Proc. Natl. Acad. Sci., India, Sect. A Phys. Sci. (July–September 2014) 84(3):345–359
DOI 10.1007/s40010-014-0140-x

REVIEW

Wavelet Based Image Watermarking: Futuristic Concepts in Information Security

Amit Kumar Singh · Mayank Dave · Anand Mohan

Received: 25 October 2013 / Revised: 3 February 2014 / Accepted: 17 February 2014 / Published online: 8 June 2014

Abstract In this paper, we have reviewed the state-of-art of the various wavelet based image watermarking techniques in spatial as well as in transform domain based on the robustness, imperceptibility, capacity and security. The embedding and extraction methods suggested by various researchers/scientists have been studied along with their advantages and disadvantages. We have also discussed some important research challenges and requirements for making the watermarking system more efficient. It will be more important for researchers to implement effective watermarking method.

Keywords Image watermarking · Steganography · Transform domain techniques · Spatial domain techniques

Introduction

With the explosive growth of information and communication technologies (ICT), various new opportunities have emerged for the creation and delivery of content in digital form which includes applications such as real time video and audio delivery, electronic advertising, digital libraries and web publishing. However, these advantages have the consequent risks of copyright protection, data piracy, and credibility which have motivated development of digital watermarking techniques. The digital watermarking is a technique for inserting information into data including image, audio and video which is later extracted or detected for variety of purposes like ensuring identification and authentication. Imagine a sample scenario where watermarking can be thought of in terms of the prisoner's problem, formulated by Simmons [1, 2].

The technique in which message signal is hidden in the host signal without any noticeable distortion to the host signal is referred as data hiding [3]. It is a form of communication that relies on channel used to transfer the host content. The data hiding techniques are classified into two categories: steganography and digital watermarking [4] Fig. 1.

Steganography means the cover writing where there is no relationship between the embedded messages with the cover. Business organizations, intelligence agencies and entertainment industry are the major application areas of steganography where this technique is used for copyright purposes [5]. Digital watermarking is the technique that hides watermark such as audio, video, text and image into a multimedia object where the watermark can be detected or extracted later to make a claim about the multimedia object [6]. The important issue with the steganography is the bandwidth of the hidden message. However, a robustness criterion is more important with watermarking. The communication criteria in steganographic system are point-to-point whereas with the watermarking system it is point-to-multipoint. Different types of watermarking techniques are shown in Fig. 2. According to the type of document the watermark techniques are classified into four categories which are text, image, audio and video watermarking [7].

A. K. Singh (✉)
Jaypee University of Information Technology, Solan, Himachal Pradesh, India
e-mail: amit_245singh@yahoo.com

M. Dave
NIT Kurukshetra, Thanesar, India
e-mail: mdave67@yahoo.com

A. Mohan
IIT (BHU), Varanasi, India
e-mail: amohan@bhu.ac.in

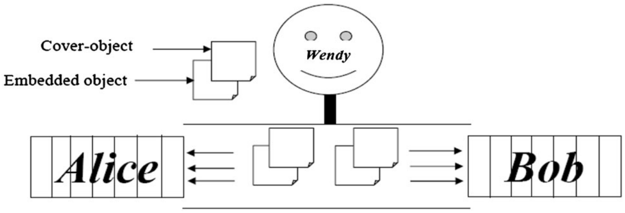

Fig. 1 The prisoners' problem [2]

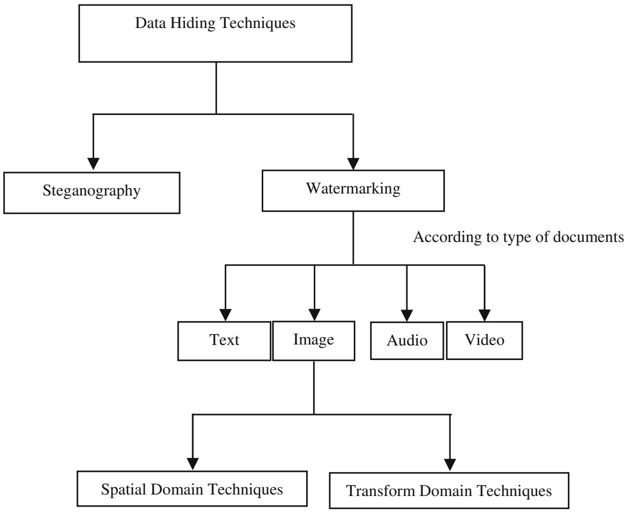
Data Hiding Techniques
Steganography
Watermarking
According to type of documents
Text
Image
Audio
Video
Spatial Domain Techniques
Transform Domain Techniques

Fig. 2 Types of data hiding techniques

The image watermarking techniques are divided into two categories [8]:

(i) Spatial domain techniques [9, 10] such as least significant bit substitution (LSB), spread spectrum, patchwork etc. and
(ii) Transform domain techniques such as discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD) etc.

The transform domain techniques are more robust against common signal processing attacks than the spatial domain techniques. The main advantages of wavelet transform domain for watermarking applications are [11–13]:

(1) Space frequency localization: Used for the analysis of edges and textured areas as it provides good space frequency localization.
(2) Multi-resolution representation: The multi-resolution property of the wavelet transform can be used to exploit the fact that the response of the human eye is different to high and low frequency components of an image.
(3) Multi-scale analysis: Wavelets have non-uniform frequency spectra which facilitate multi-scale analysis.
(4) Adaptability: Flexible and easily adaptable to a given set of images or application.
(5) Linear complexity: Linear computational complexity of O (n) is present for wavelet transform
(6) DWT can be applied to entire image without imposing block structure as used by DCT, thereby reducing blocking artifact.

The watermark techniques can also be grouped as reversible or irreversible. The reversible techniques are useful in medical applications where we require very high level of robustness at very low noise. With this technique we can recover original message without any loss of information [14–16]. The important application requirements of image watermarking based on performance parameters are shown in Table 1, where the watermarking is not secure in spite of its robustness [17, 18].

In general any watermarking system consists of two processes, encoding and recovery process [4]. The watermark embedding process (Fig. 3a) takes a watermark, original data and optional public or secret key, and it produces a watermarked image. The recovery process (Fig. 3b) takes the possibly corrupted image, it may or may not be watermarked image, secret or public key and original data or original watermark to recover a watermark from the possibly corrupted image and proprietorship is to be determined [19, 20]. So that, we can say a general watermark (W) is the function (F) of watermark data (W_d) a cover data (C_d) and a secret key (K) i.e.

$$W = F(W_d, C_d, K) \tag{1}$$

The watermark embedding process can be defined as:

$$\text{Watermark data } (E_w) = F(W, C_d, K) \tag{2}$$

Also, the watermark recovery process (Fig. 3b) can be defined as:

$$\text{Watermark } (W) = F(W \; or \; C_d, E_w, K) \tag{3}$$

Types of Digital Watermarking Systems

There are three types of watermarking systems depending upon the nature and combination of inputs and outputs [18]:

1. Blind watermarking: In blind watermarking, the extraction of watermark requires only the watermarked

Table 1 Important application requirements based on performance parameters

Watermarking performance parameters	Application areas
Robustness	Copyright protection and medical applications etc.
Imperceptibility	Claim of ownership, the receipt of copyright revenues, or the success of prosecution, validation of intended recipient, non-repudiable transmission, meta level, content labelling, network patrolling etc.
Capacity	Medical applications, secure media distribution, thumbnail embedding for authentication, and auxiliary data embedding etc.
Security	Multimedia watermarking, ownership proof, fingerprinting, e-diagnosis or medical image sharing through picture archiving and communication system (PACS) etc.

