ORIGINAL ARTICLE

Fingerprint-based robust medical image watermarking in hybrid transform

S. Prasanth Vaidya[1]

Abstract

To protect the medical images integrity, digital watermark is embedded into the medical images. A non-blind medical image watermarking scheme based on hybrid transform is propounded. In this paper, fingerprint of the patient is used as watermark for better authentication, identifying the original medical image and privacy of the patients. In this scheme, lifting wavelet transform (LWT) and discrete wavelet transform (DWT) are utilized for amplifying the watermarking algorithm. The scaling and embedding factors are calculated adaptively with the help of Local Binary Pattern values of the host medical image to achieve better imperceptibility and robustness for medical images and fingerprint watermark, respectively. Two-level decomposition is done where for the first level LWT is utilized and for the second level decomposition DWT is utilized. At the extraction side, non-blind recovery of fingerprint watermark is performed which is similar to the embedding process. The propounded design is implemented on various medical images like Chest X-ray, CT scan and so on. The propounded design provides better imperceptibility and robustness with the combination of LWT–DWT. The result analysis proves that the proposed fingerprint watermarking scheme has attained best results in terms of robustness and authentication with different medical image attacks. Peak Signal to Noise Ratio and Normalized Correlation Coefficient metrics are used for evaluating the proposed scheme. Furthermore, superior results are obtained when compared to related medical image watermarking schemes.

Keywords Medical image watermarking · Lifting wavelet transform (LWT) · Discrete wavelet transform (DWT) · Local binary pattern (LBP) · Non-blind watermarking · Electronic patient record (EPR)
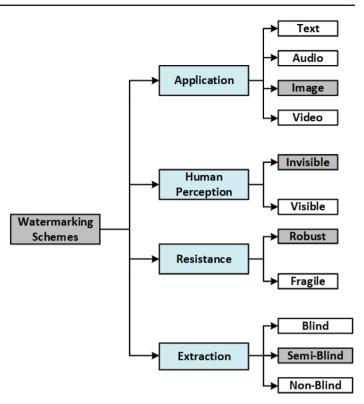
1 Introduction

The corona virus COVID-19 pandemic is the defining global health crisis of our time and the greatest challenge we have faced since World War Two. The WHO formally declared the novel corona-virus severe acute respiratory syndrome corona-virus 2 [1]. To reduce the risk of person-to-person viral transmission during the COVID-19 pandemic, government introduced social distancing and other measures. Many hospitals have closed their doors to patients who have been trying to avail the facilities and doctors are not encouraged to meet the patient directly [7]. With all these considerations, now-a-days every doctor is meditating the patients through online only. Previously many metropolitan cities and multi-specialty clinics are only maintaining online data of patients reports and records. Due to the present situation, every doctor is asking the patients and hospital management to send the record online to diagnose the patient report. Transfer of medical records of patients over a communication channel is known as telemedicine. American Telemedicine Association (ATA) defined telemedicine as the medical data that are transferred from one location to another location through electronic communication channel for improving the patients health status [32]. During the communication channel, the patients data should not be corrupted or modified or morphed at the receiver side; it may lead to serious trouble to patient while diagnosis. For small hospitals, maintaining and storing Electronic Patient Record (EPR) is of great concern [25]. The EPR data containing patient details, like diagnosis, disease, treatment and so on, have to be maintained confidentially [35]. For this reason, security to the medical image is required, which can be achieved with watermarking tech-

✉ S. Prasanth Vaidya
   vaidya269@gmail.com

1 Department of Computer Science and Engineering, Aditya Engineering College (A), Surampalem, Andhra Pradesh 533437, India

Fig. 1 Various classifications of
watermarking schemes

nique with minimum probability of error. The medical image is used as host image to deplete the chance of tampering or modification.

Depending on the information required at the extraction side to get the watermark along with the key, watermarking is classified into three types: blind, non-blind and semi-blind [40]. Without the watermark information, the watermark can be extracted in blind watermarking. Original host data and keys are required in non-blind watermarking, partial host data and key are required in semi-blind watermarking [39]. In all the three types, non-blind watermarking extraction offers better robustness compared to other two classifications.

The watermarking scheme can be classified into spatial and transform domain based on the type of embedding [29]. Transform domain provides better robustness against attacks with high embedding capacity of watermark compared to spatial domain [41].

The watermarking scheme is also classified into visible or perceptible and imperceptible or invisible watermarking based on the perceptibility of the watermark in the watermarked image. Perceptible watermarks are visible to naked eye, whereas imperceptible are not visible to the naked eye.

Another watermarking classification that is based on resistance is robust and fragile. Robust watermarking scheme can withstand intentional and unintentional attacks, whereas fragile watermarking schemes cannot withstand minor modifications on the watermarked image.

The watermarking scheme is designed based on applications of multimedia like "text, audio, image and video". The applications of watermarking scheme are Copyright Protection, Copy Control, Data Authentication, Fingerprinting, Broadcast Monitoring and so on. Various classifications of watermarking schemes are provided in Fig. 1.

Nowadays much research is going on in hybrid transform by combining different transformation techniques to increase the robustness and embedding capacity. This research article proposed a robust non-blind watermarking scheme for copyright protection, ownership identification and authentication of medical images in hybrid domain. In the proposed approach, fingerprint is considered as watermark for medical data of the patients. As the medical data of the patient are private data where the data should not be authorized by unknown persons. To make the authentic authorization of the data, direct finger print of the data is included to provide security to the medical image. Watermarking can be embedded into a host image through different transform operations, such as discrete cosine transform (DCT), discrete wavelet transform (DWT), lifting wavelet transform (LWT) and so on. However, a single transformation does not ensure all the design requirements simultaneously. To fill this gap, a hybrid digital image watermarking with a combination of LWT-DWT is proposed in this paper. The main purpose of hybrid transform is to develop LWT-DWT-based robust and invisible image watermarking scheme for obtaining a better tradeoff between imperceptibility and robustness requirements.

2 Literature survey

Anand et al. [3] propounded an improved DWT–SVD domain watermarking for medical information security. Hamming code is utilized to reduce the noise distortion of the text watermark. They have tested on two different encryption schemes and three different compression schemes and considered Chaotic-LZW (Lempel–Ziv–Welch) as the best.

