Multimedia Tools and Applications (2022) 81:26721–26738
https://doi.org/10.1007/s11042-020-10472-w

1175: IOT MULTIMEDIA APPLICATIONS AND SERVICES

Secure and robust color image dual watermarking based on LWT-DCT-SVD

Aditi Zear[1] · Pradeep Kumar Singh[2]

Received: 6 June 2020 / Revised: 12 October 2020 / Accepted: 29 December 2020 /
Published online: 9 February 2021

Abstract

Now days advancements in multimedia technology and Information and Communication technologies (ICTs) has raised various security related concerns. Digital image watermarking is one of the new and popular techniques for the protection of multimedia content. This paper proposes an approach for digital image watermarking in which Lifting wavelet transform (LWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) have been used. The host color image is decomposed using LWT and LH3, LL3 sub bands of the third level LWT are transformed by DCT and then SVD. Security of logo (image watermark) is enhanced by using message-digest (MD5) hash algorithm and then DCT-SVD are applied to it before embedding it into LH3 sub band. The robustness of Info (Text watermark) is increased by encoding it using Hamming error correcting code. Error correcting code increases the length of watermark therefore arithmetic coding is applied that provides lossless compression. Experimental results are computed for different color image models (RGB, YIQ, YCbCr) at different gain factors, size of text watermark, different types of cover image and for attacks. The proposed method has good performance for the imperceptibility of watermarked image and robustness of watermarks. The performance of this algorithm can be improved by using various optimization techniques.

Keywords Digital image watermarking · Cryptography · Compression · Lifting wavelet transform

✉ Pradeep Kumar Singh
pradeep_84cs@yahoo.com

Aditi Zear
aditizear93@gmail.com

[1] Computer Science & Engineering Department, NIT, Hamirpur, Himachal Pradesh, India

[2] ABES Engineering College, Ghaziabad, Uttar Pradesh, India

1 Introduction

From last few decades the extraordinary growth in technology of computer and computer networks provides quality of service and higher bandwidth for both wired and wireless networks. The representation of media in digital form and evolution of internet also made easy to share digital media such as image, audio and video in an effortless way. Various applications where sharing of such information is required are distributed or cloud environments, healthcare applications, education etc. However these advancements also raised some security related issues such as copyright violation, ownership identification and identity thefts. Sharing and storing sensitive information over unsecured networks is an important concern. Hence some data hiding techniques are required for the protection of multimedia data. The goal of data hiding is not to restrict the access to host channel, but to ensure that the embedded data should be inviolate and recoverable [7, 47]. There are two techniques for data hiding: Steganography and Watermarking. Steganography is defined as the technique of hiding communication, the hidden content is embedded in some cover media so that there will not be any eavesdropper's suspicion [9, 37]. In watermarking, a watermark (document or image) is embedded into digital content to protect it from unauthorized access. Later on this secret information can detected and extracted out to check the identity of digital media or real owner [26, 42, 43, 47].

The digital watermarks are playing an important role in Fingerprinting, Healthcare, Copyright protection, Source Tracking, Remote Education, Insurance Companies and Secured E-Voting Systems (http://www.digitalwatermarkingalliance.org/faqs.asp) [46, 56]. The watermark has various important characteristics such as robustness, capacity, imperceptibility, security and computational cost. Watermarking and encryption methods are providing high degree of confidentiality, integrity, availability and authenticity to sensitive data/information [26, 43, 46, 56]**.** The goal of watermarking techniques is not to restrict the access to host channel, but to ensure that the embedded data should be inviolate and recoverable. This means that watermark is embedded into host image in such a way that any attack or alteration to the watermarked image affects the watermark and similarly any attack to the embedded watermark affects the quality of watermarked image [7, 47]. Therefore any alteration or attack to the watermarked image can be detected by using imperceptibility and robustness related parameters. These parameters check whether the watermark get affected because of various attacks or not. The security of sensitive information can be ensured using cryptography However, after decryption this data becomes insecure. This vulnerability issue of decrypted data can be solved using watermarking. Therefore the combination of watermarking and cryptography provides more security and authentication to sensitive information [9, 26, 37, 42, 43, 46]. Watermarking techniques can be divided as spatial and transform domain watermarking techniques. In spatial domain [26, 42, 43, 46] watermark is embedded by modifying values of pixels. Spatial domain techniques are less robust against signal processing attacks. In transform domain techniques host image is converted into transform domain and then watermark is embedded in transform coefficients and after that inverse transform is performed. Various transform domain techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Discrete Fourier Transform (DFT). They provide more robustness as compared to spatial domain techniques [26, 42, 43, 46, 56].

Various factors such as imperceptibility, robustness, capacity and security need to be considered in the watermarking methods. Minimization of the computational complexity is also important for practical implementation. In order to reduce the computational complexity LWT (Lifting Wavelet Transform) can be used as an alternative approach for DWT [13, 19, 21, 33, 34, 40, 49] to transform image into frequency domain. LWT is also called second generation fast wavelet transform. The split and merge process used in LWT reduces computational complexity by 50% as compared to DWT [22, 36, 50].

In this paper an approach based on LWT-DCT-SVD of colored digital images is proposed. In commonly used RGB (Red, Green and blue), R, G and B channels are highly correlated [14, 16, 35] and for better watermarking algorithm (with better robustness and imperceptibility) it is important that the channels should be uncorrelated. Therefore other color image models such as YIQ, YCbCr can be used to un-correlate the R, G and B channels [1, 5, 20, 23, 28, 41, 48]. The robustness of three color image models is tested in this paper and the model that provides better robustness in either low or high gain factors is used for further analysis. The host color image is decomposed into third-level LWT and LL3, LH3 sub bands of the third level LWT are transformed by DCT-SVD. The security of logo (image watermark) is enhanced using message-digest (MD5) hash algorithm and then it is transformed using DCT-SVD before embedding it into LH3 sub band. The robustness of Info (Text watermark) is increased by encoding it using Hamming error correcting code. The error correcting code adds extra bits to the watermark, therefore a lossless compression technique arithmetic coding is applied to reduce its length in order to enhance the imperceptibility of watermarked image.

The remaining components of paper are put in order as: Section 1.1 describes related work and contribution of proposed approach is mentioned in Section 1.2. The details of the proposed algorithm (embedding and extraction algorithm) are given in Section 2. Section 3 covers the experimental results and analysis part and the conclusion of the paper is mentioned in Section 4.

