur (len=2.5 and theta =0). However, the BER value with Singh et al.[31] is always greater than 0.14 except for JPEG Compression(QF-90), Median Filtering (1 1), Scaling (Factor = 1.1), Gaussian LPF (standard Deviation = 0.4), Gaussian Noise (Var-0.001) and Salt & Pepper Noise (Density=0.001).

Table 3 shows the effect of cover image as proposed method was tested for other types of cover images like Brain, CT Scan, ultrasound, MRI, Lena and Barbara images. In addition, Table 3 also shows the PSNR, NC and BER performance comparison of the proposed method with other reported techniques [31]. In this table, the maximum NC value with proposed method has been obtained as 0.9998 for Lena image, where the BER = 0.01. However, the same NC value with Singh et al. [31] method has been obtained for Lena image, where the BER = 0.02. This Table shows that all the NC values are better than the technique proposed in [31] for all the selected images. In addition, the BER performance is also better than the existing method [31] except for the CT Scan image. Table 4 shows the PSNR, NC and BER performance of the proposed method for the different size of text watermark at gain = 0.01. This Table shows that the proposed method can embed up to 185 characters with acceptable PSNR value. However, the method can recovered up to 184 characters

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

Attacks	Singh et al. [31] method using encryption		Proposed method using encryption	
	Image watermark (NC Value)	Text watermark (BER Value in %)	Image watermark (NC Value)	Text watermark (BER Value in %)
JPEG Compression(QF-10)	0.9905	0.96	0.9913	0.48
JPEG Compression(QF-50)	0.9785	0.62	0.9708	0
JPEG Compression(QF-90)	0.9982	0	0.9993	0
Median Filtering [1 1] and [2 2]	0.9985 and 0.9752	0 and 0.93	0.9993 and 0.9479	0 and 0.94
Scaling Factor 1.1	0.8964	0	0.7251	0
Gaussian LPF with standard Deviation =0.6 and 0.4	0.9343 and 0.9913	0.36 and 0	0.8635 and 0.9959	0
Gaussian Noise with Mean=0,Var-0.01	0.7267	0.5	0.6297	0
Gaussian Noise with Mean=0,Var-0.001	0.9365	0	0.9591	0
Salt & Pepper Noise (Density=0.01)	0.7552	0.14	0.7881	0
Salt & Pepper Noise (Density=0.05)	0.6069	0.48	0.5919	0
Salt & Pepper Noise (Density=0.001)	0.9843	0	0.9938	0
Histogram equalization	0.569	0.14	0.8157	0
Unsharp contrast enhancement filter ALPHA =0.1,0.2 and 0.5	Not Reported	Not Reported	0.6201, 0.6244 and 0.6341	0
Motion Blur (len=1 and theta =0)	Not Reported	Not Reported	0.9993	0
Motion Blur (len=2 and theta =0)	Not Reported	Not Reported	0.8619	0
Motion Blur (len=2.5 and theta =0)	Not Reported	Not Reported	0.8289	0.9

Table 3 Effect of cover image at gain = 0.05

Image type	Singh et al. [31] using encryption			Proposed method using encryption		
	PSNR (dB)	NC Value	BER (%)	PSNR (dB)	NC Value	BER (%)
Brain	35.61	0.9743	0.5	31.11	0.9894	0.2
CT scan	34.64	0.9985	0	30.27	0.9984	0.12
Ultrasound	37.62	0.9983	0.6	31.15	0.9986	0.6
MRI	35.78	0.996	0.64	30.27	0.9984	0.1
Lena	37.23	0.9998	0.02	31.06	0.9998	0.01
Barbara	28.35	0.9997	0	26.86	0.9994	0

without any error. The proposed method can embed up to 184 characters. However, only 50 characters can be embedded by the method in [31].

Table 5 shows the performance comparison of the proposed method with other reported techniques [25, 33, 34]. In this table, the NC value with proposed method has been obtained as 0.9988, 0.9379 and 0.6569 against JPEG, Median Filtering, and Gaussian Noise (Var-0.5) attacks respectively. However, the NC value obtained with Rosiyadi et al. [25] method is -0.1863, 0.4585 and 0.5012 against the same attacks respectively.

The NC value with Singh and Tayal method [33] 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 0.9959, 0.9604, 0.8859 and 0.931 against the same attacks respectively. The NC value with Srivastav et al. [34] 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 0.9379, 0.9604 and 0.931 against the same attacks respectively.

From the above discussion, 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. The performance of the proposed method is more robust than the other reported technique [31] in terms of robustness, capacity and BER. However, the reported technique [31] is much better than the other existing techniques [25, 33, 34]. Finally, the proposed method offer better performance (NC and BER values) compared to other reported techniques [25, 31, 33, 34].

Table 4 Effect of size of the text watermark at gain = 0.01

Size of text watermark	PSNR(dB)	NC	BER (%)
75 Characters	27.69	0.9938	0
155 Characters	27.43	0.9932	0
185 Characters	27.38	0.9931	0.4

Table 5 Performance comparison results under NC value

Attacks	Rosiyadi et al. [25]	Singh and Tayal [33]	Srivastav et al. [34]	Proposed method
JPEG compression (QF=50)	−0.1863	Not reported	Not reported	0.9988
Median filtering [2 2]	0.4585	Not reported	0.6019	0.9379
Gaussian LPF	Not reported	0.9956	Not reported	0.9959
Gaussian noise with mean=0,Var-0.5	0.5012	Not Found	Not reported	0.6569
Gaussian noise with mean=0,Var-0.01	Not reported	0.8893	0.632	0.9604
Salt & pepper noise with (Density=0.08)	Not reported	0.7809	Not reported	0.8859
Histogram	Not reported	0.9941	0.9123	0.931
Salt & pepper noise with density=0.01	Not reported	0.9636	Not reported	0.9961