Kahlessenane et al. [14] presented a robust blind watermarking scheme that accepts the incorporation of EPR into computerized tomography scan. Zigzag scanning method is utilized in selecting the subband of wavelet transform. Their results showcase the method is good against geometric and destructive attacks.

Fares et al. [7] proposed two blind watermarking schemes with combination of DCT-Schur and DWT-Schur. Their method results provide robust against conventional attacks. Yuan et al. [47] developed color image watermarking method using DCT in spatial domain. An effective watermarking algorithm based on Lagrangian support vector regression (LSVR) & LWT is designed [24] by considering the advantages of fast implementation, fast learning speed and high generation capacity compared to previous conventional methods.

Sing et al. [36] developed a semi blind gray scale watermarking scheme by using nonsubsampled contourlet transform and redundant discrete wavelet transform (RDWT) and SVD decomposition methods. Amit et al. [34] presented a paper on spread spectrum depended watermarking system using selective DWT approach. Amit et al. [33] presented a multiple watermarking scheme using DWT, DCT and SVD decomposition. Amit et al. [31] presented a hybrid multi-level watermarking scheme by fusing DWT, DCT and SVD decomposition techniques. Chandan et al. [17] presented a paper on improved watermarking scheme by using DWT, DCT and SVD. Further set partitioning in hierarchical tree and Arnold transform are utilized to improve the security. Priyank et al. [16] proposed a watermarking scheme based on homomorphic transform, RDWT and SVD decompositions.

Watermark insertion is done using principal components to handle attacks where region of interest (ROI) of compressed image is hidden using LZW [2]. The watermark generated with compressed image ROI allows 100% reversibility of the ROI. An imperceptible and zero watermarking for robust medical images is proposed [5]. Using modified spread spectrum method, the retaliation of the imperceptible watermarking detector & watermark data, the zero watermarking process authenticates the patient identity. Kannammal et al. [15] developed an algorithm with 2-level security with embedding and also with encryption using RSA and other algorithms. Sharma et al. [30] developed a method using digital multitoning in embedding binary watermark.

Combining LSVR and LWT has reduced the time complexity as well. To overcome the issues of information security (authentication), David et al. [23] proposed a hybrid watermarking scheme using quantization index modulation method beneath ditcher modulation in collaboration with error correction forwarding in embedding. Thakur et al. [38] proposed a multilayer security for medial data by utilizing chaotic encryption.

Hosny et al. [10] proposed a novel geometrically invariant multiple zero watermarking method for medical images. A set of multi-channels shifted Gegenbauer moments of fractional orders are used to extract invariant features from color medical images. Hosny et al. [11] have computed the moments of the polar complex exponential transform (PCET) and quaternion PCET in securing medical images for authentication. Hosny et al. [9] utilized Quaternion Legendre–Fourier moments for developing color image watermarking. Hosny et al. [8] utilized highly accurate moments of polar harmonic transforms for designing watermarking algorithm.

All the literature provided above is related to only medical image watermarking. They have followed different types of watermarking approaches based on extraction, and in embedding watermark different transformation techniques methods are utilized (most commonly DWT, DCT, LWT). The proposed watermarking approach can overcome the problems of authentication by embedding the fingerprint watermark. As the medical images are vulnerable to attacks, the proposed method has overcome that by using hybrid transformation and using adaptive embedding factor values for images. In the proposed scheme, 4 subbands LL, LH, HL and HH are obtained after 1 level LWT. LL is selected based on its efficient properties. The LL subband is again decomposed for 1 level using DWT then embedding the fingerprint watermark into it. The motivation behind this combination is to enhance the imperceptibility and the robustness. The imperceptibility requirement is achieved by using magnitudes of LWT coefficients, while robustness improvements are provided by applying DWT to LWT coefficients. The watermark is embedded by modifying the coefficients of DWT using secret keys.
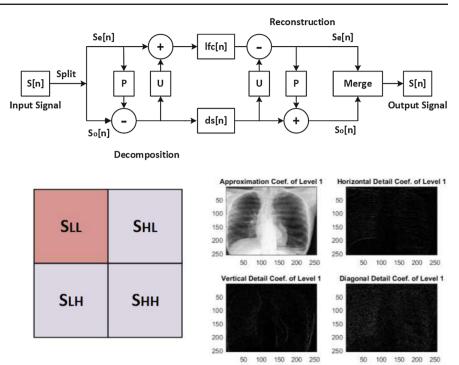
3 Methods used

3.1 Lifting wavelet transform

Over the past few years, LWT developed by Daubechies [6], enhanced as a husky tool for analysis of image because of systematic and fast implementation of LWT compared to conventional wavelet transform [18]. LWT has given best results in the area of watermarking, image compression, pattern recognition, feature extraction and image de-noising [42]. LWT saves a lot of time and also has superior results

Fig. 2 Decomposition of
Lifting Wavelet Transform

Fig. 3 1-Level Decomposition
of Discrete Wavelet Transform
Representation

in frequency localizing frequency features that conquer the drawback of conventional wavelets [21,24]. LWT decomposition of a signal is done with splitting, prediction and update steps as shown in Fig. 2.

Step 1: Splitting

In this step, the host signal $S[n]$ is decomposed into non-overlapping odd and even signal samples as $S_o[n]$ and $S_e[n]$ which can be seen in Eq. 1.

$$S_e[n] = S[2n], S_o[n] = S[2n + 1] \qquad (1)$$

Step 2: Prediction

In this step, both odd and even sample signals are correlated for predicting as shown in Eq. 2.

$$ds[n] = S_o[n] - P(S_e[n]) \qquad (2)$$

where $ds[n]$ is the difference the host signal sample and its predicted signal (high frequency component) using prediction operator $P(.)$.

