

## Chapter 2

# Medical Image Watermarking Techniques: A Technical Survey and Potential Challenges

Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan

### 2.1 Introduction

Recent advancements in high-bandwidth digital communication technologies has opened up newer opportunities of transmitting medical data across geographical boundaries through Internet, mobile networks, and other wireless/wired communication channels and thus covering rural/remote areas, accident sites, ambulance, and hospitals [1]. The transmission of medical data over an open communication channel poses different possibilities of threat that severely affect its authenticity, integrity, and confidentiality which demands for implementing some kind of medical watermarking scheme to avoid prompting attention and preventing access by an unintended recipient. The medical image watermarking provides a convenient platform to address these issues [2–6]. Despite the broad literature on various application fields, a very few work has been implemented towards the exploitation of health-oriented perspectives of watermarking [3, 5, 7–9]. The watermarking techniques in the area of

---

A.K. Singh (✉)

Department of Computer Science & Engineering, Jaypee University of Information Technology, Wanknaghat, Solan, India  
e-mail: [amit\\_245singh@yahoo.com](mailto:amit_245singh@yahoo.com)

B. Kumar

Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad, India  
e-mail: [singhbasant@yahoo.com](mailto:singhbasant@yahoo.com)

G. Singh

Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Wanknaghat, Solan, India  
e-mail: [drghanshyam.singh@yahoo.com](mailto:drghanshyam.singh@yahoo.com)

A. Mohan

Department of Electronics Engineering, Indian Institute of Technology (BHU), Varanasi, India  
e-mail: [profanandmohan@gmail.com](mailto:profanandmohan@gmail.com)

telemedicine require extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. The confidentiality, reliability and availability are important security requirements with electronic patient record (EPR) data exchange through unsecured channels [1, 5, 10].

The subsequent section of the chapter is structured as follows: Section 2.2 presents a brief literature review of current state-of-the-art medical as well as digital image watermarking techniques. Section 2.3 presents the potential challenges and fruitful discussion in the medical image watermarking techniques. Section 2.4 provides summary of the chapter.

## 2.2 Review of Available Watermarking Techniques

In this section, the authors are presenting a detailed literature review on the current state-of-the-art medical as well as digital image watermarking techniques using error correcting codes (ECC) [1, 2, 9, 11, 12], multiple watermarking methods [8, 13–15], hybrid techniques [16–44], watermarking using machine learning techniques [45–70], biometric watermarking [71, 72], watermarking with compression techniques [73–79] and some other perspectives of the watermarking [80–103]. Further, the techniques have been carried out to explore the limitations of existing techniques with special reference to their suitability in medical image watermarking. Some novel/improved state-of-the-art techniques are discussed below:

### 2.2.1 Watermarking Techniques Using Error Correcting Codes

In order to that Singh et al. [1, 12], Mostafa et al. [2], Giakoumaki et al. [9] and Terzija et al. [11] have proposed state-of-the-art technique to embed an encoded watermark with the help of error correcting codes (ECC) to improve the robustness of watermark. The ECC based watermarking methods attempt to find a trade-off between the number of bits to be embedded and the number of bit-errors that can be corrected. Singh et al. [1] proposed a medical image watermarking technique in which the technique embeds medical text watermarks into selected sub-band of discrete wavelet transform (DWT) cover medical image coefficients using spread-spectrum technique. In the embedding process, the cover image is decomposed up to third level DWT coefficients. Three different text watermarks are embedded into the selected horizontal and vertical sub-band DWT coefficients of the first, second and third level, respectively. The selection of these coefficients for embedding purpose is based on threshold criteria. Robustness of the proposed watermarking scheme is further enhanced by applying error correcting code to the ASCII representation of the text watermark and the encoded text watermark is finally embedded into the cover medical image. It is observed that the proposed scheme correctly extracts the embedded watermarks without error and provides high degree

robustness against numerous known attacks while maintaining the imperceptibility of watermarked image. Mostafa et al. [2] have proposed a watermarking method for telemedicine applications, which provides a way to secure EPR information in order to reduce the storage space and transmission cost. In this method, the EPR information is embedded after the second level of decomposition of the cover image using discrete wavelet packet transform (DWPT). Here, the EPR information is initially coded using Bose, Ray-Chaudhuri, Hocquenghem (BCH) code and then embedded to improve the robustness. However, this method has the disadvantage of higher decoding time of BCH codes. Giakoumaki et al. [9] proposed a wavelet based multiple watermarking scheme for medical image. According to characteristic and requirements, different watermarks such as signature, index, caption and reference are assigned at different decomposition level and sub-bands of DWT coefficients of medical image and BCH error correcting codes are used to improve the robustness of the watermark.

Terzija et al. [11] proposed a method for improving efficiency and robustness performance of the watermarks by using three different error correction codes, namely, (15,7)-BCH, (7,4)-Hamming Code and (15-7)-Reed-Solomon code are investigated. These codes are applied to the ASCII representation of the text which is used as watermark. The watermark is embedded into the original cover image by first decomposing the cover up to second level using discrete DWT with the pyramidal structure and then the watermark is added to the largest DWT coefficients that represent high- and middle-frequencies of the cover image. It is shown that Reed-Solomon code performs better due to its excellent ability to correct errors, however, the ECCs considered are not able to deal with bit error rates (BER) greater than 10–20%. Singh et al. [12] also presents an ECCs based watermarking method in DWT-SVD domain using four different error correcting codes such as Hamming, the BCH, the Reed–Solomon and hybrid error correcting (BCH and repetition code) codes for encoding of text watermark in order to achieve additional robustness for sensitive text watermark. The performance of proposed algorithm is evaluated against various signal processing attacks by varying the strength of watermarking and covers image modalities. The experimental results demonstrate that this algorithm provides better robustness without affecting the quality of watermarked image. Among the four error correcting codes tested, it has been observed that the hybrid code achieves better results in terms of robustness.

### 2.2.2 Multiple Watermarking Techniques

For the ownership identity authentication purpose, multiple watermarking methods have been proposed by Giakoumaki et al. [8], Navas et al. [13], Kannammal et al. [14], Singh et al. [15] to achieve higher security than single watermarks. Giakoumaki et al. [8] described wavelet-based multiple watermarking scheme that addresses the problems of medical confidentiality protection. This method uses third level decomposition of the cover image using DWT to embed the watermarks into selected

detailed coefficient of cover image. To extract multiple watermark bits, a quantization function is applied to each of the marked coefficients. The advantages of this method are its robustness, reliability, efficiency, reduced distortion and resistance to attacks. However, it involves higher computational complexity. Navas et al. [13] have proposed a blind method for telemedicine applications based on integer wavelet transform (IWT) which groups the wavelet coefficients of the cover image into different wavelet blocks based on human visual system (HVS). The EPR data is first encrypted and then embedded into the non-Region of Interest (NROI) part of the cover medical image. Region of Interest (ROI) part containing the important medical information for diagnosis is stored without any noise. The proposed method can embed and recover at most '3400' characters without any noise that is important for EPR information hiding but the computational cost of this method is high.

Kannammal et al. [14] proposed a digital watermarking method where ECG and patients' demographic text act as two level watermarks. During embedding, DWT is applied on the original image and the image is decomposed into three sub-bands. Next, the texture matrix for each sub-band is calculated. The wavelet coefficients are selected for watermarking using threshold values. The method can be used for providing authentication, confidentiality and integrity of the medical information. Singh et al. [15] proposed a wavelet based spread-spectrum multiple watermarking scheme considering medical watermarks in the form of both text and image. The experimental results are obtained by varying the watermark size and gain factor. The performance of developed scheme has been evaluated against various attacks. The robustness of text watermark has been enhanced by using BCH code.

### 2.2.3 Hybrid Watermarking Techniques

Further, some noted researchers are using *hybrid watermarking* techniques to enhance the performance of watermarking systems [16–44]. Lou and Sung [16] described two transform methods (DCT and DWT) to embed a random watermark into an image. After the third level decomposition of the cover image by DWT, DCT is applied to the selected sub-bands (HL3 and LH3). These DCT coefficients are recorded in zig-zag order. A watermark of zero means and variance of one is embedded into these sub-bands. The original image is not required for watermark extraction process. The experimental results show that the proposed method keeps the image quality good and robust against known attacks. Ouhsein et al. [17] have proposed a watermarking method using multiple parameters discrete fractional Fourier (MPDFRF) and DWT. In this embedding process, the cover image is decomposed into four wavelet sub-bands using DWT. After each sub-band is segmented into blocks, the MPDFRF transform is applied to each block. The watermark image is then embedded into the blocks. The experimental results show the good visual imperceptibility and robustness against known attacks. Jiansheng et al. [18] have proposed an algorithm for digital image watermarking based on DWT and DCT. This method of embedding uses decomposition of the host image into multilevel

( $n = 3$ ) wavelet transform and the DCT coefficients of the watermark is embedded in the high frequency band of DWT coefficients. In this method, the high frequency coefficients are plotted into  $2 \times 2$  image sub blocks, and entropy and square values of each image sub-block is calculated. The experimental result shows that the method is robust against known signal processing attacks.

