J Digit Imaging (2014) 27:714–729
DOI 10.1007/s10278-014-9700-5

Watermarking Techniques used in Medical Images: a Survey

Seyed Mojtaba Mousavi · Alireza Naghsh · S. A. R. Abu-Bakar

Published online: 29 May 2014

Abstract The ever-growing numbers of medical digital images and the need to share them among specialists and hospitals for better and more accurate diagnosis require that patients' privacy be protected. As a result of this, there is a need for medical image watermarking (MIW). However, MIW needs to be performed with special care for two reasons. Firstly, the watermarking procedure cannot compromise the quality of the image. Secondly, confidential patient information embedded within the image should be flawlessly retrievable without risk of error after image decompressing. Despite extensive research undertaken in this area, there is still no method available to fulfill all the requirements of MIW. This paper aims to provide a useful survey on watermarking and offer a clear perspective for interested researchers by analyzing the strengths and weaknesses of different existing methods.

Keywords Medical image watermarking · Fragile watermarking · Robust watermarking · Reversible watermarking · Medical confidentiality · Authentication

S. M. Mousavi · S. A. R. Abu-Bakar (✉)
Computer Vision, Video, and Image Processing (CvviP) Research Laboratory, Department of Electronics and Computer Engineering, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia
e-mail: syed@fke.utm.my

S. M. Mousavi
e-mail: mosavi59@gmail.com

A. Naghsh
Department of Electrical Engineering, Najafabad Branch, Islamic Azad University, Isfahan, Iran
e-mail: naghsh_a@yahoo.com

Introduction

The widespread emergence of computer networks and the popularity of electronic managing of medical records have made it possible for digital medical images to be shared across the world for services such as telemedicine, teleradiology, telediagnosis, and teleconsultation. Instant diagnosis and understanding of a certain disease as well as cutting down the number of misdiagnosis has had extensive social and economic impact, clearly showing the need for efficient patient information sharing between specialists of different hospitals. In the handling of medical images, the main priority is to secure protection for the patient's documents against any act of tampering by unauthorized persons. Thus, the main concern of the existing electronic medical system is to develop some standard solution to preserve the authenticity and integrity of the content of medical images [1, 2].

Accordingly, one solution for tackling the above issue is the use of digital watermarking. In other words, watermarking can enhance the security of medical images by inserting special information, called a watermark or hidden data, in a nonconspicuous way. Watermark information is usually inserted in a binary format to the pixel value of the host image. This information can later be retrieved and checked whether the medical image is distributed with the actual source (authenticity) or belongs to the correct patient (integrity) [3].

Watermarking methods can be classified based on different views. In the following, different categories of watermarking methods are explained. Based on the embedding information concept, watermarking algorithms can be classified as either spatial or transform domain [4]. In the spatial domain, the watermark information is directly embedded in the pixel value of the host or cover image. These methods are fast and simple and also provide high capacity for embedding watermarks. Spatial domain methods may have some advantages and may overcome cropping attacks, but their main drawback is their

weaknesses against noise or lossy compression attacks. In addition, upon discovering the method, embedded watermarks can easily be modified by a third party [4, 5]. In the transform domain, the watermarked image is obtained by embedding the watermark onto the transformed version of the original image [6]. Some of these transforms and a discussion on their benefits and weaknesses are provided in the following sections.

According to human perception, the watermarking methods can be grouped into visible and invisible watermarks. A popular illustration of visible methods is logos, which are put at the corners of images or videos for content or copyright protection. Invisible watermarks are useful for application such as authentication, integrity verification, and copyright protection. Sometimes, visible and invisible watermarking can be used simultaneously. In this case, the invisible watermark can be considered as a backup for the visible one. This is called the dual watermarking technique [7].

Invisible watermarking methods can be divided into four groups: fragile, semi-fragile, robust, and hybrid methods [8, 9]. The fragile method allows the watermark to easily be destroyed by the smallest of modifications. Applications for this kind of watermarking are limited to authentication and integrity verification. The semi-fragile method protects the hidden data against intentional attacks, but is fragile against malicious attacks. The robust watermarking method, which is usually used for copyright protection purpose, should be resistant against multiple different attacks. The robustness of these methods can be measured by applying different attacks on the watermarked images and comparing the embedded and extracted watermark by different benchmarks. The lists of various attacks and benchmarks are introduced in the following sections. Finally, the hybrid watermarking is a mixture of robust and fragile techniques to provide authentication, integrity verification, and copyright protection simultaneously [8, 10].

In addition to above groupings, reversibility (also known as lossless or invertible watermarking) is another important aspect in watermarking. Compared to the conventional watermarking schemes, reversible data hiding restores not only the watermark but also the original multimedia perfectly, which is a critical requirement for medical and military applications. The main characteristic of reversible methods is the ability to recover the original image without any distortion after extracting the watermark bits, besides providing tamper proofing and authentication. By using a reversible data hiding algorithm to embed patient information and diagnostics data into the medical image, medical officers can recover perfectly both the hidden information as well as the image itself [11].

In this paper, we present a perspective of digital watermarking for medical images. Thus, the remainder of this paper is arranged as follows. First of all, basic watermarking concepts such as system components, attacks, application, and requirements are introduced. Afterwards, gives an overview on different commonly used transformations in the medical image watermarking process is given and the advantages and the disadvantages of them are explained. Various benchmarks for evaluating the performance of watermarking methods are presented in "Overview on Watermarking Benchmarks and Performance Analysis." In the last part the importance, advantages, and requirements of medical image watermarking are explained. This section also contains a valuable review of watermarking methods for medical images followed by a summary provided in "Summary."

Basic Concepts in Watermarking Scheme

Overview of a Data Security System

The watermarking concept is closely related to two other fields: cryptography and steganography. These areas fall under the domain called data security system. Cryptography is a method for sending a message in a secure format that only the authorized person can decode and read. This is known as a "secret writing." Even though the encrypted message can be protected during the transmission, once the message is decrypted, it is not protected anymore, and this is the main shortcoming of cryptography techniques when compared with watermarking [7]. Furthermore, most of the cryptographic methods are complex and provide weak copyright protection property.

Steganography is derived from the Greek word "steganos" and "graphei" which mean "covered" and "writing," respectively. In spite of some similarities between steganography and watermarking, there are some differences between them as explained below:

- The objective of steganography is to embed an unrelated secret message into a cover work, while in watermarking, the embedded information and cover work are related to each other.
- In steganography, the message should be invisible, but in watermarking, the embedded information can be either visible or invisible.
- The main goal of steganography is to hide the message into the cover data in a way so that an invader cannot detect it, while the main purpose of watermarking is to embed the data into the cover data in a way that it cannot be removed or replaced by an intruder [7].

Based on these pros and cons, it can be concluded that watermarking is the best choice for preserving the security of a digital image. In addition, the data can be encrypted before embedding the watermark, as a second layer of protection.

Figure 1 shows an overview of a security system and different classification of watermarking scheme.

Different Parts of a Typical Watermarking System

Digital watermarking is the procedure of embedding information (i.e., a watermark) into the host object in such a way that the watermark image/data can be detected by authorized individuals, for assertion of authenticity purposes [13]. The host signal can be a video, audio, image, 3D mesh, etc., while the watermark can be a logo, image, serial number, owner's ID, name, or any other information which shows ownership of the host signal. These signatures are normally converted into a binary sequence before being embedding into the host signal. The following steps are the standard practice for the watermarking procedure [14]. Each part is explained shortly and a typical watermarking system is shown in Fig. 2.

- Embedding: In this part, the original image and the proposed watermark enter to the system, and according to the embedding algorithm, the watermarked image will be produced.
- Distribution: Ability of others to access the watermarked image. For instance, it can be sold to the customers or it can be published through the internet.
- Attacks: Modification of the watermarked image intentionally or unintentionally, by a third party. This concept will be explained in the next section.
- Extraction: Process of separating the hidden information from the watermarked image. Extracting algorithms can be divided into three parts: nonblind, semi-blind, and blind. In nonblind or private watermarking, the original image is required during the extraction process. The original watermark or other side information is necessary to perform the extraction in semi-blind methods. In blind or public watermarking, the extraction process is done without any side information, original image, or original watermark.
- Detection: In this part, the quality of watermarked images and accuracy of extracted watermarks will be evaluated by measuring the similarity between the extracted and the original one.

Distortion and Attacks on Watermarking System

In image watermarking techniques, the main consideration is the evaluation of the robustness and effectiveness of the watermarking method through measurement of the impact of different attacks upon the watermarked image. Based on the watermarking method used, the image may be robust against a specific group of attacks. For instance, in order to increase robustness against geometrical attacks, Fourier-based methods may be a good solution. This section gives an overall vision on different groups of attack that may be used by invaders to remove the watermark from the watermarked image.

These attacks, either intentional or unintentional [16], can be classified into two main classes: signal processing attacks and geometric distortion attacks [9]. Some examples for each class are specified in Table 1.