1.1 Related work

Digital Image Watermarking (DIW) in combination with cryptography is efficient for authentication, confidentiality and security. Cryptography converts information into an unreadable cipher. However, after decryption this data becomes insecure. Hence this vulnerability issue of decrypted data is solved using DIW. The compression techniques used with DIW can also enhance the imperceptibility of the watermarked image. Because after compression the watermark bits required to be embedded in the cover image reduces to some extent. Therefore compression can be used to increase the embedding capacity. The amalgamation of DIW, cryptography and compression for the protection of digital content provides security and robustness to watermark and also enhances the imperceptibility of watermarked image [15, 25, 45, 46, 51]. The review of some proposed watermarking algorithms in which cryptography or compression is applied along with DIW is given below:

Data hiding scheme based on Least Significant Bit (LSB) for producing colored medical images is proposed in [8] where QR code is used as watermark accommodating the entire patient's data. The size of image is not affected as the dispersal of embedded watermark is over the whole image. This robust technique resists rotational attacks which are demonstrated through testing. Perpetual hash and Fast Discrete Cosine transform based blind, robust and zero watermarking technique is proposed in [27]. Logistic chaotic encryption of the watermark ensures improved safety factor. The first level of FDCT contains this encrypted data in low frequency coefficients. Techniques in [31, 32] are experimentally proven to be inferior as compared to this technique in terms of imperceptibility and robustness characteristics.

Using second level DWT and SVD, Avaghi et al. in [4] proposed a blind watermarking technique. Encryption is applied to the watermarked image to provide better protection. Visual encryption of the watermarked image is done with fingerprint image using IWT. Both intentional and unintentional attacks are thus prevented with these techniques. As compared to [6] it provides better security and authentication. For improving medical data authenticity a watermarking technique based on RONI is proposed in [38]. Fourth level LWT is used to place multiple character watermarks inside the cover image. This technique is tested robust and secure. For telemedicine applications, a secure encryption-watermarking approach is introduced by Dagadu and Li in [10]. Security of medical information is ensured using LWT-LSB in this watermarking method. For real-time and mobile applications also, this method is suitable which is indicated by experimental results. Watermarking technique for medical images based on DWT-KLT is proposed in [2]. Fuzzy interference system for optimization of visibility factor and turbo error correcting code for reducing the channel noise distortion is used in this approach. This method is suitable for medical data security as demonstrated by experimental results.

For medical applications a fragile watermarking is developed in [44] and to provide secure medical transmission SVD and Arnold transform is used. LSB of the cover image is embedded with two different watermarks bits of size ‘12 bits’ and ‘20 bits’. This method imperceptibly embeds watermark and is robust for other attacks. The non-fragile tempered images and other important tempering issues are not tested in this proposed method. Elhoseny et al. [12] introduced a secure patient information transmission model in IOT. To provide secure patient information transmission, combination of AES and RSA cryptographic method along with steganography is used. The proposed method is computationally expensive. SWT and DCT based zero watermarking is proposed in [11]. The visual feature vector of the host image is embedded with the watermark which is extracted using SWT-DCT. Using chaotic map the watermark is encrypted to improve the authenticity. Against conventional and geometric attacks this watermarking technique is proven robust. The pixel value of the host image does not change and maintains low complexity even after embedding more data which is experimentally demonstrated. A watermarking technique based on biometric is proposed in [3] for protecting medical data. Encrypted EPR report and minutia feature of the fingerprint is considered as watermark in this method. The ROI part of the cover is embedded with the watermark. To generate final watermark image compression using arithmetic coding scheme is done on resulting watermark image. Inside the cover image a pseudo random number_Id and final watermark data is placed. The reliability and proficiency of the method for authentication of medical data is shown by different results.

1.2 Contribution of the research

The main objectives of the research are to provide secure watermarking algorithm which provides robustness to the embedded watermark that can withstand different kind of attacks. Along with that we also focused on improving the imperceptibility of the watermarked image. The main challenge faced while implementing secure, robust and imperceptible watermarking technique is combining cryptography and compression [46]. Furthermore, it is challenging to find out the color component in the cover image for embedding watermarks in order to meet research objectives. In this method popular transform domain techniques such as LWT, DCT, SVD are used. As compared to general wavelets, reconstructing image using LWT provides increase in smoothness and reduction in aliasing effects [22, 36, 50]. LWT also helps to increase intactness of watermark, prevents loss of information and improves robustness of watermark. In addition to this LWT also requires less memory, computation and computational complexities [5, 20, 24, 28, 39, 55]. DCT has property of energy compaction [1, 17, 18, 23, 29, 30, 47, 52–55]. SVD is used so that the slight variations in the singular values do not affect the quality of watermarked image. The other contribution of this research is given below:

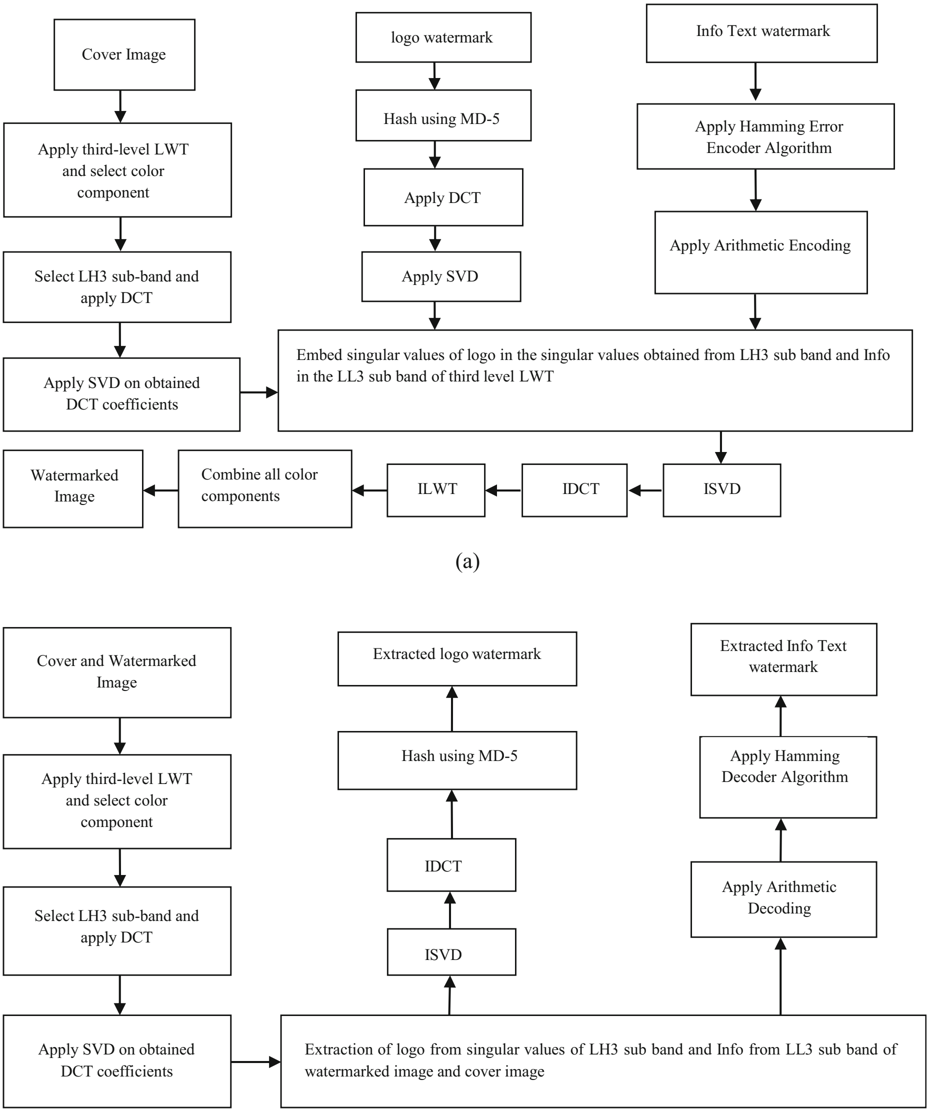
- In this approach, multiple (text and image) watermarks are embedded into single cover image. These two watermarks helps in increasing security with good performance in terms of BER, NC and PSNR. The Signature image watermark's security is improved by using message-digest (MD5) hash algorithm. The Info text watermark contains important information related to image is embedded into the higher LWT sub-band for authentication purpose and its robustness is enhanced using Hamming error correcting code. Arithmetic coding is applied to compress the encoded text watermark which is further used to improve the imperceptibility of watermarked image.
- Conversion of color image from RGB color space to YIQ and YCbCr color space removes the correlation that exists between the R, G and B color components which results in improved robustness and imperceptibility [14, 16, 35, 41, 48, 50].
- Embedding multiple text and image watermarks into cover image can save storage and bandwidth requirements [24, 29, 39, 53–55].

2 Proposed algorithm

Proposed algorithm has been divided into embedding and extraction process as shown in Figs. 1 and 2. The size of cover image and watermarked image used for the implementation of the proposed algorithm is 512 × 512 × 3 and 64 × 64 respectively. The results are validated according to the standard parameters used to evaluate watermarking algorithm. The proposed algorithm depends on image size and type of cover and watermark image. It may show variations in PSNR, BER and NC values when we increase or decrease the size of cover and watermark image. However for evaluating the proposed algorithm according to different parameters we have kept the size of cover image and watermark image constant. The algorithm is tested for different cover image and watermark image combinations in Table 4. The embedding process and extraction process for image and text watermark is defined in the following sections.

2.1 Embedding process for image watermark

Step1: Read the images
Input: Color Cover Image (512 × 512 × 3), Watermark image (64 × 64)
Step2: Select the color component to embed the watermark.
Step3: Apply 3rd-level LWT transform over selected component and select LH3 sub band.


Cover Image
Apply third-level LWT and select color component
Select LH3 sub-band and apply DCT
Apply SVD on obtained DCT coefficients
logo watermark
Hash using MD-5
Apply DCT
Apply SVD
Info Text watermark
Apply Hamming Error Encoder Algorithm
Apply Arithmetic Encoding
Embed singular values of logo in the singular values obtained from LH3 sub band and Info in the LL3 sub band of third level LWT
ISVD
IDCT
ILWT
Combine all color components
Watermarked Image
Cover and Watermarked Image
Apply third-level LWT and select color component
Select LH3 sub-band and apply DCT
Apply SVD on obtained DCT coefficients
Extraction of logo from singular values of LH3 sub band and Info from LL3 sub band of watermarked image and cover image
ISVD
IDCT
Hash using MD-5
Extracted logo watermark
Apply Arithmetic Decoding
Apply Hamming Decoder Algorithm
Extracted Info Text watermark

(a)

(b)

Fig. 1 **a** Watermark embedding and **b** Watermark extraction Process

Step4: Apply Discrete Cosine Transform to LH3 sub band and then apply SVD.

$$S_{DCT} \leftarrow DCT\ (LH3) \tag{1}$$

$$U_c S_c {V_c}^T \leftarrow SVD(S_{DCT}) \tag{2}$$

Step5: Hash the logo (image watermark) using MD5 and then apply DCT-SVD to the resulting hash coefficients.

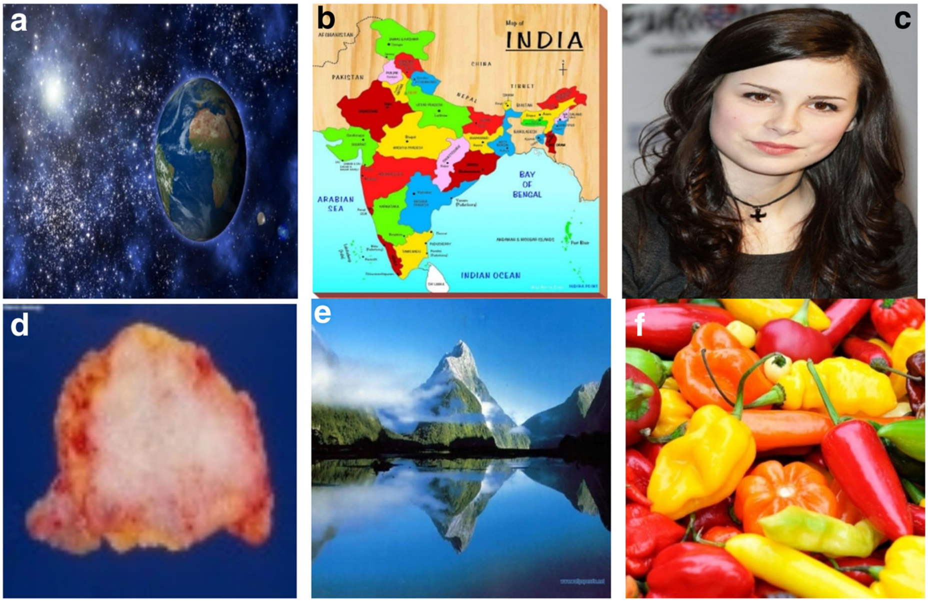


Fig. 2 **a** Earth, **b** India-map, **c** Lena Meyer, **d** Lump, **e** Mountain, **f** Peppers

$$W1 \leftarrow \text{hash}\ (\text{Watermark}) \tag{3}$$

$$W_{DCT} \leftarrow \text{DCT}\ (W1) \tag{4}$$

$$U_w S_w {V_w}^T \leftarrow \text{SVD}\ (W_{DCT}) \tag{5}$$

Step6: Embed the watermark into selected sub band of cover image

$$S_{wat} \leftarrow S_c + (k * S_w) \tag{6}$$

Step7: Apply inverse SVD, inverse DCT and inverse LWT in order to obtain modified selected color component.