Hadi et al. [19] proposed a method based on two transform methods, Fresnel and DWT. Before embedding the watermark, the cover image is transformed first by Fresnel transform to generate the encrypted cover image. After the second decomposition of cover image using DWT, the encrypted copyright information is embedded into the decomposed cover image. The method uses chaotic sequence as key to encrypt the copyright information. The chaotic sequence is very sensitive to any change in its value, so that the eavesdropper has to obtain exactly its value which is difficult and time consuming. However, encrypting the copyright information before watermarking has become unavoidable, but the delay encountered during embedding and extraction of the watermark is also an important factor in telemedicine applications. Cao et al. [20] proposed an adaptive blind watermarking method based on DWT and Fresnel diffraction transform. Initially, the cover image is decomposed (up to third level) by DWT, the binary kinoform of the watermark image is embedded. The experimental results have shown that the watermark image via Fresnel diffraction transforms has good concealment performance. The kinoform is more secure than simple permutation. However, the proposed method is suitable for binary digital watermark only. Lai and Tsai [21] proposed a hybrid image-watermarking scheme based on DWT and SVD. The method applied SVD on the selected sub-band of the DWT cover image and the singular values of the selected sub-bands of the cover image are modified with half of the watermark image. The watermark extraction is just reversing the embedding process. With SVD, small modification of singular values does not affect the visual recognition of the cover image, which improves the robustness and transparency of the method. However, both the computational cost and storage space requirements in this method are high. Nakhaie and Shokouhi [22] have proposed a no-reference objective quality measurement method based on spread-spectrum technique and DWT using ROI processing. In this embedding process, the original image is first divided into two separate parts, ROI and NROI, and DWT and DCT are applied on ROI and NROI parts, respectively. The binary watermark is embedded into DCT transform of NROI part of the cover image.

Ahire and Kshirsagar [23] proposed a blind watermarking algorithm based on DCT-DWT that embeds a binary image into the gray image. After the third level decomposition by DWT, the selected sub-bands are divided into block of  $4 \times 4$ . The DCT is applied on each block. For embedding binary watermark information corresponding pseudorandom sequences are added in the middle frequency coefficients of the DCT block. The watermark extraction process is same as the embedding process but in reverse order. Its advantages are that the proposed algorithm takes the full advantages of the multi resolution and energy compression of DWT and DCT respectively. The experimental results show that the imperceptibility of the watermarked image is acceptable and the method is robust for common signal

processing attacks. *The proposed method can be also applied on color images. However, the authors have not considered watermark security problems such as reshaping or visual cryptography before embedding.* Umaamaheshvari and Thanushkodi [24] proposed a frequency domain watermarking method to check the integrity and authenticity of the medical images. In the embedding process, DCT is first applied to the original image to generate a resultant transformed matrix. A hybrid transformed image is obtained next on applying Daubechies 4 wavelet transform on the resultant transformed matrix. Now, the least significant bit (LSB) value of every two bytes of the hybrid transformed image is computed followed by the XOR operation. Furthermore, each pixel value of the binary watermark image is compared with the resultant XOR value to obtain a modified embedded transformed image which is then mapped back to its original position. The extraction process is just reversing the embedding process. The Daubechies 4 wavelet transform technique used by the authors is useful for local analysis but it has higher computational overhead.

Soliman et al. [25] proposed an adaptive watermarking scheme based on swarm intelligence. After the first level decomposition of DWT cover image, DCT is applied only on low frequency components. Now, for each block of DCT coefficient a quantization parameter is determined from HVS by using luminance and texture masks followed by particle swarm optimization (PSO) training. Hajjaji et al. [26] proposed a medical image watermarking method based on DWT and K-L transform. The K-L transform is applied only on sub-bands of the second level DWT of the cover image. A binary signature owned by the hospital center is generated by SHA-1 hash function and rest of the patient record is concatenated with this binary signature. Before embedding the patient record into the cover image, it is coded by the serial turbo code. The method achieved high robustness and good imperceptibility against signal processing attacks. Kannammal and Subha Rani [27] focused on the issue of the security for medical images and proposed an encryption based image watermarking method in frequency and spatial domain. The method uses medical image as watermark which is embedded in the selected DWT sub-band of the cover image. For the watermark embedding, the LSB method is used. After embedding process, the watermarked image is then encrypted. Based on the experimental results, RC4 encryption algorithm was found to perform better than AES and RSA algorithms in terms of encryption/decryption time. The method achieved high robustness and security against signal processing attacks. Al-Haj [28] presented a region based watermarking algorithm for medical images. The method used multiple watermarks (robust and fragile) in spatial (LSB) and frequency domain (DWT and SVD). The robust watermark is embedded in NROI part of the cover image using frequency domain technique to avoid any compromise on its diagnostic value. The fragile watermark is embedded into ROI of the cover image using the spatial domain technique. The method achieved high robustness against JPEG and salt & pepper attacks.

Priya et al. [29] proposed a medical image watermarking method based on spatial and frequency domain embedding. This method uses LSB and DWT, DCT and DFT for watermarking. After transforming the cover image, the image is read in zig-zag manner. Based on the experimental results, DWT provides better

performance in term of robustness and imperceptibility than the LSB method. Gao et al. [30] presented a hybrid method for medical image watermarking based on redundancy discrete wavelet transform (RDWT) and SVD. This uses embedding process by applying first level RDWT to the cover image which decomposes the cover image into four sub-bands. Next, SVD is applied on each sub-band. The cover image itself is used as watermark and this method offers high robustness without significant degradation of the image quality against rotation attack. In addition to this, the proposed method has the ability of rotation correction function and high embedding capacity.

Rosiyadi et al. [31] proposed another hybrid watermarking method based on DCT and SVD for the copyright protection. In this embedding process, DCT is applied on the host image using the zigzag space-filling curve (SFC) for the DCT coefficients and subsequently the SVD is applied on the DCT coefficients. Finally, the host image is modified by the left singular vectors and the singular values of the DCT coefficients to embed the watermark image. In this method, genetic algorithm (GA) based technique is used to find the optimization scaling factor of the watermark image. They have experimentally shown that the proposed method is robust against several kinds of attacks. The comparison between the method based on DCT and SVD using GA and the hybrid method based on DCT-SVD has been presented by Rosiyadi et al. in [32]. It is shown that the robustness of the extracted watermark and the visual quality of the watermarked image of the method using GA technique is better than the hybrid method. Horng et al. [33] proposed a blind watermarking method based on DCT, SVD and GA. It is shown that this method is robust and offers high imperceptibility against several known attacks. Horng et al. [34] proposed an adaptive watermarking method based on DCT, SVD and GA. In this embedding process, the host image luminance masking is used and the mask of each sub-band area is transformed into frequency domain. Subsequently, the watermark image is embedded by modifying the singular values of DCT-transformed host image with singular values of mask coefficients of host image and the control parameter of DCT-transformed watermark image using GA. It is shown that this method is robust against several known attacks. A region based robust and secure watermarking method is presented by Sharma et al. [35] for medical applications. The method initially uses DWT and DCT to embeds multiple watermark information in to the cover medical image. Further, the security of the image and text watermark information is enhanced by message-digest (MD5) hash algorithm and Rivest–Shamir–Adleman (RSA) respectively before embedding into the medical cover image. In order to enhance the robustness of the text watermark hamming error correction code is also applied on the encrypted watermark. The experimental results has been shown that the method is robust for important signal processing attacks.

Pandey et al. [36] presents a secure DWT and SVD based multiple watermarking methods for Tele-ophthalmology applications. To enhance the security of the method, secure hash algorithm (SHA-512) is used for generating hash corresponding to iris part of the cover digital eye image. The suggested technique initially divides the digital eye image into Region-of-Interest (ROI) containing iris and Non



Region-of-interest (NROI) part where the text and image watermarks are embedded into the NROI part of the DWT cover image. The performance in terms of Normalized Correlation (NC) and bit error rate (BER) of the developed scheme is evaluated and analyzed against known signal processing attacks and “Checkmark” attacks. The method is found to be robust against all the considered attacks. In [37], the authors present a watermarking method using lifting wavelet transform (LWT) and block based DCT are applied to the cover image followed by the normalizing an image. Further, the DC coefficients from all blocks are gathered and singular value matrix is constructed using SVD. The watermark image is embedded in this singular value matrix after scrambling the image, which increases the security of the proposed scheme.

Potential researchers have proposed image watermarking techniques based on combination of DWT, DCT and SVD [38–44]. Singh and Tayal [38] proposed a hybrid algorithm for image watermarking based on DWT, DCT, and SVD by first decomposing the host and the watermark image into first level DWT. This is followed by transforming both the high frequency band (HH) of the cover image and watermark image using DCT and SVD. The 'S' vector of watermark information is embedded in the 'S' component of the host image. The performance of Haar, Daubechies2, Biorthogonal1.1, and Coiflet1 filters against different signal processing attacks has been evaluated and compared. Khan et al. [39] proposed a hybrid method for image watermarking using DWT, DCT and SVD in a zig-zag order. The proposed method has been extensively tested against known attacks and has been found to give superior performance for robustness and imperceptibility compared to the existing methods based on DCT–SVD or DWT only. Srivastava and Saxena [40] proposed a semi-blind image watermarking method based on DWT, DCT and SVD. In this embedding process, the host and the watermark images are decomposed into first level DWT and then the watermark is transformed by DCT and SVD before embedding it into middle frequency band of the cover image. The method is robust against various attacks. Harish et al. [41] also developed a hybrid method based on DWT, DCT and SVD. This embedding process uses modification of the singular values of the DCT coefficients of the cover image with the singular values of the watermark image. The proposed method is shown to be robust against various attacks. Zear et al. [42] proposed a robust and secure hybrid multiple watermarking technique through discrete wavelet transforms (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) and neural network using medical images. Two different text watermark information is compressed and encoded by arithmetic and hamming error correction code respectively. The compressed and encoded text watermark is embedding into the cover image. Further, Arnold transform is applied on the image watermark before embedding into the cover. The performance of the algorithm has been extensively evaluated in terms of PSNR, NC and BER.