Step 3: Update

The even samples are updated with the help of step 1 and step 2 i.e., detailed signal ($ds[n]$ and update operator ($U(.)$). The rough shape of the host signal can be obtained with low frequency component $lfc[n]$ as shown in Eq. 3.

$$lfc[n] = S_e[n] + U(ds[n]) \qquad (3)$$

3.2 Discrete wavelet transform (DWT)

DWT breaks down an image or signal into four subbands, S_{LL} lower resolution approximation module, and other three spatial directional modules are horizontal module S_{HL}, vertical module S_{LH} and module S_{HH}. The characteristics of the DWT image multi-resolution break down, and the image features are extremely consistent for selecting the spatial orientation. The filters applied on the DWT will be done along the rows and columns with the help of low pass and high pass resolvers (Lo_D, Hi_D), respectively. Mathematically, the host signal or image $S(a, b)$, the first level break down is shown in Eq. (4). The decomposition of signal into subbands and sample X-ray image 1-level decomposition is represented in Fig. 3.

$$\begin{aligned} LL(i, j) &= \langle S(a, b), \Psi^0(a - 2i, b - 2j) \rangle \\ LH(i, j) &= \langle S(a, b), \Psi^1(a - 2i, b - 2j) \rangle \\ HL(i, j) &= \langle S(a, b), \Psi^2(a - 2i, b - 2j) \rangle \\ HH(i, j) &= \langle S(a, b), \Psi^3(a - 2i, b - 2j) \rangle \end{aligned} \qquad (4)$$

3.3 Local binary pattern (LBP)

Ojala et al. [26,27] first developed LBP, initially utilized to calculate the local contrast in analysis of texture in images. LBP is utilized in many fields of image and video processing like text analysis, image authentication and image forgery detection due to its property of efficient texture feature descriptor [20]. LBP breaks down an image into multiple

sub-blocks of size $n \times n$. The centre pixel value is utilized as a threshold value to decide the neighbouring pixel values by setting the smaller values as 0 and remaining as 1 by comparing with centre pixel, i.e., threshold value. The clockwise values of the binary values are considered and converted to decimal form. The LBP is formulated as shown in Eq. 5. The sample block operator of 3×3 block and its local binary pattern conversion from binary to decimal are shown in Fig. 4.

$$LBP(a_j, b_j) = \sum_{i=0}^{i=\infty} S(P_i - P_j)2^i \tag{5}$$

where P_j is central pixel (a_j, b_j) value and P_i are corresponding pixel values. S is sign function defined as

$$S(a) = \begin{cases} 1, & x \geq 0, \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

The most important property of the LBP function in real-world applications is its robustness to monotonic gray-scale changes caused by illumination variations compared to other features. Other advantage of LBP is it has high discriminative power with simple computation.

3.4 Arnold transform

In the propounded watermarking scheme, Arnold Cat Transform is endorsed to provide assurance about the security of the scheme. The general Arnold Cat Transform is interpreted as follows:

$$\begin{pmatrix} g' \\ h' \end{pmatrix} = \begin{pmatrix} 1 & i \\ j & ij+1 \end{pmatrix} \begin{pmatrix} g \\ h \end{pmatrix} (\text{mod} N) \tag{7}$$

where (g, h) is the native position of the pixels in the image and (g', h') are the corresponding positions of the pixels in the image after permutation. The controls panels a and b will be used to change the position of the image pixels, and N is the size of the image. For different image sizes and parameters, period T will be different in Arnold transform. The image pixels will be back to its native position after certain permutations. Here, in applying the Arnold transform, the image gets scrambled and also we can use the T value as a key to provide better security to the scheme [44].

4 The propounded watermarking design

In the propounded watermarking scheme, approximation coefficients of LWT and S_{LL} lower resolution approximation module of DWT is utilized in immersing the fingerprint watermark of the patient because of maximum energy of the image is strenuous in low resolution approximation and

also more robust and efficient to attacks of image and signal processing. Immersing the fingerprint watermark in the S_{LL} is highly perceivable for human eye. The propounded watermark embedding design using the combination of LWT–DWT with LBP feature values and semi-blind watermark extraction using the keys are given in the following subsections. The idea of applying two transform or hybrid transform is based on the fact that combined transforms could compensate the drawbacks of each other, resulting in effective watermarking. The LBP features are considered for calculating scaling and embedding factor adaptively because of its robustness to monotonic gray-scale changes caused by illumination variations compared to other features. The reason for combination of LWT–DWT combination can be observed from the Table 1. A medical image has been tested with combination of 2 level DWT, 2-level LWT and combination of LWT–DWT with various attacks. From the results, it is clear that the combination is robust to attacks compared to their transformations. For calculating the embedding factor, LBP features are utilized since it extracts texture features of an image which is robustness to monotonic grayscale changes.
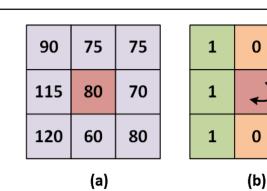
4.1 Propounded watermark embedding design using LWT–DWT–LBP

In this embedding scheme, adaptive watermark is embedded in the hybrid transform of medical image with patient fingerprint watermark. The propounded watermarking embedding design is represented in Fig. 5.

Algorithm 1 Propounded Watermark Embedding Algorithm

HMI^{fpw}=Medical watermark_embedding (HMI, FPW)
Input: Host Medical Image (HMI), Fingerprint Watermark (FPW)
Output: Scrambled Medical Watermarked image ($^{A}HMI^{fpw}$)
1: Read HMI, FPW
2: [CA, CH, CV, CD] = LWT(HMI)
3: [LL, LH, HL, HH] = DWT(CA)
4: $\alpha = \mu(LBPFeatures(HMI))$, $\beta = (1 - \alpha)$
5: $\widehat{HMI} = \alpha \times LL + \beta \times FPW$
6: $LL1' = $ IDWT($\widehat{HMI}$, LH, HL, HH)
7: $HMI^{fpw} = $ IDWT($LL1'$, CH, CV, CD)
8: $^{A}HMI^{fpw}$=Arnold(HMI^{fpw})

In the above propounded watermark embedding Algorithm 1, HMI represents host medical image, FPW represents fingerprint watermark, and μ represents the mean of the LBP features. The steps of embedding fingerprint watermark into the medical image are given below.