Step8: Concatenate modified color component with other two color components to obtain watermarked image.

Step9: Convert the watermarked image to RGB color space if they are watermarked in YIQ and YCbCr color space.

2.2 Extraction process for image watermark

Step1: Read the images

Input: Color Cover Image (512 × 512 × 3), Color Watermarked image (512 × 512 × 3)

Step2: Select the color component from watermarked and cover image for watermark extraction.

Step3: Apply 3rd-level LWT transform over selected component of watermarked and cover image and select their corresponding LH3 sub band.
Step4: DCT-SVD is applied to the selected LH3 sub band of cover and watermarked image.

$$S_{DCT} \leftarrow DCT\ (LH3) \tag{7}$$

$$U_c S_c V_c^{\ T} \ \leftarrow SVD\ (S_{DCT}) \tag{8}$$

$$S_{WDCT} \leftarrow DCT\ (LH3) \tag{9}$$

$$U_{w1} S_{w1} V_{w1}^{\ T} \leftarrow SVD\ (S_{WDCT}) \tag{10}$$

Step5: Extract the watermark from corresponding SVD coefficients of cover and watermark image.

$$W_{ext} \leftarrow (S_{w1} - S_c)/k \tag{11}$$

Step6: Apply inverse SVD and inverse DCT to W_{ext}.
Step7: Rehash the inverse DCT coefficients to obtain final extracted watermark

2.3 Embedding process for text watermark

Text watermark (Info) is embedded using following process:

Step1: Read the images
Input: Color Cover Image (512 × 512 × 3)
Step2: Select the color component for watermark embedding
Step3: Apply LWT on selected color component, decompose it into its sub bands and select LL3 sub-band.
Step4: Text watermark (Info) is converted into binary bits.
Step5: Apply Hamming encoder and then Arithmetic encoding algorithm to the info watermark and replace 0 by -1.
Step6: Embed the watermark into cover image's LL3 sub band using following equation.

$$B'(x, y) = B(x, y)(1 + k^* W_t) \tag{12}$$

$B_i^{'}(x, y)$	After embedding LL3 LWT coefficients
B(x,y)	Before embedding LL3 LWT coefficients
W_t	Text watermark bits and k is the gain factor.

Step7: Apply inverse LWT in order to obtain watermarked selected component.
Step8: Concatenate the watermarked component with other two color components.

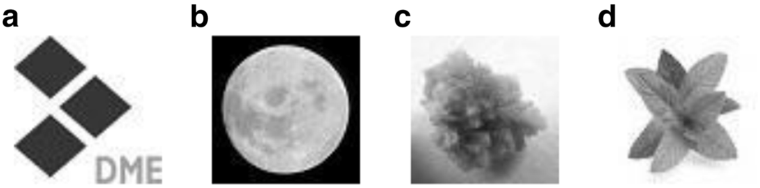


Fig. 3 **a** logo, **b** moon, **c** stone, **d** peppermint

Step9: Convert the watermarked image into RGB color space if they were previously converted into YIQ or YCbCr color image model.

2.4 Extraction process for text watermark

Watermark (Info) can be extracted by following method: -

Step1: Read the images

Input: Color Cover Image (512 × 512 × 3), Color Watermarked image (512 × 512 × 3)

Step2: Select the color component from the cover and watermarked image for watermark extraction.
Step3: Apply 3rd-level LWT transform on selected component of watermarked and cover image and select their corresponding LL3 sub-bands.
Step4: Extract the text watermark bits from the coefficients of LL3 sub band of watermark and cover image.

$$\mathrm{Wt_i}' = \frac{\mathrm{B}^{'}(\mathrm{x},\mathrm{y})-\mathrm{B}(\mathrm{x},\mathrm{y})}{\mathrm{k}*\mathrm{B}(\mathrm{x},\mathrm{y})} \tag{15}$$

Step5: Apply Arithmetic decoder and then Hamming decoder algorithm to the extracted text watermark bits.
Step6: Convert the extracted bits into text to get final extracted Info watermark.

3 Experimental results and analysis

The performance of this hybrid approach for text watermarking has been evaluated in terms of Peak Signal to Noise Ratio (PSNR) for watermarked image, Normalized Correlation (NC) for image watermark and BER (Bit Error Rate) for text watermark [24, 29, 39, 52–55]. The color image having size 512 × 512 × 3 and watermark image having size 64 × 64 are considered for watermarking. The standard evaluation criteria used to check the effectiveness of

Aditi Zear (22678)
Department of Computer Science and Engineering
National Institute of Technology, Hamirpur, Himachal Pradesh, 171001

Fig. 4 Text watermark (Info)

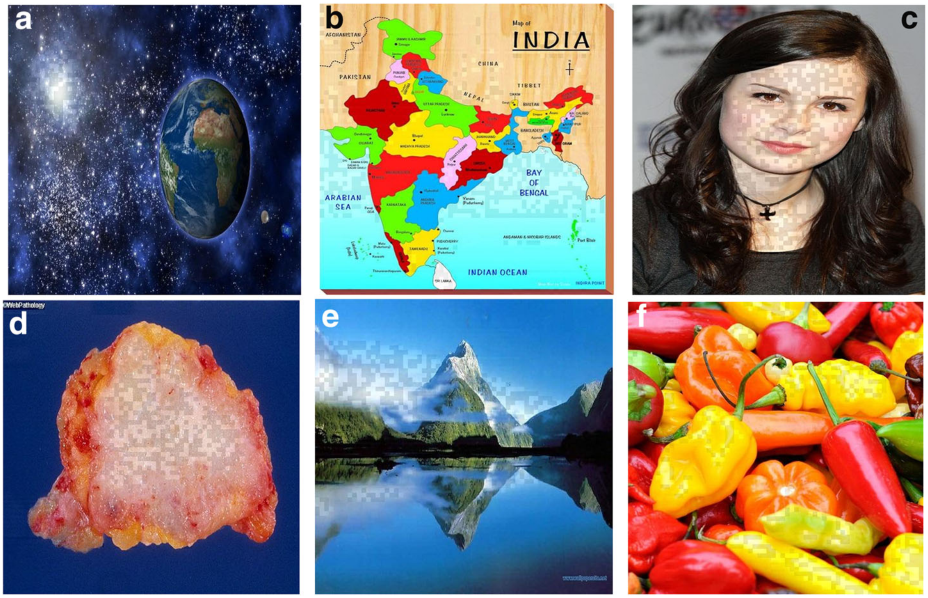


Fig. 5 Watermarked, **a** Earth, **b** India-map, **c** Lena Meyer, **d** Lump, **e** Mountain, **f** Peppers