Singh et al. [43] have presents a secure multiple watermarking method based on DWT, DCT and SVD. For identity authentication purpose, the proposed method uses medical image as the image watermark, and the personal and medical record of the patient as the text watermark. In order to enhance the security of the text



watermark, the encryption is applied to the ASCII representation of the text watermark before embedding. The experimental results have shown that the method is robust for various signal processing and “Checkmark” attacks. In order to improve the performance of the method proposed, DWT applied on watermark image instead of DCT as proposed in [44].

### 2.2.4 Watermarking Using Machine Learning Techniques

Wavelet based image watermarking using machine learning techniques are proposed in [45–70]. Although these proposed methods offer high imperceptibility and robustness but they involve high computational complexity. Peng et al. [45] proposed a blind watermarking method based on multi-wavelet and support vector machine (SVM). In this watermarking process, first level multi-wavelet is performed on each block of image and then the watermark information is embedded into lower frequency sub-band of the cover image using modulation technique. Here, the watermark information consists of two components, a reference information and owner signature of binary logo image. The reference information is used to train SVM during watermark extraction process. Based on experimental results, it is shown that the proposed method achieves high imperceptibility and robustness over other methods [46–48]. However, the computational complexity of this method is higher.

Vafaei et al. [49] proposed a blind watermarking method based on DWT and Artificial Neural Network (ANN). In this watermarking method the third level DWT is applied on the cover image and the binary image watermark is then embedded repetitively into the selected wavelet coefficients. ANN is used to balance between the robustness of the extracted watermark and the quality of the watermarked image. The proposed method offers good imperceptibility and high robustness simultaneously to cropping, filtering and noise addition attacks. However, the time complexity of the method is very high. Sridevi and Fathima [50] proposed a watermarking method based on DWT and using GA and fuzzy inference system to find the embedding strength. In this embedding process, the cover image is decomposed by DWT and the watermark is embedded into the selected sub-band. This method is robust without much degradation of the image quality. The PSNR values of retrieved watermark are very low but the visual quality is good. However, this method is not resistant to the noise attack.

Kang et al. [51] proposed a blind wavelet based watermarking method using Principal Component Analysis (PCA) technique. Their method uses embedding an encrypted watermark image into the main component of the wavelet domain of the cover image. Before embedding the watermark, it is encrypted in order to enhance the security of the watermark information. Wang et al. [52] proposed a blind DWT based watermarking method using neural network where DWT is applied on cover image and weight factors are calculated for the wavelet coefficients and the watermark is then embedded into selected coefficients. The proposed method is tested against JPEG compression attack only (up to 70% quality factor). Tsai et al.

[53] proposed DWT based blind watermarking method using neural network and HVS characteristics wherein noticeable differences profile is employed to embed the watermark. The proposed method has better transparency performance than Joo's et al. [54] and Wang and Pearmain [55] methods.

Ni et al. [56] proposed a watermarking method based on DWT and Hidden Markov Model (HMM) by applying the fourth level DWT on cover image to build vector trees and then the watermark is embedded into designated trees. Before embedding the watermark, it is coded with repeat accumulation error-correcting code. Miyazaki [57] proposed a watermarking detection method based on DWT and Bayesian estimation. Shao et al. [58] proposed a discrete multiwavelet transform (DMWT) based blind watermarking method using SVM in which the cover image is decomposed by DMWT and the watermark is embedded into one of the selected sub-band. Before embedding the watermark, it is transformed by Arnold transformation. This method has better image quality of the watermarked image and robustness of the extracted watermark against number of signal processing attacks than method suggested by Li et al. [59]. Hsieh [60] proposed a watermarking method based on DWT and fuzzy logic based on applying third level DWT on cover image and calculating the entropy of the coefficient. The coefficients with larger entropy are selected for watermark embedding.

Surekha and Sumathi [61] proposed a watermarking method based on DWT and GA. In this embedding process, the cover image is decomposed by DWT and the watermark information is embedded into detail sub-bands of the cover. The method uses GA to optimize the watermark strength factor at every chosen sub-band. Ramanjaneyulu and Rajarajeswari [62] proposed a DWT based watermarking method using GA by applying third level DWT on cover image, selecting suitable sub-bands for watermark embedding and optimization is achieved using GA. This method achieves better imperceptibility and robustness performance than other methods [63–66]. Ramamurthy and Varadarajan [67] proposed two different DWT based image watermarking methods and compared them. The first method is based on neural network and the other method is based on fuzzy logic. They found that the first method is good for filtering attacks whereas the second method is good for cropping, jpeg, rotation and salt and pepper attack.

Dang and Kinsner [68] proposed an image watermarking method based on DWT and neural network wherein the colour image of the cover image is decomposed by DWT using HVS model and then the watermark is embedded into the selected coefficients. Imran and Ghafoor [69] proposed non-blind DWT-SVD based image watermarking method using PCA technique. In this method, the color cover and watermark images are decomposed by DWT and then SVD is applied on the selected sub-band. Subsequently, the singular value of the watermark image is embedded into the singular value of the cover image. Before the embedding process, PCA is used to un-correlate the R (Red), G (Green) and B (Blue) channels of the color cover and watermark image. Mangaiyarkarasi and Arulselvi [70] proposed a medical image watermarking method based on DWT and independent component analysis (ICA). After the second level decomposition of the cover image by DWT, the binary logo watermark is embedded into the selected sub-band of the cover image. The

proposed embedding method highly depends on the computation of noise visibility function (NVF). Fast ICA method is used for the watermark extraction process. The proposed method offers high robustness and good image quality against signal processing attacks.

### ***2.2.5 Biometric Watermarking***

Use of biometric image as watermark [71, 72] has been proposed to achieve two level security. Selvy et al. [71] proposed watermarking method based on biometrics (Iris), wavelet-based contourlet transform (WBCT) and SVD. In this embedding process, second level decomposition is performed on randomized cover image. The SVD is applied on all the sub-bands of cover and watermark images where the singular value of the host image is modified with the singular value of the watermark image. The iris biometric has high universality, high distinctiveness, high permanence and high performance than the other biometric traits. Also, WBCT contains the directional information of the image which is not provided by DWT. Wioletta [72] proposed a biometric (Iris) based medical image watermarking method using DWT to embed iris watermark into the cover medical image. This method offers high robustness in lower frequency component of DWT cover image against signal processing attacks. The combination of biometric and watermarking methods provides the security solutions to the medical image watermarking. However, noise in sensed data, non-universality, intra class variations and inter class similarity are the some limitations of the biometric based methods.

### ***2.2.6 Joint Compression and Watermarking***

In recent time, the transmission and storage of digital documents/information over the unsecured channel is an enormous concern and nearly all of the digital documents are compressed before the document is stored or transmitted to save the bandwidth requirements. As a solution to these, noted researchers are combine the watermarking and compression to addressing the optimal trade-off between major performance parameters including embedding and compression rate, storage space, robustness and embedding alteration against different known signal processing attacks. In order to that Mary et al. [73] proposed an encryption and compression based watermarking method in LSB domain. The cover and watermark image is compressed and encrypted by JPEG 2000 compression technique and modified RC6 block cipher respectively before the embedding process. Further, the encrypted watermark image is embedding into the compressed cover image using LSB to addressing the robustness, capacity and security of the watermarking system. Zargar and Singh [74] proposed a lossy BTC compression based watermarking method in DWT domain. In this paper, BTC compression has been applied on watermark

image before embedding into the cover. The robustness and transparency performance of the proposed method is better than fractal-based compression. Guo and Liu [75] proposed a joint watermarking and compression technique using BTC. The method is also addressing the problem of blocking effect and false contour problem as suffered by BTC. The performance of the proposed method is extensively evaluated by the parameters HVS-PSNR and BER and found to be robust for various known attacks except JPEG and JPEG2000. Further, the method achieved superior robustness than other reported techniques [76]. Goudia et al. [77] proposed a robust joint JPEG 2000 compressing and watermarking technique using DWT and quantization. The experimental results investigated that the method is robust for different attacks at higher quantization step size with minimum degradation in the visual quality of the watermarked image.

A lossless compression based watermarking technique is proposed by Badshah et al. [78] using tele-radiology images. The ROI part of the watermark is considered along with a key to generate a new watermark. The generated watermark is compressed by LZW technique and the compressed watermark is embedding into the RONI part of the cover image. The experimental results established that the performance of the different compression method is investigated and found that the LZW compression technique offer better compression ratio performance than other conventional compression techniques. The method also verifies the tempering in the watermark after extraction and decompression process. Lin et al. [79] also proposed a DCT based color image watermarking whereas the watermark information is embedding into the low frequencies coefficients of the DCT transformed cover image. The method is robust and imperceptible at different modulus values.

### 2.2.7 Others Perspectives

Further, some others significant contribution of wavelet based watermarking techniques are proposed by noted researchers in [80–103]. Reddy and Chatterji [80] suggested a watermarking method to protect the digital watermark where weight factors for the wavelet coefficients are calculated and the watermark bits are added to significant coefficients of all DWT sub-bands. In the recovery process, the extracted watermark bits are combined and normalized. Although this method is shown to be robust against cropping attack however, the proposed method can detect noise up to 40% only. Lin and Ching [81] proposed a blind wavelet-based image hiding method that hides more than one image inside the host image and maintains the quality of watermarked image. In the watermark embedding process, watermark image is embedded into low frequency components of the DWT cover image. The embedded information is scrambled to ensure security and robustness of the watermark simultaneously. The extraction process is same as embedding process but in reverse order.

Chang et al. [82] have proposed a multipurpose watermarking method based on integer-DWT (IWT) that achieves both the copyright protection and image

authentication simultaneously. The IWT is easy to implement and has fast multiplication-free implementation. However, the IWT has poor energy compaction than common wavelet transforms. In [83], Yusof and Khalifa have proposed two different watermarking methods. In the first embedding process, first level DWT coefficients of gray-scale watermark is embedded into the second level DWT of the cover image in all sub-bands. However, in the second method, first level DWT coefficients of gray scale watermark are embedded into the second level DWT of the cover image in the selected sub-band. The size of watermark is one fourth the size of cover image. Both methods are robust and offer higher imperceptibility against signal processing attacks.