A valuable literature survey of different watermarking tools, attacks, and benchmark can be found in reference [17]. According to this survey, attacks on watermarked images are divided into four main groups: simple attacks, detection-disabling attacks, ambiguity attacks, and removal attacks, as given in Table 2. Other types of watermarked image attacks are cryptographic and protocol attacks [18]. Discussion on video watermarking attacks, cryptography attacks, and steganography attacks are not within the scope of this paper. Interested readers can refer to related works.

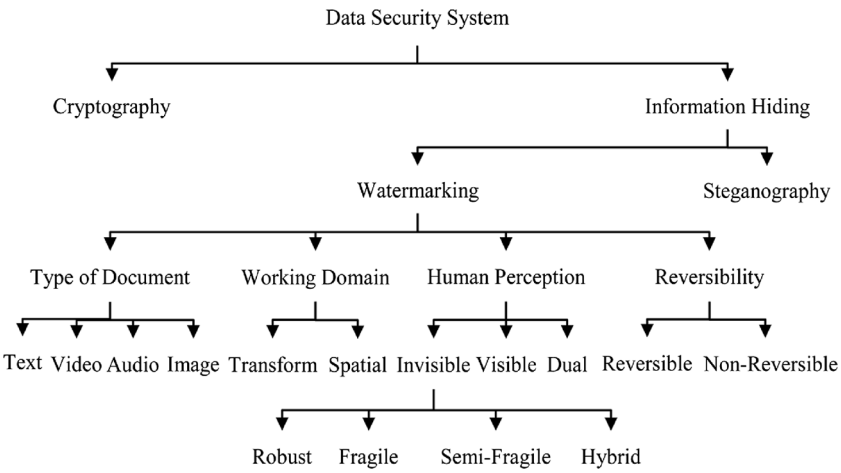

Fig. 1 Overview of a data security system [12]

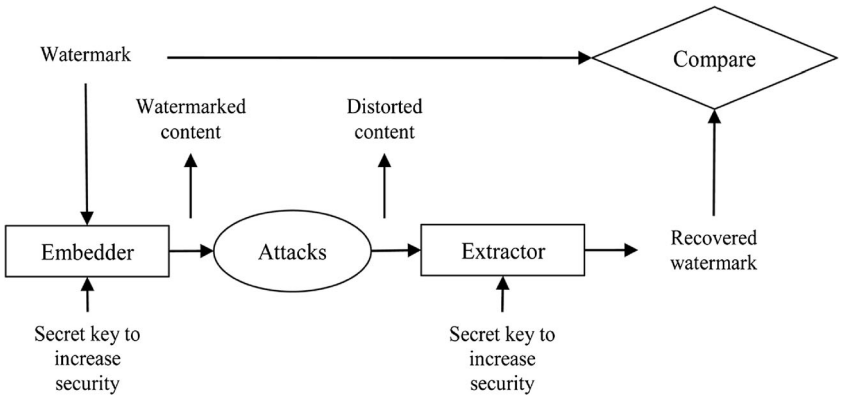

Fig. 2 Typical watermarking system framework [15]

Digital Watermarking System Applications

Watermarking algorithms are application dependent. Different algorithms have different restrictions and conditions. Some of the watermarking applications are given as follows [9, 14]:

- Copyright Protection: In this application, the owner's copyright information is invisibly inserted into the digital image, and ownership can be proven in the case of dispute, by extracting this information. For this, the watermark should be robust against legitimate and illegitimate attacks. This kind of watermark is not appropriate for preventing the user from making a copy of the digital image.
- Fingerprinting: In this application, the owner must embed different watermarks according to each customer identity. It means that the data, which are used as a watermark, will be chosen according to the customer's information. This method enables the owner to find the source of illegal copies and easily find the customer who breaks any license agreement. This watermark should be also robust and invisible.
- Authentication and Integrity Verification: The purpose of this application is to find out whether any modification has been done upon the digital image or not, and then localize the place of tampering. In this application, fragile or semi-fragile watermarking algorithms should be applied, which are not robust against content modification. Broadcast monitoring, content description, and covert communication are other applications of digital image watermarking.

Digital Image Watermarking System Requirements

In this part, the basic requirements for designing a general watermarking system are explained [6, 9, 13]. For specific usage, such as in medical applications, some other features such as imperceptibility and reversibility must be added as explained fully in the medical part [19].

Table 1 First classification for watermark attacks

Main class	Examples
Signal processing attacks	Compression (JPEG-like)
	Color manipulation (intensity, gamma correction, component adjustments)
	Noise (add noise, de-noise, replace bit-planes)
	Filtering (high pass, low pass, Gaussian, and sharpening)
	Scanning
	Averaging
Geometric distortions (de-synchronization attack)	Rotate
	Scaling
	Translation
	Remove column/row
	Cropping

Table 2 Second classification for watermark attacks

Main class	Examples
Simple attacks	Frequency-based compression
	Addition of noise
	Cropping
	Correction
Detection-disabling Attacks	Geometric distortion like:
	Zooming
	Shift direction
	Rotation
	Cropping
	Pixel permutation, removal, insertion
Ambiguity attacks	Several inserted watermarks and cannot recognize their orders
Removal attacks	Collusion attack
	De-noising

- Fidelity: This factor determines the similarity between the watermarked and un-watermarked image. In other words, fidelity is the amount of imperceptibility of the watermark in the watermarked image.
- Robustness: In contrast to fragile watermarking, robustness implies resistance against a variety of innocent and malicious attacks. Cropping, resizing, and compression are examples of unintentional attacks, which may commonly happen when processing a digital image. Noise addition and geometrical distortion are two instances of malicious attacks, which may be used by attackers to disable the watermark.
- Data Payload (Capacity): This factor shows the maximum amount of data, which can be embedded into an image without noticeably reducing image quality. The influence of capacity on the robustness and perceptibility of watermarked image is not negligible; for instance, by increasing the data payload, the robustness will decrease and the perceptibility will increase. The dimensions of the host image should also be considered, since the greater the image resolution, the greater is the amount of watermark is applicable in terms of bits.
- Security: This factor is regarding the application of the different kinds of keys, such as public or private, so that unauthorized persons cannot remove the watermark.
- Computational Complexity (Speed): This factor is regarding the computation time for embedding and extracting the watermark, which directly determines the computational complexity. For example, real-time application requires fast algorithms. However, for high-security applications, the embedding and extracting methods are usually more time consuming.
- Perceptibility: This factor is about the amount of distortion that appears on a watermarked image after inserting a watermark. For invisible watermarks, this factor should be as low as possible.

Overview on Watermarking Techniques

Generally, watermarking algorithms are divided into two main categories: spatial domain and transform domain [4]. The following are brief descriptions of the characteristics of each group.

Spatial Domain Techniques

In the spatial domain, the watermark information is embedded directly in the pixel value of the host or cover image, and to preserve the image quality, the watermark is usually embedded into the least significant bits of the host image. These methods are fast and simple and provide high capacity for embedding watermarks. The other advantage of these techniques is that a small watermark can be embedded several times, so the possibility of removing all watermarks by any kind of attack is very low. Hence, even a single surviving watermarking may fulfill the needs [5, 20–22].

However, spatial domain approaches cannot survive against noise or lossy compression attacks [4]. Furthermore, once the method is uncovered, embedded watermark can be easily modified by a third party. One of the simplest spatial domain techniques is the least significant bit (LSB) method. As shown in Fig. 3, the input image is firstly binarized by the LSB method. Second, the rightmost bits of each pixel are replaced by input watermark bits. Finally, the modified binary pixel values are converted back to decimal pixel values [21, 23–26].

Another method in the category of spatial domain watermarking is the local binary pattern (LBP) method [20, 27]. This method was previously successfully used for texture analysis, face recognition, and crowd estimation [28–30]. In LBP, watermarking the image is first divided into nonoverlapping square blocks. Next, the local pixel contrast is obtained by measuring the spatial relation between the central pixel and its neighboring pixels in each block. These pixels are then used for the embedding and extracting of watermarks according to the rules mentioned in [20]. The advantages of LBP-based methods over LSB methods are their robustness against luminance change, contrast adjustment, and their fragility to other attacks such as filtering and blurring. In other words, LBP-based techniques can be used in semi-fragile watermarking applications [20].

Histogram modification [31] is another spatial domain method that takes the global characteristics of the original image into account for embedding watermarks. This scheme tries to shift the values between the minimum and maximum points of the histogram to perform data hiding [11]. A very small amount of side information is generated by this method, and it can also be implemented easily, but the embedding capacity of this method is limited by the number of max points that occur.

Transform Domain Techniques

In transform domain watermarking, prior to embedding the watermark, transformation such as discrete Fourier transform (DFT) [32–36], discrete-cosine transform (DCT) [37–45], discrete-wavelet transform (DWT) [9, 22, 46–65], dual tree complex wavelet transform (DTCWT) [66–68], contourlet [69–72], or singular value decomposition (SVD) [44, 47, 49, 52, 73–83] is applied onto the host image to produce the transformation domain coefficients. The watermarked image is obtained by modifying these transformation coefficients. The robustness can be increased by modifying the coefficients that the human visual system (HVS) is less sensitive to [6].