Step 1 Scan the fingerprint watermark and host medical image
Step 2 Applying LWT for 1–Level to host medical image produces approximation coefficients (CA) and details coefficients (CH, CV, CD)
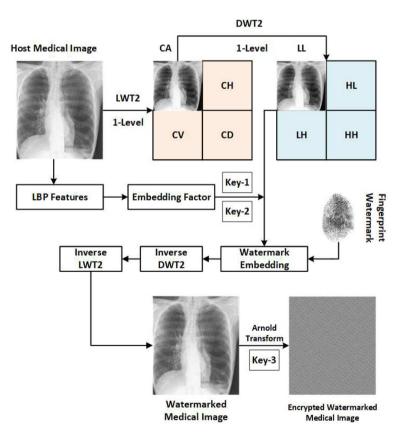
Fig. 4 3×3 Block LBP operator **a** Image block and **b** Local Binary Pattern of (**a**) block

Binary: 10001011
Decimal: 139

(a)   (b)

Table 1 Reason for selecting the combination of transformations

Model\attacks	DWT 2-Level	LWT 2-Level	LWT–DWT
S & P Attack	0.9920	0.9925	0.9935
Gaussian Attack	0.9605	0.9617	0.9673
Scaling Attack	0.9980	0.9985	1.00
Rotation	0.9905	0.9912	0.9956
Cropping	0.9895	0.9908	0.9937
Mean Filtering	0.9669	0.9684	0.9797

Fig. 5 Propounded Watermark Embedding Design using LWT–DWT–LBP

Step 3 For the approximation coefficients (CA), 1–Level DWT is applied by producing low (LL), diagonal (LH, HL) and high (HH) resolution coefficients.

Step 4 Low-resolution approximation (LL) is considered for embedding fingerprint watermark using the mean of the LBP features of host medical image

Step 5 Embedding of the fingerprint watermark is done using the embedding and scaling factor as represented in Algorithm 1 and is also shown below where α and β are scaling and embedding factor values.

$$\widehat{HMI} = \alpha \times LL + \beta \times FPW \tag{8}$$

Step 6 Inverse DWT is applied by combining watermarked LL subband with remaining subbands.

Step 7 Inverse LWT is applied by combining watermarked CA with remaining coefficients to form Imperceptible Watermarked Medical Image.

Step 8 Further, to improve security, Arnold transform is applied to the watermarked medical image with a secret key in generating the scrambled watermarked medical image.

The function of Arnold transform is to scramble the image so that the intruders cannot know the image. The reason for adding at the end of the embedding is to overcome tampering of medical images. To add extra security to the host medical image Arnold Transform is applied at the end of the process.

4.2 Propounded watermark extraction design using LWT–DWT–LBP

In this extraction scheme, adaptive patient fingerprint watermark is extracted in the hybrid transform from watermarked medical image. The propounded watermarking extraction design is represented in Fig. 6.

Algorithm 2 Propounded Watermark Extraction Algorithm

---
fpw^E =Medical watermark_extraction ($^{A}HMI^{fpw}$, LL, α)
Input: Imperceptible watermarked Medical Image ($^{A}HMI^{fpw}$), LL of host medical image, Scaling and Embedding Factor, Secret Key
Output: Extracted finger print watermark (fpw^E)
1: Read $^{A}HMI^{fpw}$
2: HMI^{fpw} = Inverse Arnold($^{A}HMI^{fpw}$)
3: $[CA_w, CH_w, CV_w, CD_w]$ = LWT(HMI^{fpw})
4: $[LL_w, LH_w, HL_w, HH_w]$ = DWT(CA_w)
5: $fpw^E = \frac{LL_w - (\alpha \times LL)}{\beta}$

In the above propounded watermark extraction Algorithm 2, $^{A}HMI^{fpw}$ represents scrambled watermarked host medical image, LL represents the decomposition of the watermark with LWT followed by DWT subband, and $\alpha \& \beta$ represents the embedding and scaling factor. The steps of extraction of fingerprint watermark from imperceptible watermarked medical image are given below.

Step 1 Scan the scrambled watermarked host medical image($^{A}HMI^{fpw}$)

Step 2 Apply inverse Arnold transform with secret key (Key-3) to descramble the medical image in generating watermarked host medical image.

Step 3 Applying LWT for 1–Level to watermarked host medical image produces watermarked approximation coefficients (CA_w) and watermarked details coefficients ((CH_w, CV_w, CD_w))

Step 4 For the watermarked approximation coefficients (CA_w), 1–Level DWT is applied by producing watermarked low (LL_w), diagonal (LH_w, HL_w) and watermarked high (HH_w) resolution coefficients.

Step 5 Watermarked low-resolution approximation (LL_w) is considered for extracting fingerprint watermark by using the same keys (Key-1 & Key-2) that are used in embedding the watermark represented in Algorithm 2.
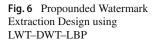
5 Experimental results

The propounded medical image watermarked scheme is evaluated and scrutinized by numerous medical images like X-Ray, CT, US and MRI. For the easy analysis, the image names are considered as alphabets. The medical images of size 512×512 pixels and the fingerprint images of size 128×128 pixels are considered and shown in Figs. 7 and 8. "Matlab" is utilized in executing the propounded schemes. The sample twelve medical images are taken from Fontaine medical records [22] dataset. The fingerprints are taken from Kaggle dataset [13]. Effectiveness of the propounded watermarking scheme is thoroughly estimated by applying attacks against it. Peak-signal-to-noise-ratio (PSNR) and structural similarity index (SSIM) are the measures utilized for estimating perceptual characteristics [43]. PSNR is utilized in calculating the visual similarity between the host image and the watermarked image [34]. After embedding the watermark, both the host image and watermarked image should look a like with minor distinction between them [12].
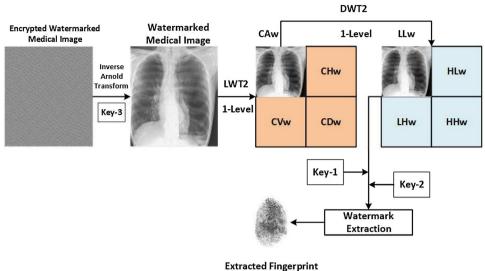
$$MSE = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(HMI_{i,j} - (HMI^{fpw})_{i,j} \right)^2}{mn} \tag{9}$$

$$PSNR = 20 \log_{10} \left(\frac{MAX_{HMI}}{\sqrt{MSE}} \right) \tag{10}$$

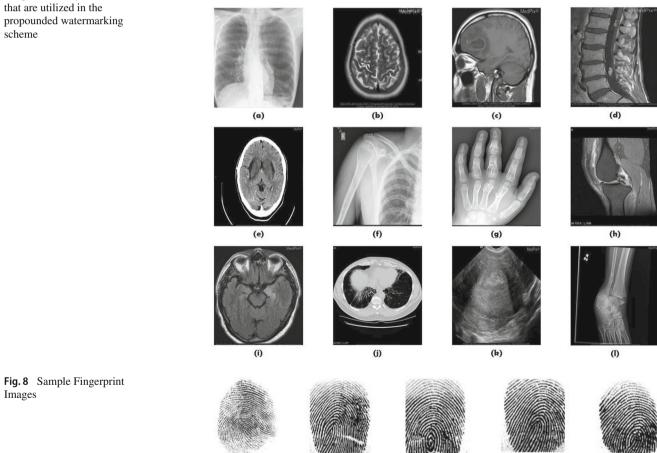where MAX_{HMI} is maximum gray scale value of the image.