watermarking algorithm is the imperceptibility of the watermarked image and robustness of embedded watermarks. Peak Signal to Noise Ratio (PSNR) value is used to check the imperceptibility of watermarked image. The robustness of the embedded watermarks is checked using Bit Error Rate (BER) parameter for text watermark and Normalized Correlation (NC) parameter for image watermark.

The algorithm can be tested for different size of text watermark, image watermark and cover image. For testing purpose we have downloaded images from internet. However these images can be application specific such as medical images for telemedicine applications. We have used only three standard parameters for testing the proposed algorithm. In addition to these standard parameters, various other parameters such as number of changing pixel rate (NPCR), unified averaged changed intensity (UACI), and structural similarity index (SSIM) can be used for evaluating the proposed approach. Image watermark's security is increased by using MD-5. Info watermark containing information related to image for authentication purposes is used as text watermark.

Figure 2a-f shows the cover images: Earth, India-map, Lena Meyer, Lump, Mountain, and Peppers. Figure 3a-d shows the watermark images: logo, moon, stone and peppermint. Text watermark is given in Fig. 4. Figure 5a-f shows the corresponding watermarked images.

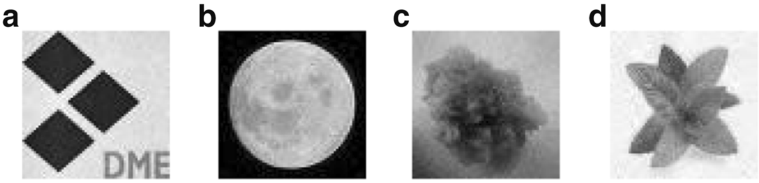


Fig. 6 Extracted Watermarks, **a** logo, **b** moon, **c** stone, **d** peppermint

Table 1 PSNR, BER, NC values for various Color Image models at Various Scaling Factors

Color Model	Color Component	Scaling factor	PSNR	BER	NC
RBG	R	0.01	34.59	45	0.0838
		0.08	33.54	0	0.9789
		0.15	31.91	0	0.9875
	G	0.01	34.58	22.50	0.7325
		0.08	33.28	0	0.9925
		0.15	32.86	0	0.9983
	B	0.01	34.59	47.85	0.7450
		0.08	33.69	0	0.9835
		0.15	33.34	0	0.9931
YIQ	Y	0.01	34.54	0	0.8765
		0.08	31.74	0	0.9961
		0.15	28.91	0	0.9950
	I	0.01	34.60	46.78	−0.3997
		0.08	34.13	0	0.9770
		0.15	33.16	0	0.9976
	Q	0.01	34.60	45	0.5526
		0.08	33.91	45.71	0.9948
		0.15	32.68	50	0.9972
YCbCr	Y	0.01	34.52	0	0.9083
		0.08	31.07	0	0.9984
		0.15	27.59	0	0.9972
	Cb	0.01	34.555	38.57	0.1263
		0.08	32.40	0	0.9889
		0.15	29.41	0	0.9902
	Cr	0.01	34.58	50.357	−0.1864
		0.08	32.89	0	0.9919
		0.15	30.43	39.64	0.9940

Figure 6a-d shows the corresponding extracted watermarks The size of text watermark Info is considered as 80 characters for Tables 3, 4 and 5. In Table 3, BER, PSNR and NC values for this approach has been computed for different scaling factors.

Table 2 PSNR, BER, NC values for various text watermark size at various scaling factors

SN	Number of characters	Scaling factor	PSNR (db)	BER(%)	NC
1.	20	0.01	34.55	0	0.9065
		0.05	33.44	0	0.9961
		0.1	31.32	0	0.9989
		0.15	29.37	0	0.9979
2.	40	0.01	34.52	0	0.9086
		0.05	32.80	0	0.9963
		0.1	29.98	0	0.9987
		0.15	27.60	0	0.9976
3.	60	0.01	34.50	0	0.9078
		0.05	32.32	0	0.9962
		0.1	29.09	0	0.9986
		0.15	26.55	0	0.9970
4.	80	0.01	34.47	0	0.9092
		0.05	31.91	0	0.9963
		0.1	28.31	0	0.9989
		0.15	25.59	0	0.9975

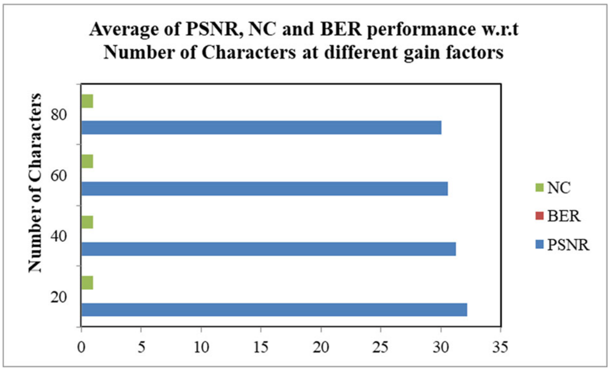


Fig. 7 Average of PSNR, BER, NC values for various Text Watermark Size at different gain Factors

In Table 1, the performance of algorithm is tested for different components in three color image models i.e. RGB, YIQ, YCbCr. The size for text watermark used for this table is 40 characters. The maximum PSNR value is 34.60 at gain factor 0.01 in Y component of YIQ model and minimum PSNR value is 27.59 in Y component of YCbCr model. Maximum NC value is obtain at Y component of YCbCr model i.e. 0.9984 and minimum NC value is −0.3997 obtained in I component of YIQ model. The BER is 0% in different components of color image model and the highest BER obtained is 50.357% in Cr component of YCbCr model. Only the Y component of YIQ and YCbCr model provides high NC values with 0% BER. The NC values are higher in YCbCr model for Y component. Therefore Y component of YCbCr model is use for further performance testing.