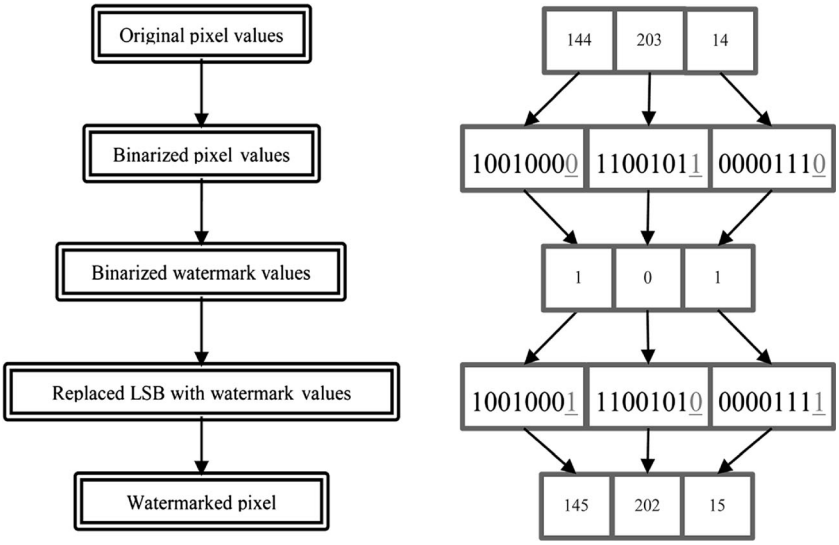

Fig. 3 LSB watermarking procedure

Table 3 shows some differences between the spatial and transformation domain watermarking techniques with regard to capacity, robustness, imperceptibility, processing time, and complexity. Afterwards, the following subsections survey a number of transform domain techniques used in watermarking.

Discrete-Fourier Transform

The discrete Fourier transform is a well-known mathematical operation that transforms the image from the spatial domain to frequency domain [18]. Let $f(x,y)$ represents an image of size $M\times N$, $x=0,1,2,\ldots,M-1$ and $y=0,1,2,\ldots,N-1$. The forward and reverse discrete Fourier transforms are given in Eqs. (1) and (2), respectively [84]:

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j2\pi\left({}^{ux}/_{M}+{}^{vy}/_{N}\right)} \quad (1)$$
$$=R(u,v)+jI(u,v)$$

Table 3 Comparison between spatial and transform domain watermarking methods

	Spatial domain watermarking	Transform domain watermarking
Definition	Embedding directly onto image pixels	Embedding on transform coefficients
Capacity	High	Low
Robustness	Low	High
Imperceptibility	Highly controllable	Lower controllable
Processing time	Low	High
Complexity	Low	High

$$f(x,y)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v)e^{j2\pi\left({}^{ux}/_{M}+{}^{vy}/_{N}\right)} \quad (2)$$

where $F(u,v)$ is the DFT coefficient, $u=0,1,2,\ldots,M-1$, and $v=0,1,2,\ldots,N-1$. The two other parameters $R(u,v)$ and $I(u,v)$ denote the real and imaginary parts of the Fourier transform, respectively.

The polar representation of the Fourier transform can also be shown by [84]:

$$F(u,v)=|F(u,v)|e^{j\phi(u,v)} \quad (3)$$

where $|F(u,v)|$ is magnitude spectrum and $\phi(u,v)$ is phase spectrum, which are respectively given by:

$$|F(u,v)|=\left[R^2(u,v)+I^2(u,v)\right]^{1/2} \quad (4)$$

$$\phi(u,v)=\tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \quad (5)$$

The magnitude and phase contain the least and the most amount of information, respectively, about the image and provide potential candidates for embedding watermark information. Phase-based watermarking, as proposed in [36, 85], shows better robustness against attacks. Moreover, any attempt for removing watermarks causes significant degradation in the image quality. This is because the phase conveys essential information on the image [35, 85]. Embedding the watermark in the magnitude part of DFT [34] generates lower

visual distortion, as this component contains little information about the image.

Other valuable properties of the magnitude component are shift and translation invariant. With these properties, the embedded watermark will not be affected by a translation or shift in the spatial domain. Surprisingly, both magnitude and phase-based watermarking have similar robustness against compression schemes such as JPEG [85]. However, on the downside, this transform is not suitable for nonstationary signals. Furthermore, spatial and frequency information cannot be resolved simultaneously by Fourier transform. To do so, short-time frequency transform (STFT) and the wavelet transform are two options for space-frequency representation of the signal.

Discrete-Cosine Transform

The DCT-based method is a block-based technique. By using this transform, the image will be divided into three frequency bands: low (FL), middle (FM), and high (FH) frequency regions, as shown in Fig. 4.

Coefficients in the FL region carry the most part of the energy of the transformed image, while coefficients in the FH contain the least amount of energy [44]. Forward and inverse equations for 2D-DCT are given in Eqs. (6) and (7), respectively:

$$G(u,v) = \frac{2}{\sqrt{mn}}\alpha(u)\alpha(v)\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} g(x,y) \times \cos\frac{(2x+1)u\pi}{2m} \times \cos\frac{(2y+1)v\pi}{2n} \quad (6)$$

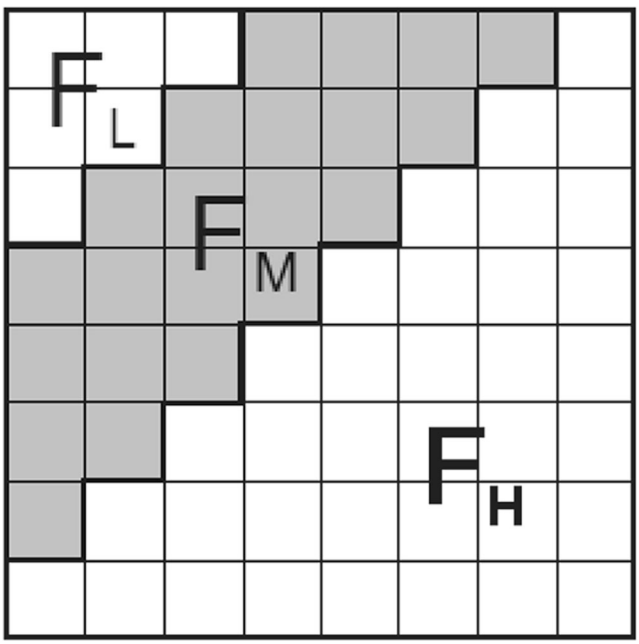

Fig. 4 DCT regions definition [43]

$$g(x,y) = \frac{2}{\sqrt{mn}}\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\alpha(u)\alpha(v)G(u,v) \times \cos\frac{(2x+1)u\pi}{2m} \times \cos\frac{(2y+1)v\pi}{2n} \quad (7)$$

where $g(x,y)$ is the spatial domain pixel value, $G(u,v)$ is the DCT coefficient, the block size is defined by m and n, and α's coefficients are calculated as follows:

$$\alpha(u),\alpha(v) = \begin{cases} {}^{1}/_{\sqrt{2}} & if\ u,v = 0 \\ 1 & \text{else} \end{cases} \quad (8)$$

The middle sub-band coefficients of the DCT transform are commonly used for embedding the watermark to avoid modifying the important visual parts of the image (low frequencies). Furthermore, DCT-based watermarking systems are the most robust against lossy compression [4, 39, 83]. The drawback of DCT-based approaches is that the original image is distorted in a nonreversible manner such that it cannot be recovered precisely [86].

Discrete Wavelet Transform

The wavelet transform is a powerful mathematical tool that has been used in many different areas of applications. Multi-scale capabilities of the wavelet transform that highlight the local and global characteristics of the signal make it an efficient tool in image processing and in particular watermarking application. The wavelet transform decomposes the image into four sub-bands of different frequencies, namely, approximation image (LL_k), horizontal (HL_k), vertical (LH_k), and diagonal (HH_k) details where k denotes the decomposition level [77]. This process can be applied repeatedly on the approximation part (LL_1) to reach a certain final scale based on the user's request [46–48, 51, 87] (see Fig. 5).

In watermarking applications, lower decomposition levels are more vulnerable to image alteration as they have a lower proportion of energy as compared to higher decomposition levels. This energy is defined as:

$$E_k = \frac{1}{N_k M_k}\sum_i\sum_j |I_k(i,j)| \quad (9)$$

where k is the decomposition level, I_k denotes coefficients of the corresponding sub-band, and N_k and M_k are sub-band dimensions.

