Digital Watermarking: Applicability for Developing Trust in Medical Imaging Workflows State of the Art Review

Asaad F. Qasim[1, 2], Farid Meziane[1] and Rob Aspin[1]

[1] School of Computing, Science and Engineering, University of Salford, Greater Manchester, M5 4WT, UK

[2] Ministry of Higher Education and Scientific Research, Baghdad, Iraq

A.Qasim@edu.salford.ac.uk, F.Meziane@salford.ac.uk, R.Aspin@salford.ac.uk

Abstract

Medical images can be intentionally or unintentionally manipulated both within the secure medical system environment and outside, as images are viewed, extracted and transmitted. Many organisations have invested heavily in Picture Archiving and Communication Systems (PACS), which are intended to facilitate data security. However, it is common for images, and records, to be extracted from these for a wide range of accepted practices, such as external second opinion, transmission to another care provider, patient data request, etc. Therefore, confirming trust within medical imaging workflows has become essential. Digital watermarking has been recognised as a promising approach for ensuring the authenticity and integrity of medical images. Authenticity refers to the ability to identify the information origin and prove that the data relates to the right patient. Integrity means the capacity to ensure that the information has not been altered without authorisation.

This paper presents a survey of medical images watermarking and offers an evident scene for concerned researchers by analysing the robustness and limitations of various existing approaches. This includes studying the security levels of medical images within PACS system, clarifying the requirements of medical images watermarking and defining the purposes of watermarking approaches when applied to medical images.

Keywords: *Medical Imaging; Digital Watermarking; Reversible Watermarking; Integrity; Authentication*

Contents

1. Introduction and Motivation

Through the exponential development of modern technologies in the areas of communication and computer networks, the conventional diagnosis has mostly migrated to a technology enabled e-diagnosis. Most Hospital Information Systems (HIS) and medical imaging systems generate and store medical images in different modalities such as X-ray, Ultrasound, Magnetic Resonance Imaging (MRI) and Computerised Tomography (CT). These images are usually managed within a digital workflow based on the Digital Imaging and Communications in Medicine (DICOM) standard [1].

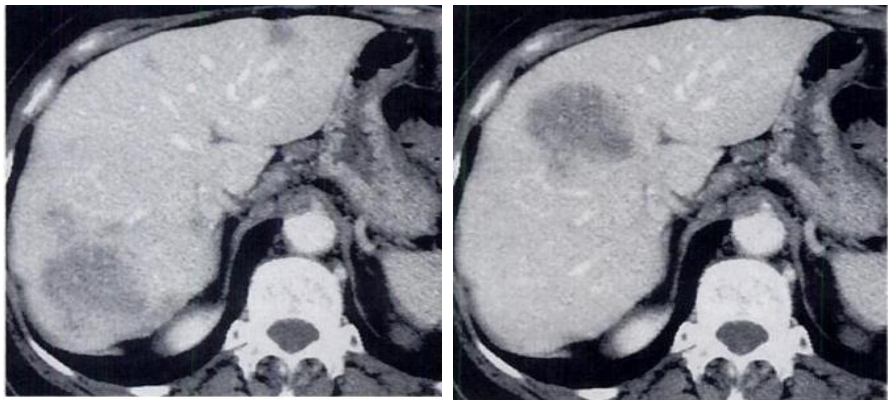
1.1. Introduction

In healthcare systems, a hierarchical scheme can be considered as a pyramid with hospitals at the base and the general Picture Archiving and Communication Systems (PACS) at its top. Images are taken in a hospital and are immediately saved in the PACS. Within few minutes, these images are transferred to an upper PACS, which collects data coming from hospitals belonging to the same division. These files stay in this system for some hours, typically staying for the night, during which time their integrity is not maintained accurately. Then, these files are transmitted to the hierarchically higher PACS until they reach the top-PACS. In the top-PACS, the data are eternally saved and collected in tapes, physical drives or optical supports with associated hash signature, to become ready for the diagnostic workflow operations. Furthermore, the data are encrypted utilising the secret key of the PACS manager. This operation is called consolidation [2].

For security purposes, the authorised archive is managed off-line, while available data are kept on the top-PACS discs. In most situations, it is difficult to foretell the security issues for each intermediate system, and the data could be altered intentionally or unintentionally: this is the first serious case. Moreover; the data are not directly consolidated when reaching the top-PACS but after approximately 24/36 hours. During this time, PACS professionals, which have access to both the metadata as well as the image's pixels due to the structure of DICOM images, are permitted to edit the files as needed for adjusting potential flaws in patients' data. This matter indicates to the second significant case which allows the malicious PACS manipulation to modify the images before the consolidation process. Hospital's system can retrieve the images from the top-PACS when requested by the physicians. In the case of expected claims, such as regular medical reports, files are pre-fetched in the hospital's PACS, e.g. through night-time or transmitted as soon as possible. The separation between the legal archive (secured data) and

the available data (used by clinicians) points out the last crucial case of PACS scenario. If the medical images have been modified in the top-PACS discs, there will be no possibility to automatically discover the manipulation because the authorised archive is saved off-line and the data are not quickly accessible. Definitely, it will be possible to discover the alterations that have been applied to the data in PACS discs, but it might be too late for patients' safety [2].

Furthermore, transmitting medical images between hospitals, located at various locations and different administrative organisations has become a common practice for many reasons, such as diagnosis, treatment, distance learning, training purposes, teleconferences between clinicians and medical consultation between physicians and radiologists [3]. Malicious alterations on the medical images are feasible for getting counterfeit health insurance demands by some insurance company or for hiding medical situations for gaining personal advantages [4]. For instance, *Fig. 1*. shows a liver disease of a patient which is altered by changing the position of the infected region of the liver by using available software (e.g. Adobe Photoshop) [5]. Many other cases of manipulation can be applied, but the issue is how they can be detected? Actually, by merely seeing the images, detecting such reasonable manipulations that include entirely forged abnormalities would be impossible.



(a) Original image (b) Manipulated image

Fig. 1: CT image altered by changing the position of the infected region of the liver [5].