Yeh et al. [84] have presented a watermarking method that enables ownership protection. After the first level decomposition of the cover image by DWT, watermark information is embedded in the blocks located at the even and odd columns of the high-low (HL) sub-band low-high (LH) sub-band respectively. During embedding the watermark bit, mean value of all four sub-band wavelet coefficients in the block is calculated [85] and modified. The watermark extraction process is just the reverse of the embedding process. The experimental results show that the method is better than the Chang's method [82]. The proposed algorithm can also be applied to color images. Yang and Hu [86] have proposed a watermarking method based on spatial and frequency domain technique. The secret information is embedded in the spatial domain using min-max algorithm to improve the embedding capacity. However, the watermark information is embedded into the selected sub-bands (HL and LH) of the IWT image using coefficient-bias approach. The experimental results indicate that a hidden data can be successfully extracted and a host image can be losslessly restored. Moreover, the resultant perceptual quality generated by the proposed method is good. Kumar et al. [10] proposed a method for telemedicine application based on DWT. The watermark information (doctor's signature) is converted into the binary image and is embedded into the second level decomposition of DWT cover image. Subsequently, two different pseudo-random noise (PN) sequence pairs are generated and the coefficient of chosen sub-band is modified. During the watermark extraction process in this method, same pseudo random matrix is generated which is used during the embedding process of the watermark. The proposed method is robust against the common signal processing attacks. The method is non-blind which requires original image in the recovery process.

Abdallah et al. [87] proposed a blind wavelet-based image watermarking method using quantization of selected wavelet coefficients. After the third level decomposition of the cover image, perceptually significant wavelet coefficients are used to embed the watermark bits. In this method, some wavelet coefficients are selected and assigned as 0 or 1 using quantization process. This process is repeated until all the watermark bits have been recovered. The proposed scheme has better imperceptibility than the Dugad's scheme [88]. Bekkouche and Chouarfia [89] proposed two different image watermarking methods. The first method is the combination of reversible watermarking and code division multiple access (CDMA) in spatial domain, whereas the second method is the combination of reversible watermarking and CDMA in the frequency (DCT and DWT) domain. The experimental results

show that the combination of the reversible watermarking and CDMA in DCT domain is more robust against signal processing attacks. The proposed method increases security, authentication, confidentiality and integrity of the image and patient information simultaneously. Although CDMA system has a very high spectral capacity however, the system suffers from self-jamming and near-far problem.

Pal et al. [90] proposed a medical image watermarking method based on DWT. In this method, multiple copies of the same data are embedded into the cover image using bit replacement method. To recover hidden information from the damaged copies, the proposed algorithm finds the closest twin of the embedded information using bit majority algorithm. The experimental results have shown that the proposed algorithm embeds a large payload at a low distortion level. However, the algorithm is inefficient for salt and pepper noise above 40% and JPEG compression above 5%.

Bhatnagar et al. [91] proposed non-blind method based on DWT. In this method, the watermark is embedded in the selected blocks made by zigzag sequence using third level decomposition by DWT of the cover. The blocks are selected based on their variance which further serves as the measure of watermark magnitude that could be imperceptibly embedded in each block. The variance is calculated in a small moving square window process which also computes the mean of the standard deviation values derived for the image. The proposed method is time efficient and robust against signal processing attacks. However, the proposed method is less effective for histogram equalization and wrapping attacks. In [92], a blind watermarking method based on the DWT has been proposed. After the third level decomposition by DWT, the selected sub-bands (LH3) are divided into blocks. In the embedding process, the largest two wavelet coefficients in the block are selected and their significant difference is calculated. After quantizing the maximum wavelet coefficient, the binary watermark bits are embedded into the selected sub-band. During the extraction process, an adaptive threshold value is designed to extract the watermark under different conditions. Experimental results show that the method is robust and the watermarked image quality is good against JPEG compression and low-pass filtering attacks. Lin et al. [93] also proposed a wavelet-tree-based watermarking method using distance vector of binary cluster. In this method, wavelet trees are classified into two clusters using the distance vector to denote binary watermark bits. For embedding, the statistical difference and the distance vector of wavelet tree are compared to select the watermark bits for embedding. The experimental results as reported by authors have shown that the watermarked image quality is very good and the method is robust against known attacks.

Zhang et al. [94] proposed a blind watermarking algorithm based on sparse representation of the compressed sensing (CS) theory and IWT. In this embedding process, IWT is first applied on cover image to obtain the transform coefficients that consist of sparse matrix of image on the row and column followed by a random projection. The histogram shrinkage technology on host image is used to prevent the data overflow. With the help of Arnold transform, scrambled watermark is embedded with the help of IWT and compressed sensing theory. The extraction process is same as embedding but in the reverse order. The proposed method achieved



improved robustness and imperceptibility than Lin method [95] and it also enhanced security of the watermark system. However, the algorithm complexity is high.

Wang et al. [96] proposed a semi blind and adaptive watermarking method based on DWT. For the watermark embedding purpose, third level DWT coefficients are categorized into Set Partitioning in Hierarchical Trees (SPIHT). Those trees are further decomposed into a set of bit planes. Now, the binary watermark is embedded into the selected bit planes with adaptive watermark embedding strength. The proposed method is robust and imperceptible against signal processing attacks. Also, the method has good computational efficiency for practical applications. Chen and Zhao [97] developed a robust and blind watermarking technique for 3D images using contourlet transform and depth-image-based rendering (DIBR). The watermark generated through spread spectrum method and each watermark bits is embedding into the selected coefficients of the cover contourlet sub-bands through proper quantization. The PSNR, NC and BER performance of the method is extensively evaluated and found that the low BER performance at different views than other reported methods [98, 99].

Zolotavkin and Juhola [100] proposed a robust watermarking method using QIM. The performance of the method is measured by WNR and document to Watermark Ratio (DWR). The method is found to be robust It provides high robust for additive white Gaussian noise and gain attack. Wang and Allebach [101] proposed a halftone image watermarking in which watermark is embedding into the halftone by using synchronization pattern. The performance of the method is evaluated in terms of PSNR, normalized HVS mean square error and watermark rate and found to be good visual quality and achieved high watermark capacity. An improved spread transform dither modulation based robust and secure watermarking technique was proposed by Cao et al. [102]. The watermark is only embedding into the selected embedding sub-space. The security and robustness performance of the method is extensively evaluated for estimation of projection vector and amplitude scaling attacks respectively. Heidari and Naseri [103] proposed a quantum watermarking method in which quantum signal/information is embedding into the quantum cover image. The method scrambled the watermark information along with the keys are embedding into the cover using LSB technique. The performance is examined in terms of PSNR and authors reported that the method is robust.

Further, Table 2.1 summarizes some inspiring and pioneering robust image watermarking algorithms.

## 2.3 Potential Challenges and Discussion

The foregoing section presented a detailed review of transform domain specially wavelet based watermarking techniques using ECCs, hybrid techniques, multiple watermarking, biometrics, joint compression and watermarking, machine learning. The analysis of merits and limitations of these techniques with respect to major watermarking benchmark parameters i.e. robustness, imperceptibility, security and

**Table 2.1** Summary of inspiring and pioneering robust image watermarking algorithms

Ref. No.	Methodology used	Decomposition level	Cover images/Watermark image	Filter used	Remarks
[1]	DWT, BCH code	Up to third level	MR Image of size $512 \times 512$ / Maximum size of message = 381 bits	Haar	<ul style="list-style-type: none"> <li>Max PSNR = 49.12 dB.</li> <li>Max BER = 0.0603 against JPEG attacks.</li> </ul>
[2]	DWPT, BCH code	Second level	Medical images of size $512 \times 512$ /Message bits of 2048 bits and watermark logo image of size $128 \times 128$	Haar	<ul style="list-style-type: none"> <li>Radiological image is the more robust against attacks</li> <li>Obtained PSNR = 39.0999 dB, NC is 1.000 and BER 0.0 without attack.</li> </ul>
[9]	Haar Wavelet Quantization Function, BCH, ROI	Fourth level	Medical Images/bit format	Haar	<ul style="list-style-type: none"> <li>Addressing health information management Issues</li> <li>Robust against JPEG attack</li> <li>Highest PSNR 46.66</li> <li>Max BER (%) = 43.6 for MRA image at JPEG (QF = 75).</li> <li>Normalized hamming distance is determined for different medical images upto fourth level</li> </ul>
[11]	Improved robustness using (7,4)-Hamming code, (15,7)-BCH and (15,7)-Reed-Solomon code, DWT	Second Level	Picture of the university/ Maximum size of message = 360 bits	Haar	<ul style="list-style-type: none"> <li>Reed-Solomon code behaves best.</li> <li>The ECCs considered are not able to deal with error rates greater than 10–20%.</li> </ul>
[12]	DWT, SVD, and four different ECCs	Second Level	Medical images of size $512 \times 512$ /Image and text watermark of size $256 \times 256$ and 20 Characters respectively	Haar	<ul style="list-style-type: none"> <li>Hybrid code performed better results in terms of robustness.</li> <li>Without attacks, max PSNR = 37.22 dB whereas NC = 1 and BER = 0</li> </ul>