By comparing the energy of the sub-bands in the same level, i.e. (LL_3,HL_3,LH_3 *and* HH_3), it can be seen that the energy accumulation in the horizontal detail (HL_k) is significantly more than those of the vertical and diagonal details, hence suggesting that this sub-band is more robust to image modification. In other words, even though the approximation

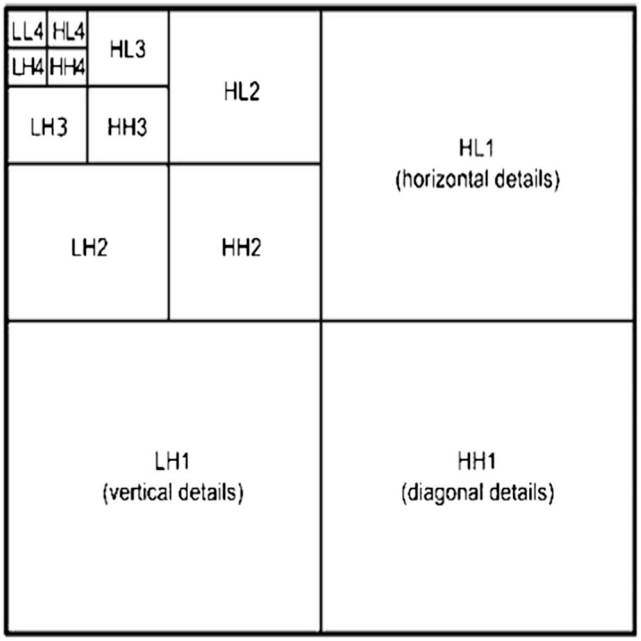

Fig. 5 Wavelet decompositions of an image

image (LL_k) has the highest portion of the energy of the original image, embedding the watermark in this part will degrade the image quality. Therefore, the horizontal sub-band in each level can be chosen as the best candidate area for embedding the watermark, in order to achieve image quality preservation and offer robustness simultaneously [64, 65, 88].

A review on the wavelet-based watermarking methods, consisting of two parts, can be found in [9]. Based on this review, DWT-based methods can model the human visual system (HVS) more accurately than DFT and DCT. Thus, by finding less sensitive areas for the HVS, the system can embed more watermarks in that region without degrading the quality of the watermarked image. Furthermore, these methods are the most robust against noise [83]. Additionally, in comparison to DCT-based transform, wavelet-based methods produce less visual artifacts because the techniques do not require the image to be decomposed into blocks.

Nevertheless, wavelet-watermarking techniques do suffer from other problems and these are given as follows:

- Oscillations: One of the complexities of wavelet based processing is an oscillation of wavelet coefficients around the singularities. This is because wavelets are band-pass functions.
- Shift Variance: The other factor, which complicates wavelet-domain processing, is that a small shift in the signal greatly perturbs the wavelet coefficient oscillation pattern around singularities.
- Aliasing: Whenever wavelet and scaling coefficients change, the inverse DWT cannot cancel the aliasing and this causes artifacts in the reconstructed signal.
- Lack of Directionality: The lack of directional selectivity greatly complicates modeling and processing of geometric image features like ridges and edges.

These shortcomings have been solved by using the dual tree complex wavelet transform (DTCWT), which has been provided by Kingsbury [67] and completed by Selesnick et al. [66].

Contourlet Transform

The other transform-based scheme is the contourlet transform (CT), introduced by Minh Do and Martin Vetterli [70, 71]. CT separates a given image into low- and high-frequency sub-bands by using a Laplacian pyramid decomposition (LPD) filter. Afterwards, directional information can be obtained by applying directional filter banks (DFB) on these band-pass images. The DFB is designed to represent the directionality of the high-frequency components of the image. Figure 6 shows the first two levels of decomposition of the contourlet transform. According to Rahimi and Rabbani [69], watermarking in the contourlet domain shows better robustness against a variety of attacks and demonstrates acceptable invisibility in comparison to wavelet domain watermarking. This is because contourlet transform has superior capability in extracting the directional edges and contours of the image.

Singular Value Decomposition

The concept of singular value decomposition, or SVD, goes back to the linear algebra theorem [78]. It shows that a rectangular matrix can be decomposed into three matrices (with nonnegative real entries) U, S, and the conjugate transpose V. U and V are orthogonal square matrices and S is a rectangular diagonal matrix with its values arranged in descending order. Mathematical representation of a square matrix A of order of N after SVD transform is given as follows [44, 77–79]:

$$A = U\,S\,V^T = [u_1, u_2, \ldots, u_N] \begin{bmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_N \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_N \end{bmatrix} \quad (10)$$

where $U \in R^{N\times N}$ and $V \in R^{N\times N}$ are unitary matrices, i.e., $UU^T = I_n$ and $VV^T = I_n$. The columns of matrices U and V are called the left and right singular vectors of matrix A, respectively. As mentioned before, $S \in R^{N\times N}$ is a diagonal matrix ($S = \mathrm{diag}(\delta_1, \delta_2, \ldots \delta_N)$) with singular values $\delta_i (i = 1,2,\ldots N)$. The operand T is used for the conjugate transpose operation. For matrix A of order r ($r \le N$), if the diagonal entries of matrix S preserve their

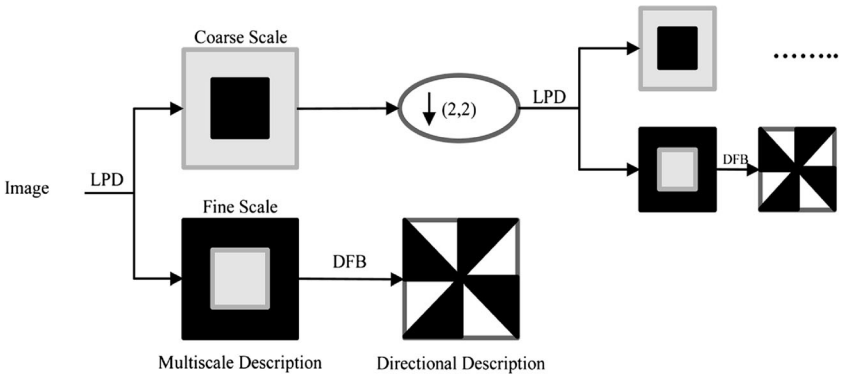

Fig. 6 Contourlet decomposition filter bank. Multi-scale decomposition is computed by LPD and directional description is obtained by applying DFB on each band-pass channel [69]

descending orders as $\delta_1 \geq \delta_2 \geq \ldots \geq \delta_r \geq \delta_{r+1} = \delta_{r+2} \ldots = \delta_N = 0$, then the matrix A can be written as:

$$A = \sum_{i=1}^{r} \delta_i u_i v_i^T \tag{11}$$

where u_i and v_i are ith eigenvector of U and V and δ_i is ith singular value.

During the past years, the SVD transform has been widely used in robust image watermarking [79]. The main idea in SVD-based watermarking methodology is to embed the watermark into the singular values by applying the SVD onto whole or small blocks of the cover image [80]. Unlike most of the common watermarking methods, SVD can be used for nonsquare matrices because of its nonsymmetrical decomposition property. In spite of the robust performance of SVD-based watermarking techniques, they cannot outperform the robustness of frequency-based methods against different attacks [76]. The best approach to enhance the robustness of SVD-based methods is to employ this transform along with the frequency based transforms such as SVD-DCT [44, 74, 79, 81], SVD-DWT [47, 49, 52, 76, 77, 83], and SVD-DTCWT [78, 82].

Overview on Watermarking Benchmarks and Performance Analysis

In medical image watermarking, it is required to preserve the quality of the image, and the patient information, after extracting the watermark. Therefore, for evaluating a watermarked image, two groups of benchmarking are needed; the first is to evaluate the quality of watermarked image, and the second is to measure the correctness of the extracted watermark.

Imperceptibility Evaluation of Watermarked Image

By embedding a watermark into a cover image, some distortions on the image will occur. In the next section, several important distortion metrics of watermarked images that are used in different literatures are explained [6, 8, 9, 89]. In these equations, I(i,j) represents the original image, I_w is the watermarked image, and the image dimensions are shown by $N \times M$ (See Table 4).

- Mean Square Error (MSE): MSE between original and watermarked image is measured by:

$$MSE = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i,j) - I_w(i,j))^2 \tag{12}$$

- Peak-Signal-to-Noise Ratio (PSNR): The PSNR between the original and watermarked image is obtained by:

$$\text{PSNR}\ (I, I_w) = 10 \times \log_{10} \frac{\left(\text{MAX}_I^2\right)}{\text{MSE}} \tag{13}$$

where MAX_I is the maximum possible pixel value of the original image I. Larger PSNR means the original and watermarked image are more similar to each other. To have acceptable perceptual value, the PSNR should be greater than 30 dB.