1.2. Motivation for Medical Image Watermarking

Security requirements of medical information are mostly derived from legislative rules and strong ethics of the security policy, that professionals and concerned patients must follow [6]. This requires three mandatory features: confidentiality, reliability and availability. Confidentiality indicates that only the authorised people, in the normally scheduled situations,

have access to the data. Reliability may be decomposed into two aspects: *i) Integrity* which verifies that the information has not been changed, and, *ii) Authentication* which ensures that the data belongs to the right patient and is delivered from the verified source. Availability defines the capability of the authorised users to utilise the information system in the normally scheduled situations of access and practice [7].

Confidentiality of the image data can be accomplished by applying many techniques such as encryption, access control and firewall. Integrity can be fulfilled by encrypting the images when sharing them over the network. Authentication needs measures being implemented to discover whether confidentiality and/or the integrity of the data has been breached [8].

Two techniques are commonly employed to ensure integrity and authenticity within the data; metadata and digital watermarking [4, 9]. In medical imaging, the metadata refers to the data stored along with the image [9]. The common approach of metadata inclusion is Part 15 of the DICOM standard, where the digital signature data is placed in its header [1]. The metadata has also been employed to offer confidentiality, using the data of DICOM header to encrypt the images [10]. Existing metadata techniques do not provide a robust link between the medical image and its metadata. It is, therefore, almost easy to decay the metadata rendering the image unreliable. This shortcoming can be fixed with digital watermarking [9]. Digital watermarking is a technique that hides data known as a watermark into the digital object such that the concealed watermark can then be detected/extracted to make a confirmation about the object [11]. Image watermarking is one of the earliest techniques to improve integrity and authenticity of the digital data. In recent times, authentication is one of the main watermarking requirements in medical applications [12].

1.3. Digital Watermarking Requirements

The essential requirements for designing a general watermarking scheme can be described as follows [13]:

- **Fidelity**

It is the most important feature in the watermarking system which defines the similarity between both the original and watermarked images. The watermark should remain invisible to human perception although the incidence of slight distortions in the host image [14].

- **Robustness**

This requirement signifies the ability of the watermarking scheme to resistant to different image processing attacks. These attacks aim to frustrate the watermark from fulfilling its intended purpose. The wide class of existing attacks can be categorized into four groups: removal, geometric, protocol and cryptographic attacks [15, 16]. Watermarking algorithms cannot survive with all types of attacks. Some of the algorithms are strong against several attacks. However, they fail to comply with other stronger operations. Furthermore, not all applications require robust watermark, but in some applications, it is needed to be fragile [17].

- **Data Payload (Capacity)**

This property refers to the number of bits that can be concealed without affecting the image quality. This factor defines how many bits can be embedded as a watermark so that it can be efficiently discovered through the extraction process. The embedding capacity depends on the required application. Several watermarking applications have various capacity requirements [18].

- **Security**

The capability of resisting the intentional attacks. A watermarking scheme is supposed to be secure if the unauthorised user cannot extract the watermark without having full information about the algorithm that has been used to embed the watermark. The security factor is crucial to the watermarking system, and only the authorised person can extract the watermark [19].

- **Computational Complexity**

This feature is defined as the amount of time required for embedding and extraction processes. For instance, the real-time application requires both fast and efficient algorithms. On the other hand, more computational complexity is needed for high-security applications [20].

- **Perceptibility**

This concept indicates the amount of degradation that occurs on a watermarked image when embedding the data. This feature should be as little as possible in the invisible watermarking schemes [13].

Watermarking capacity is determined by the other two significant features of the watermarking system, which are imperceptibility and robustness. The relationship between the properties of the watermarking scheme is shown in Fig. *2*. Obviously, a high capacity can be achieved by

sacrificing either robustness or imperceptibility or both. Therefore, a suitable trade-off might be found depending on the application [17].

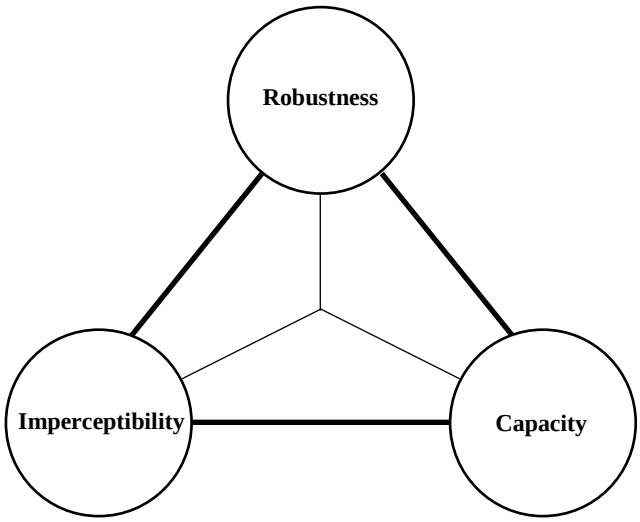


Fig. 2: The properties of the watermarking system, trade-off triangle between the three essential features: robustness, capacity and imperceptibility.

In addition to the previously mentioned requirements, some other special features are desired for medical imaging watermarking. These requirements are imperceptibility, reversibility and reliability. It is evident that developing new watermarking approaches to fulfil these requirements remains a significant and relevant research area [13].

- **Imperceptibility**

Usually referred to as invisibility or fidelity, it describes the greatest requirement of watermarking schemes. It states that the original and watermarked images should be perceptually similar [20] and might be achieved by reducing either robustness, capacity or both [19]. The standard two statistical benchmarks for estimating the perceptual level of invisibility between the original and watermarked images are Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) index [13].

- **Reversibility**

In medical fields, if an image is changed during the workflow process a collapse in trust is formed, regarding the validity of the images, with the hazard that any slight difference could lead to misdiagnosis with possible life-threatening, or legal, implications. Consequently, the necessity to strictly retrieve the original data from the watermarked image is high [21]. Reversible or lossless watermarking methods satisfy this requirement in that they guarantee

extraction of the watermark along with exactly reconstructing the unmodified original image [22]. However, a watermarked image is not distortion-free, especially in reversible techniques, but the modified image is employed as a cover for carrying out the watermark, not for diagnostic purposes and the recovered image is used for diagnosis, intervention planning, etc. [23].