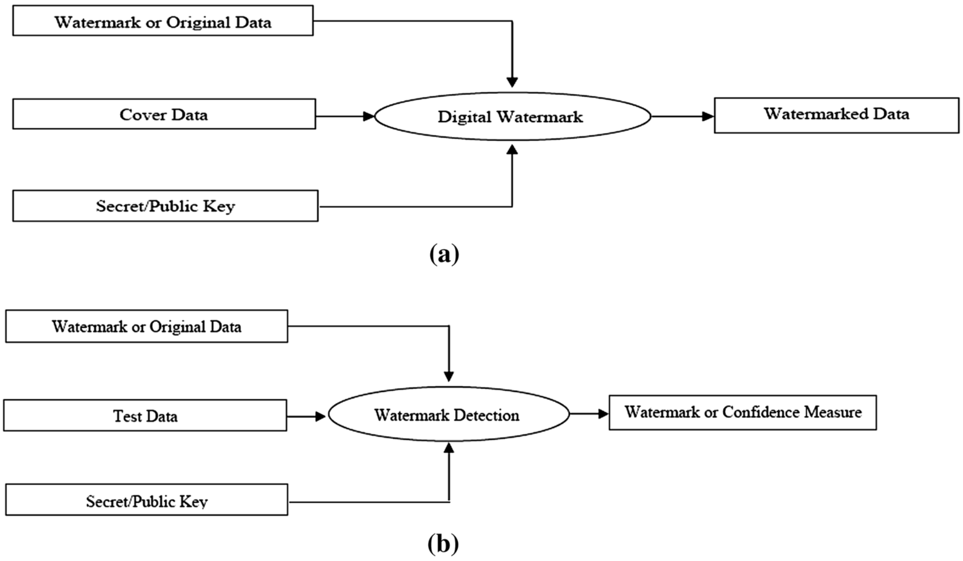

Fig. 3 Watermark **a** embedding and **b** recovery process [4]

image and it doesn't demand the original image or any of its characteristics. Such systems extract the watermark from the test sample. This watermarking system is also known as public watermarking.

2. Non-blind watermarking: In non-blind watermarking, copies of both the original data and the embedded watermark are required along with the test data for extraction. In the watermark embedding systems the watermark is extracted from the distorted data and the original data is used as a clue to find where the watermark is present in the distorted data. The output of this type of watermarking is either yes or no depending upon whether the watermark is present or not in the test data. This type of watermarking is expected to be quite robust.
3. Semi-blind watermarking: This watermarking system also gives the same output as the non-blind watermarking without requiring the original data for detection. However, it has a drawback that the robustness is poor compared with the other two systems. Fingerprinting and copy control are potential applications of such type of watermarking.

Characteristics of Digital Watermarks

There are various important characteristics that watermarks exhibit, which are discussed detail in [21]:

1. Robustness: A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information. Two issues are catered by robustness. Firstly, whether or not the watermark is present after distortion in the data and secondly whether it can be detected by the watermark detector.
2. Security: The watermarking security implies that the watermark should be difficult to remove or alter without damaging the cover image. The security requirement of a watermarking system can differ slightly depending on the application.
3. Data payload: The data payload of a watermark can be defined as the amount of information that it contains. If the watermark contains N bits, then there are $2^\wedge N$ possible watermarks. Actually, there are $2^\wedge N + 1$

possibility because one possibility is that the watermark is not present. An ideal watermark should convey all the required data within any arbitrary and small portion of the content.

4. Imperceptibility: The imperceptibility can be considered as a measure of perceptual transparency of watermark. It refers to the similarity of original and watermarked images.
5. Fragility: The fragile watermark basically aims at content authentication. This is reverse of robustness. The watermarks may be designed to withstand various degrees of acceptable modifications in the watermarks on account of distortions in the media content. Here, watermark differs from a digital signature which requires a cent per cent match.
6. Computational cost: The computational cost basically refers to the cost of inserting and detecting watermarks in digital media content. So the computational complexity is another important attribute of the watermark embedding and extracting process. In some applications, it is important that the embedding process be as fast and simple as possible while the extraction can be more time consuming. In other applications, the speed of extraction is absolutely crucial. The speed requirements of inserting and detecting watermarks is highly application dependent.
7. False positive rate: This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.
8. Key restrictions: Some watermarking methods create a unique key for each piece of data, which requires the owner of the data to maintain a database of keys. Restriction placed on the ability to read the watermark is an important distinguishing characteristic. Algorithms differ in their suitability to the usage of unrestricted and restricted key.
9. Tamper resistance: Tamper-detection watermarking was developed to check the authenticity of digital photographs. Watermarks of this type are sensitive to any change of the content data; thus, by checking the integrity of the watermark, the system can determine whether or not the content has ever been modified or replaced.

Watermarking Attacks

There are several kinds of malicious attacks, which result in a partial or even total destruction of the embed identification key and for which more advanced watermarking scheme is employed [22]:

1. Active attacks: In this type of attack, the hacker tries deliberately to remove the watermark or simply make it undetectable. They are aimed at distorting an embedded watermark beyond recognition. This is a big issue in copyright protection, fingerprinting or copy control for example.
2. Passive attacks: Hacker tries to determine whether there is a watermark and identify it. However, no damage or removal is done. As the reader should understand, protection against passive attacks is important in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.
3. Forgery attacks: In such attacks, the hacker embeds a new, valid watermark rather than removing one. This will help him to manipulate the protected data as he wants and then, re-implant a new given key to replace the destructed one, thus making the corrupted image seems genuine.
4. Collusion attacks: In such attacks, the intention of the hacker is the same as for the active attacks but the approach is slightly different. He uses many instances of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in finger printing applications but is not widely spread because the attacker should be able to access several copies of the same data and that the number needed can be very important. Collusion attacks should be considered because if the attacker has access to more than one copy of watermarked image, he/she can predict/remove the watermarked data by colluding them.