[13]	IWT, ROI, HVS	First Level	Medical images of size $512 \times 512$ /max message size of 3400 characters	CDF	<ul style="list-style-type: none"> <li>Very good capacity of embedding the watermark</li> <li>PSNR = 44 dB, WPSNR = 53 dB, BER = 0</li> </ul>
[14]	Haar Wavelet Transform	Second Level	Medical image/ECG Signal and patient ID image	Haar	<ul style="list-style-type: none"> <li>PSNR = 50 dB, comparison of different wavelet filters</li> </ul>
[15]	DWT, spread-spectrum, BCH code	Second	Medical images of size $512 \times 512$ /Health centre logo as image and patient information as text	Haar	<ul style="list-style-type: none"> <li>Embedding based on threshold criteria</li> <li>Health data management</li> <li>Performance is determined in terms of PSNR, NC and BER</li> </ul>
[18]	DCT, DWT	Third Level	Lena image of $256 \times 256$ / binary image of $32 \times 32$	LPF, HPF	<ul style="list-style-type: none"> <li>PSNR 50.0285 dB and NC is 0.9782</li> <li>Robust against attacks.</li> </ul>
[21]	DWT, SVD	First	Lena image of $256 \times 256$ / Cameraman image of $128 \times 128$	Haar	<ul style="list-style-type: none"> <li>PSNR 51.14 dB and max NC 0.9994</li> <li>Performance is evaluated in terms of PSNR, NC and efficiency.</li> </ul>
[24]	DCT, Daubechies 4 wavelet transform	Fourth Level	Medical image/binary image	Daubechies-4	<ul style="list-style-type: none"> <li>PSNR value is 56 to 57 dB and SSIM value is 0.79–0.85.</li> </ul>
[25]	Particle swarm optimization, DWT-DCT domain	First Level	Medical images of size $512 \times 512$ /binary bits of size $32 \times 32$	Haar	<ul style="list-style-type: none"> <li>Robust against a wide variety of common attacks</li> </ul>
[26]	DWT, KLT, serial Turbocode	Second Level	Radiographic images of size $512 \times 512$ /patient data	Haar	<ul style="list-style-type: none"> <li>An initial visibility factor value is determined using Fuzzy Inference System (FIS)</li> <li>Performance is evaluated in terms of PSNR, WPSNR and NC</li> <li>Without attacks, the PSNR = 56.8716 dB and WPSNR = 67.7058 dB and NC = 1 when the rate of image compression goes from 10% to 70%.</li> </ul>

(continued)

**Table 2.1** (continued)

Ref. No.	Methodology used	Decomposition level	Cover images/Watermark image	Filter used	Remarks
[27]	Fusion of watermarking and encryption, LSB methods	First Level	Natural images of size $512 \times 512$ /Medical images	Non-tensor product wavelet filter banks	<ul style="list-style-type: none"> <li>– Performance of RSA, AES and RC4 is investigated.</li> <li>– RC4 encryption algorithm performs better than AES and RSA algorithms.</li> <li>– Performance is evaluated in terms of PSNR, SSIM, NC, and Correlation Value (CV)</li> <li>– Robust against different attacks</li> </ul>
[28]	DWT, SVD, ROI, NROI	First Level	Medical image of $2048 \times 2048$ /patient information and logo	Haar	<ul style="list-style-type: none"> <li>– Excellent embedding capacity</li> <li>– The algorithm was evaluated with respect to imperceptibility, robustness, capacity, and tamper localization capability.</li> <li>– Extensive use of cryptographic primitives is considered a major limitation of the method.</li> <li>– The embedding time of the watermarks is much higher than the time spent in the extraction process</li> </ul>
[31]	DCT, SVD, zigzag SFC, genetic algorithm	Apply DCT on host image	e-government document image of size $256 \times 1024$ /watermark image of size $256 \times 256$	–	<ul style="list-style-type: none"> <li>– Avoid the false-positive problem</li> <li>– population size, crossover rate, mutation rate, and generation size, are 30, 0.8, 0.01, and 50, respectively.</li> <li>– Robust against several kinds of attacks</li> </ul>

[33]	Joint encryption watermarking, LSB, QIM, RC4	-	Image of $576 \times 690$ /massage along with key	-	<ul style="list-style-type: none"> <li>- A capacity rate of 1 and 0.5 bits of message per pixel.</li> <li>- Performance is determined in terms of PSNR and Entropy.</li> <li>- PSNR is greater than 49 dB</li> <li>- Robust against various attacks</li> <li>- Fusion of watermarking and cryptography</li> <li>- Encoding and decoding time is determined for different size of EPR watermark</li> <li>- Health data management</li> <li>- Robust against various attacks including checkmark</li> </ul>
[35]	DWT, DCT, MD5, RSA, Hamming error correction code, ROI and NROI	Second Level	Medical images of size $512 \times 512$ /Watermark images of size $256 \times 256$ , text watermark of 33 characters	Haar	<ul style="list-style-type: none"> <li>- Robust against various kind of attacks</li> <li>- PSNR is evaluated by the subjective method also.</li> <li>- Health data management</li> </ul>
[36]	DWT, SVD SHA-512, ROI and NROI	Fourth Level	Medical image of size $1024 \times 1024$ / watermark image of size $512 \times 512$ and text watermark of size 5145 bits	Haar	<ul style="list-style-type: none"> <li>- Robust against various kind of attacks</li> <li>- PSNR is evaluated by the subjective method also.</li> <li>- Health data management</li> </ul>
[42]	DWT, DCT, SVD, BPNN, Arnold transform, arithmetic compression technique, Hamming error correction	Third level	CT-scan image of size $512 \times 512$ /Lump watermark image of size $256 \times 256$ and text watermark of 190 characters	Haar	<ul style="list-style-type: none"> <li>- Health data management</li> <li>- Robust against various attacks including checkmark</li> <li>- Performance is calculated in terms of PSNR, NC and BER</li> <li>- Visual quality of the watermarked image is evaluated by the subjective method also</li> </ul>
[43]	DWT, DCT, SVD, encryption	Second level	Medical image of size $512 \times 512$ /watermark image of size $256 \times 256$ and text watermark of 50 characters	Haar	<ul style="list-style-type: none"> <li>- Health data management</li> <li>- Robust against various attacks including checkmark</li> <li>- Performance is calculated in terms of PSNR, NC and BER</li> <li>- Visual quality of the watermarked image is evaluated by the subjective method also</li> </ul>

(continued)

Table 2.1 (continued)

Ref. No.	Methodology used	Decomposition level	Cover images/Watermark image	Filter used	Remarks
[44]	DWT, DCT, SVD, encryption	Second Level	Digital image of size $512 \times 512$ /watermark image of size $256 \times 256$ and text watermark of 185 characters	Haar	<ul style="list-style-type: none"> <li>Health data management</li> <li>Robust against various attacks including checkmark</li> <li>Performance is calculated in terms of PSNR, NC and BER</li> <li>Visual quality of the watermarked image is evaluated by the subjective method also</li> </ul>
[45]	Multi wavelet, SVM, Modulation technique	First level	Lena, Peppers, Boat/binary logo	–	<ul style="list-style-type: none"> <li>PSNR = 42.38, BER = 0–0.3</li> <li>Robust against common attacks</li> </ul>
[49]	DWT, PCA	Third level	Digital image of size $512 \times 512$ /binary watermark image of size $32 \times 32$	Haar	Robust against common attacks
[78]	LZW, ROI	–	ROI size of the cover medical = $100 \times 100$ , secret key length = 64/ uncompressed watermark binary stream = 80,256 values	–	LZW gives the better compression ratios than other conventional methods
[80]	DWT, HVS characteristics	Fourth Level	Lena of size $512 \times 512$ /gray scale logo of size $64 \times 64$	Haar	Robust, detected up to 40% noise
[81]	DWT, Scrambled the Embedded Information	Third Level	Lena and Baboon/digital image of size $512 \times 512$	Haar	The method can hide up to three full size images where the PSNR above 32 dB
[89]	Cryptography tools, CDMA in Frequency (DWT, DCT) and Spatial Domain (LSB)	First Level	Medical/gray image	–	Compared the results on the basis of PSNR, MSE, Mean Absolute Error and SNR



[90]	DWT, Bit Majority method	First level	Medical Images, logo images	<ul style="list-style-type: none"><li>– PSNR values are 41.19–42.34 dB and SSIM values are 0.96–0.988 for different images</li></ul>
[91]	DWT, segmentation using ZIG-ZIG sequence	Third level	Gray-scale images of size 256 × 256/8-bit gray scale logo of size 32 × 32	<ul style="list-style-type: none"><li>– Max PSNR = 57.74 and embedding and extraction time is 11.07 s</li><li>– Robust against intentional or un-intentional variety of attacks.</li></ul>
[97]	contourlet transform	First Level	DIBR 3D images	<ul style="list-style-type: none"><li>– Using Middlebury Stereo Datasets for experimental purpose</li><li>– Performance is evaluated in terms of PSNR, NC, SSIM, BER, mean opinion score</li><li>– Robust against Geometric Attacks</li></ul>
[113]	DDM based on CSF filter, LSB, DWT	Second Level	Fundus image/Text data	<ul style="list-style-type: none"><li>– Performance comparable with the standard PSNR</li></ul>

*IWT* integer wavelet Transform, *DWT* discrete wavelet transform, *PSNR* peak signal-to-noise-ratio, *DCT* discrete cosine transform, *ROI* Region-of-interest, *CSF* contrast sensitive function, *SST* spread-spectrum technique, *HM* histogram modification, *LPF* low pass filter, *HPF* high pass filter, *WPSNR* weighted peak signal to noise ratio, *CDF* Cohen-Daubechies Feauveau, *BER* bit error rate, *NC* normalized cross-correlation, *DWPT* discrete wavelet packet transform, *PCA* principal component analysis, *CDMA* code division multiple access, *GA* genetic algorithm, *SFC* space-filling curve, *QIM* quantization index modulation, *DIBR* depth-image-based rendering, *LZW* Lempel–Ziv–Welch, *LSB* least substitution bit, *KLT* Karhunen-Loeve transform

capacity revealed that it is difficult to achieve satisfactory performance with respect to imperceptibility, robustness, embedding capacity and security simultaneously. Therefore, it is clear that there are different methods for improving one or a subset of these parameters but they compromise with other remaining parameters. Thus, there is need to develop effective watermarking methods that can offer optimum trade-off between these parameters for telemedicine application. Further, medical image watermarking for telemedicine necessarily requires watermark security against different attacks. Besides this, computational cost of watermarking is also an important parameter to determine the suitability of the watermarking technique. Some important investigations by the authors in the area of medical image watermarking are:

1. *Security of the watermarks*: Most of the medical watermarking methods fall short of this requirement [104, 105]. Some digital watermarking will not need any security because there is hardly any stimulus to disrupt the watermark but others require security against attacks of different kinds. Various researches have been done in recent years to create medical watermark systems which are secure against active attack [27, 106–108]. However, spread spectrum [1, 10, 22, 102] and biometric watermarking [48], or multimodal biometric watermarking security mechanisms [109, 110] are be considered to enhance the security of the watermark. In addition, for the security issues, encrypting EPR data before watermarking has become unavoidable, but the delay encountered during embedding and extraction of the watermark is also an important factor in telemedicine applications [12, 43]. Therefore, watermark constitution by using encryption methods should be simple to save execution time. Recently, the speed has become an important factor if the situation demands in some important applications such as tele-diagnosis and telemedicine.
2. *Selection of ROI and NROI part for embedding watermark*: Any image comprises of two sections called ROI and NROI [35]. ROI is an area that has sensitive data, so it cannot be allowed to be modified because most of the information is present in this area [105]. NROI is an area of image that does not have an important data i.e. background of image. The proper selection of NROI for watermarking is crucial for example in medical images where the area under concern has to be the least required portion conveying any information. It will give better protection if the data is embedded outside of ROI [111, 112].
3. *Selection of DWT sub-bands for embedding watermark*: The selection of sub-bands for embedding watermark is a challenge as it affects robustness against various types of attacks. It has been proved that embedding the watermark in diagonal sub-band coefficients is more robust as compared to horizontal and vertical coefficients [105, 113]. There is no need to have knowledge on the coefficients selected for data embedding when pseudo bits are also embedded [81, 82]. Also, watermark embedding into color image provides greater space against the

watermark embedding into gray scale image. This space will hide more watermark information [114].

4. *Embedding more than one watermark into cover media*: Huge amount of bandwidth is required for the transmission of the image data for telemedicine purposes. The addition requirement of bandwidth for the transmission of the metadata can be avoided if the data is hidden in the image itself [9, 15]. Since the EPR and the image embedded into one, bandwidth for the transmission can be reduced in telemedicine applications. However, this will increase the computational cost of the watermarking method.
5. *Improve the robustness of extracted watermark*: Various noted researchers are using error correcting codes [1, 2, 9, 11, 12], hybrid techniques [16–44], machine learning techniques [45–70], and some other novel perspectives [80–103] methods to improved the robustness of the extracted watermark(s). However, these methods are compromising with other performance parameters of the watermarking systems. Further, use of ECC for digital watermarking is still an open problem [105].
6. *Simultaneous compression and watermarking*: The medical/digital images require a huge amount of memory in original form and thus there is a need for compression in data hiding [115]. It has been observed that the JPEG/JPEG200 compression which is applied on majority of the digital information/data to reduce the bandwidth requirements during transmission is one of the most common and unavoidable attacks to watermarking systems [75, 77, 116]. In order to achieve the goals of green computing and low delay, some of the researchers have been studying combined watermarking and compression using quantization in theoretical point of view [117, 118]. Simultaneous compression and watermarking is one of the robust techniques to combat piracy attacks [75]. Medical applications may consider using combined watermarking and compression algorithm to improve the performance.

## 2.4 Summary

This chapter has presented state-of-the-art in the field of medical image watermarking techniques. Novel and improved medical image watermarking techniques are invented regularly which are addressing the health data management issues and preventing the medical related identity theft. Based on the extensive review, we have noticed that numerous watermarking techniques are designed for specific applications, while the others are not well established yet but have a great potential. This necessitates development of robust and secure watermarking methods to protect integrity and confidentiality of patient's crucial medical data against unauthorized access and tampering.

## References

1. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible spread-spectrum watermarking for telemedicine applications. *Proc. Natl. Acad. Sci., India Sect. A: Phys. Sci.* **85**(2), 295–301 (2015). doi:[10.1007/s40010-014-0197-6](https://doi.org/10.1007/s40010-014-0197-6)
2. S.A.K. Mostafa, N. El-sheimy, A.S. Tolba, F.M. Abdelkader, H.M. Elhindy, Wavelet packets-based blind watermarking for medical image management. *Open Biomed. Eng. J.* **4**, 93–98 (2010)
3. A. Al-Haj, Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. *J. Digit. Imaging* **28**(2), 179–187 (2015)
4. H.-M. Chao, C.-M. Hsu, S. Miaou, A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Trans. Inf. Technol. Biomed.* **6**(1), 46–53 (2002)
5. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, Relevance of watermarking in medical imaging, in *Proceedings of the IEEE EMBS Conference on Information Technology Applications in Biomedicine*, Arlington, USA, pp. 250–255, 2000
6. G. Coatrieux, L. Lecornu, Ch. Roux, B. Sankur, A review of image watermarking applications in healthcare, in *Proceedings of IEEE-EMBC Conference*, New York, USA, pp. 4691–4694, 2006
7. U.R. Acharya, D. Anand, P.S. Bhat, U.C. Niranjana, Compact storage of medical images with patient information. *IEEE Trans. Inf. Technol. Biomed.* **5**(4), 320–323 (2001)
8. A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, A medical image watermarking scheme based on wavelet transform, in *Proceedings of 25th Annual International Conference of IEEE-EMBS*, San Francisco, pp. 1541–1544, 2004
9. A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Secure and efficient health data management through multiple watermarking on medical images. *Med. Biol. Eng. Comput.* **44**, 619–631 (2006)
10. B. Kumar, H.V. Singh, S.P. Singh, A. Mohan, Secure spread spectrum watermarking for telemedicine applications. *J. Inf. Secur.* **2**, 91–98 (2011)
11. N. Terzija, M. Repges, K. Luck, W. Geisselhardt, Digital image watermarking using discrete wavelet transform: performance comparison of error correction codes, in *Proceedings of International Association of Science and Technology for Development*, 2002
12. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible dual watermarking for telemedicine applications. *Wirel. Pers. Commun.* **80**(4), 1415–1433 (2014)
13. K.A. Navas, S.A. Thampy, M. Sasikumar, ERP hiding in medical images for telemedicine, in *Proceedings of World Academy of Science and Technology*, vol. 28, pp. 266–269, 2008
14. A. Kannammal, K. Pavithra, S. SubhaRani, Double watermarking of DICOM medical images using wavelet decomposition technique. *Eur. J. Sci. Res.* **70**(1), 55–46 (2012)
15. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Multiple watermarking on medical images using selective DWT coefficients. *J. Med. Imaging Health Inf.* **5**(3), 607–614 (2015)
16. D.-Ch. Lou, Ch.-H. Sung, Robust image watermarking based on hybrid transformation, in *Proceedings of IEEE International Carnahan Conference on Security Technology*, Taiwan, pp. 394–399, 2003
17. Md. Ouhsein, E.E. Abdallah, A.B. Hamza, An image watermarking scheme based on wavelet and multiple-parameter fractional Fourier transform, in *Proceedings of IEEE International Conference on Signal Processing and Communications*, Dubai, United Arab Emirates, pp. 1375–1378, 2007
18. M. Jiansheng, L. Sukang, T. Xiaomei, A digital watermarking algorithm based on DCT and DWT, in *Proceedings of International Symposium on Web Information Systems and Applications*, Nanchang, P.R. China, pp. 104–107, 2009
19. A.S. Hadi, B.M. Mushgil, H.M. Fadhil, Watermarking based Fresnel transform, wavelet transform, and chaotic sequence. *J. Appl. Sci. Res.* **5**(10), 1463–1468 (2009)