- **Reliability**

This may be decomposed into two parts [24]:

- ***Integrity:*** The capability of proving that the data has not been changed without authorisation.
- ***Authentication:*** The ability to identify information origin and confirming that the data refers to the right patient.

This paper offers a review of digital watermarking schemes and compares some recent works in watermarking medical imaging to define some research issues for the future. The rest of the paper is organised as follows. Section 2 illustrates the basic principles of digital watermarking. Section 3 reviews the recently published approaches in the field of medical imaging watermarking and highlights the limitations of some of these algorithms. In section 4, evaluation benchmarks of watermarking algorithms were demonstrated. Finally, discussion and conclusions drawn from this research will be stated in sections 2.

2. Digital Watermarking

Digital watermarking is the hiding of information (the watermark) within the digital data, such that the embedded watermark can be identified or extracted later to produce a confirmation of the validity of the data [11].

2.1. Principal Components of a Watermarking System

The basic model of the digital watermarking scheme consists of three components [6, 14] as shown in *Fig. 3*:

- **Watermark Generation**

This function creates a suitable watermark according to the desired applications. In simple applications, the embedded data can be a text or another image. In the developed applications, the watermark may have particular properties based on the desired objectives. For example, in

medical applications, the watermark may need the patient information or image features to confirm the integrity and authenticity of the watermarked data.

- **Watermark Hiding**

The hiding process is done at the source end. In this step, the watermark is inserted into the original data by applying a certain algorithm and a secret key to generate the watermarked data.

- **Watermark Extracting**

The extraction process is done by reversing the implemented hiding algorithm and use the secret key and/or the original data to detect/extract the embedded watermark.

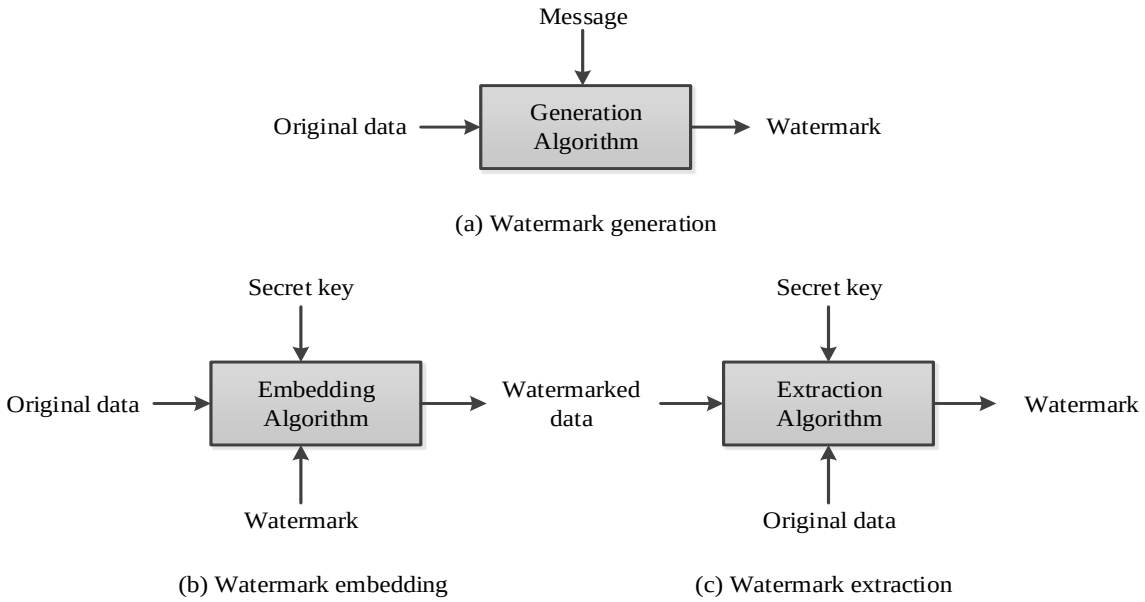


Fig. 3: Main components of watermarking schemes.

2.2. Digital Watermarking Classifications

Digital watermarking schemes can be classified into many groups in various ways (Fig. *4*), such as document type, embedding domain, perceptibility and reversibility [13]. Based on the embedding techniques, watermarking systems can be categorised into spatial and transform domain [25]. On the other hand, the watermarking methods can be divided according to human perception into visible, invisible and dual watermarking techniques. Popular examples of visible watermarks are the sealing and logos, which are placed on the images, videos and TV channels corners for content protection and ownership verification. Moreover, invisible

watermarks are hidden in such a way that they cannot be seen, but they can be removed by utilising the exact algorithm. Invisible watermarking schemes are suitable for many purposes like authentication, integrity control and ownership verification of digital files. In some application, visible and invisible watermarks can be applied together. This technique is called the dual watermarking, and in this situation, the invisible watermark is assumed as a backup for the visible one [26].