SSIM is a measure utilized to evaluate structural similarity between the host image and the watermarked image [37,48]. SSIM includes luminance, contrast and structural functions used for comparing. SSIM value should be near to unity.

Fig. 6 Propounded Watermark Extraction Design using LWT–DWT–LBP

Fig. 7 Sample Host Medical images of X-Ray, CT, US, MRI that are utilized in the propounded watermarking scheme

Fig. 8 Sample Fingerprint Images
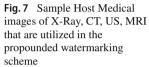
SSIM is mathematically shown as:

$$SSIM(HMI, HMI^{fpw}) = l, c, s\{((HMI, HMI^{fpw}))\} \tag{11}$$

Normalized Correlation coefficient (NCC) aids in estimating the robustness of the propounded method with attacks [46]. NCC computes the similarity between the patient fingerprint and extracted patient fingerprint. The values nearer to one mean the propounded method is sustain the image and signal processing attacks [4,19].

$$NCC = \frac{\sum \sum fpw \times fpw^E}{(\sqrt{\sum fpw^2})(\sqrt{\sum (fpw^E)^2})} \tag{12}$$

Number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI) are the evaluating measures that are utilized for calculating the credibility of the propounded scheme against different attacks [45]. NCPR calculates the number of changing pixel rate, and UACI calculates the difference of average change in the intensities between the watermarked image and encrypted watermarked image [28] Table 2.

$$NCPR = \frac{\sum_{i,j} D\{i, j\}}{M \times M} \tag{13}$$

where $M \times M$ is the size of the image and $D\{i, j\}$ denotes

$$D\{i, j\} = \begin{cases} 0 & (HMI^{fpw}) = (^A HMI^{fpw}) \\ 1 & (HMI^{fpw}) \neq (^A HMI^{fpw}) \end{cases} \tag{14}$$

$$UACI = \frac{1}{M \times M} \left[\sum_{i,j} \frac{(HMI^{fpw}) - (^A HMI^{fpw})}{255} \right] \times 100 \tag{15}$$

The imperceptibility test and robustness testing with the metrics on the twelve medical images with no attacks are shown in Table 3. These measures attained values nearer to one which claims for good structural similarity between the host image and watermarked image. Visible similarity for the propounded scheme is measured with PSNR values which are above 30 dB which means the quality of the watermarked image is good. The SSIM is a metric used to quantify perceptual quality of an image during the communication channel. The SSIM values are calculated between original medical image and watermarked image. The SSIM values for all the images are above 0.98, which means the proposed algorithm has provides good image quality after watermark embedding. The closer the SSIM values to 1 means the quality of the watermarked image is high. From the results table, it is

Table 2 Adaptively calculated embedding factor values for medical images

Images	Embedding factor	Images	Embedding factor	Images	Embedding factor
a	0.2526	e	0.0905	i	0.2931
b	0.1353	f	0.2322	j	0.1289
c	0.2247	g	0.2743	k	0.2360
d	0.2434	h	0.2004	l	0.0898

Table 3 Propounded scheme performance analysis with help of measure values

Images	PSNR(dB)	SSIM	NCPR	UACI	NCC
a	36.00	0.9884	0.9995	0.2321	1.00
b	34.12	0.9863	0.9512	0.2977	1.00
c	37.07	0.9815	0.9948	0.2192	1.00
d	36.09	0.9865	0.9978	0.2761	1.00
e	34.81	0.9806	0.9638	0.2884	1.00
f	36.56	0.9821	0.9989	0.2744	1.00
g	35.43	0.9857	0.9988	0.2837	1.00
h	37.80	0.9665	0.9814	0.2847	1.00
i	34.52	0.9868	0.9971	0.2754	1.00
j	33.85	0.9844	0.9674	0.3333	1.00
k	36.47	0.9878	0.9782	0.2798	1.00
l	34.61	0.9738	0.9723	0.2788	1.00

clear that for all the medical images the quality of the image is good. The similarity between the patient fingerprint and the extracted fingerprint is measured with NCC. The closer the value of NCC to one symbolizes for resilience of the propounded method against attacks. NPCR and UACI have the ability to assess potentiality of the propounded scheme against various attacks. The NPCR and UACI measure values are above their limiting values.

The embedding factor values are calculated adaptively by utilizing the LBP features of the host medical image. The adaptively calculated values for the sample twelve medical images are given in Table 2.

The watermarked images with fingerprint watermark, scrambled and unscrambled watermarked images with Arnold and Inverse Arnold transform, Extracted fingerprint watermarks are shown in Fig. 9. Robustness analysis of the propounded watermarking scheme under attacks of Salt & Pepper Noise (0.001), Gaussian Noise (0.01, 0.002), Sharpening, Scaling (2, 0.5), and JPEG Compression is shown in Table 4. From this table, the extracted fingerprint watermark is of good quality which can be viewed from third column and NCC values nearer to 1 tell the fingerprint is extracted successfully.

Fig. 9 Sample watermarked images after embedding with patient fingerprint watermark, Scrambled watermarked Images, Descrambled Images, Extracted Fingerprint Watermarks

The NCC values for all the sample images (a to l) with Salt & Pepper, Gaussian Noise, Speckle Noise, Scaling, JPEG Compression, Mean Filtering, Median Filtering, Rotation and Cropping attacks are provided, respectively.

In case of **Salt** & **Pepper noise** attack, medical images are distorted by adding salt & pepper noise with density 0.001 and 0.002. The NCC values of the extracted watermark drop from 0.99 to 0.96 on an average when the noise density increases. In **Gaussian noise**, medical images are distorted in the similar way with mean and variance (0, 0.002) and (0.01, 0.002). The NCC values of extracted fingerprints drop

upto 0.95 on average. In Speckle noise with density 0.0001, the extracted fingerprint has a high NCC with 0.98.