In Table 2 the performance is evaluated for different size of text watermark at various gain factors. Maximum PSNR value obtained is 34.55 for text watermark of size 20 at gain factor 0.01 and minimum value obtained is 25.59 for 80 characters at gain factor 0.15. Therefore the PSNR values decrease with increase in number of characters and gain factor.

Figure 7 represents Table 2 graphically. Values of PSNR, NC and BER are averaged for different characters. Table 3 shows the performance of the algorithm at different scaling factors. The highest and lowest PSNR values are 34.47 and 24.31 at gain factors 0.01 and 0.18 respectively. The BER is 0 for all gain factors. Maximum NC value is 0.9989 which is obtained at 0.1 gain factor and lowest NC value is 0.9092 at gain factor 0.01. Figure 8 is used for the graphical representation of Table 3. However the scaling factor ‘0.06’ is considered for

Table 3 PSNR, BER, NC values at various scaling factors

SN	Scaling factor	PSNR(db)	BER(%)	NC
1.	0.01	34.47	0	0.9092
2.	0.02	34.02	0	0.9821
3.	0.05	31.91	0	0.9963
4.	0.06	31.13	0	0.9975
5.	0.08	29.65	0	0.9988
5.	0.1	28.31	0	0.9989
6.	0.12	27.13	0	0.9986
7.	0.15	25.59	0	0.9975
8.	0.18	24.31	0	0.9961

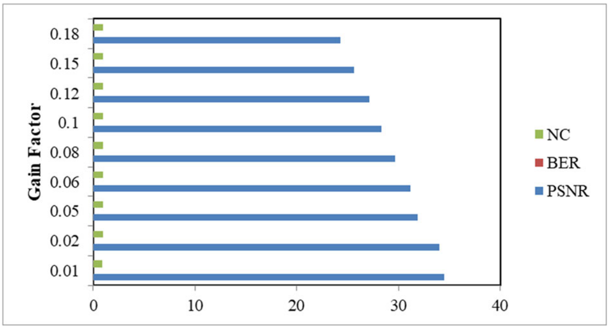


Fig. 8 PSNR, BER, NC values at various scaling factors

the experimental purpose in Tables 4 and 5 because it provides PSNR value greater than 30 i.e. 31.31 with robust NC value of 0.9975.

Table 4 shows the BER, PSNR and NC values for various images (cover and watermark). The maximum PSNR obtained is 32.61 for Mountain as cover image and logo as watermark image Minimum value for PSNR is 29.51 for India Map cover image and logo as watermark. NC value obtained for mountain image is 0.9976 which is also the highest NC value and minimum NC value is 0.9383 for peppers as cover image and mint watermark.

The BER is '0' for maximum cover and watermark images except 44.10% BER are obtained for for India-map cover image and logo watermark image. Figure 9 shows Table 4 graphically. The BER and NC values of this approach against various attacks are given in Table 5.

The lowest NC value is obtained for Average filter attack i.e. 0.4968 and highest NC value is obtained for Gaussian noise (m = 0, v = 0.001) which is 0.9892. The BER is 0 for maximum attacks however maximum value for BER is obtained at Rotation (5°) i.e. 54.107. Figure 10 demonstrates the graphical representation of Table 5.

Table 6 shows the comparison our proposed method with technique proposed in [45]. The maximum NC value obtained by our technique is 0.9965 and maximum value of NC is [45] for 0.9837. The method proposed in [45] has better NC values as compared to our proposed technique for Average filter ([3 3]) and Speckle (v = 0.01), and the values corresponding to these attacks are 0.7346 and 0.8819 respectively. However the NC values of our proposed method for these attacks are 0.4968 and 0.8389. For other attacks the NC performance of our proposed method is better than the approach in [45].

From these experimental results we can conclude that the performance of this algorithm depends on the type of color image model, cover image, watermarks size, scaling factors, size

Table 4 PSNR, BER, NC Performance for various images (Cover and Watermark) at Gain 0.06

SN	Cover Image	Watermark image	PSNR (db)	BER (%)	NC
1.	Lena Meyer	logo	31.13	0	0.9975
2.	Mountain	logo	32.61	0	0.9976
3.	Earth	moon	30.47	0	0.9966
4.	Lump	stone	31.07	0	0.9894
5.	India map	logo	29.51	44.10	0.9787
6.	peppers	mint	30.74	0	0.9383

Table 5 BER, NC results for various Attacks at Gain 0.06

SN	Attacks	BER (%)	NC
1.	JPEG 10	0	0.9668
2.	JPEG 20	0	0.9788
3.	JPEG 50	0	0.9837
4.	JPEG 80	0	0.9965
5	Histogram Equalization	38.75	0.6913
6.	Median Filter	0	0.6870
7.	Average Filter ([3 3])	3.04	0.4968
8.	Salt & Peppers noise (d=0.02)	45.54	0.9201
9.	Salt & Peppers noise (d=0.03)	46.78	0.8365
10.	Salt & Peppers noise (d=0.01)	0	0.9690
11.	Gaussian noise (m=0.01, v=0.002)	0	0.9822
12.	Gaussian noise (m=0.01, v=0.001)	0	0.9892
13.	Gaussian noise (m=0.01, v=0.006)	0	0.9477
14.	Gaussian noise (m=0.02, v=0.006)	0	0.9631
15.	Speckle (variance=0.02)	13.57	0.9579
16.	Speckle (v=0.01)	0	0.9844
17.	Speckle (v=0.05)	43.25	0.8389
18.	Rotation (2°)	44.107	0.8596
19.	Rotation (5°)	54.107	0.6295
20.	JPEG 70+Speckle(0.02)	47.14	0.9439
21.	JPEG 70+Gaussian noise (m=0, v=0.005)	0	0.9539
22.	JPEG 30+Salt & Peppers noise (d=0.01)	0	0.9563
23.	Salt & Peppers noise (d=0.01)+Gaussian noise (m=0.02, v=0.005)	0	0.9028
24	Gaussian noise (m=0.01, v=0.005)+Speckle(0.01)	0	0.9546
25.	Salt & Peppers noise (d=0.01)+Speckle(0.01)	46.07	0.9629

of text watermark, and noise variations. The PSNR value highly depends on scaling factor and number of characters. As we increase the scaling factor and number of characters the PSNR value decreases. NC values are not showing any pattern (increasing or decreasing) in relation with text watermark size and scaling factor. Even for high scaling factor NC values decrease. For some attacks and cover image BER is high. This may happen because of combined encryption and compression. If some bits get garbled because of some attacks then the extracted text watermark may show high bit error rate.