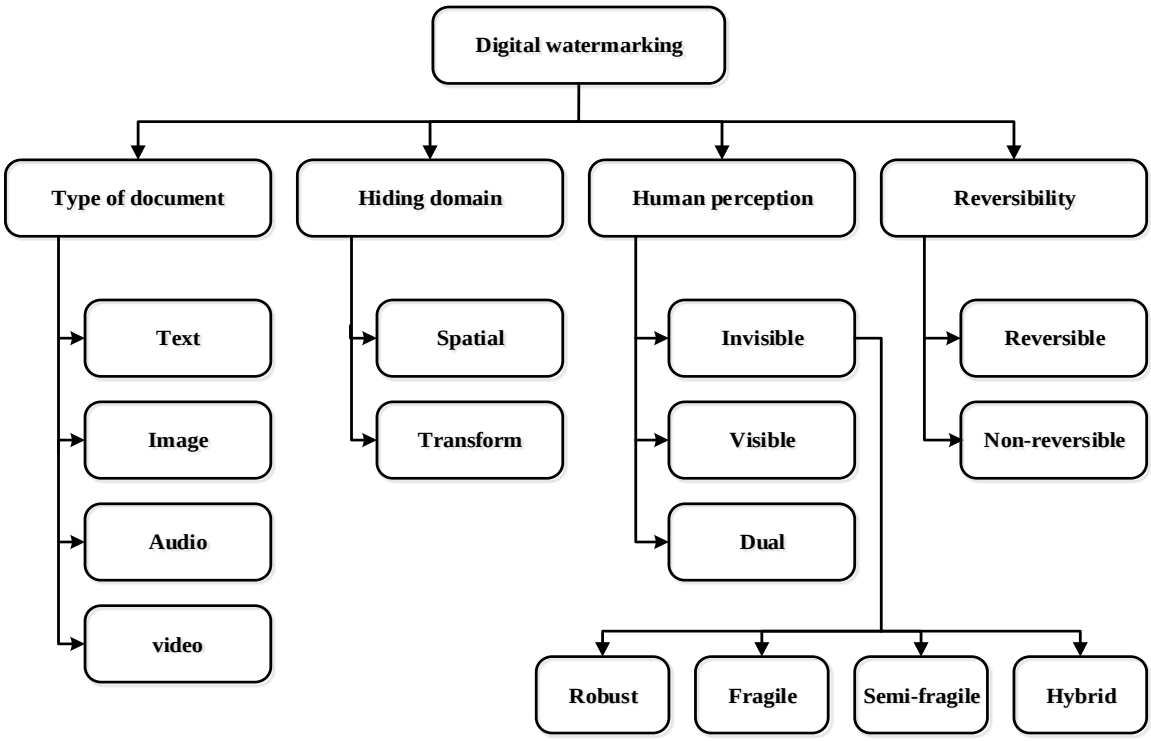


Fig. 4: Digital watermarking classifications based on the document type, domains of hiding the watermark, human perception and reversibility feature.

Invisible watermarking approaches can be further divided, based on their robustness, into four categories: robust, fragile, semi-fragile and hybrid techniques [13]. The robust system, which is typically used for copyright protection, copy control, fingerprinting and broadcast monitoring, should be able to survive against a wide range of attacks, while the fragile watermarking methods are intolerable to the smallest modifications. This technique is designed with a goal to verify the authentication and integrity of multimedia contents. The semi-fragile method is intermediate in robustness, in such that it is robust against authorised operations and fragile with unauthorised operations. This watermarking method is also used for authentication and integrity purposes [27]. Finally, the hybrid approach is a combination of fragile and robust methods to achieve the authenticity, integrity and ownership protection simultaneously [13].

In addition to the previous classifications, the reversible watermarking also called invertible or lossless watermarking is another significant feature of watermarking techniques. Compared to the traditional watermarking systems, reversible algorithms can restore both the embedded watermark and the original data exactly. This feature is a crucial requirement for many fields such as medical, military and law-enforcement applications [22].

2.3. Digital Watermarking Techniques

Current watermark embedding techniques can be divided into two main groups. The following are a brief explanation of the properties of each group.

2.3.1. Spatial Domain Techniques

In these methods, the watermark is inserted into the cover image by directly modifying the pixel values of the original image. These algorithms are simple, fast and offer high embedding capacity [25]. Also, a small watermark can be hidden several times. This advantage provides additional robustness against any attack because of the possibility of removing all watermarks is very low. Spatial domain techniques may have some benefits, but their main drawback is that they cannot survive against many operations like adding noise and lossy compression methods. Moreover, when discovering the utilised watermarking method, the hidden watermark can easily be altered by an unauthorised user [28].

2.3.1.1. Least Significant Bit

Least Significant Bit (LSB) method represents one of the earliest and simplest spatial domain techniques. It can be applied to any form of the watermarking. In this technique, the LSB of the cover image is replaced with the watermark. The watermark bits are encoded in a sequence which serves as the key. This sequence should be known to retrieve the embedded bits. As shown in *Fig. 5*, the decimal pixels value of the original image is first converted to binary. Then, the rightmost bits of each pixel are substituted by the watermark bits. Lastly, the changed binary pixels are returned to its original decimal values [29].

2.3.1.2. Local Binary Pattern

Local Binary Pattern (LBP) is a different method of spatial domain techniques. Firstly, the original image is segmented into non-overlapping square blocks. Secondly, the local pixel differences between the central pixel and its adjacent pixels in each block are calculated. Then, these pixels are utilised for embedding the watermark bits according to the rules mentioned in [30]. LBP based methods are robust against luminance variation and contrast adjustment, but

fragile with other operations like blurring and filtering. In other words, this technique is suitable for semi-fragile watermarking applications [13]. LBP operator, originally designed for effective texture analysis, object/pattern recognition and crowd estimation [31].

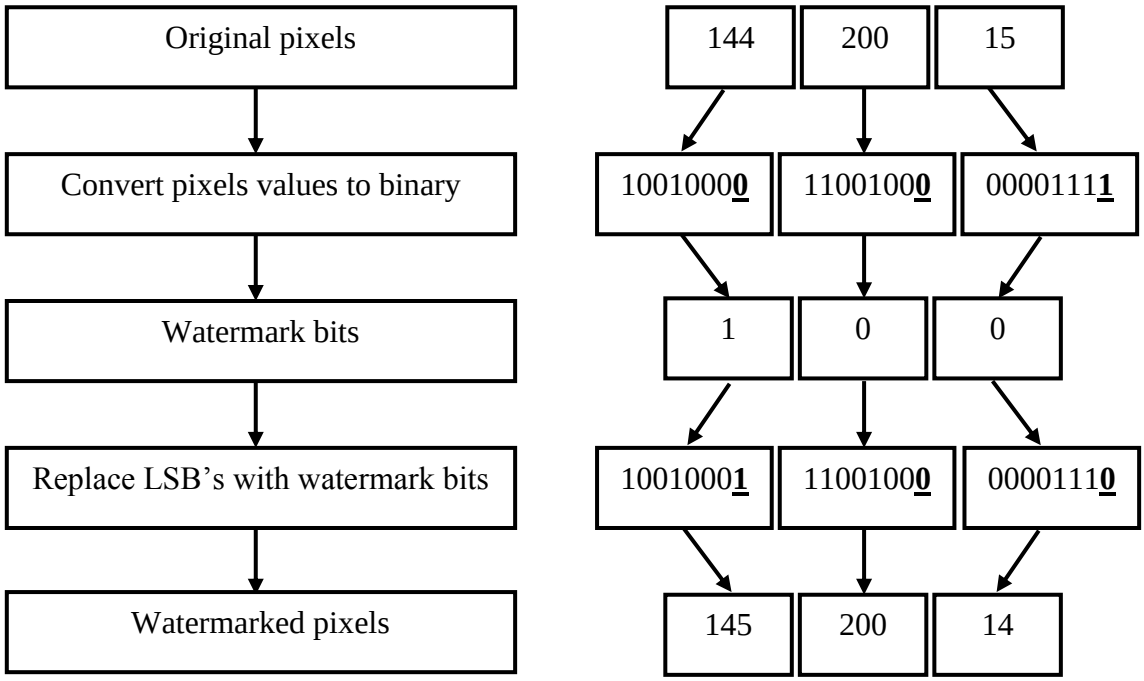


Fig. 5: LSB watermarking technique.