Table 4 Evaluating parameters for watermarked image

Evaluator	Equation
MSE	$\frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i,j) - I_w(i,j))^2$
PSNR	$10 \times \log_{10} \frac{\left(\text{MAX}_I^2\right)}{\text{MSE}}$
SSIM	$\frac{\left(2\mu_I \mu_{I_W} + c_1\right)(2\text{cov} + c_2)}{\left(\mu_I^2 + \mu_{I_W}^2 + c_1\right)\left(\sigma_I^2 + \sigma_{I_W}^2 + c_2\right)}$
IF	$1 - \frac{\sum_{i,j} (I(i,j) - I_w(i,j))^2}{\sum_{i,j} (I(i,j))^2}$
NRMSE	$\sqrt{\frac{\sum_{y=0}^{N-1} \sum_{x=0}^{M-1} [I(x,y) - I_w(x,y)]^2}{\sum_{y=0}^{N-1} \sum_{x=0}^{M-1} [I(x,y)]^2}} \times 100$
WPSNR	$\left(\frac{\left(\text{MAX}_I^2\right)}{\text{NORM}\left\{ \frac{1}{1+\delta^2 \text{block}} \right\} \times \text{MSE}} \right)$

- Structural Similarity (SSIM) Index: This method gives a similarity measure between two images [90]. SSIM can take a value in the range of −1 to 1, when a value of 1 means that the two images are completely similar to each other.

$$\mathrm{SSIM}(I, I_W) = \frac{(2\mu_I\mu_{I_W} + c_1)(2\mathrm{cov} + c_2)}{\left(\mu_I^2 + \mu_{I_W}^2 + c_1\right)\left(\sigma_I^2 + \sigma_{I_W}^2 + c_2\right)} \quad (14)$$

$$\begin{cases} c_1 = (k_1 L)^2 & k_1 = 0.01 \\ c_2 = (k_2 L)^2 & k_2 = 0.03 \end{cases}$$

where μ_I and μ_{I_W} are the average of I and I_w, respectively, σ_I^2 and $\sigma_{I_W}^2$ are the variance of I and I_w, respectively, cov is the covariance of I_w, c_1 and c_2 are variables to stabilize the division with weak denominator, and L is the dynamic range of pixel values ($L=2^{\text{number of bits per pixel}}-1$).

- Image Fidelity (IF): This measurement determines the similarity between the watermarked and un-watermarked image. In other words, fidelity is the amount of imperceptibility of the watermark in a watermarked image. The higher the IF, the more imperceptible the embedded data is in the watermarked image [9].

$$IF = 1 - \frac{\sum_{i,j}(I(i,j) - I_w(i,j))^2}{\sum_{i,j}(I(i,j))^2} \quad (15)$$

Percentage Normalized Root Mean Square Error: % NRMSE between the original image and the embedded image value is computed by:

$$\left(\%\mathrm{NRMSE}(I, I_w) = \sqrt{\frac{\sum_{y=0}^{N-1}\sum_{x=0}^{M-1}[I(x,y) - I_w(x,y)]^2}{\sum_{y=0}^{N-1}\sum_{x=0}^{M-1}[I(x,y)]^2}} \times 100 \quad (16)$$

- Weighted Peak Signal to Noise Ratio (WPSNR): This metric uses a weighting factor in calculating PSNR which is called noise visibility function (NVF) and is calculated by [8]:

$$\mathrm{WPSNR} = \left(\frac{(MAX_I^2)}{\mathrm{NVF} \times \mathrm{MSE}}\right) \quad (17)$$

where NVF is a texture masking function that can measure the amount of texture in the image by using the Gaussian model. The NVF formulation is given in Eq. (18):

$$\mathrm{NVF} = \mathrm{NORM}\left\{\frac{1}{1 + \delta^2 \mathrm{block}}\right\} \quad (18)$$

where δ is the luminance variance for the 8×8 block. The NORM shows that the NVF is normalized between 0 and 1. For instance, for a flat region, the NVF is close to 1, while for a textured or edge region, the value is closer to 0.

Robustness Evaluation of Extracted Watermark

For binary sequence information, the following quantitative metrics can be used to measure the reliability of an extracted watermark (Table 5). In these equations, $W(i,j)$ represents the original watermark while $W'(i,j)$ represents the extracted watermark.

- Correlation Coefficient (CRC): The CRC can be used to measure compatibility between the original and extracted watermark. The minimum and maximum values of this matrix are 0 and 1, respectively [9].

$$\mathrm{CRC} = \frac{\sum_i\sum_j W(i,j)W'(i,j)}{\sqrt{\sum_i\sum_j W(i,j)^2 * \sum_i\sum_j W'(i,j)^2}} \quad (19)$$

- Similarity Measure (SIM): SIM is used to measure the similarity between an original and extracted watermark [9] and is given by:

$$\mathrm{SIM} = \frac{\sum_i\sum_j W(i,j)W'(i,j)}{\sum_i\sum_j W'(i,j)^2} \quad (20)$$

- Bit Error Rate (BER): This is a useful evaluator when the watermark is a binary sequence. BER shows the probability of binary patterns that are decoded incorrectly. Therefore, the lower is the BER, the better is the performance of the watermarking system [9].

$$\mathrm{BER} = \frac{\mathrm{DB}}{\mathrm{NB}} \quad (21)$$

Table 5 Evaluation parameters for extracted watermark

Evaluator	Equation
CRC	$\frac{\sum_i\sum_j W(i,j)W'(i,j)}{\sqrt{\sum_i\sum_j W(i,j)^2 * \sum_i\sum_j W'(i,j)^2}}$
SIM	$\frac{\sum_i\sum_j W(i,j)W'(i,j)}{\sum_i\sum_j W'(i,j)^2}$
BER	$\frac{\mathrm{DB}}{\mathrm{NB}}$
AR	$\frac{\mathrm{CB}}{\mathrm{NB}}$

where DB is the number of bits that is decoded incorrectly and NB is the total number of original watermark bits.

- Accuracy Ratio (AR): This is also used for indicating the similarity between the original and watermarked image. The more AR is closer to 1, the more similar the extracted watermark is to the original one [9].

$$AR = \frac{CB}{NB} \tag{22}$$

where CB is the number of correct bits and NB is the total number of original binary watermarks.

Medical Image Watermarking

Importance of Medical Image Watermarking

Watermarking in the medical field has many practical applications, including telediagnosis, teleconferences among clinicians, and distant learning of medical personnel. Exchanging medical images between clinicians, specialists, and radiologists provides a platform for discussing and consulting diagnostic and therapeutic measures. In this case, the electronic patient report (EPR) and medical images are sent separately to the destination. Using watermarking techniques and integrating the EPR into the medical images will not only guarantee the confidentiality and security of the sent data but also the integrity of the medical images. Furthermore, authentication of watermarks and tampering detection methods can be used to identify the source of medical images and locating the tampered area, respectively [19].

Advantages of Medical Image Watermarking

In this section, some advantages of medical image watermarking are explained.

- Memory and Bandwidth Saving: By integrating both the medical image and EPR, the huge amount of bandwidth normally required for telemedicine application will be reduced.
- Detachment Avoidance: Detachment or misplacement refers to allocating the EPR to the wrong medical image. If EPR and medical images are sent separately from each other, the possibility of detachment increases. To avoid misplacement, the patient's information needs to be integrated into its medical image.
- Confidentiality: By using watermarking techniques, the patient report can be hidden inside the medical image without being seen by unauthorized persons.
- Security: To prevent the patient's information and medical images from being tampered with, watermarking can be used for hiding the EPR inside the medical image. This prevents attackers from easily changing the medical image or the patient information [19].

Requirements of Medical Image Watermarking

In addition to the basic requirements of a typical watermarking system, as previously explained, some other specific features are needed for the medical watermarking system. These are explained below:

- Imperceptibility: The amount of invisibility of a watermarked image in comparison to nonwatermarked image is called imperceptibility and can be measured by statistical standard metrics such as SSIM or PSNR.
- Reversibility: Due to the image quality, the applied method for medical watermarking should be reversible, meaning that one should be able to exactly recover the original image after extracting the watermark [4].
- Integrity Control: The ability to verify that the image has not been modified without authorization.
- Authentication: Identification of the image source and verification that the image belongs to the correct patient [4].

It is clear that finding and developing new watermarking techniques to satisfy these requirements is still a necessary relevant research area.

Overview of Medical Watermarking Methods

As pointed out in a survey paper written by Navas et al. [19], the objectives of medical image watermarking (MIW) can be divided into two parts: (1) to control integrity and authentication and (2) to hide the electronic patient record (EPR) information.

Another paper [90] divided medical image watermarking methods into three separate categories according to their application: authentication, data hiding, and both authentication and data hiding combined. In the following subsections, each category will be reviewed and discussed. A literature summary of these techniques is also provided in Table 6.