20. C. Cao, R. Wang, M. Huang, R. Chen, A new watermarking method based on DWT and Fresnel diffraction transforms, in *Proceedings of IEEE International Conference on Information Theory and Information Security*, Beijing, pp. 433–430, 2010
21. C.-C. Lai, C.-C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* **59**(11), 3060–3063 (2010)
22. A.A. Nakhaie, S.B. Shokouhi, No reference medical image quality measurement based on spread spectrum and discrete wavelet transform using ROI processing, in *Proceedings of 24th Canadian Conference on Electrical and Computer Engineering*, pp. 121–125, 2011
23. V.K. Ahire, V. Kshirsagar, Robust watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) for copyright protection of digital images. *IJCSNS* **11**(8), 208–213 (2011)
24. A. Umaamaheshvari, K. Thanushkodi, High performance and effective watermarking scheme for medical images. *Eur. J. Sci. Res.* **67**(2), 283–293 (2012)
25. M. Soliman, A.E. Hassanien, N.I. Ghali, H.M. Onsi, An adaptive watermarking approach for medical imaging using swarm intelligent. *Int. J. Smart Home* **6**(1), 37–50 (2012)
26. M.A. Hajjaji, E.-B. Bourennane, A.B. Abdelali, A. Mtibaa, Combining Haar wavelet and Karhunen Loeve transforms for medical images watermarking. *Biomed. Res. Int.* **2014**, 1–15 (2014)
27. A. Kannammal, S. Subha Rani, Two level security for medical images using watermarking/encryption algorithms. *Int. J. Imaging Syst. Technol.* **24**(1), 111–120 (2014)
28. A. Al-Haj, A. Amer, Secured telemedicine using region-based watermarking with tamper localization. *J. Digit. Imaging* **27**(6), 737–750 (2014)
29. S. Priya, B. Santhi, P. Swaminathan, Study on medical image watermarking techniques. *J. Appl. Sci.* **14**(14), 1638–1642 (2014)
30. L. Gao, T. Gao, G. Sheng, S. Zhang, Robust medical image watermarking scheme with rotation correction, in *Intelligent Data Analysis and Its Applications, Vol. 2*, *Advances in Intelligent Systems and Computing*, ed. by J.-S. Pan et al. (Eds), vol. 298, (Springer, New York, 2014), pp. 283–292
31. D. Rosiyadi, S.-J. Horng, P. Fan, X. Wang, Copyright protection for e-government document images. *IEEE Multimedia* **19**(3), 62–73 (2012)
32. D. Rosiyadi, S.-J. Horng, N. Suryana, N. Masthurah, A comparison between the hybrid using genetic algorithm and the pure hybrid watermarking scheme. *Int. J. Comput. Theory Eng.* **4**(3), 329–331 (2012)
33. S.-J. Horng, D. Rosiyadi, T. Li, T. Takao, M. Guo, M.K. Khan, A blind image copyright protection scheme for e-government. *J. Vis. Commun. Image Represent.* **24**(7), 1099–1105 (2013)
34. S.-J. Horng, D. Rosiyadi, P. Fan, X. Wang, M.K. Khan, An adaptive watermarking scheme for e-government document images. *Multimedia Tools Appl.* **72**(3), 3085–3103 (2014)
35. A. Sharma, A.K. Singh, S.P. Ghrra, Robust and secure multiple watermarking technique for medical images. *Wirel. Pers. Commun.* **92**(4), 1611–1624 (2017)
36. R. Pandey, A.K. Singh, B. Kumar, A. Mohan, Iris based secure NROI multiple eye image watermarking for teleophthalmology. *Multimedia Tools Appl.* **75**, 14381 (2016). doi:[10.1007/s11042-016-3536-6](https://doi.org/10.1007/s11042-016-3536-6)
37. Y. Niu, X. Cui, Q. Li, J. Ding, A SVD-based color image watermark algorithm in DWT domain, in *Advanced Graphic Communications, Packaging Technology and Materials*, *Lecture Notes in Electrical Engineering*, vol. 369, (Springer, New York, 2015), pp. 303–309
38. A. Singh, A. Tayal, Choice of wavelet from wavelet families for DWT–DCT–SVD image watermarking. *Int. J. Comput. Appl.* **48**(17), 9–14 (2012)
39. M.I. Khan, M.M. Rahman, M.I.H. Sarker, Digital watermarking for image authentication based on combined DCT, DWT, and SVD transformation. *Int. J. Comput. Sci.* **10**(5), 223–230 (2013)
40. A. Srivastava, P. Saxena, DWT-DCT-SVD based semi blind image watermarking using middle frequency band. *IOSR J. Comput. Eng.* **12**(2), 63–66 (2013)

41. N.J. Harish, B.B.S. Kumar, A. Kusagur, Hybrid robust watermarking techniques based on DWT, DCT, and SVD. *Int. J. Adv. Electr. Electron. Eng.* **2**(5), 137–143 (2013)
42. A. Zear, A.K. Singh, P. Kumar, A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia Tools Appl.* (2016). doi:[10.1007/s11042-016-3862-8](https://doi.org/10.1007/s11042-016-3862-8)
43. A.K. Singh, M. Dave, A. Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools Appl.* **75**(14), 8381–8401 (2016)
44. A.K. Singh, Improved hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools Appl.* **76**, 8881–8900 (2016). doi:[10.1007/s11042-016-3514-z](https://doi.org/10.1007/s11042-016-3514-z)
45. H. Peng, J. Wang, W. Wang, Image watermarking method in multiwavelet domain based on support vector machines. *J. Syst. Softw.* **83**, 1470–1477 (2010)
46. G.D. Fu, H. Peng, Sub sampling-based wavelet watermarking algorithm using support vector regression, in *Proceedings of EUROCON, Warsaw*, pp. 9–12, 2007
47. J. Zhang, N.-C. Wang, F. Xiong, Hiding a logo watermark into the multiwavelet domain using neural networks, in *Proceedings of 14th IEEE International Conference on Tools with Artificial Intelligence*, pp. 477–482, 2002
48. H.-H. Tsai, D.-W. Sun, Color image watermark extraction based on support vector machines. *Inf. Sci.* **177**(2), 550–569 (2007)
49. M. Vafaei, H. Mahdavi-Nasab and H. Pourghassem (2013) A new robust blind watermarking method based on neural networks in wavelet transform domain, *World Appl. Sci. J.*, Vo. 22, No. 11, pp. 1572–1580.
50. T. Sridevi, S.S. Fathima, Watermarking algorithm using genetic algorithm and HVS. *Int. J. Comput. Appl.* **74**(13), 26–30 (2013)
51. X. Kang, W. Zeng, J. Huang, X. Zhuang, Y.-Q. Shi, Digital watermarking based on multi-band wavelet and principal component analysis. *Proc. SPIE* **5960**, 1–7 (2005)
52. Z. Wang, N. Wang, B. Shi, A novel blind watermarking scheme based on neural network in wavelet domain, in *Proceedings of the 6th Word Congress on Intelligent Control and Automation, Dalian, China*, pp. 3024–3027, 2006
53. H.-H. Tsai, C.-C. Liu, K.-C. Wang, Blind wavelet based image watermarking based on HVS and neural networks, in *Proceeding of the Joint Conference on Information Sciences, Kaohsiung, Taiwan*, 2006
54. S. Joo, Y. Suh, J. Shin, H. Kikuchi, A new robust watermark embedding into wavelet DC components. *ETRI J.* **24**(5), 401–404 (2002)
55. Y. Wang, A. Pearmain, Blind image data hiding based on self reference. *Pattern Recogn. Lett.* **25**(15), 1681–1689 (2004)
56. J. Ni, C. Wang, J. Huang, R. Zhang, Performance enhancement for DWT-HMM image watermarking with content-adaptive approach, in *Proceeding of International Conference on Image Processing*, pp. 1377–1380, 2006
57. A. Miyazaki, Improvement of watermark detection process based on bayesian estimation, in *18th European Conference on Circuit Theory and Design*, pp. 408–411, 2007
58. Y. Shao, W. Chen, C. Liu, Multiwavelet based digital watermarking with support vector machine technique, in *Control and Decision Conference*, pp. 4557–4561, 2008
59. C.-h. Li, Z.-d. Lu, K. Zhou, An image watermarking technique based on support vector regression, in *Proceeding of International Symposium Communications and Information Technology*, vol. 1, pp. 183–186, 2005
60. M.-S. Hsieh, Perceptual copyright protection using multiresolution wavelet-based watermarking and fuzzy logic. *Int. J. Artif. Intell. Appl.* **1**(3), 45–57 (2010)
61. P. Surekha, S. Sumathi, Implementation of genetic algorithm for a dwt based image watermarking scheme. *ICTACT J. Soft Comput.* **2**(1), 244–252 (2011)
62. K. Ramanjaneyulu, K. Rajarajeswari, Wavelet-based oblivious image watermarking scheme sing genetic algorithm. *IET Image Process.* **6**(4), 364–373 (2012)