Performance Measures

The performance of the watermarking algorithm can be evaluated on the basis of its robustness and imperceptibility. A larger peak signal to noise ratio (*PSNR*) indicate that the watermarked image more closely resembles the original image meaning that the watermark is more imperceptible. Generally, watermarked image with *PSNR* value greater than 28 is acceptable [23]. *PSNR* is defined as

$$PSNR = 10 \log \frac{(255)^2}{MSE} \tag{4}$$

where the mean square error (*MSE*) is defined as

$$MSE = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} \left(I_{ij} - W_{ij}\right)^2 \tag{5}$$

where I_{ij} is a pixel of the original image of size $X \times Y$ and W_{ij} is a pixel of the watermarked image of size $X \times Y$. The robustness of the algorithm is determined in term of correlation factor. The similarity and differences between original watermark and extracted watermark is measured by the normalized correlation (*NC*). Its value is generally 0 to 1. Ideally it should be 1 but the value 0.7 is acceptable [23].

$$NC = \frac{\sum_{i=1}^{X} \sum_{j=1}^{Y} \left(W_{orignalij} \times W_{recoveredij} \right)}{\sum_{i=1}^{X} \sum_{j=1}^{Y} W_{originalij}^{2}} \tag{6}$$

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

Bit error rate (BER) is defined as ratio between number of incorrectly decoded bits and total number of bits. It is suitable for random binary sequence watermark. Ideally it should be 0.

$$\begin{aligned} BER = {} & (\text{Number of incorrectly decoded bits}) \\ & /(\text{Total number of bits}) \end{aligned} \tag{7}$$

Wavelet Based Watermarking

Terzija et al. [24] have proposed a method for improving efficiency and robustness of the image watermarks. Three different error correction codes, (15,7)-BCH, (7,4)-Hamming code and (15-7)-Reed–Solomon code, are applied to the ASCII representation of the text Universitaet Duisburg which is being used as watermark. In order to be able to use only seven-bit ASCII instead of eight-bit ASCII value, the German letter or umlaut ä is changed into ae, thereby allowing the use of (15,7)-BCH and (15,7)-Reed–Solomon codes. For embedding, the original image is first decomposed up to second level using the DWT with the pyramidal structure and watermark is added to the largest coefficients in all bands of details which represent the high and middle frequencies of the image. The Reed–Solomon code shows the best results due to its excellent ability to correct errors. But the limitation of the proposed technique is that, it is unable to correct the error rates greater than 20 %. Tian [25] has presented a reversible watermarking technique which is based on integer wavelet transform (IWT). The compressed bit stream of the location map is combined with compressed bit stream of the changeable bits and SHA-256 hash them into one big bit stream followed by arithmetic coding. The IWT is easy to implement (multiplication free implementation) but it has poor energy compaction properties as compared to other wavelet transform commonly used. The SHA-256 is a strong hash function but it has message size limitation (2^{64}only). Giakoumaki et al. [26] described wavelet-based multiple watermarking scheme that addresses the problems of medical confidentiality protection and both origin and data authentication. After the third level decomposition of the cover image by DWT, if associated value of the key with the location is one, then that location will be selected for embedding purpose. To extract multiple watermark bits, a quantization function is applied to each of the marked coefficients. The advantages of this method are that it is robust, reliable and efficient. It also satisfies requirements like reduced distortion and resist attacks. The proposed multiple watermarking schemes prevent rounding and other unacceptable alterations in the image with the help of integer changes in the spatial domain. Also, the method is using multiple watermarks that increased the efficiency of the system. However, the method has higher computational cost. Lou and Sung [27] described two transform methods (DCT and DWT) to embed the random watermark into an image. After the third level decomposition of the cover image by DWT, DCT applied to selected sub-bands only. DCT coefficients are selected to generate two sets, the watermark information with zero mean and a variance of unity. The watermark information is next embedded into these sub-bands in order to create two new sets. To determine the presence of the watermark, the correlation is compared to a threshold. The advantages of the proposed method are robust against various attacks and keep the image quality well. Also, this technique does not relies upon the original image therefore it may be applied easily to networks like Internet. However, the method does not assess the watermark security parameter.

Dandapat et al. [28] have described a wavelet based technique for embedding medical data in a medical image. The diagnostic distortion measure (DDM) that is based on contrast sensitive function filter, evaluates and separates the wavelet coefficients and consider the patient data as a string of bits that are embedded into the sets of diagnostically coefficients by using LSB method. The embedment of data into the mid and high frequency sub-bands of the host image showed lower values of DDM and higher values of PSNR. The proposed method is uses spatial domain method (LSB) and transforms domain method (DWT) which removes the disadvantages of each other. Furthermore, the contrast sensitive function can describe the inverse relationship between contrast sensitivity and spectral frequency. But the cost computing in DWT techniques is higher along with longer compression time. Xuan et al. [29] used the spectrum technique for embedding the data in wavelet coefficients. With histogram modification, the overflow and underflow conditions are prevented. The IWT is easy to implement and has fast multiplication-free implementation. However, it has poor energy compaction than common wavelet transform. Moreover, Cohen–Daubechies–Feauveau (CDF (2,2)) filter is better than other wavelet families in terms of embedding capacity and visual quality of embedded images. The spread spectrum watermarking scheme requires the original image in the extraction process but it does not provide a maximum use of the human visual system (HVS).

Reddy and Chatterji [30] described a watermarking method to protect digital watermark. In the embedding process, firstly they find the weight factors for the wavelet coefficients and threshold weight, after that they add watermark bits to significant coefficients of all sub-bands. In the recovery process, the extracted watermark bits are combined and normalized. The method is more robust against cropping attack. However, the proposed method can detect up to 40 % noise only. Giakoumaki et al. [31] reviewed various papers and discuss the major issues in the medical field. The proposed method based on wavelet to discourse health data management issues. According to characteristic and requirements, different watermark, such as signature, index, caption and reference are assigned at different decomposition level and sub-bands. With the help of error correcting code (BCH code), the robustness of the method has improved. With proper quantization of coefficients, the watermarks are embedded and examined. If the outcome binary value is equal to the value of the watermark bit to be embedded, the coefficient is left intact; otherwise, it is modified, though the method is unable to explain the image inherent characteristics. Lin and Ching [32] proposed a blind wavelet-based image hiding method that hide more than one image inside the host image and maintain the quality of watermarked image. During the embedding process after the third level of decomposition of the cover image by DWT, watermark image is embedded into low frequency components of the cover image. The extraction process is same as embedding but in reverse order. The authors have also scrambled the embedding information to ensure security and robustness. However, images can be removed when the high pass filter and the low pass filter employed in the wavelet transform. Chang et al. [33] have proposed a multipurpose watermarking method, which is based on integer-DWT (IWT). It can achieve the copyright protection and image authentication simultaneously and IWT is easy to implement and has fast multiplication-free implementation. However, the IWT has poor energy compaction than common wavelet transform. Ouhsain et al. [34] have proposed a watermarking method using multiple parameters, discrete fractional Fourier (MPDFRF) and DWT. The experimental results demonstrated better visual imperceptibility and an improved resiliency against several attacks. The proposed method used MPDFRF that has random eigenvectors, random magnitude and random phase which provides a suitable criterion for image encryption. However, sampling of MPDFRF may loose many important properties and the computational cost is high. Yusnita and Khalifa [35] have proposed two methods, in the first method of embedding process, DWT is applied on the cover image and after the second level of decomposition, the watermark information are embedded. The size of watermark is one forth the size of cover image and the gain factor having range from 2 to 8. The extraction process is reverse for both methods. DWT generally suffers from shift sensitivity, poor directionality, absence of phase information and higher computational cost.