2.3.1.3. Histogram Modification

Another watermarking technique in the spatial domain category is the histogram modification which benefits from the global features of the host image for embedding the watermark [32]. This scheme hides the watermark by shifting the maximum and zero points (or minimum if no zero points exist) of the histogram. This method can be executed easily, but the hiding capacity is restricted by the number of maximum points that appear [33].

2.3.2. Transform Domain Techniques

Transformation techniques are applied to the original image before encoding the watermark to provide more robustness against various image processing attacks compared to the spatial domain techniques. These methods generate the transform domain coefficients. The watermarked data can be achieved by changing these coefficients [25]. The most popular transform domain techniques utilised in watermark embedding are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). DCT and DFT give the spectral description of the input image while DWT transforms the input image into predictions onto basis vectors.

2.3.2.1. Discrete Cosine Transform

DCT is one of the greatest attractive methods implemented to transform the data from the spatial domain to transform domain. It is a linear transform, which maps an n-dimensional vector to a set of n-coefficients. DCT is robust to JPEG compression because JPEG standard is based on DCT technique. However, DCT lacks resistance to strong geometric attacks like scaling, cropping, translation, rotation, etc. [18].

By applying this technique, the image will be segmented into three frequency groups: low (FL), middle (FM) and high (FH). Most of the energy is focused in the low-frequency region, while high-frequency part contains the least amount of energy. The mathematical equations of forward and inverse transform of 2D-DCT are shown in *Eq. 1* and *Eq. 2*, respectively [34].

$$C(u,v) = \frac{2}{\sqrt{mn}}\alpha(u)\alpha(v)\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} f(x,y) * cos\frac{(2x+1)u\pi}{2m} * cos\frac{(2y+1)v\pi}{2n} \qquad (1)$$

$$f(x,y) = \frac{2}{\sqrt{mn}}\sum_{u=0}^{m-1}\sum_{v=0}^{n-1} \alpha(u)\alpha(v)f(x,y) * cos\frac{(2x+1)u\pi}{2m} * cos\frac{(2y+1)v\pi}{2n} \qquad (2)$$

Where *m* and *n* define the block size, *f(x, y)* represents the spatial domain pixel value, *C (u, v)* is the DC coefficient and $\alpha(u), \alpha(v)$ can be calculated in *Eq. 3*:

$$\alpha(u), \alpha(v) = \begin{cases} 1/\sqrt{2} & if\ u,v = 0 \\ 1 & else \end{cases} \qquad (3)$$

The DC coefficients are used for hiding the watermark to prevent changing the significant part of the image because they contain middle sub-band coefficients of the DCT. All other coefficients are titled the AC coefficients [13].

2.3.2.2. Discrete Wavelet Transform

DWT is a vigorous mathematical tool that has been utilised in various applications. It provides a proper spatial localisation and has multi-resolution characteristics, which are similar to the theoretical models of the human visual system. This method is robust against median and low-pass filtering. However, it is not strong to geometric attacks [18]. DWT separates the image hierarchically into four sub-bands: LL, HL, LH and HH as shown in *Fig. 6*, where L=low and H=high. The LL sub-band includes an approximation of the image, while the other three sub-bands covers the missing details. Moreover, the LL sub-band resulted from any stage can also

be decomposed continuously to gain another level until reaching the required number of levels based on the application [35].

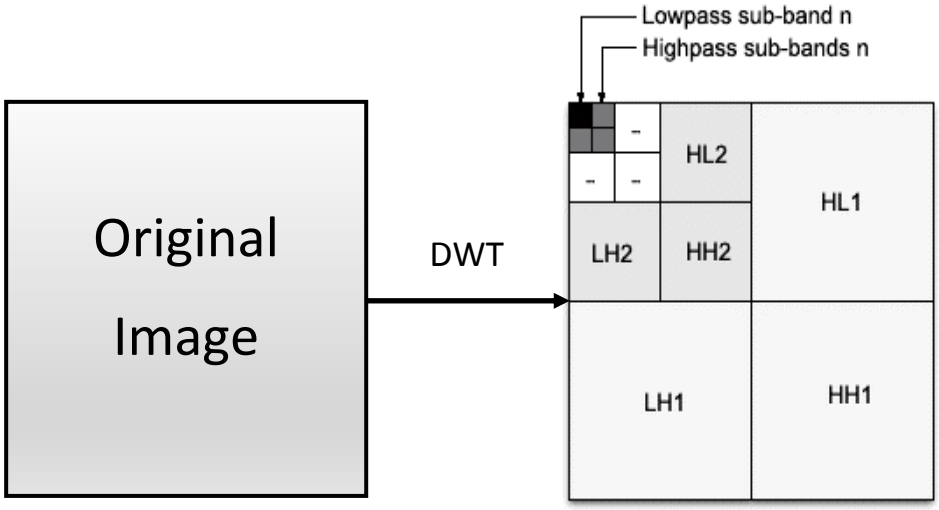


Fig. 6: Four levels of DWT decomposition which divide the input image into four sub-bands in each level (LL, HL, LH and HH).

In digital watermarking systems, lower decomposition levels of the image, which contain a lower amount of energy, are more suitable to modifications. This energy is calculated by *Eq. 4* [13]:

$$E_k = \frac{1}{N_k M_k} \sum_i \sum_j |I_k(i,j)| \qquad (4)$$

Where *k* is the level of the decomposition, *Nk* and *Mk* are the dimensions of the sub-band, and *Ik* indicates the coefficients of the corresponding sub-band.