6 Conclusions

This paper is presented a new robust hybrid multiple watermarking technique using fusion of DWT, DCT, and SVD instead of applying DWT, DCT and SVD individually or combination of DWT-SVD / DCT-SVD. Subsequently, simultaneous embedding of multiple watermarks (text and image) into the same multimedia object which provides extra level of security with acceptable performance in terms of robustness and imperceptibility. In addition, security of the text watermark is enhanced by using encryption. Encryption of text watermark using as EPR data before watermarking may have become unavoidable in recent applications like medical but the delay encountered during embedding and extraction will be an important factor. In the proposed method simple encryption algorithm is used to save execution time during embedding and extraction processes. Overall, the proposed method is better than the other reported technique in terms of robustness and embedding capacity. Therefore the proposed method may find potential application in prevention of patient identity theft in medical applications.

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.

I would like to further research on lossless data hiding techniques specially for medical applications, 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.

References

1. Awasthi M, Lodhi H (2013) Robust image watermarking based on discrete wavelet transform, discrete cosine transform & singular value decomposition. Adv Electron Electr Eng 3(8):971–976

2. Bender W, Gruhl D, Morimoto N, Lou A (1996) Techniques for data hiding. IBM Syst J 35(3&4):313–336
3. Chellappa R, Theodoridis S (2014) Academic press library in signal processing: signal processing theory and machine learning. 1
4. Craver S (1997) On public-key steganography. In: The Presence of an Active Warden Technical Report RC 20931, IBM
5. NHS Executive (2001) Information for Health: An Information Strategy for the Modern NHS 1998–2005. Wetherby: Department of Health Publications; 1998 and NHS Executive. Building the Information Core - Implementing the NHS Plan. London: Department of Health
6. Golshan F, Mohammadi K (2013) A hybrid intelligent SVD-based perceptual shaping of a digital image watermark in DCT and DWT domain. Imaging Sci J 61(1):35–46
7. Gunjal BL, Mali SN (2012) Applications of digital image watermarking in industries. CSI Commun
8. Harish NJ, Kumar SBB, Kusagur A (2013) Hybrid robust watermarking techniques based on DWT, DCT, and SVD. Int J Adv Electr Electron Eng 2(5):137–143
9. Hartung F, Ramme F (2000) Digital rights management and watermarking of multimedia content for m-commerce applications. IEEE Commun Mag 38(11)
10. Horng S-J, Rosiyadi D, Fan P, Wang X, Khan MK (2014) An adaptive watermarking scheme for e-government document images. Multimedia Tools Appl 72(3):3085–3103
11. Horng S-J, 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
12. Katzenbeisser S, Petitcolas FAP (2000) Information hiding techniques for steganography and digital watermarking. Artech House, London
13. Kelkar V, Shaikh H, Mohd. I K (2013) Analysis of robustness of hybrid digital image watermarking technique under various attacks. Int J Comput Sci Mob Comput 2(3):137–143
14. Khan MI, Rahman M, Sarker IH (2013) Digital watermarking for Image authentication based on combined DCT, DWT, and SVD Transformation. Int J Comput Sci Issues 10(5):223–230
15. 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
16. 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
17. 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
18. 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
19. Madhesiya S, Ahmed S (2013) Advanced technique of digital watermarking based on SVD-DWT-DCT and Arnold transform. Int J Adv Res Comput Eng Technol 2(5):1918–1923
20. Mallat SG (1989) The theory for multiresolution signal decomposition: the wavelet representation. IEEE Trans Pattern Anal Mach Intell 11(7):693–654
21. Mohanty SP (1999) Watermarking of digital images. M.S. Thesis, Indian Institute of Science, India
22. Navas KA, Cheriyan AM, Lekshmi M, Tampy SA, Sasikumar M (2008) DWT-DCT-SVD based watermarking. Third International conference on Communication Systems Software and Middleware and Workshops, COMSWARE, pp. 271–274
23. Nidhi HD, Jani NN (2012) Image watermarking algorithm using DCT, DWT and SVD. Int J Comput Appl, pp. 13–16
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. Rosiyadi D, Horng S-J, Fan P, Wang X (2012) Copyright protection for e-government document images. IEEE MultiMedia 19(3):62–73
26. 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 Comput Theory Eng (IJCTE) 4(3):329–331
27. Simmons GJ (1984) The prisoners' problem and the subliminal channel. In: Advances in Cryptology, Proceedings of CRYPTO 83, Plenum Press, pp. 51–67
28. Singh AK, Dave M, Mohan A. A Hybrid Algorithm for Image Watermarking against Signal Processing Attack. S. Ramanna et al. (Eds.) Proceedings of 7th Multi-Disciplinary International Workshop in Artificial Intelligence, Krabi-Thailand, December 9–11, 2013, Lecture Notes in Computer Science (LNCS) Vol. 8271, pp. 235–246, Springer
29. 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. doi:10.1007/s40010-014-0140-x, **Springer**
30. 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

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 A, Tayal A (2012) Choice of wavelet from wavelet families for DWT-DCT-SVD image watermarking. Int J Comput Appl 48(17):9–14
34. Srivastava A, Saxena P (2013) DWT-DCT-SVD based semiblind image watermarking using middle frequency band. IOSR J Comput Eng 12(2):63–66
35. Terzija N, Repges M, Luck K, Geisselhardt W (2002) Digital image watermarking using DWT: performance comparision on error correcting codes. Vis Imaging Image Process Proc (364)
36. 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, Beijing, pp. 1034–1038

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 research interests include Data Hiding, Biometrics & Cryptography. Dr. Singh has served as TPC member and reviewers for various conferences and journals.