The medical images are **re-sized** at various scales: up-sampled twice and down-sampled half the size of the medical image. Even in varying the scaling of the image, the proposed method NCC values achieved high with 0.99.

In case of **Mean and Median Filtering** attacks, the mask of size 3×3 is applied. The extracted fingerprint watermark NCC values have achieved 0.97 for mean filtering and 0.98 for median filtering on an average.

Table 4 Robustness analysis of the propounded watermarking scheme under attacks

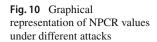| Attacks	Attacked Watermarked Images	Extracted Fingerprints	NCC Values
Salt & Pepper Noise(0.001)			0.9938
Gaussian Noise (0.01,0.002)			0.9923
Sharpening			0.9975
Scaling (2,0.5)			0.9985
JPEG Compression (80)			0.9999

In case of **rotation** attack, the medical images are rotated with 2 degrees in clock wise direction. The extracted fingerprint watermark has a high NCC with 0.97 on an average.

In case of **cropping**, 10 percent of the medical image is cropped. The extracted fingerprint has NCC with 0.98 on an average.

NCPR and UACI measure values under five attacks for sample images (a, b, c, d, e) are graphically represented in

Figs. 10 and 11. The attacks are "Salt & Pepper noise (0.001), Salt & Pepper noise (0.002), Gaussian noise (0, 0.0002), Gaussian noise (0.01, 0.0002) and Speckle noise(0.001)" indicated as Atk 1 to Atk 5. It can be observed that NPCR and UACI values under different attacks are satisfactory and are under acceptable range Table 5.

Potency of the propounded method can be seen in Table 6 where it is compared with the other medical watermarking

Table 5 Robustness evaluation using NCC under various attacks

Attacks	Metric value	NCC values											
		a	b	c	d	e	f	g	h	i	j	k	l
Salt & Pepper Noise	0.001	0.9935	0.9821	0.9914	0.9958	0.9392	0.9950	0.9888	0.9920	0.9969	0.9792	0.9941	0.9664
	0.002	0.9890	0.9707	0.9852	0.9918	0.9116	0.9912	0.9849	0.9871	0.9941	0.9628	0.9899	0.9386
Gaussian noise	(0,0.002)	0.9673	0.9453	0.9613	0.9754	0.8529	0.9708	0.9626	0.9682	0.9823	0.9361	0.9745	0.9137
	(0.01,0.002)	0.9725	0.9612	0.9696	0.9809	0.8971	0.9771	0.9680	0.9749	0.9856	0.9548	0.9795	0.9410
Speckle Noise	0.0001	0.9964	0.9988	0.9952	0.9994	0.9611	0.9987	0.9899	0.9995	0.9996	0.9974	0.9996	0.9977
Scaling	(2,0.5)	0.9999	0.9988	0.9997	0.9997	0.9978	0.9998	0.9998	0.9996	0.9998	0.9985	0.9996	0.9987
JPEG compression	90	0.9997	0.9942	0.9990	0.9992	0.9908	0.9996	0.9997	0.9987	0.9996	0.9943	0.9991	0.9961
Mean filtering	3 × 3	0.9797	0.9675	0.9882	0.9896	0.8571	0.9833	0.9925	0.9891	0.9925	0.9314	0.9890	0.9508
Median filtering	3 × 3	0.9977	0.9012	0.9831	0.9892	0.8942	0.9969	0.9962	0.9778	0.9934	0.9370	0.9875	0.9514
Rotation	2 degrees	0.9956	0.9936	0.9928	0.9934	0.9958	0.9914	0.9923	0.9933	0.9941	0.9937	0.9929	0.9916
Cropping	10 %	0.9937	0.9925	0.9778	0.8901	0.9925	0.9003	0.8713	0.9727	0.9759	0.9604	0.9914	0.8197
Scaling + JPEG Compression	(0.75, 90)	0.9912	0.9904	0.9715	0.8910	0.9909	0.8998	0.8705	0.9713	0.9741	0.9600	0.9908	0.8188
Scaling + Rotation	(0.75, 2 degrees)	0.9865	0.9898	0.9815	0.9010	0.9915	0.9006	0.8815	0.9801	0.9816	0.9649	0.9913	0.8288

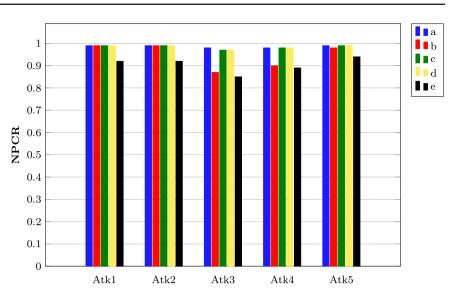**Fig. 10** Graphical representation of NPCR values under different attacks

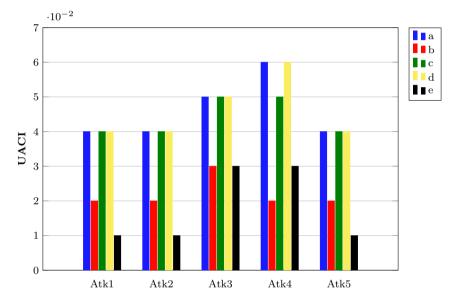**Fig. 11** Graphical representation of UACI values under different attacks

Table 6 Robustness comparison between propounded method and other watermarking prevailing methods