2.3.2.3. Discrete Fourier Transform

DFT denotes the most popular technique to convert the images from the spatial domain to transform domain [36]. It offers more robustness against geometric attacks. DFT decomposes an image in sine and cosine form. Therefore, watermark embedding can be implemented in two ways: direct hiding and the template based hiding [37]. Consider $f(x,y)$ an image of size $M \times N$, with $x = 0,1,2,\ldots,M-1$, and $y = 0,1,2,\ldots,N-1$. The forward discrete Fourier transform and its inverse transform are shown in *Eq. 5* and *Eq. 6*, respectively [13]:

$$F(u,v) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y) e^{-j2\pi\left(\frac{ux}{N}+\frac{vy}{M}\right)} \qquad (5)$$

$$= R(u,v) + jI(u,v)$$

$$f(x,y) = \frac{1}{NM}\sum_{u=0}^{N-1}\sum_{v=0}^{M-1} F(u,v)e^{j2\pi\left(\frac{ux}{N}+\frac{vy}{M}\right)} \quad (6)$$

Where: *F(u,v)* is the DFT coefficient, *u*=0,1,2,…,*M*−1, and *v*=0,1,2,…,*N*−1, *R(u,v) and I(u,v)* are the real and imaginary parts of DFT, respectively.

The polar of the DFT [13] can also be explained by *Eq. 7*:

$$F(u,v) = |F(u,v)|e^{j\emptyset(u,v)} \quad (7)$$

Where $|F(u,v)|$ and $\phi(u,v)$ represent amplitude and phase components respectively, which can be calculated by *Eq. 8* and *Eq. 9*:

$$|F(u,v)| = [R^2(u,v) + I^2(u,v)]^{1/2} \quad (8)$$

$$\emptyset(u,v) = tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \quad (9)$$

The watermark can be embedded in the amplitude part, which contains little information about the image, to reduce the visual distortion [36].

Table 1 provides a comparison between the spatial and transform domains techniques regarding the embedding domain, robustness, imperceptibility, capacity, complexity and processing time.

Table 1: Comparison between spatial and transform domains

	Spatial domain	**Transform domain**
Embedding technique	Directly into the image pixels	Into the transform coefficients
Robustness	Low	High
Imperceptibility	Highly controllable	Lower controllable
Capacity	High	Low
Complexity	Low	High
Processing time	Low	High

3. State of the Art

In this section, a list of significant published work in the area of medical images watermarking will be reviewed. This survey aims to highlight the advantages and limitations of recently published techniques concerning the medical images integrity and authenticity and Electronic Patient Record (EPR) data hiding. It is also aimed to provide a path for future researchers to address the limitations of existing watermarking techniques.

3.1. Schools of Thought in Medical Image Watermarking

There are three kinds of medical images watermarking approaches; classical methods, a Region of Interest (ROI) and Region of Non Interest (RONI) watermarking approaches and reversible watermarking techniques. Whatever algorithm is used, the computational complexity should not cause a delay in the clinician's time [38]. The following subsections discuss the existing digital watermarking methods applied to medical images. A comparison of these techniques regarding the robustness, capacity, imperceptibility and objective is also illustrated in Table *3*.

3.1.1. Classical Methods while Minimising the Distortion

In conventional watermarking methods, the watermark is embedded in the whole cover image by replacing some details like LSBs or losing some details when using lossy image compression methods [38]. When implementing a digital watermarking scheme for a medical image, the images must not be perceptually changed because no radiologist will agree to use the degraded image for taking a decision, no matter how small the alteration is. Hence, the watermarking algorithm must be reversible [2]. The irreversible watermarking approaches remain subjected to an admission by radiologists while the original images stay usually preferred for investigation purposes [39].

3.1.2. Region of Interest and Region of Non-Interest Watermarking Methods

Coatrieux, et al. [40] assumed that medical images can be divided into two regions ROI and RONI. ROI section includes the informative region which is used for diagnostic purposes and must be stored without any distortion. However, RONI usually represents the black background of the image, but occasionally it can contain grey level parts of slight interest [41]. In ROI watermarking, spatial or transform domain techniques is utilised for hiding the watermark. The encoded watermark may be robust or fragile based on the purpose and the application in hand.

Table 2: A comparison of existing schools of medical image watermarking

Hiding School	Hiding Technique	Robustness	Imperceptibility	Capacity	Reversibility	Objective
Classical methods	Spatial domain	Fragile	High	High	×	Integrity Authentication
	Transform domain	Robust	Low	Low	×	Ownership protection
ROI & RONI methods	Spatial domain	Fragile	High	Dependent	×	Integrity Authentication
	Transform domain	Robust	Low	Dependent	×	Ownership protection
Reversible methods	Compression based	Fragile	High	High	✓	Integrity Authentication
	Histogram based	Robust Semi-fragile	Low	Low	✓	Ownership protection
	Quantization based	Fragile	High	High	✓	Integrity Authentication
	Expansion based	Fragile	High	High	✓	Integrity Authentication

These watermarks are implemented in a particular way without impacting the visual image quality [42, 43].

Using ROI sections for embedding the watermark may deform the pixels in those regions which may consequently cause the wrong diagnosis. On the other hand, RONI watermarking approaches embed watermarks in areas that unimportant in medical diagnosis, but they have several drawbacks such as they can be only implemented if RONI exists, the amount of information to be embedded depend on the RONI area size and ROI may not be protected against malicious attacks.

3.1.3. Reversible Watermarking Methods

The embedding of the secret message as a watermark, no matter how trivial the modification is, can cause degradation to the host image quality. In some applications, such as military, medical, legal and archival applications, where the authentication requirements are often essential, there are typically strict restraints on data reliability that prevent any deformation in the watermarking operation. For example, modifying a patient's medical image could affect the patient's life by causing errors in diagnosis and treatment. As a result, reversible watermarking techniques have been developed which can stop this shortcoming by applying a technique that can recover both the embedded watermark and the original image. Reversible watermarking techniques can be utilised for image authentication. Reversible watermarks for authentication applications offer a comprehensive framework, the authentication feature maintains the integrity of the image, while the advantage of reversibility protects the quality [21]. The reversible watermarking technique can be deemed as a special case of digital watermarking [21]. *Fig. 7* demonstrates the simple reversible watermarking scheme.