Authentication

The only purpose of this work [10] is content authentication of computed tomography (CT) images. The main focus is on a

Table 6 Literature summary for different watermarking methods: (1) image modality, (2) objective, (3) watermark, (4) embedding region, (5) embedding technique, (6) reversibility, (7) tamper localization, (8) tamper recovery, and (9) fragility and robustness

Name	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Qershi [90]	MR US CT CR	Authentication Data hiding	EPR ROI hash message ROI embedding map Average of ROI blocks Compressed ROI	ROI RONI	DE DWT	√	√	√	Fragile Robust
Memon [8]	CT US X-ray MRI	Security Confidentiality Integrity control Authentication	Patient's information Doctor's code LSBs of ROI	ROI RONI	Hybrid	√	√	√	Fragile Robust
Memon [10]	CT	Authentication	Patient's information Message Authentication code Hospital logo	RONI	LSB	√	–	–	Fragile
Guo [86]	CT MRI US	Integrity Authentication	Patient's information Hash of original image	Whole image	DE	√	√	–	Fragile.
Navas [19]	DICOM	Authentication	ROI	RONI	DWT	√	–	–	Robust
Navas [19]	–	Data hiding	Encrypted of EPR ECG or EEG	Whole image	LSB	–	–	–	Fragile
Navas [19]	–	Data hiding	Encrypted of EPR ECG or EEG	Whole image	LSB of DCT	–	–	–	Robust
Zain [4]	US	Integrity Authentication	Hash of ROI	LSB of RONI	LSB	√	–	–	Fragile
Lin [92]	MRI	Authentication Copyright protection	Patient data (128×128 image) ROI information	RONI	SVD DWT	–	√	–	Robust

blind, fragile watermarking method, which is embedded on the region of noninterest (RONI) of medical images so that the image quality of the region of interest (ROI) is preserved. The segmentation method has been used instead of drawing a square or ellipse for separating the ROI and RONI. The algorithm is claimed to perform segmentation efficiently by accurate ROI detection while increasing the embedding capacity. Furthermore, the embedding part used the LSB method that has multiple advantages—simplicity, high capacity, and very low distortion to the watermarked image. The PSNR of a watermarked image varies from 60 to 51 dB by increasing the embedded data from 8 to 64 kb. In the extraction part, the comparison between the extracted and original logo was done for subjective authentication, and for objective authentication, comparisons were made between the embedded and extracted message authentication code (MAC). The drawback of this approach is that the embedding of the watermark was done in RONI only. Because the attacker can separate the ROI and put his/her own RONI and embeds his/her watermark on it, ROI may not be secured against malicious attacks. The other shortcoming is that this method cannot differentiate between intentional and unintentional attacks, as any manipulation on the image signifies that the image is not authentic. For example, in order to save the bandwidth during the transmission of medical images, JPEG compression may be applied to these images, but this algorithm will detect this process as an attack and show that the image is not authentic.

The other medical watermarking was done by Zain et al. [4], whose purpose was integrity verification and authentication of ultrasound (US) DICOM images. In the first step, the ROI was separated by a rectangular shape from the RONI. The second step was to calculate the hash value of the whole image by means of an SHA256 hash function. To increase security, a secret key was used to create a hash value as well as a secret key for the embedded watermark. The last step was to embed the hash value into the LSBs of RONI. The PSNR of the watermarked image varies from 249.6 to 31.7 dB by increasing the embedded payload from 270 to 510 kb.

The extraction process consists of four steps. Firstly, the watermark is extracted from the LSBs of the watermarked region. Then, the LSBs of the watermarked region are converted to their original values, which in the US image is zero.

After that, the hash value of the image is calculated. In the last part, the results of step two and three are compared to each other. The received image is authenticated if the comparison result shows a high degree of similarity between them.

Both previous papers [4, 10] and similarly [91] used watermarking on RONI for authentication purpose. It is worth pointing out here that only if the pixels in the RONI have zero values can these methods be reversible; otherwise, these schemes are irreversible.

In [92], the purpose was authentication and copyright protection. The watermark was a combination of the patient data and the ROI feature. Prior to watermark embedding, the ratio of ROI and RONI was defined to keep the uniformity of ROI definition by different doctors. The PSNR of the watermarked image is not mentioned in this work.

Data Hiding

The main objective of data hiding is to increase the hiding capacity for medical images [93]. One of the distinctive characteristics of medical images in comparison to nonmedical images is their large smooth area. In this paper, the authors segmented the medical images into smooth and nonsmooth areas (instead of ROI and RONI) and used a high embedding capacity method. The proposed method was based on difference expansion (DE) technique which was proposed by Tian (2003) [94]. DE is a reversible, efficient and simple method with a high embedding capacity. This method is based on calculating the average and different values of every two adjacent pixels in both horizontal and vertical directions [95]. In Tian's method, a pair of pixels (x, y) is chosen, and the following transform is performed on them:

$$l = \frac{x+y}{2}, h = x - y \tag{23}$$

where l is the average value, h is the difference value, and x and y are pixel values. The operator x produces the greatest integer equal to or less than x. This method follows two principle rules. The first one is preserving the same average value before and after data embedding. The second one is embedding the watermark bit by modifying the difference between two adjacent pixels (h). "h" is modified according to the following equations:

$$h' = \begin{cases} 2 \times h + b, & \text{expandable } h \\ \left|\frac{h}{2}\right| \times 2 + b, & \text{changeable } h \end{cases} \tag{24}$$

where b is one bit of the embedding payload B, which can be 0 or 1, and h' is the modified difference value after embedding the watermark bit (b). For an expandable and changeable h value, Eq. (24) is used to calculate h'. The h is changeable if:

$$\left|\left\lfloor\frac{\mathrm{h}}{2}\right\rfloor \times 2 + \mathrm{b}\right| \leq \min(2(255-\mathrm{l}), 2\mathrm{l}+1) \tag{25}$$

and h is expandable if:

$$|2 \times \mathrm{h} + \mathrm{b}| \leq min(2(255 - l), 2l + 1) \tag{26}$$

Finally, the embedding process is completed by using the inverse transform function that is given in Eq. (27):

$$x' = 1 + \left\lfloor\frac{h'+1}{2}\right\rfloor, y' = l - \left\lfloor\frac{h'}{2}\right\rfloor \tag{27}$$

where x' and y' are new pixel values after embedding the watermark bit (b). This procedure is continued until all payloads B are embedded into the original image and a watermarked image is obtained.

The other paper with data hiding purpose is presented in reference [96]. In this paper, the watermark was embedded into the area near to the ROI, but not inside the region. This method can preserve the quality of the image in the ROI, but would not protect the area against attack. The best PSNR is 22.36 dB after embedding 5.9 kb data.

Data Hiding and Authentication

In [90], the authors proposed a hybrid method to achieve ROI authentication, tamper localization, recovering the tampered area, and hiding patient information. In this paper, the input DICOM image was divided into ROI and RONI. Then, by means of DE (which is a reversible method), patient information and ROI hash message were embedded into the ROI. Secondly, by using a robust technique (based on DWT), recovery data, which included the ROI embedding map, the average value of blocks inside ROI, and a compressed form of ROI, were inserted into the RONI. Finally, by means of DWT, a second watermark was embedded into the border of RONI. This watermark contained information on the vertices to define ROI and the number of bits in the second watermark. The PSNR of the watermarked image changes from 69.7 to 65.2 dB by increasing the watermark from 104.1 to 413.8 kb. This method shows acceptable robustness against both cropping attack and salt and pepper noise. A weakness of this method is the manual selection of ROI in the embedding part. Furthermore, this method embeds the EPR in the ROI by means of a fragile watermark, and this fragile watermark may not be an appropriate method for embedding the EPR. This is because the EPR is important information and fragile methods cannot preserve it against attacks.

In [97], the author used cryptography and watermarking in a single system in a way that embeds an encrypted version of the patient information. In this method, the corrupted details of the medical image after watermarking were recovered by means of reversible property. The best PSNR after embedding the watermark information reached to 59.8 dB. Advantages of this method are simplicity, high capacity, high security, and reversible quality of the patient information. However, this method is incapable of handling overflow or under flow and only supports 8-bit images. The other disadvantage of this method is the use of a symmetric key for cryptography, which has lower security than an asymmetric key.

In [8], a blind hybrid watermarking method was used. The robust watermark is made up of patient information, doctor identification code, and LSBs of the region of interest, which after encryption were embedded into the RONI of the medical image. The fragile watermark was a binary pattern and was embedded on ROI for integrity control. In this method, instead of using histogram modification for preventing the underflow or overflow, a location map was generated and the suspect block was left without watermarking. The evaluation method for quality measurement of watermarked image was WPSNR. As for the performance, the watermarked image shows a good WPSNR of around 60 dB, but this method is not robust against attacks and the given example does not show acceptable results.

Summary

Preserving security and authenticity of medical images has become a necessity since the ever-increasing distribution of digital medical images between clinical centers and hospitals. This manifests through the widespread usage of telemedicine, teleradiology, telediagnosis, and teleconsultation. Over previous years, various medical watermarking algorithms have been proposed by a number of different researchers in this field, but each proposed method has a number of associated drawbacks as well as strengths. In this paper, we have demonstrated a comprehensive survey on medical image watermarking and discussed important issues relevant to each method. At first, the main framework of the security system is depicted, and the location of digital watermarking is shown in the scheme. In this paper, we explained the essential parts of the typical watermarking system, along with an analysis of different attacks, applications, and requirements of digital watermarking. Afterwards, the advantages and disadvantages of various transform techniques used in watermarking algorithms were discussed. During the course, useful metrics to measure the quality of watermarked image and accuracy of extracted watermark were presented. We also illustrated the importance of medical watermarking in general, discussing the advantages it holds. Finally, we presented a number of medical watermarking methods with explanations and comparisons drawn between them.