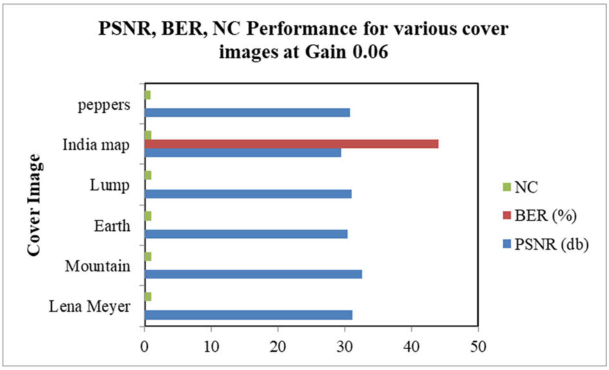


Fig. 9 PSNR, BER, NC Performance for various images (Cover and Watermark) at Gain 0.06

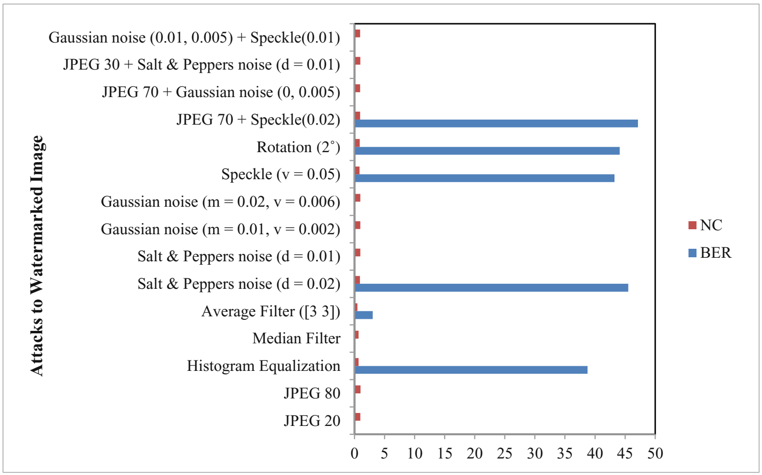


Fig. 10 BER, NC results for various Attacks at Gain 0.06

4 Conclusion

In this paper, hybrid image watermarking technique using LWT-DCT-SVD has been proposed. The important properties of the proposed approach are: 1) LWT provides increase in smoothness and reduction in aliasing effects, prevents loss of information and improves robustness of watermark. In addition to this LWT also requires less memory and computational complexity. Therefore combination of LWT-DCT-SVD achieves excellent performance. 2) Embedding multiple watermarks into single cover image increases capacity and also helps in authentication. 3) Conservation of transmission bandwidth by using multiple watermarks. 4) Compression of text watermark using Arithmetic coding helps in embedding more bits into cover image or can be used to improve imperceptibility. Therefore the proposed method is suitable for the protection of digital documents from theft/modification/alteration in different social applications.

In future we will increase the efficiency of proposed algorithm by testing it with other security related algorithms and compression techniques. The BER performance of the proposed method requires improvement.

We would like to improve the performance of proposed method by using various optimization techniques. Deciding the scaling factor with which the watermark should be embedded

Table 6 Comparing NC performance of proposed method with Singh [45]

SN	Attacks	Singh [45]	Our Method
1.	JPEG 10	0.6996	0.9668
2.	JPEG 80	0.9837	0.9965
3.	Histogram Equalization	0.5882	0.6913
4.	Average Filter ([3 3])	0.7346	0.4968
5.	Salt & Peppers noise (d=0.01)	0.8077	0.9690
6.	Salt & Peppers noise (d=0.02)	0.7028	0.9201
7.	Speckle (v=0.01)	0.8819	0.8389
8.	Rotation (5°)	0.0376	0.6295

into the cover image is major research gap which requires consideration. Therefore we will try to improve the proposed algorithm by determining the optimal scaling factor with the help of machine learning techniques.

References

1. Ahmidi N, Safabakhsh R (2004, April) A novel DCT-based approach for secure color image watermarking. In Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on (Vol. 2, pp. 709-713). IEEE.
2. Ali Hajjaji M, Bourennane E-B, Abdelali AB, Mtibaa A (2014) Combining Haar wavelet and Karhunen Loeve transforms for medical images watermarking. Biomed Res Int:1–20
3. Aparna P, Kishore PVV (2018) Bio -metric based efficient medical image watermarking in ehealthcare application. IET Image Process 13(3):421–428
4. Araghi TK, Manaf AA (2019) An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. Future Gener Comput Syst 101:1223–1246
5. Arya MS, Siddavatam R, Ghrera SP (2011, May) A hybrid semi-blind digital image watermarking technique using lifting wavelet transform-singular value decomposition. In electro/information technology (EIT), 2011 IEEE International Conference on (pp. 1-6). IEEE.
6. Bao L, Zhou Y (2015) Image encryption: generating visually meaningful encrypted images. Inf Sci 324: 197–207
7. Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. IBM systems journal 35(3.4): 313–336
8. Boonyapalanant A, Ketcham M, Piyaneeranart M (2019) Hiding patient injury information in medical images with QR code. Adv Intell Syst Comput:258–267
9. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90(3):727–752
10. Dagadu JC, Li J (2018) Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. Multimed Tools Appl:1–24
11. Dai Q, Li J, Bhatti UA, Chen Y-W, Liu J (2019) SWT-DCT-based robust watermarking for medical image. Smart Innov Syst Technol:93–103
12. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6:20596–20608
13. Ganic E, Eskicioglu AM (2004, September) Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In Proceedings of the 2004 Workshop on Multimedia and Security (pp. 166-174). ACM.
14. Ghafoor A, Imran M (2012) A non-blind color image watermarking scheme resistent against geometric attacks. Radioengineering 21(4):1246–1251
15. Gul E, Ozturk S (2020) A novel triple recovery information embedding approach for self-embedded digital image watermarking. Multimed Tools Appl:1–26
16. Gunjal BL, Mali SN (2011) Comparative performance analysis of DWT-SVD based color image watermarking technique in YUV, RGB and YIQ color spaces. Int J Comput Theory Eng 3(6):714–719
17. Hu X, Lian X, Chen L, Zheng Y (2008, June) Robust blind watermark algorithm of color image based on neural network. In Neural Networks and Signal Processing, 2008 International Conference on (pp. 430-433). IEEE.
18. Hu HT, Chang JR, Hsu LY (2016) Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception. AEU-International Journal of Electronics and Communications 70(10):1374–1381
19. Jagadeesh B, Kumar PR, Reddy PC (2013) Robust digital image watermarking scheme in discrete wavelet transform domain using support vector machines. Int J Comput Appl 73(14):1–7
20. Jinna SK, Ganesan L (2009) Lossless image watermarking using lifting wavelet transform. International Journal of Recent Trends in Engineering 2(1):191–195
21. Kashyap N, Sinha GR (2012) Image watermarking using 3-level discrete wavelet transform (DWT). International Journal of Modern Education and Computer Science 4(3):50–56
22. Kejgir SG, Kokare M (2012) Lifting wavelet transform with singular value decomposition for robust digital image watermarking. International Journal of Computer Applications 39(18):10–18
23. Kumar A, Agarwal P, Choudhary A (2016) A digital image watermarking technique using cascading of DCT and Biorthogonal wavelet transform. In Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing (pp. 21-29). Springer India.