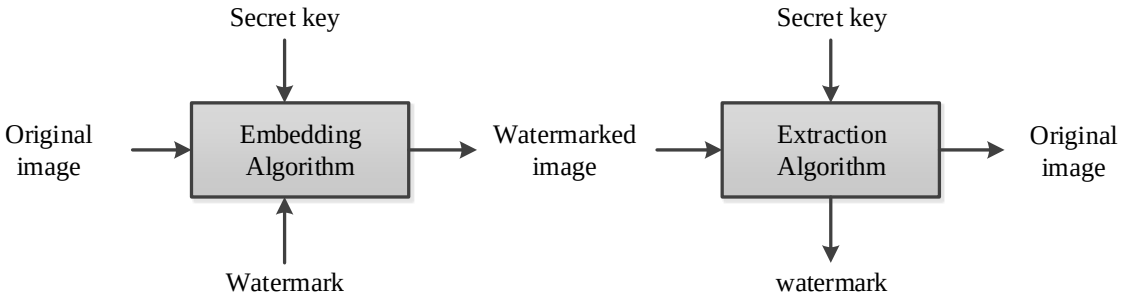


Fig. 7: Basic reversible watermarking scheme.

A patented work on reversible watermarking was introduced by Honsinger, et al. [44]. They embedded the digital signature of the image into the original image to verify its authenticity by

implementing a spatial additive watermark method joint with modulo additions 256. Macq [45] suggested an expansion to the patchwork algorithm to design a robust reversible watermarking technique. Both approaches proposed by Honsinger, et al. [44] and Macq [45] suffer from salt and pepper noise and delays in retrieving the watermark because of the use of modulo additions 256. A different method was designed by De Vleeschouwer, et al. [46] through utilising circular interpretation of bijective transformations of the histograms to reduce the salt and pepper noise found in the previous approaches. Some metrics evaluated the algorithm, but they did not show the results that compare payload capacity to image distortion.

Feng, et al. [47] categorised reversible watermarking approaches into three groups: Data Compression (DC), Difference Expansion (DE) and Histogram Bin Shifting (HBS). Some challenges met the authors in this area are also summarised. Pan, et al. [48] classified the reversible watermarking systems into additive and substitution methods based on hiding technique. The comparison is presented in the experiential study of particular reversible schemes on medical images. Caldelli, et al. [49] proposed a different survey by categorising the reversible watermarking methods into three types: robust, fragile and semi-fragile techniques. They also classified the reversible watermarking according to the hiding domain into spatial and transform techniques. Recently, reversible watermarking approaches based on DE concept have been suggested in many types of research, and they typically exceed the other kinds of techniques methods in that they offer high embedding capacity and low computational complexity compared to the other methods [21].

The following subsections present a review of reversible watermarking methods by classifying them into four groups: compression based, histogram modification based, quantization based and expansion based techniques.

3.1.3.1. Compression Based Technique

In the case of reversible watermarking, additional information is required to be encoded along with the watermark to recover the original unmodified image. As a result, the length of the watermark is much more than the traditional methods. A simple technique to improve the capacity will be by compressing a part of the host image [21, 47].

Several reversible watermarking approaches are stated in the literature and are being implemented. Xuan, et al. [50] developed a high-capacity and distortion-free reversible technique utilising integer wavelet transform and compounding method. The proposed system embeds the watermark in the high-frequency coefficients by histogram shifting and applying

pre-processing steps to avoid the overflow/underflow problems. Celik, et al. [51] offered a popular compression-based method. Firstly, the image pixels are subjected to L-level scalar quantization. Secondly, the remainders are compressed by implementing Context-based Adaptive Lossless Image Codec (CALIC) compression algorithm, and watermark data are integrated with it. Finally, the watermarked image is generated by adding the data to the quantized image. In the retrieval process, the watermarked image is quantized, and the remainders are decompressed to extracting the watermark and recovering the original image.

Furthermore, Arsalan, et al. [52] employed compounding technique, which introduced by Xuan, et al. [50], with a genetic algorithm to improve the embedding capacity. In the first step, the image is converted into transform domain by applying integer wavelet transform. Then, the transformed image is segmented into blocks, and the threshold value is calculated for each block. Compounding process is executed for each block has a value larger than a particular threshold. The genetic algorithm has the ability to select the optimal/near-optimal threshold, which organises the compounding operation and the efficient payload. The weakness of the proposed scheme is the time consuming for the training phase. Also, the genetic algorithm must be applied to each cover image.

3.1.3.2. Histogram Modification Based Technique

Comparing to other approaches of reversible watermarking which are not strong against image processing and distortions, histogram modification has been introduced to overcome the robustness issues. In these methods, the embedding target is replaced by the histogram bin to enhance the robustness of the reversible algorithm [47]. In general, most embedding methods in this type are block-based, and therefore they have the strength to resist some operations. The hiding capacity level in this approach is low, but the robustness is the main benefit of this scheme [53].

In the scheme presented by De Vleeschouwer, et al. [54], the original image is separated into blocks of neighbouring pixels. Then, each block is divided into two regions, and consistent histograms are computed. In their approach, circular interpolation is utilised to shift the histogram bins according to the watermark bit. A high distortion may happen when highest and lowest bits are shifted to the other side. Therefore, the authors enhanced their scheme by using the bijective transformations [46]. The massive distortion produced by the change of the maximum and the minimum bit is controlled by permitting at most two shifts. Another histogram based techniques were developed by [32, 55] by only embedding the data in the peak

bin pixels. However, these approaches require additional overhead to retrieve the watermark and reconstruct the original image, but they provided a reasonable watermarked image quality.