Acknowledgments The authors would like to acknowledge Universiti Teknologi Malaysia (UTM) for providing facilities and resources to get this work done. Also many thanks to the Research Management Center (RMC) of Universiti Teknologi Malaysia as well as Malaysian International Scholarship (MIS) for funding and supporting this research and providing excellent research environment in which this work was conducted and the scientific research targets fully accomplished.

References

1. Kuang LQ, Zhang Y, Han X: A Medical image authentication system based on reversible digital watermarking, in Information Science and Engineering (ICISE), 2009 1st International Conference. pp 1047–1050, 2009.
2. Bhatnagar G, Jonathan WU QM: Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform. Futur Gener Comput Syst 29(1):182–195, 2013
3. Pan W, Coatrieux G, Cuppens-Boulahia N, Cuppens F, Roux C: Medical image integrity control combining digital signature and lossless watermarking, in Data Privacy Management and Autonomous Spontaneous Security In: Garcia-Alfaro J, et al Eds. Springer Berlin: Heidelberg, 2010, pp 153–162.
4. Zain JM, Clarke M: Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. Int J Comput Sci Netw Secur 7(9):19–28, 2007
5. Wu N-I, Hwang M-S: Data hiding current status and key issues. Int J Netw Secur 4(1):1–9, 2007
6. Heylena K, Dams T: An image watermarking tutorial tool using matlab. Mathematics of Data/Image Pattern Recognition, Compression, and Encryption with Applications XI, Proc. of SPIE 2008. 7075, 70750D: p. 1–12.
7. Mohanty SP, Ramakrishnan KR: A dual watermarking technique for images, in Proceedings of the 7th ACM International Multimedia. ACM Press, 1999, pp 49–51.
8. Memon NA, Chaudhry A, Ahmad M, Keerio ZA: Hybrid watermarking of medical images for ROI authentication and recovery. Int J Comput Math 88(10):2057–2071, 2011
9. Jabade VS, Gengaje SR: Literature review of wavelet based digital image watermarking techniques. Int J Comp Appl 31(1):28–35, 2011
10. Memon NA, Gilani SAM: Watermarking of chest CT scan medical images for content authentication. Int J Comput Math 88(2):265–280, 2010
11. Kaur M, KAUR R: Reversible watermarking of medical images authentication and recovery-a survey. J Inf Oper Manag 3(1):241–244, 2012
12. Cheddad A, Condell J, Curran K, Mc Kevitt P: Digital image steganography: Survey and analysis of current methods. Signal Process 90(3):727–752, 2010
13. Mohanty SP: Digital Watermarking : A Tutorial Review. 1999.
14. Adnan WAW, Hitarn S, Abdul-Karim S, TamJis MR: A review of image watermarking, in Research and Development, 2003. SCORED 2003. Proceedings. Student Conference. pp 381–384, 2003.
15. Memon NA: Watermarking of medical images for content authentication and copyright protection, in Computer Science and Engineering. 2010, GIK Institute of Engineering Sciences and Technology Topi: Swabi, pp 1–166.
16. Hajjaji MA, Mtibaa A, Bourennane E-B: A watermarking of medical image : new approach based on “multi-layer” method. Int J Comp Sci Issues (IJCSI) 8(4):33–41, 2011

17. Le THN, Nguyen KH, Le HB: Literature survey on image watermarking tools, watermark attacks, and benchmarking tools, in Second International Conferences on Advances in Multimedia, IEEE Computer Society, 2010, pp 67–73.
18. Hanhan AHAM: Digital image watermarking, in Faculty of Engineering Electrical Engineering Department. AN-Najah National University, 2011.
19. Navas KA, Sasikumar M: Survey of medical image watermarking algorithms, in International Conference: Sciences of Electronic Technologies of Information and Telecommunications. TUNISIA, 2007, pp 1–6.
20. Wenyin Z, Shih FY: Semi-fragile spatial watermarking based on local binary pattern operators. Opt Commun 284(16–17):3904–3912, 2011
21. Van Schyndel RG, Tirkel AZ, Osborne CF: A digital watermark, in Image Processing Proceedings. (ICIP), IEEE Int Conf 86–90,1994.
22. Badran EF, Sharkas MA, Attallah OA: Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images, in Radio Science Conference, NRSC, National, 2009, pp 1–8.
23. Celik MU, Sharma G, Tekalp AM, Saber E: Lossless gneralized-LSB data embedding. IEEE Trans Image Process 14(2):253–266, 2005
24. Agung BWR, Adiwijaya, Permana FP: Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression, in Communication, Networks and Satellite (ComNetSat), 2012 IEEE International Conference. pp 167–171, 2012.
25. Dehkordi AB, Esfahani SN, Avanaki AN: Robust LSB watermarking optimized for local structural similarity, in Electrical Engineering (ICEE), 19th Iranian Conference. pp 1–1, 2011.
26. Bamatraf A, Ibrahim R, Salleh MNBM: Digital watermarking algorithm using LSB, in Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference. pp 155–159, 2010.
27. Chang JD, Chen BH, Tsai CS: LBP-based fragile watermarking scheme for image tamper detection and recovery, in Next-Generation Electronics (ISNE), 2013 IEEE International Symposium. pp 173–176, 2013.
28. Shu, L., F. Wei, A.C.S. Chung, and Y. Dit-Yan, Facial expression recognition using advanced local binary patterns, yallis entropies and global appearance features, in Image Processing, 2006 I.E. Int Conf 665–668, 2006.
29. Ahonen T, Hadid A, Pietikäinen M: Face recognition with local binary patterns. In T. Pajdla, J. Matas (Eds.) Computer Vision - ECCV 2004, Springer Berlin Heidelberg. pp 469–481, 2004.
30. Wenhua M, Lei H, Changping L: Advanced local binary pattern descriptors for crowd estimation. in Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on. 2008.
31. Ni Z, Shi Y-Q, Ansari N, Su W: Reversible data hiding. IEEE Trans Circ Syst V Technol 16(3):354–362, 2006
32. Solachidis V, Pitas L: Circularly symmetric watermark embedding in 2-D DFT domain. Image Process IEEE Trans 10(11):1741–1753, 2001
33. Kaushik AK: A novel approach for digital watermarking of an image using DFT. Int JElectronComp Sci Eng 1(1):35–41, 2012
34. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H: Robust watermarking method in DFT domain for effective management of medical imaging. SIViP pp 1–16, 2013.
35. Ramkumar M, Akansu AN, Alatan AA: A robust data hiding scheme for images using DFT, in Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference. pp 211–215, 1999
36. Ruanaidh JJKO, Dowling WJ, Boland FM: Phase watermarking of digital images, in Image Processing, 1996. Proc Int Conf pp. 239–242,1996.
37. Das S. Kundu M: Hybrid Contourlet-DCT Based Robust Image Watermarking Technique Applied to Medical Data Management. In: Kuznetsov S, Mandal D, Kundu M, Pal S (Eds.) Pattern Recognition and Machine Intelligence, Springer Berlin Heidelberg. pp 286–292, 2011.
38. Kundur D, Hatzinakos D: Digital watermarking for telltale tamper proofing and authentication. Proc IEEE 87(7):1167–1180, 1999
39. Hernandez JR, Amado M, Perez-Gonzalez F: DCT-domain watermarking techniques for still images: detector performance analysis and a new structure. IEEE Trans Image Process 9(1):55–68, 2000
40. Yang B, Schmucker M, XiaMu N, Busch C, Sun S: Reversible image watermarking by histogram modification for integer DCT coefficients, in Multimedia Signal Processing, IEEE 6th Workshop pp 143–146, 2004.
41. Yang B, Schmucker M, Funk W, Busch C, Sun S: Integer DCT-based reversible watermarking for images using compounding technique. Proc SPIE 5306:405–415, 2004
42. Rohani M, Avanaki AN: A watermarking method based on optimizing SSIM index by using PSO in DCT domain, in Computer Conference, 2009. CSICC 2009. 14th International CSI pp 418–422,2009.
43. Langelaar GC, Setyawan I, Lagendijk RL: Watermarking digital image and video data. A state-of-the-art overview. Signal Proc Mag IEEE 17(5):20–46, 2000
44. Ali M, Ahn CW, Pant M: A robust image watermarking technique using SVD and differential evolution in DCT domain. Opt Int J Light Electron Opt 125(1):428–434, 2014
45. Li J, Du W, Bai Y, Chen YW: 3D-DCT based zero-watermarking for medical volume data robust to geometrical attacks, in Wireless Communications and Applications. In: Sénac P, Ott M, Seneviratne A Eds. Springer Berlin: Heidelberg, 2012, pp 433–444.
46. Hyung-Kyo L, Hee-Jung K, Ki-Ryong K, Jong-Keuk L: ROI medical image watermarking using DWT and bit-plane, in Asia-Pacific Conference on Communications, Perth, Western Australia p. 512–515,2005.
47. Long M, Changjun L, Shuni S: Digital watermarking of spectral images using DWT-SVD, in Communications, Circuits and Systems Proceedings, 2006 International Conference on p. 15–18,2006.
48. Kasmani SA, Naghsh-Nilchi A: A new robust digital image watermarking technique based on joint DWT-DCT transformation, in Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on, 2008, pp 539–544.
49. Wang M-S, Chen W-C: A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. Comp Stand Interfaces 31(4):757–762, 2009
50. Kalra GS, Talwar R, Sadawarti H: Robust blind digital image watermarking using DWT and dual encryption technique, in Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on 225–230,2011.
51. Keyvanpour M-R, Merrikh-Bayat F: Robust dynamic block-based image watermarking in DWT domain. Procedia Comput Sci 3:238–242, 2011
52. Makhloghi M, Tab FA, Danyali H: A new robust blind DWT-SVD based digital image watermarking, in Electrical Engineering (ICEE), 2011 19th Iranian Conference on. Tehran pp 1–5,2011.
53. Giakoumaki A, Pavlopoulos S, Koutouris D: A medical image watermarking scheme based on wavelet transform, in Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE. pp 856–859, 2003.
54. Wen-Nung L, Tze-Liang H, Guo-Shiang L: Verification of image content integrity by using dual watermarking on wavelets domain, in Image Processing, 2003. ICIP 2003. Proceedings. Int Conf pp II-487-490,2003.