63. W.-H. Lin, Y.-R. Wang, S.-J. Horng, A wavelet-tree based watermarking method using distance vector of binary cluster. *Expert Syst. Appl.* **36**(6), 9869–9878 (2009)
64. S.H. Wang, Y.P. Lin, Wavelet tree quantization for copyright protection watermarking. *IEEE Trans. Image Process.* **13**(2), 154–165 (2004)
65. E. Li, H. Liang, X. Niu, An integer wavelet based multiple logo-watermarking scheme, in *Proceedings of the IEEE WCICA*, pp. 10256–10260, 2006
66. B.K. Lien, W.H. Lin, A watermarking method based on maximum distance wavelet tree quantization, in *Proceeding of 19th Conference on Computer Vision, Graphics and Image Processing*, pp. 269–276, 2006
67. N. Ramamurthy, S. Varadarajank, Robust digital image watermarking scheme with neural network and fuzzy logic approach. *Int. J. Emerg. Technol. Adv. Eng.* **2**(9), 555–562 (2012)
68. H.V. Dang, W. Kinsner, An intelligent digital colour image watermarking approach based on wavelets and general regression neural networks, in *Proceeding of 11th IEEE International Conference on Cognitive Informatics and Cognitive Computing*, Kyoto, pp. 115–123, 2012
69. Md. Imran, A. Ghafoor, A PCA-DWT-SVD based color image watermarking, in *Proceeding of International Conference on Systems, Man, and Cybernetics, COEX*, Seoul, Korea, pp. 1147–1152, 2012
70. P. Mangaiyarkarasi, S. Arulselvi, Medical image watermarking based on DWT and ICA for copyright protection, in *Recent Advancements in System Modelling Applications*, Lecture Notes in Electrical Engineering, ed. by R. Malathi, J. Krishnan (Eds), vol. 188, (Springer, New York, 2013), pp. 21–33
71. P.T. Selvy, V. Palanisamy, E. Soundar, A novel biometrics triggered watermarking of images based on wavelet based Contourlet transform. *Int. J. Comput. Appl. Inf. Technol.* **2**(2), 19–24 (2013)
72. W. Wioletta, Biometric watermarking for medical images—example of Iris code. *Tech. Trans.* **1-M**(5), 409–416 (2013)
73. S.J. Jereesha Mary, C. Seldev Christopher, S. Sebastin Antony Joe, Novel scheme for compressed image authentication using LSB watermarking and EMRC6 encryption. *Circuits Syst.* **7**, 1722–1733 (2016)
74. A. Javeed Zargar, A.K. Singh, Robust and imperceptible image watermarking in DWT-BTC domain. *Int. J. Electron. Secur. Digit. Forensics* **8**(1), 53–62 (2016)
75. J.-M. Guo, Y.-F. Liu, Joint compression/watermarking scheme using majority parity guidance and half toning-based block truncation coding. *IEEE Trans. Image Process.* **19**(8), 2056–2069 (2010)
76. M.H. Lin, C.C. Chang, A novel information hiding scheme based on BTC. *Proc. Int. Conf. Comput. Inf. Technol.* **14–16**, 66–71 (2004)
77. D. Goudia, M. Chaumont, W. Puech, N.H. Said, A joint JPEG2000 compression and watermarking system using a TCQ-based quantization scheme. *Vis. Inf. Process. Commun.* **II**(VIPIC 2011), 78820C–78820C (2011)
78. G. Badshah, S.-C. Liew, J. Md Zain, M. Ali, Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. *J. Digit. Imaging* **29**(2), 216–225 (2016)
79. S.D. Lin, S.-C. Shie, J.Y. Guo, Improving the robustness of DCT-based image watermarking against JPEG compression. *Comput. Stand. Interfaces* **32**(1–2), 54–60 (2010)
80. A. Reddy, B.N. Chatterji, A new wavelet based logo-watermarking scheme. *Pattern Recogn. Lett.* **26**(7), 1019–1027 (2005)
81. C.-Y. Lin, C. Yu-Tai, A robust image hiding method using wavelet technique. *J. Inf. Sci. Eng.* **22**(1), 163–174 (2006)
82. C.C. Chang, W.L. Tai, C.C. Lin, A multipurpose wavelet based image watermarking, in *Proceedings of international conference on innovative computing, information and control*, Beijing, pp. 70–73, 2006
83. Y. Yusof, O.O. Khalifa, Imperceptibility and robustness analysis of DWT-based digital image watermarking, in *International Conference on Computer and Communication Engineering*, Kuala Lumpur, Malaysia, pp. 1325–1330, 2008

84. J.P. Yeh, C.-W. Lu, H.-J. Lin, H.-H. Wu, Watermarking technique based on DWT associated with embedding rule. *Int. J. Circuits, Syst. Signal Process.* **4**(2), 72–82 (2010)
85. C.-Y. Lin, Y.-T. Ching, A robust image hiding method using wavelet technique. *J. Inf. Sci. Eng.* **22**, 163–174 (2006)
86. C.-Y. Yang, W.-C. Hu, Reversible data hiding in the spatial and frequency domains. *Int. J. Image Process.* **3**(6), 373–382 (2010)
87. H.A. Abdallah, M.M. Hadhoud, A.A. Shaalan, F.E.A. El-samie, Blind wavelet-based image watermarking. *Int. J. Signal Process. Image Process. Pattern Recogn.* **4**(1), 15–28 (2011)
88. R. Dugad, K. Ratakonda, N. Ahuja, A new wavelet-based scheme for watermarking images, in *Proceeding of the IEEE International Conference on Image Processing*, Chicago, IL, USA, pp. 419–423, 1998
89. S. Bekkouché, A. Chouarfia, A new watermarking approach—combined RW/CDMA in spatial and frequency domain. *Int. J. Comput. Sci. Telecommun.* **2**(4), 1–8 (2011)
90. K. Pal, G. Ghosh, M. Bhattacharya, Biomedical image watermarking in wavelet domain for data integrity using bit majority algorithm and multiple copies of hidden information. *Am. J. Biomed. Eng.* **2**(2), 29–37 (2012)
91. G. Bhatnagar, Q.M.J. Wu, B. Raman, Robust gray-scale logo watermarking in wavelet domain. *Comput. Electr. Eng.* **38**(5), 1164–1176 (2012)
92. W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, P. Yi, An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Trans. Multimedia* **10**(5), 746–757 (2008)
93. W.-H. Lin, Y.-R. Wang, S.-J. Horng, A wavelet-tree-based watermarking method using distance vector of binary cluster. *Expert Syst. Appl.* **36**(6), 9869–9878 (2009)
94. Q. Zhang, Y. Sun, Y. Yan, H. Liu, Q. Shang, Research on algorithm of image reversible watermarking based on compressed sensing. *J. Inf. Comput. Sci.* **10**(3), 701–709 (2013)
95. W.J. Lin, Reconstruction algorithms for compressive sensing and their applications to digital watermarking, Beijing Jiaotong University, Beijing, 2011
96. S. Wang, D. Zheng, J. Zhao, Adaptive watermarking and tree structure based image quality estimation. *IEEE Trans. Multimedia* **16**(2), 311–325 (2014)
97. Lei Chen and Jiying Zhao, Robust Contourlet-based watermarking for depth-image-based rendering 3D images, 2016 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Nara, Japan, pp. 1–4.
98. Y.H. Lin, J.L. Wu, A digital blind watermarking for depth-image based rendering 3D images. *IEEE Trans. Broadcast.* **57**, 602–611 (2011)
99. H.D. Kim, J.W. Lee, T.W. Oh, H.K. Lee, Robust DT-CWT watermarking for DIBR 3D images. *IEEE Trans. Broadcast.* **58**, 533–543 (2012)
100. Y. Zolotavkin, M. Juhola, A new scalar quantization method for digital image watermarking. *J. Electr. Comput. Eng.* **2016**, 1–16 (2016)
101. F. Wang, J.P. Allebach, Printed image watermarking using direct binary search Halftoning, in *IEEE International Conference on Image Processing*, pp. 2727–2731, 2016
102. J. Cao, H. Li, W. Luo, J. Huang, An improved spread transform dither modulation for robust and secure watermarking, in *IEEE International Conference on Image Processing*, pp. 2718–2722, 2016
103. S. Heidari, M. Naseri, A Novel LSB based quantum watermarking. *Int. J. Theor. Phys.* **55**(10), 4205–4218 (2016)
104. A.K. Singh, B. Kumar, M. Dave, S.P. Ghrera, A. Mohan, Digital image watermarking: techniques and emerging applications, in *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, (IGI Global, USA, 2016), pp. 246–272. doi:[10.4018/978-1-5225-0105-3.ch011](https://doi.org/10.4018/978-1-5225-0105-3.ch011)
105. A.K. Singh, M. Dave, A. Mohan, Wavelet based image watermarking: futuristic concepts in information security. *Proc. Natl. Acad. Sci., India Sect. A: Phys. Sci.* **84**(3), 345–359 (2014)

106. F. Cayre, C. Fontaine, T. Furon, Watermarking security: theory and practice. *IEEE Trans. Signal Process.* **53**(10), 3976–3987 (2005)
107. L.P. Freire, P. Comesana, J.R.T. Pastoriza, F.P. Gonzalez, Watermarking security: a survey, in *Transactions on Data Hiding Multimedia Security*, Lecture Notes in Computer Sciences, vol. 4300, (Springer, New York, 2006), pp. 41–72
108. Y.-S. Seo, M.-S. Kim, H.J. Park, H.-Y. Jung, H.-Y. Chung, Y. Hug, J.-D. Lee, A secure watermarking for JPEG2000. *Int. Conf. Image Process.* **2**, 530–533 (2001)
109. M. Vatsa, R. Singh, A. Noore, Feature based RDWT watermarking for multimodal biometric system. *Image Vis. Comput.* **27**(3), 293–304 (2009)
110. A.K. Jain, U. Uludag, Hiding Biometric Data. *IEEE Trans. Pattern Anal. Mach. Intell.* **25**(11), 1494–1498 (2003)
111. J. Zain, M. Clarke, Security in telemedicine: issue in watermarking medical images, in *International Conference: Science Of Electronic, Technologies of Information and Telecommunications*, 2005
112. N.A. Memon, S.A.M. Gilani, NROI watermarking of medical images for content authentication, in *Proceedings of 12th IEEE International Multitopic Conference*, Karachi, Pakistan, pp. 106–110, 2008
113. S. Dandapat, J. Xu, O. Chutatape, S.M. Krishnan, Wavelet transform domain data embedding in a medical image, in *Proceedings 26th Annual International Conference of IEEE-EMBS*, San Francisco, CA, USA, pp. 1541–1544, 2004
114. R. Ridzon, D. Levicky, Content protection in gray scale and color images based on robust digital watermarking. *Telecommun. Syst.* **52**(3), 1617–1631 (2011)
115. S.P. Nanavati, P.K. Panigrahi, Wavelets: applications to image compression-I. *Resonance* **10**(2), 52–61 (2005)
116. Y. Zhou, Joint robust watermarking and image compression, in *IEEE International Workshop on Information Forensics and Security*, WA, USA, pp. 1–6, 2010
117. Y. Zhou, E.-H. Yang, Joint robust watermarking and compression using variable-rate scalar quantization, in *Proceedings of The 11th Canadian Workshop on Information Theory*, Ottawa, Canada, 2009
118. L. Guillemot, J. Moureaux, Indexing lattice vectors in a joint watermarking and compression scheme, in *IEEE International Conference on Acoustics, Speech, Signal Processing*, Toulouse, France, 2006

Medical Image Watermarking

Techniques and Applications

Singh, A.K.; Kumar, B.; Singh, G.; Mohan, A. (Eds.)

2017, XXIV, 244 p. 82 illus., 50 illus. in color., Hardcover

ISBN: 978-3-319-57698-5