Navas et al. [36] have proposed a blind method for telemedicine applications that based on IWT. Based on the HVS, proposed method grouped into different wavelet blocks. Now, electronic patient record (EPR) is embedded into non-region of interest (NROI) part and the image areas which contain the important information for medical diagnosis are stored without any noise. The data and image recovery process is same as embedding but in reverse order. After the embedding and recovery process of the watermark, EPR data encrypted and decrypted that are important for transmission and security. The proposed method can embed and recover at most 3,400 character without any noise that is important for EPR information hiding but the computational cost is too high. Jiansheng et al. [37] have proposed an algorithm for digital image watermarking based on two transform method (DCT and DWT). In embedding, the host image is decomposed into *n* level wavelet transform and the watermark information is embedded only in the high frequency band of DWT image. Before embedding the watermark information, it is DCT transformed. Here, the high frequency coefficients are plotted into 2 × 2 image sub blocks and the entropy and square values of each image sub-block is calculated. The watermark distilling process is the reverse of the embedding process. This algorithm has strong capability of embedding signal and anti-attack. The algorithm can conceal watermark. Furthermore, when attacks are employed directly on the watermark image, it does not damage the watermark directly but at high cost of computing and the computational speed is lower.

Hadi et al. [38].proposed a method based on two transform methods (Fresnel and DWT) with the help and encouragement of chaotic sequence using logistics map. Before the embedding process, cover image is encrypted first by Fresnel transform to generate the encrypted image. After the second level decomposition of DWT image, encrypted message are embedded into the decomposed image. The method provides a balance between security, complexity, computational overheads and computational power etc. However, the encryption of message is time which is more time consuming process.

Mostafa et al. [39] have proposed a method for telemedicine applications. The method provides a way to secure EPR information in order to reduce the storage space and transmission cost. After the second level of decomposition by discrete wavelet packet transform (DWPT), EPR information is embedded. Before embedding the EPR information, it has been coded by BCH code to improve the robustness of the method. However, BCH codes group is a time-consuming decoding process. Yeh et al. [40] have presented a watermarking method that enables ownership protection. After the first level decomposition of the cover image by DWT, watermark information embedded in the blocks located at the even columns of the high–low (HL) sub-band and the blocks located at the odd columns of the low–high (LH) sub-band. To embed a watermark bit, the mean value of the four coefficients in the block is calculated [32] and each of the four coefficients is modified. The watermark extraction process is just the reverse of the embedding process. The experimental results are better than the Chang's method [33]. The proposed algorithm can also be applied on color images but the authors do not address the watermark security problems such as reshaping or visual cryptography before embedding.

Cao et al. [41] proposed an adaptive blind watermarking method based on DWT and Fresnel diffraction transform. After the third level decomposition of the cover image by DWT, the binary kinoform of the watermark image is embedded. The watermark extracting process is the invert process of the embedding process. The experimental result showed that watermark image via Fresnel diffraction transforms has good concealment performance. Comparing with the simple permutations, the kinoform is more secure. However, the proposed method is suitable for binary digital watermark only. Lai and Tsai [42] proposed a hybrid image watermarking scheme based on DWT and SVD. After the first level decomposition of the cover image by Haar wavelet, SVD is applied to selected sub-band only. Now, dividing the watermark image into two parts, singular values in HL and LH sub-band are modified with half of the watermark image and then SVD is applied to them. 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, computational cost is high and the proposed method uses SVD transform technique that requires extra storage.

Yang and Hu [43] have proposed a watermarking method based on spatial and frequency domain technique. With the min–max algorithm, secret message is embedded in the spatial domain. After IWT decomposition of the cover image watermark information is embedded into LH and HL sub-band using the 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. Peng et al. [44] proposed a blind watermarking method based on multi-wavelet and support vector machine (SVM). In the embedding process, first level multi-wavelet performed on each block of image. With modulation technique, the watermark information is embedding into lower frequencies sub-band of the cover image. Here, the watermark information consist of two sub information, a reference information and owner signature of binary logo image. The reference information is used to train SVM during watermark extraction process. Based on results, the proposed method is high imperceptibility and robustness. However, the computational complexity of the method is so high. Kumar et al. [45] have proposed a method for telemedicine application based on DWT. The watermark information (doctor signature) converted into binary image and embedded into the second level decomposition of DWT cover image. Subsequently, n different pseudo-random noise (PN) sequence pairs are generated and the coefficient of chosen sub-bands is modified. In the watermark extraction process, same pseudo random matrices are to be generated after the decomposition of the watermarked image. For the selected sub-band coefficients, average correlation is determined and based on the conditions assigned as 0 or 1. The process is repeated until all the watermark bits have been recovered. The proposed method is robust against the common signal processing attacks. The method is non-blind which requires original image in the recovery process. Also, the spread spectrum watermarking scheme does not provide a maximum use of the HVS. Nakhaie and Shokouhi [46] have proposed a no-reference objective quality measurement method based on spread spectrum technique and DWT using region of interest (ROI) processing. In the embedding, the original image is first divided into two separate parts, ROI and NROI. Now DWT and DCT are applied on ROI and NROI parts respectively. When a no-reference method is used, there is no special requirement for the system. Spread spectrum watermarking scheme is robust to common watermark attacks since the watermark is inserted in the perceptually significant regions of the data. However, if the mark is too fragile, the extracted mark will be lost by small degradations making it difficult to differentiate between medium or highly degraded images.

Abdallah et al. [47] proposed a blind wavelet-based image watermarking method based on quantization of certain wavelet coefficients within certain amplitude ranges in a binary manner to embed meaningful information in the image. After the third level decomposition of the cover image, perceptually significant wavelet coefficients are used to embed the watermark bits only. The watermark detection process is same as the embedding. Now based on the quantization process, some wavelet coefficients are selected and assigned as zero or one. The process is repeated until all the watermark bits have been recovered. The proposed scheme is expected to produce watermarked images with less degradation than the Dugad's scheme [48] but with a higher computation cost.

Ahire and Kshirsagar [49] 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, DCT is applied on the four selected sub-bands. Now, the watermark information in the form of binary is embedded in all four selected DWT sub-bands and the watermark bits are embedded with the help of the generated sequences. The process is repeated for all other blocks. The watermark extraction process is same as 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 proposed method can be also applied on color images. However, authors have not considered watermark security problems such as reshaping or visual cryptography before embedding. Bekkouche and Chouarfia [50] proposed two digital image watermarking methods: the first method is the combination of LSB and a cryptography tool, whereas the second method uses code division multiple access (CDMA) in the frequency and spatial domain. In insertion process of the first method, CDMA in spatial domain is first applied on the image obtained using the first method. The extraction process is just the reverse of insertion process. The proposed method increases security, authentication, confidentiality and integrity of medical 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.

Umaamaheshvari and Thanushkodi [51] 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 when Daubechies 4 wavelet transform is applied on the resultant transformed matrix. Now, the 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. Then, the watermark embedded transformed matrix is 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 and higher complexity. Soliman et al. [52] 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, a quantization parameter is determined from HVS by using luminance mask and texture mask followed by particle swarm optimization (PSO) training. The extraction process is just reverse of the embedding procedure. PSO does not require the original image to extract the watermark but it suffers from the partial optimism. Kannamma et al. [53] proposed a digital watermarking method where electrocardiograph and patients' demographic text act as two level watermarks. In the embedding, DWT is first applied on the original image and is decomposed into three sub-bands. Now, the texture matrix for each sub-band is calculated. The locations for the watermarking are chosen with the help of threshold values. The method can be used for providing authentication, confidentiality and integrity of the medical information and since patient ID and ECG signal as watermarks are used, the memory required in hospital information system (HIS) is also reduced. However, the method is good for Haar wavelet only.