55. Guorong X, Chengyun Y, Yizhan Z, Shi YQ, Zhicheng N: Reversible data hiding based on wavelet spread spectrum, in Multimedia Signal Processing, 2004 I.E. 6th Workshop on pp 211–214,2004.
56. Kaarna A, Parkkinen J: Multiwavelets in watermarking spectral images, in Geoscience and Remote Sensing Symposium, 2004. IGARSS '04. Proceedings. 2004 I.E. Int pp 3225–3228,2004.
57. Kamstra L, Heijmans HJAM: Reversible data embedding into images using wavelet techniques and sorting. Image Process IEEE Trans 14(12):2082–2090, 2005
58. Na L, Xiaoshi Z, Yanling Z, Huimin W, Shifeng L: Robust algorithm of digital image watermarking based on Discrete Wavelet Transform, in Electronic Commerce and Security, 2008 Int Symp 942–945,2008.
59. Lin T-C, Lin C-M: Wavelet-based copyright-protection scheme for digital images based on local features. Inf Sci 179(19):3349–3358, 2009
60. Lin WH, Wang YR, Horng SJ: A block-based watermarking method using wavelet coefficient quantization, in Algorithms and Architectures for Parallel Processing. In: Hua A, Chang SL Eds. Springer Berlin: Heidelberg, 2009, pp 156–164.
61. Memon NA, Gilani SAM: Adaptive data hiding scheme for medical images using integer wavelet transform, in Emerging Technologies, 2009. ICET 2009. International Conference on. Islamabad, 2009, pp. 221–224.
62. Youngseock L, Jihah N, Jongweon K: Digital image watermarking using bidimensional empirical mode decomposition in wavelet domain, in Multimedia, 2009. ISM '09. 11th IEEE International Symposium on pp. 583–588,2009.
63. Arsalan M, Malik SA, Khan A: Intelligent reversible watermarking in integer wavelet domain for medical images. J Syst Softw 85(4):883–894, 2012
64. Agreste S, Puccio L: Wavelet-based watermarking algorithms: theory, applications and critical aspects. Int J Comput Math 88(9):1885–1895, 2011
65. Giakoumaki A, Pavlopoulos S, Koutsouris D: Multiple image watermarking applied to health information management. Inf Technol Biomed IEEE Trans 10(4):722–732, 2006
66. Selesnick IW, Baraniuk RG, Kingsbury NC: The dual-tree complex wavelet transform. Signal Process Mag IEEE 22(6):123–151, 2005
67. Kingsbury N: The dual-tree complex wavelet transform: a new efficient tool for image restoration and enhancement, in Proc. EUSIPCO pp 319–322,1998.
68. Kingsbury N: The dual-tree complex wavelet transform: a new technique for shift invariance and directional filters, in Proc. 8th IEEE DSP Workshop: Bryce Canyon, 1998, pp 319–322.
69. Rahimi F, Rabbani H: A dual adaptive watermarking scheme in contourlet domain for DICOM images. BioMed Eng OnLine 10(1): 1–18, 2011
70. Do MN, Vetterli M: Contourlets: a directional multiresolution image representation, in Image Processing. 2002. Proceedings. 2002 Int Conf pp I-357-360, 2002.
71. Do MN, Vetterli M: The contourlet transform: an efficient directional multiresolution image representation. Image Process IEEE Trans 14(12):2091–2106, 2005
72. Khalighi S, Tirdad P, Rabiee HR: A contourlet-based image watermarking scheme with high resistance to removal and geometrical attacks. EURASIP J Adv Signal Process 2010:1–13, 2010
73. Aslantas V: An optimal robust digital image watermarking based on SVD using differential evolution algorithm. Opt Commun 282(5): 769–777, 2009
74. Mansouri A, Mahmoudi A: Aznaveh, and F. Torkamani Azar, Secure Digital Image Watermarking Based on SVD-DCT Advances in Computer Science and Engineering. In: Sarbazi-Azad H, et al Eds. Springer Berlin: Heidelberg, 2009, pp 645–652.
75. Al-Nuaimy W, El-Bendary MAM, Shafik A, Shawki F, Abou-El-azm AE, El-Fishawy NA, Elhalafawy SM, Diab SM, Sallam BM, Abd FE: El-Samie, and H.B. Kazemian, *An SVD audio watermarking approach using chaotic encrypted images*. Digit Signal Proc 21(6): 764–779, 2011
76. Tsai H-H, Jhuang Y-J, Lai Y-S: An SVD-based image watermarking in wavelet domain using SVR and PSO. Appl Soft Comput 12(8): 2442–2453, 2012
77. Ali M, Ahn CW: An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. Signal Process 94:545–556, 2014
78. Liu R, Tan T: An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimed 4(1):121–128, 2002
79. Lei BY, Soon IY, Li Z: Blind and robust audio watermarking scheme based on SVD–DCT. Signal Process 91(8):1973–1984, 2011
80. Lai C-C: An improved SVD-based watermarking scheme using human visual characteristics. Opt Commun 284(4):938–944, 2011
81. Patra JC, Phua JE, Bornand C: A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digit Signal Proc 20(6):1597–1611, 2010
82. Mansouri A, Mahmoudi Aznaveh A, Torkamani Azar F: SVD-based digital image watermarking using complex wavelet transform. Sadhana 34(3):393–406, 2009
83. Faragallah OS: Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. Int J Electron Commun (AEU) 67(3):189–196, 2013
84. Gonzalez RC, Woods RE: Digital image processing, 3rd Edition. Prentice-Hall, Inc,2006.
85. Muharemagic E, Furht B: Survey of watermarking techniques and applications. 2006 pp 1–30.
86. Guo X, Zhuang TG: A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22(1):53–64, 2009
87. Chang C-Y, Wang H-J, Pan S-W: A robust DWT-based copyright verification scheme with Fuzzy ART. J Syst Softw 82(11):1906–1915, 2009
88. Gunjal BL, Mali SN: ROI Based embedded watermarking of medical images for secured communication in telemedicine. Int J Comp Commun Eng pp 293–298,2012
89. Kutter M, Petitcolas FAP: A fair benchmark for image watermarking systems. Electronic Imaging '99. Security and Watermarking of Multimedia Contents: Sans Jose, 1999, **3657**:226–239.
90. Al-Qershi OM, Khoo BE: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. J Digit Imaging 24(1):114–125, 2011
91. Zain J, Baldwin L, Clarke M: Reversible watermarking for authentication of DICOM images, in Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society pp 3237–3240,2004.
92. Lin C-H, Yang C-Y, Chang C-W: Authentication and protection for medical image, vol. 6422. Springer, Berlin Heidelberg, 2010, pp 278–287
93. Al-Qershi OM, Khoo BE: High capacity data hiding schemes for medical images based on difference expansion. J Syst Softw 84(1): 105–112, 2011
94. Tian J: Reversible data embedding using a difference expansion. Circ Syst V Technol IEEE Trans 13(8):890–896, 2003
95. Yeo D-G, Lee H-Y, Kim BM: High capacity reversible watermarking using differential histogram shifting and predicted error compensation. J Electron Imaging 20(1):013001–1-11, 2011
96. Wakatani A: Digital watermarking for ROI medical images by using compressed signature image, in System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on. pp 2043–2048,2002.
97. Viswanathan P, Krishna PV: Fusion of cryptographic watermarking medical image system with reversible property, in Computer Networks and Intelligent Computing.In: Venugopal KR, Patnaik LM Eds. Springer Berlin: Heidelberg, 2011, pp 533–540.