Methods/attacks	[38]	[36]	[34]	[33]	[31]	[24]	[17]	[16]	Proposed
S & P (0.001)	–	–	–	0.9843	0.9938	0.9657	0.9969	0.9987	0.9969
Gaussian Noise (0,0.001)	–	0.9965	–	0.9365	0.9591	0.9342	0.9874	0.9903	0.9941
Median Filt [2 2]	0.6923	0.9949	0.9939	0.9752	0.9379	1	–	0.9981	0.9987
JPEG Comp (90)	0.9896	0.9951	0.9935	0.9785	0.9988	1	–	0.9993	0.9997
Scaling [2 0.5]	–	–	–	0.7375	–	0.9957	–	0.9992	0.9999
Mean Filt[2 2]	–	–	0.9951	–	–	1	–	0.9968	0.9983

methods like [16,17,24,31,33,34,36,38]. From the comparison results, it is clear that the propounded method has competed with the remaining techniques in terms of robustness. In Table 7, the imperceptibility of the watermarking schemes are compared with the proposed scheme, from all the methods the proposed method imperceptibility is high except for [16] method and in comparison with [24] proposed method results are better for noise attacks, and for all the remaining attacks they are almost similar. Graphical comparison (Same attacks of Table 6) of propounded method
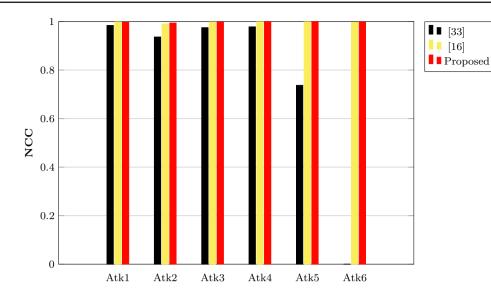
Fig. 12 Graphical comparison of proposed method

Table 7 Imperceptibility comparison between propounded method and other watermarking prevailing methods

Methods	PSNR values
[38]	35.52
[36]	33.21
[34]	34.64
[33]	32.48
[31]	34.64
[24]	45.42
[17]	34.68
[16]	55.85
Proposed	36.00

with [16,33] is shown in Fig. 12. From the figure, it is clear that the robustness of the propounded method is far above than the other methods under similar attacks.

6 Conclusion and future work

The propounded scheme in this paper provides a novel method of medical image watermarking scheme in hybrid domain in which salient features of LWT, DWT and LBP are considered. LBP values are used to calculate the embedding factor values adaptively which acts as keys. Embedding fingerprint watermark of the patient in speculating component safeguards better robustness and imperceptibility of the watermark in resisting image and signal processing attacks. A triple layer security is provided to the scheme with Arnold transform which protects the medical image from modifications and tampering. The performance of the propounded scheme is better compared to other watermarking schemes in terms of metric evaluation. This paper provides an adaptive medical image watermarking scheme using hybrid transform

and fingerprint of patient as watermark for e-health care systems.

References

1. Albahri, O.S., Zaidan, A.A., Albahri, A.S., Zaidan, B.B., Abdulkareem, K.H., Al-Qaysi, Z.T., Alamoodi, A.H., Aleesa, A.M., Chyad, M.A., Alesa, R.M., et al.: Systematic review of artificial intelligence techniques in the detection and classification of covid-19 medical images in terms of evaluation and benchmarking: taxonomy analysis, challenges, future solutions and methodological aspects. J. Infect. Public Health **13**, 1381 (2020)
2. Alshanbari, H.S.: Medical image watermarking for ownership & tamper detection. Multimed. Tools Appl. **80**, 1–16 (2020)
3. Anand, A., Singh, A.K.: An improved DWT–SVD domain watermarking for medical information security. Comput. Commun. **152**, 72–80 (2020)
4. Aparna, P., Kishore, P.V.V.: Biometric-based efficient medical image watermarking in e-healthcare application. IET Image Process. **13**(3), 421–428 (2019)
5. Cedillo-Hernandez, M., Cedillo-Hernandez, A., Nakano-Miyatake, M., Perez-Meana, H.: Improving the management of medical imaging by using robust and secure dual watermarking. Biomed. Signal Process. Control **56**, 101695 (2020)
6. Daubechies, I., Sweldens, W.: Factoring wavelet transforms into lifting steps. J. Fourier Anal. Appl. **4**(3), 247–269 (1998)
7. Fares, K., Khaldi, A., Redouane, K., Salah, E.: DCT & DWT based watermarking scheme for medical information security. Biomed. Signal Process. Control **66**, 102403 (2021)
8. Hosny, K.M., Darwish, M.M.: Invariant image watermarking using accurate polar harmonic transforms. Comput. Electr. Eng. **62**, 429–447 (2017)
9. Hosny, K.M., Darwish, M.M.: Robust color image watermarking using invariant quaternion Legendre–Fourier moments. Multimed. Tools Appl. **77**(19), 24727–24750 (2018)
10. Hosny, K.M., Darwish, M.M.: New geometrically invariant multiple zero-watermarking algorithm for color medical images. Biomed. Signal Process. Control **70**, 103007 (2021)
11. Hosny, K.M., Darwish, M.M., Li, K., Salah, A.: Parallel multi-core CPU and GPU for fast and robust medical image watermarking. IEEE Access **6**, 77212–77225 (2018)