Pal et al. [54] proposed a medical image watermarking method based on DWT. With the help of bit replacement, multiple copies of the same data are embedded into the cover image. To recover hidden information from damaged copies, the proposed algorithm finds the closest twin of the embedded information by bit majority algorithm. The experimental results have shown that the proposed algorithm embed 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. [55] proposed non-blind method based on DWT. After the third level decomposition by DWT, watermark is embedded in the selected blocks made by zig–zag sequence. The blocks are selected based on their variances which further serve as the measure of watermark magnitude that could be imperceptibly embedded in each block. Now, the variance calculated in a small moving square window process computes the mean of the standard deviation values derived for the image. The proposed method is highly robust against number of signal processing attacks and time efficient. However, the proposed method is less effective for histogram equalization and wrapping attacks.

Zhang et al. [56] proposed a blind watermarking algorithm based on sparse representation of the compressed sensing (CS) theory and IWT. In the 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 CS theory. The extraction process is same as embedding but in reverse order. The proposed method combined the CS theory and IWT to improve the robustness and imperceptibility than Lin method [57] and enhanced the security of the watermark system. However, the algorithm complexity is too high. Selvy et al. [58] proposed watermarking method based on biometrics (Iris), wavelet-based contour-let transform (WBCT) and SVD. In the embedding process, second level decomposition is performed on randomized host image and SVD is applied on all the sub-band of cover image and watermark image. After modification of the singular value of host image with the help of watermark image inverse WBCT and inverse randomization is performed to obtain the watermarked image. The proposed method uses the iris biometric which has high universality, high distinctiveness, high permanence and high performance than the other biometric traits. Also, WBCT contains the directional information of the image. However, noise in sensed data, non-universality, intra class variations and inter class similarity are the some limitations of the biometric based method.

Sang et al. [59] proposed a watermark generation algorithm based on cascaded iterative Fourier transform (CIFT). With CIFT algorithm, two random phase masks of the watermark image are obtained which are then put into an optical system to generate embedded watermark image. To detect the watermark, embedded watermark is extracted from the host image along with a secret key. Then, the recovered watermark is compared with the original one. The proposed method has good imperceptibility and robustness and also assesses the security level. However, the computational complexity is too high. Liu et al. [60] proposed an image watermarking technique based on optical double random phase encoding (DRPE). The watermark taken as statistically random real valued white noise that is added directly to the host image. The optical DRPE process transforms the unique barcode image into a random noise. With the help of inverse DRPE process followed by low pass filter, barcode is recovered and separated from original image. The proposed method has good robustness and access to quantify the security level. However, in the discrete model of DRPE algorithm, the relation between the continuous optical counterpart and the discrete model breaks down. Vafaei et al. [61] proposed a blind watermarking method based on DWT and neural networks. In the embedding process, third level DWT applied on cover image and divides the selected sub-bands into different blocks. With the help of neural network, the watermark strength and quantized the selected coefficients are adjusted. Now, the binary image watermark is embedded into the coefficients. The method has good imperceptibility and high robustness simultaneously to different types of attacks such as cropping, filtering and noise addition. However, the computational complexity of the method is too high. Sridevi and Fatima [62] also proposed a watermarking DWT based method using genetic algorithm (GA) and fuzzy inference system to find the embedding strength. In the embedding process, the cover image decomposed by DWT and the watermark is embedding into the selected sub-band. Before embedding the watermark, permutation is performed on the watermark with key. The method is robust without much degradation of the image quality. However, the noise attack is not resistant to the method. The PSNR values of retrieved watermark are very low but the visual quality is good.

The above mentioned techniques are summarized in Table 2.

Discussion and Research Challenges

Various factors such as imperceptibility, robustness, capacity and security need to be considered in the watermarking methods. Depending upon the application requirements there can be tradeoff between these factors. Further, the security factor of watermarking methods can also differ slightly depending on the application. Minimization of the computational complexity is important for practical implementation. The robustness is achieved by using wavelet based image watermarking techniques. In such techniques, the frequency and spatial information of the transform data in multiple resolutions is modified to embed the watermark. The imperceptibility may be achieved by using HVS model [63] along with the wavelet based watermarking, although it will increase the computational complexity. The wavelet based watermarking is also compatible with new image standard JPEG 2000. The embedding and detection process of watermarking method plays a very important role to increase or decrease the overall performance of the wavelet-based watermarking techniques. The current state-of-the-art in wavelet based image watermarking as available in the literature is given below.

1. The methods proposed in [24, 31, 39] embeds an encoded watermark with the help of error correcting codes (ECC) to improve the robustness of the watermark. Also, use of ECC for digital watermarking is still an open problem.
2. The methods proposed in [27, 28, 34, 41, 42, 50] based on the combination of two or more transform techniques achieved high robustness of the extracted watermark and good image quality of the watermarked image.
3. The method proposed by Tian [25] embeds a losslessly compressed watermark by JBIG2 and arithmetic