24. Lefèvre P, Carré P, Gaborit P (2019) Application of rank metric codes in digital image watermarking. Signal Process Image Commun 74:119–128
25. Li M, Yuan X, Chen H, Li J (2020) Quaternion discrete fourier transform-based color image watermarking method using quaternion QR decomposition. IEEE Access 8:72308–72315
26. Liu S, Pan Z, Song H (2017) Digital image watermarking method based on DCT and fractal encoding. IET Image Process 11(10):815–821
27. Liu J, Li J, Ma J, Sadiq N, Ai Y (2019) FDCT and perceptual hash-based watermarking algorithm for medical images. Smart Innov Syst Technol, pp. 157–168.
28. Loukhaoukha K, Chouinard JY (2009, May) Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification. In Information Theory, 2009. CWIT 2009. 11th Canadian Workshop on (pp. 177-182). IEEE.
29. Mingzhi C, Yan L, Yajian Z, Min L (2013) A combined dwt and dct watermarking scheme optimized using genetic algorithm. J Multimed 8(3):299–305
30. Mohananthini N, Yamuna G (2012, March) Watermarking for images using wavelet domain in Back-Propagation neural network. In Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on (pp. 100-105). IEEE.
31. Mothi R, Karthikeyan M (2019) Protection of bio medical iris image using watermarking and cryptography with WPT. Measurement 136(3):67–73
32. Murali P, Sankaradass V (2018) An efficient ROI based copyright protection scheme for digital images with SVD and orthogonal polynomials transformation. Optik 170(10):242–264
33. Nagpal S, Bhushan S, Mahajan M (2016) An enhanced digital image watermarking scheme for medical images using neural network, DWT and RSA. International Journal of Modern Education and Computer Science (IJMECS) 8(4):46–56
34. Nandi S, Santhi V (2016) DWT–SVD-based watermarking scheme using optimization technique. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 69-77). Springer India.
35. Nasir IA, Abdurrman AB (2013, July) A robust color image watermarking scheme based on image normalization. In Proceedings of World Congress on Engineering (Vol. 3, pp. 1-6).
36. Poonam P, Kundu S, Kumar S, Chander K (2012, September) Efficient genetic algorithm based image watermarking using DWT-SVD techniques. In Computing Sciences (ICCS), 2012 International Conference on (pp. 82-87). IEEE.
37. Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. IEEE security & privacy 99(3):32–44
38. Rathi SC, Inamdar VS (2014) Medical images authentication through watermarking preserving ROI. Health Inform – Int J (HIIJ) 1(1):27–42
39. Roy SS, Basu A, Chattopadhyay A (2020) On the implementation of a copyright protection scheme using digital image watermarking. Multimed Tools Appl:1–14
40. Saini H (2014, February) Efficient hybrid watermarking approach by using SVD, DWT, and back propagation neural network. In Advance Computing Conference (IACC), 2014 IEEE International (pp. 985-990). IEEE.
41. Santhi V, Thangavelu A (2009) DWT-SVD combined full band robust watermarking technique for color images in YUV color space. Int J Comput Theory Eng 1(4):424–429
42. Sharma A, Singh AK, Ghrera SP (2015) Secure hybrid robust watermarking technique for medical images. Procedia Computer Science 70:778–784
43. Sharma A, Singh AK, Ghrera SP (2017) Robust and secure multiple watermarking for medical images. Wirel Pers Commun 92(4):1611–1624
44. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images. IEEE Access 6(1):10269–10278
45. Singh AK (2019) Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. Multimed Tools Appl 78(21):30523–30533
46. Singh AK, Kumar C (2020) Encryption-then-compression-based copyright protection scheme for E-governance. IT Professional 22(2):45–52
47. Singh AK, Dave M, Mohan A (2016) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl 14(75):8381–8401
48. Su Q, Liu X, Yang W (2009, April) A watermarking algorithm for color image based on YIQ color space and integer wavelet transform. International Conference on Image Analysis and Signal Processing, 2009. IASP, (pp. 70-73). IEEE.
49. Vafaei M, Mahdavi-Nasab H, Pourghassem H (2013) A new robust blind watermarking method based on neural networks in wavelet transform domain. World Appl Sci J 22(11):1572–1580
50. Venkatram N, Reddy LSS, Kishore PVV, Fields G, Vaddeswaram GD, Pradesh A (2014) Blind medical image watermarking with LWT–SVD for telemedicine applications. Image 20:23

51. Wang J, Wan WB, Li XX, De Sun J, Zhang HX (2020) Color image watermarking based on orientation diversity and color complexity. Expert Syst Appl 140:112868
52. Yadav AK, Mehta R, Kumar R (2015, August) Gray scale image watermarking using fuzzy entropy and lagrangian twin SVR in DCT domain. In Contemporary Computing (IC3), 2015 Eighth International Conference on (pp. 19-24). IEEE.
53. Zear A, Singh AK, Kumar P (2017) Robust watermarking technique using back propagation neural network: a security protection mechanism for social applications. Int J Inf Comput Secur 9(1–2):20–35
54. Zear A, Singh AK, Kumar P (2018) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl 77(4):4863–4882
55. Zear A, Singh AK, Kumar P (2018) Multiple watermarking for healthcare applications. J Intell Syst 27(1): 5–18
56. Zheng Z, Saxena N, Mishra KK, Sangaiah AK (2018) Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications. Futur Gener Comput Syst 88:92–106