12. Huang, Y., Niu, B., Guan, H., Zhang, S.: Enhancing image watermarking with adaptive embedding parameter and PSNR guarantee. IEEE Trans. Multimed. **21**(10), 2447–2460 (2019)
13. JinZhuXing. Fingerprint database. February 2020. https://www.kaggle.com/peace1019/fingerprint-dataset-for-fvc2000-db4-b
14. Kahlessenane, F., Khaldi, A., Kafi, R., Euschi, S.: A DWT based watermarking approach for medical image protection. J. Ambient Intell. Humaniz. Comput. **12**(2), 2931–2938 (2021)
15. Kannammal, A., Subha Rani, S.: Two level security for medical images using watermarking/encryption algorithms. Int. J. Imaging Syst. Technol. **24**(1), 111–120 (2014)
16. Khare, P., Srivastava, V.K.: A secured and robust medical image watermarking approach for protecting integrity of medical images. Trans. Emerg. Telecommun. Technol. **32**(2), e3918 (2021)
17. Kumar, C., Singh, A.K., Kumar, P.: Improved wavelet-based image watermarking through SPIHT. Multimed. Tools Appl. **79**(15), 11069–11082 (2020)
18. Lei, B., Soon, Y., Zhou, F., Li, Z., Lei, H.: A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. Signal Process. **92**(9), 1985–2001 (2012)
19. Li, B.-J., Wang, Q.-B., Duan, D.-P., Chen, J.-A.: Using grey intensity adjustment strategy to enhance the measurement accuracy of digital image correlation considering the effect of intensity saturation. Opt. Lasers Eng. **104**, 173–180 (2018)
20. Liao, S., Zhu, X., Lei, Z., Zhang, L., Li, S.Z.: Learning multi-scale block local binary patterns for face recognition. In: International Conference on Biometrics, pp. 828–837. Springer (2007)
21. Loukhaoukha, K., Chouinard, J.Y.: Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification. In: 2009 11th Canadian Workshop on Information Theory, pp. 177–182. IEEE (2009)
22. Makhanov, S.: Medical record database. February (2020). https://www.onlinemedicalimages.com/index.php
23. Mata-Mendoza, D., Cedillo-Hernandez, M., Garcia-Ugalde, F., Cedillo-Hernandez, A., Nakano-Miyatake, M., Perez-Meana, H.: Secured telemedicine of medical imaging based on dual robust watermarking. Vis. Comput., 1–18 (2021). https://link.springer.com/article/10.1007/s00371-021-02267-3
24. Mehta, R., Rajpal, N., Vishwakarma, V.P.: A robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform. Int. J. Mach. Learn. Cybern. **82**, 379–395 (2017)
25. Memon, N.A., Chaudhry, A., Ahmad, M., Keerio, Z.A.: Hybrid watermarking of medical images for ROI authentication and recovery. Int. J. Comput. Math. **88**(10), 2057–2071 (2011)
26. Ojala, T., Pietikainen, M., Harwood, D.: Performance evaluation of texture measures with classification based on kullback discrimination of distributions. In: Proceedings of 12th International Conference on Pattern Recognition, vol. 1, pp. 582–585. IEEE (1994)
27. Ojala, T., Pietikäinen, M., Harwood, D.: A comparative study of texture measures with classification based on featured distributions. Pattern Recognit. **29**(1), 51–59 (1996)
28. Mohamed Parvees, M.Y., Samath, J.A., Parameswaran Bose, B.: Secured medical images—a chaotic pixel scrambling approach. J. Med. Syst. **40**(11), 1–11 (2016)
29. Sanivarapu, P.V., Rajesh, K.N., Reddy, N.R., Reddy, N.C.: Patient data hiding into ECG signal using watermarking in transform domain. Phys. Eng. Sci. Med. **43**(1), 213–226 (2020)
30. Sharma, S., Zou, J.J., Fang, G.: Significant difference-based watermarking in multitoned images. Electron. Lett. **56**(18), 923–926 (2020)
31. Singh, A.K.: Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed. Tools Appl. **76**(6), 8881–8900 (2017)
32. Singh, A.K., Dave, M., Mohan, A.: Multilevel encrypted text watermarking on medical images using spread-spectrum in DWT domain. Wirel. Pers. Commun. **83**(3), 2133–2150 (2015)
33. Singh, A.K., Dave, M., Mohan, A.: Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed. Tools Appl. **75**(14), 8381–8401 (2016)
34. Singh, A.K., Kumar, B., Dave, M., Mohan, A.: Multiple watermarking on medical images using selective discrete wavelet transform coefficients. J. Med. Imaging Health Inform. **5**(3), 607–614 (2015)
35. Singh, A.K., Kumar, B., Dave, M., Mohan, A.: Robust and imperceptible dual watermarking for telemedicine applications. Wirel. Pers. Commun. **80**(4), 1415–1433 (2015)
36. Singh, S., Rathore, V.S., Singh, R., Singh, M.K.: Hybrid semi-blind image watermarking in redundant wavelet domain. Multimed. Tools Appl. **76**(18), 19113–19137 (2017)
37. Starovoytov, V.V., Eldarova, E.E., Takuadinovich Iskakov., K.: Comparative analysis of the SSIM index and the pearson coefficient as a criterion for image similarity. Eurasian J. Math. Comput. Appl. **8**(1), 76–90 (2020)
38. Sriti, T., Singh, A.K., Ghrera, S.P., Elhoseny, M.: Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed. Tools Appl. **78**(3), 3457–3470 (2019)
39. Vaidya, P., Chandra Mouli, P.V.S.S.R.: A robust semi-blind watermarking for color images based on multiple decompositions. Multimedi. Tools Appl. **76**(24), 25623–25656 (2017)
40. Vaidya, S.P.: Multiple decompositions-based blind watermarking scheme for color images. In: International Conference on Recent Trends in Image Processing and Pattern Recognition, pp. 132–143. Springer (2018)
41. Vaidya, S.P., Chandra Mouli, P.V.S.S.R.: Adaptive digital watermarking for copyright protection of digital images in wavelet domain. Procedia Comput. Sci. **58**, 233–240 (2015)
42. Verma, V.S., Jha, R.K., Ojha, A.: Significant region based robust watermarking scheme in lifting wavelet transform domain. Expert Syst. Appl. **42**(21), 8184–8197 (2015)
43. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. **13**(4), 600–612 (2004)
44. Wu, L., Zhang, J., Deng, W., He, D.: Arnold transformation algorithm and anti-Arnold transformation algorithm. In: 2009 First International Conference on Information Science and Engineering, pp. 1164–1167. IEEE (2009)
45. Yue, W., Noonan, J.P., Againa, S., et al.: NPCR and UACI randomness tests for image encryption. Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. **1**(2), 31–38 (2011)
46. Yoo, J.-C., Ahn, C.W.: Image matching using peak signal-to-noise ratio-based occlusion detection. IET Image Process. **6**(5), 483–495 (2012)
47. Yuan, Z., Qingtang, S., Liu, D., Zhang, X., Yao, T.: Fast and robust image watermarking method in the spatial domain. IET Image Process. **14**(15), 3829–3838 (2020)
48. Zhou, M., Wei, X., Wang, S., Kwong, S., Fong, C.K., Wong, P.H., Yuen, W.Y., Gao, W.: SSIM-based global optimization for CTU-level rate control in HEVC. IEEE Trans. Multimed. **21**(8), 1921–1933 (2019)

Dr. S. Prasanth Vaidya is currently working as Associate Professor in Department of Computer Science and Engineering, Aditya Engineering College (A), Surampalem, Andhra Pradesh, India. He received his Ph.D., in Computer Science and Engineering (Digital Watermarking), from Vellore Institute of Technology, Vellore. He received B.Tech degree in Computer Science and Engineering from Acharya Nagarjuna University and M.Tech degree in Information Technology from GITAM University, India. His current research interests are digital image processing, pattern recognition, computer vision, and digital watermarking. He has published 13 refereed research papers in various international journals and conferences. He is a reviewer for many international conferences and journals.