Table 2 Summary of some wavelet based watermarking techniques

S no.	Methodology used	Decomposition level	Cover images/watermark image	Filter used	Remarks	Reference number
1	Error correction codes-(7,4)-Hamming code, (15,7)-BCH and (15,7)-Reed–Solomon code, DWT	Second level	University of Duisburg/ASCII code of the message	Haar	Reed–Solomon had shown the best error correction capability, The ECCs not greater than 10–20 %	24
2	IWT, SHA-256 hash, arithmetic coding	First level	Lena/gray scale	Haar	Applied to digital audio and video as well	25
3	Wavelet-based multiple watermarking scheme, DWT	Third level	Medical images/digital signature and patient information in binary form	Haar	Average PSNR is 41.93 dB	26
4	DCT, DWT	Third level	Lena/text data	Haar	PSNR is 40.58 dB	27
5	DDM based on CSF filter, LSB, DWT	Second level	Fundus image/text data	CSF filter	Performance comparable with the standard PSNR	28
6	SST, HM, IWT	First level	Lena, Baboon, Barbara and medical/bit information	CDF(2,2)	Different payload different PSNR	29
7	DWT, HVS characteristics	Fourth level	Lena/gray scale logo	Haar	Robust, detected up to 40 % noise	30
8	Haar wavelet quantization function, BCH	Fourth level	Medical images/bit format	Haar	Highest PSNR 46.66	31
9	DWT, scrambled the embedded information	Third level	Lena and Baboon/digital image	Haar	PSNR above 32 dB	32
10	Integer-DWT, zero-watermarking	First level	Lena, Baboon and Peppers/binary image	Haar	PSNR 50.17 dB	33
11	Discrete fractional Fourier and DWT	First level	Sail boat and cameraman/gray scale image	LPF, HPF	PSNR above 54.84 dB	34
12	DWT	Second level	Baby, boat and hill/gray scale image	LPF, HPF	PSNR depends on gain (gain = 2 and 8).	35
13	IWT, ROI	First level	Medical/text data	CDF	PSNR 44 dB, WPSNR 53 dB	36
14	DCT, DWT	Third level	Lena/binary image	LPF, HPF	PSNR 50.0285 dB and NC is 0.9782	37
15	Fresnel transform, DWT with support of chaotic sequence using logistics map	Second level	Cat and horse/text Watermark	Haar	Decrypt the copywrite information	38
16	DWPT, BCH code	Second level	Medical images/vector image and gray scale image of hospital logo	Haar	PSNR 39.0999 dB, NC is 1.000 and BER 0.0	39
17	DWT	First level	Baboon, frog, princes etc./binary images	–	PSNR and NC values better [33]	40
18	DWT and Fresnel diffraction transforms	Third level	Lena/binary image	Haar	Different PSNR at different similarity degree	41
19	DWT, SVD	First	Cameraman and Lena/gray image	Haar	PSNR 51.14 dB and max NC 0.9994	42
20	Min–Max algorithm, IWT	First level	Lena, Jet, Peppers, Elaine, Gold hill and Sailboat/gray image	–	Capacity 0.491/bpp at PSNR 34.99 dB	43
21	Multi wavelet, SVM, modulation technique	First level	Lena, Peppers, Boat/binary logo		PSNR = 42.38, BER = 0–0.3	44
22	Spread-spectrum, DWT	Second level	Medical Images/binary image	Haar	Higher security and robustness.	45
23	No-reference method, SST, DWT, DCT	Third level	Medical(MRI)/binary image	–	Different PSNR at different JPEG	46
24	Daubechies wavelet transform	Third level	Baboon and Hat/binary image	Daubechies-4	Less degradation than [47]	47
25	DCT, DWT	Third to fifth	Lena/binary image	Haar	Good imperceptibility and higher robustness	49

Table 2 continued

S no.	Methodology used	Decomposition level	Cover images/watermark image	Filter used	Remarks	Reference number
26	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	50
27	DCT, Daubechies 4 wavelet transform	Fourth level	Medical image/binary image	Daubechies-4	PSNR and SSIM value is 56–57 dB and 0.79–0.85 respectively	51
28	Particle swarm optimization, DWT–DCT domain	First level	Medical images/binary image		Robust against a wide variety of common attacks	52
29	Haar wavelet transform	Second level	Medical image/binary image	Haar	PSNR 50 dB, comparison of different wavelet filters	53
30	DWT, bit majority method	First level	Medical images, logo images		PSNR values are 41.19–42.34 dB and SSIM values are 0.96–0.988 for different images	54
31	DWT, segmentation	Third level	Lena/gray image	Daubechies	PSNR 57.74 and embedding and extraction time is 11.07 s	55
32	CS theory, IWT	First level	Lena, Baboon, Pepper and Plane/binary image	Haar	Average PSNR value up to 44.93 dB	56
33	Biometrics, WBCT, SVD	Second level	Iris, Mandrill, Lena, Boat/binary image	Laplacian and directional filter banks	PSNR 48.0992 dB	58
34	CIFT, double random phase encoding	–	Lena, Baboon/binary image	Low pass filter	PSNR and NC value is good	59
35	Spread-space spread-spectrum, double random phase encoding	–	Barcode/binary image	–	Scaling factor and BER is calculated for different barcode widths (16–256) at different quantization levels (2–16).	60
36	DWT, neural network	Third level	Lena, Baboon, Aeroplane, Barbara/binary image	Digital filters	PSNR 48.25 and maximum NC 1	61
37	DWT, fuzzy logic, GA, HVS	First level	Lena, Boat, Peppers, Baboon/binary image	Digital filters	PSNR 42.35 and maximum NC 0.999	62

IWT integer wavelet transform, *DWT* discrete wavelet transform, *PSNR* peak signal-to-noise-ratio, *DCT* discrete cosine transform, *DDM* diagnostic distortion measure, *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, *NC* normalized cross-correlation, *DWPT* discrete wavelet packet transform, *CDMA* code division multiple access, *CIFT* cascaded iterative Fourier transform, *GA* genetic algorithm coding scheme. Besides these two compressed scheme, an SHA-256 hash of the original image has been embedded for authentication purpose.

4. The method proposed in [31, 33, 53] embeds multiple watermark. Hence, these proposed method achieved the copyright protection and image authentication simultaneously.
5. The method proposed by Xuan et al. [29] embeds the data and pseudo bits so that the decoder does not know which coefficients have been selected for data embedding. The proposed method enhances the data hiding capacity and high visual quality of marked images. Also, the method using histogram modification prevents the overflow and underflow of data.
6. The method proposed by Lin and Ching [32] scrambled the embedded information to ensure security and robustness. Also, the method can embed up to three full size images while maintaining recognisability of the three extracted embedded images.
7. The adaptive method proposed by Soliman et al. [52] is using swarm intelligent technique. The method achieved high robustness, watermark image quality and reliable for tracing colluders.
8. The method proposed by Selvy et al. [58] provide two level of security (watermarking and iris biometrics) for simultaneously verifying the individual and protecting the biometric template.
9. The method proposed by Hadi et al. [38] based on chaotic sequence using logistic map and embed the encrypted message. The method provides a good balance between speed, security, complexity and computational power.

From the above it is clear that wavelet based image watermarking techniques have been found to give high robustness, imperceptibility, capacity and security.

1. Selection of wavelet filters: The choice of wavelet filters influences the performance of wavelet-based watermarking system. In the wavelet domain, several efficient image watermarking techniques have been developed [64–69]. Watermarking is performed in spatial domain or frequency domain. These two domain methods have their own merits and de-merits and so a hybrid algorithm may be considered in order to improve the robustness without much degradation of the image quality. DFT, DCT, DWT and SVD based watermarking methods use fewer high energy frequency components to embed the information. However, the directional information like the directional edges of the image gets lost. This loss of information can be avoided by using discrete contourlet transform. With this transform, we use Laplacian pyramid for multi-resolution representation of the image followed by a directional decomposition on each band pass image using directional filters.
2. Design of detector: The correlation detector is commonly used for detection in techniques where the watermark is embedded into the DWT coefficients of the image. The designers should make detectors that are optimal and robust [70].
3. Digital images compression: The images require a huge amount of memory in original form and thus there is a need for compression in data hiding [71]. While compressing an image, two important points should be considered. Firstly, minimum possible bytes should be used for storage and secondly the image should not be distorted during compression. A suitable methodology is required to reach a compromise because these two objectives are conflicting. Also, it is more appropriate to embed information such as watermark during compression itself. Simultaneous compression and watermarking is one of the robust techniques to combat piracy attacks [72]. Some of the important applications such as medical applications can consider using combined algorithm to improve the performance.
4. Selection of 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 [27–29]. There is no need to have knowledge on the coefficients selected for data embedding when pseudo bits are also embedded [32, 33]. Also, watermark embedding into color image provides greater space against the watermark embedding into gray scale image. This space will hide more watermark information [73].
5. Selection of ROI and NROI for embedding: Any image comprises of two sections called ROI and NROI [36]. 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 [74]. 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 [43]. It will give better protection if the data is embedded outside of ROI [75, 76].
6. Security of the watermark: Most of the watermarking methods fall short of this requirement. 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. A lot of research has been done in recent years to create digital watermark systems which are secure against active attack [19, 20, 77]. However, spread spectrum [78–81] and biometric watermarking [58] or multimodal biometric watermarking security mechanisms may be considered to enhance the security of the watermark.

Conclusion

In this paper, we have presented detailed review of some state-of-the-art watermarking techniques based on DWT. Various contemporary watermarking schemes were compared based on their robustness, capacity and imperceptibility and security. A number of research challenges and future directions for the development of robust and computationally efficient watermarking schemes have been discussed. There is no single technique that can provide satisfactory performance against all parameters. Depending upon the application the most important parameter may be identified for which best approaches have been discussed. When many such approaches are used to improve multiple performance parameters, the combined effect need to be tested practically. This is recommended to be included as the future scope for research.

References

1. Simmons GJ (1984) The prisoners' problem and the subliminal channel. In: Chaum D (ed) Advances in cryptology, proceedings of CRYPTO '83. Plenum Press, New York, pp 51–67
2. Craver S (1997) On public-key steganography in the presence of an active warden. IBM technical report RC 20931
3. Bender W, Gruhl D, Morimoto N (1996) Techniques for data hiding. IBM Syst J 35:313–336
4. Katzenbeisser S, Petitcolas F (2000) Information hiding techniques for steganography and digital watermarking. Artech House, London
5. Armstrong T, Yetsko K (2004) Steganography, CS-6293 research paper, Instructor: Dr. Andy JuAn Wang
6. Liao K, Lian S, Guo Z, Wang J (2010) Efficient information hiding in H.264/AVC video coding. Telecommun Syst 49:261–269
7. Mohanty SP (2000) Watermarking of digital images. M.S. thesis, Indian Institute of Science, India
8. Wolak CM (2000) Digital watermarking. Preliminary proposal, Nova Southeastern University, USA
9. Nikolaidis N, Pitas I (1999) Digital image watermarking: an overview. In: IEEE international conference on multimedia computing and systems, pp 1–6
10. Cox IJ, Miller M (2002) The first 50 years of electronic watermarking. J Appl Signal Process 2002:126–132
11. Meerwald P, Uhl A (2001) Survey of wavelet-domain watermarking algorithms. In: Proceedings of the SPIE security and watermarking of multimedia contents III, San Jose, pp 505–516
12. Suhad H, Moussa A, Amjad H (2009) Digital image watermarking using localized biorthogonal wavelets. Eur J Sci Res 26:594–608
13. Paquet AH, Ward RK (2002) Wavelet-based digital watermarking for authentication. In: Proceedings of the IEEE Canadian conference on electrical and computer engineering, Winnipeg, pp 879–884
14. Feng J-B, Lin I-C, Tsai C-S, Chu Y-P (2006) Reversible watermarking: current and key issues. Int J Netw Secur 2:161–170
15. Lee S, Yoo CD, Kalker T (2007) Reversible image watermarking based on integer-to-integer wavelet transform. IEEE Trans Inf Forensics Secur 2:321–330
16. Terry M (2009) Medical identity theft and telemedicine security. Telemed e-Health 15:1–5
17. Langelaar GC, Setyawan I, Lagendijk RL (2000) Watermarking digital image and video data: a state-of-the-art overview. IEEE Signal Process Mag 17:20–46
18. Ye C, Ling H, Zou F, Lu Z (2013) A new fingerprint scheme using social network analysis for majority attack. Telecommun Syst 54:315–331
19. Cayre F, Fontaine C, Furon T (2005) Watermarking security: theory and practice. IEEE Trans Signal Process 53:3976–3987
20. Freire LP, Comesana P, Troncoso-Pastoriza JR, Perez-Gonzalez F (2006) Watermarking security: a survey. In: Shi YQ (ed) Transactions on data hiding and multimedia security. LNCS. Springer, Berlin, pp 41–72
21. Huang H-C, Fang W-C (2010) Techniques and application of intelligent multimedia data hiding. Telecommun Syst 44:241–251
22. Vallabha VH (2003) Multiresolution watermark based on wavelet transform for digital images. Cranes Software International Limited, Bangalore
23. Singh AK, Dave M, Mohan A (2013) A hybrid algorithm for image watermarking against signal processing attacks. In: Ramanna S, Lingras P, Sombattheera C, Krishna A (eds) The 7th multi-disciplinary international workshop on artificial intelligence, Krabi, Thailand. LNCS, vol 8271. Springer, Berlin, pp 235–246
24. Terzjia N, Repges M, Luck K, Geisselhardt W (2002) Digital image watermarking using discrete wavelet transform: performance comparison of error correction codes. International Association of Science and Technology for Development
25. Tian J (2002) Wavelet based reversible watermarking for authentication. In: Proceedings of SPIE security watermarking multimedia contents IV, San Jose, CA, pp 679–690
26. Giakoumaki A, Pavlopoulos S, Koutsouris D (2003) A medical image watermarking scheme based on wavelet transform. In: Proceedings of 25th annual international conference of IEEE-EMBS, pp 856–859
27. Lou D-C, Sung C-H (2003) Robust image watermarking based on hybrid transformation. In: IEEE International Carnahan conference on security technology, Taiwan, pp 394–399
28. Dandapat S, Xu J, Chutatape O, Krishnan SM (2004) Wavelet transform domain data embedding in a medical image. In: Proceedings 26th annual international conference of IEEE EMBS, San Francisco, pp 1541–1544
29. Xuan G, Yang C, Zheng Y, Shi Y Q, Ni Z (2004) Reversible data hiding based on wavelet spread spectrum. In: IEEE international workshop on multimedia signal processing, Siena
30. Reddy AA, Chatterji BN (2005) A new wavelet based logo-watermarking scheme. Pattern Recogn Lett 26:1019–1027
31. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Med Biol Eng Comput 44:619–631
32. Lin C-Y, Ching Y-T (2006) A robust image hiding method using wavelet technique. J Inf Sci Eng 22:163–174
33. Chang C-C, Tai W-L, Lin C-C (2006) A multipurpose wavelet-based image watermarking. In: Proceedings of international

conference on innovative computing, information and control, pp 70–73

34. Ouhsain M, Abdallah EE, Hamza AB (2007) An image watermarking scheme based on wavelet and multiple-parameter fractional fourier transform. In: IEEE international conference on signal processing and communications, Dubai, United Arab Emirates, pp 1375–1378
35. Yusnita Y, Khalifa OO (2008) Imperceptibility and robustness analysis of dwt-based digital image watermarking. In: International conference on computer and communication engineering, Kuala Lumpur, Malaysia, pp 1325–1330
36. Navas KA, Thampy A, Sasikumar M (2008) ERP hiding in medical images for telemedicine. Proc World Acad Sci Technol 3:44–47
37. Jiansheng M, Sukang L, Xiaomei T (2009) A digital watermarking algorithm based on DCT and DWT. In: International symposium on web information systems and applications, Nanchang, China, pp 104–107
38. Hadi AS, Mushgil BM, Fadhil HM (2009) Watermarking based Fresnel transform, wavelet transform, and chaotic sequence. J Appl Sci Res 5:1463–1468
39. Mostafa SAK, El-sheimy N, Tolba AS, Abdelkader FM, Elhindy HM (2010) Wavelet packets-based blind watermarking for medical image management. Open Biomed Eng J 4:93–98
40. Yeh JP, Lu C-W, Lin H-J, Wu H-H (2010) Watermarking technique based on DWT associated with embedding rule. Int J Circuits Syst Signal Process 2:23–28
41. Cao C, Wang R, Huang M, Chen R (2010) A new watermarking method based on DWT and Fresnel diffraction transforms. In: IEEE international conference on information theory and information security, Beijing, pp 430–433
42. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59:3060–3063
43. Yang C-Y, Hu W-C (2010) Reversible data hiding in the spatial and frequency domains. Int J Image Process 3:373–382
44. Peng H, Wang J, Wang W (2010) Image watermarking method in multiwavelet domain based on support vector machines. J Syst Softw 83:1470–1477
45. Kumar B, Singh HV, Singh SP, Mohan A (2011) Secure spread-spectrum watermarking for telemedicine applications. J Inf Secur 2:91–98
46. Nakhaie AA, Shokouhi SB (2011) No reference medical image quality measurement based on spread spectrum and discrete wavelet transform using ROI processing. J Inf Secur Res 2:121–125
47. Abdallah HA, Hadhoud MM, Shaalan AA, El-samie FEA (2011) Blind wavelet-based image watermarking. Int J Signal Process Image Process Pattern Recogn 4:15–28
48. Dugad R, Ratakonda K, Ahuja N (1998) A new wavelet-based scheme for watermarking images. In: IEEE international conference on image processing, Chicago, IL, USA, pp 419–423
49. Ahire VK, Kshirsagar V (2011) Robust watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) for copyright protection of digital images. Int J Comput Sci Netw Secur 11:208–213
50. Bekkouche S, Chouarfia A (2011) A new watermarking approach—combined RW/CDMA in spatial and frequency domain. Int J Comput Sci Telecommun 2:1–8
51. Umaamaheshvari A, Thanushkodi K (2012) High performance and effective watermarking scheme for medical images. Eur J Sci Res 67:283–293
52. Soliman MM, Hassanien AE, Ghali NI, Onsi HM (2012) An adaptive watermarking approach for medical imaging using swarm intelligence. Int J Smart Home 6:37–50
53. Kannamma A, Pavithra K, SubhaRani S (2012) Double watermarking of DICOM medical images using wavelet decomposition technique. Eur J Sci Res 70:46–55
54. Pal K, Ghosh G, Bhattacharya M (2012) Biomedical image watermarking in wavelet domain for data integrity using bit majority algorithm and multiple copies of hidden information. Am J Biomed Eng 2:29–37
55. Bhatnagar G, Wu QMJ, Raman B (2012) Robust gray-scale logo watermarking in wavelet domain. Comput Electr Eng 38:1164–1176
56. Zhang Q, Sun Y, Yan Y, Liu H, Shang Q (2013) Research on algorithm of image reversible watermarking based on compressed sensing. J Inf Comput Sci 10:701–709
57. Lin W (2011) Reconstruction algorithms for compressive sensing and their applications to digital watermarking. Beijing Jiaotong University, Beijing
58. Selvy PT, Palanisamy V, Soundar E (2013) A novel biometrics triggered watermarking of images based on wavelet based contourlet transform. Int J Comput Appl Inf Technol 2:19–24
59. Sang J, Zhang B, Hong D, Xiang H, Xu H, Sang N (2013) An image watermarking technique based on cascaded iterative fourier transform. Int J Light Electron Opt 124:4522–4525
60. Liu S, Hennelly BM, Sheridan JT (2013) Digital image watermarking spread-space spread-spectrum technique based on double random phase encoding. Opt Commun 300:162–177
61. Vafaei M, Mahdavi-Nasab H, Pourghassem H (2013) A new robust blind watermarking method based on neural networks in wavelet transform domain. World Appl Sci J 22:1572–1580
62. Sridevi T, Fatima SS (2013) Watermarking algorithm using genetic algorithm and HVS. Int J Comput Appl 74:26–30
63. Carli M, Campisi P, Neri A (2006) Perceptual aspects in data hiding. Telecommun Syst 33:117–129
64. Bamerger RH, Smith MJT (1992) A filter bank for the directional decomposition of images: theory and design. IEEE Trans Signal Process 40:882–893
65. Yang S-H (2003) Filter evaluation for DWT-domain image watermarking. Electron Lett 39:1723–1725
66. Do MN, Vetterli M (2005) The contourlet transform: an efficient directional multiresolution image representation. IEEE Trans Image Process 14:2091–2106
67. Jaylakshmi M, Merchant SN, Desai UB (2006) Blind watermarking in contourlet domain with improved detection. In: International conference on intelligent information hiding and multimedia signal processing, pp 449–452
68. Do MN, Vetterli M (2006) Contourlets: a directional multiresoluational image representation. In: International conference on image processing, pp 497–501
69. Sahraeian SME, Akhaee MA, Hejazi SA, Marvasti F (2010) Contourlet-based image watermarking using optimum detector in a noisy environment. IEEE Trans Image Process 19:967–980
70. Rahman SMM, Ahmad MO, Swamy MNS (2009) A new statistical detector for DWT-based additive image watermarking using the Gauss–Hermite expansion. IEEE Trans Image Process 18:1782–1796
71. Nanavati SP, Panigrahi PK (2005) Wavelets: applications to image compression-I. Resonance 10:52–61
72. Guo J-M, Liu Y-F (2010) Joint compression/watermarking scheme using majority-parity guidance and halftoning-based block truncation coding. IEEE Trans Image Process 19:2056–2069
73. Ridzon R, Levicky D (2011) Content protection in grayscale and color images based on robust digital watermarking. Telecommun Syst 52:163–1617
74. Zhang L, Zhou P-P (2010) Localized affine transform resistant watermarking in region-of-interest. Telecommun Syst 44:205–220
75. Zain J, Clarke M (2005) Security in telemedicine: issue in watermarking medical images. In: International conference: science of electronic, technologies of information and telecommunications

76. Memon NA, Gilani SAM (2008) NROI watermarking of medical images for content authentication. In: Proceedings of 12th IEEE international multitopic conference, Karachi, Pakistan, pp 106–110
77. Seo Y-S, Kim M-S, Park HJ, Jung H-Y, Chung H-Y, Hug Y, Lee J-D (2001) A secure watermarking for JPEG2000. Int Conf Image Process 2:530–533
78. Blake J, Latifi S (2011) Digital watermarking security. Def Sci J 61:408–414
79. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6:1673–1687
80. Malvar HS, Florencio DAF (2003) Improved spread spectrum: a new modulation technique for robust watermarking. IEEE Trans Signal Process 51:898–905
81. Perez-Freire L, Perez-Gonzalez F (2009) Spread-spectrum watermarking security. IEEE Trans Inf Forensics Secur 4:2–24