In order to raise the hiding capacity, Lin, et al. [56] offered a multilevel reversible method using the histogram of difference image for hiding the data. The difference image is produced by utilising the difference between two neighbouring pixels. The image is partitioned into non-overlapping (4x4) blocks, and then a variance matrix of size (3x4) is created for every block. For data hiding, histogram shifting is applied to each difference block. Although this approach has a high capacity due to implementing a multi-level embedding method, it suffers from the massive amount of side-information like saving the peak value for all blocks. Tsai, et al. [57] proposed a high capacity scheme by employing a residue image. This remainder indicates a difference between an original pixel and every other pixel in the non-overlapping block rather than the difference between neighbouring pixels. Though, since they need a highest and zero points for each block for obtaining the reversibility feature, that information should be involved to message bits and therefore reducing the hiding capacity of the scheme.

Khan and Malik [58] reported a new high capacity reversible watermarking method which exploits the idea of down sampling for improving the implementation. Down sampling offers two sub-sampled forms, the reference and the data hiding to produce area for embedding by utilising histogram shifting. Moreover, to obtain a blind scheme, the location map was compressed and embedded in the watermarked image. The proposed system provided an excellent imperceptibility versus capacity trade-off and can detect tamper attacks.

3.1.3.3. Quantization Based Technique

Though quantization based watermarking approaches are, in general, robust, reversible quantization based watermarking methods are typically fragile in nature [21]. In Cheung and Wu [59] system, a Sequential Quantization Strategy (SQS) has been suggested to make the variation of a pixel value dependent on the other pixels. Therefore, a balance between security enhancements can be achieved for authenticity and integrity verification. The combination between proposed SQS and the reversible watermarking mechanism has increased the opportunity of detecting the illegal modifications. Saberian, et al. [60] introduced a Weighted Quantization Method (WQM) which is able to be executed in both spatial and transform domains. Comparing to other schemes, the deformation produced by this approach is not capacity dependent.

In general, the classical Quantization Index Modulation (QIM) watermarking methods cannot recover the original image due to the irreversible alterations that produced in the watermarked image because of using the quantization algorithm. Nevertheless, Ko, et al. [61] proposed a reversible watermarking method for medical image applications using the QIM-based technique. The capacity of the developed system was improved by taking the benefits of the suggested nest structure. Ko, et al. [62] outperformed the proposed nested approach by developing a reversible method employing QIM with Fractional Discrete Cosine Transform (FDCT) to reconstruct the original image correctly.

3.1.3.4. Expansion Based Technique

The concept of DE was first introduced in 2003 [63]. It offered a new way to the reversible watermarking techniques. The proposed scheme embeds one bit of watermark data into the LSB of the difference value of two pixels. The selected pairs can either be any two neighbouring (horizontal or vertical) pixels or any two pixels selected in a pre-defined pattern. The weakness of this approach is the reduction of the hiding capacity because of the unexpected but required location map. Alattar [64] extended the previous scheme by hiding two bits into the differences of a triple of pixels. The proposed algorithm used spatial and spectral triplets of pixels to conceal a pair of bits to raise the embedding capacity. A spatial triplet denotes any three pixels chosen from the corresponding spectral, or colour part. On the other hand, the spectral triplet can be any three pixels values picked from various spectral components.

Soon after the DE has been suggested, Alattar [65] developed a novel reversible watermarking using DE of quads of colour images. This method embeds three bits in the DE of a group of four pixels. The simplest method of selecting the quads is to suppose every 2x2 adjacent pixels are a quad. The maximum hiding capacity of the proposed system is considered to be 0.75 bpp. However, in practice, the capacity is estimated to be lower because some quads may not be usable due to overflow/underflow problems. For example, the difference may be (more than 255 or less than 0) for 8-bits depth grayscale images. Alattar [66] generalised the previous algorithms by implementing DE of vectors, instead of pairs, triplets and quads, to improve the embedding capacity of colour images. The proposed system hides several bits in the difference of each vector of connected pixels.

A significant development of the DE technique introduced by Thodi and Rodriguez [67], which is called Prediction Error (PE) expansion. In this method, PE is used instead of DE of two adjacent pixels since the error is slighter than the difference between pixels' value. The

embedding process is done by expanding the PE values. To prevent overflow/underflow issues, only expandable pixels are chosen for embedding process. A compressed location map of the selected embedded locations is also combined with the watermark bits. Thodi and Rodríguez [68] enhanced their previous approach by combining PE and histogram shifting instead of location map. Histogram shifting method requires an overflow/underflow map, which requires comparatively less space than location map. This approach reduced the deformation at low hiding amounts and moderated the capacity control issue that is caused by the location map.

According to Khan, et al. [21], the simple difference between histogram shifting and location map approaches is the degradation produced in the hiding process. In the case of using location map, only watermarked pixels are changed, and then the deformation only happens in these pixels. While, in histogram shifting technique, pixels that are not employed for watermarking are also suffering from deformation due to the using of shifting operation.

Most watermarking systems based on DE techniques are pixel-wise or block based where the damage of data does not impact the next one. However, destroying the location map causes a mismatching to all later pixels. So, these schemes are also fragile under attacks, and they are suitable for authenticity and integrity applications. Also, not all pixels can be used for carrying the watermark bits because of the overflow/underflow problems. Therefore, a threshold to avoid these problems is needed [47].

3.2. Purposes of Medical Image Watermarking

Navas and Sasikumar [69] have divided medical images watermarking methods into two groups: authentication and integrity control, and embedding the EPR data. Al-Qershi and Khoo [70] classified medical images watermarking schemes based on the purposes of the application into three classes: authentication (containing tamper detection and restoration), EPR hiding and systems that merge both authentication and EPR hiding to verify the information source and detect the manipulations. In the following subsections, each group will be explained and discussed. A summary of these approaches is also illustrated in Table *3*.

3.2.1. Authentication Schemes

There are several approaches for preserving the authentication of the medical images. One method is based on hiding the EPR data to prove that the information relates to the right patient.

Table 3: Summary of different watermarking techniques stated in the literature.

Authors	**Purpose**	**Watermark**	**Embedding region**	**Embedding technique**	**Reversibility**	**Robustness**
Lee, et al. [71]	High capacity	Original LSBs Message bits Side information	Whole image	Integer-to-integer wavelet transform Bit-shifting	✓	Fragile
Fontani, et al. [2]	Authentication	DICOM metadata Location map	Whole image	Integer-to-integer wavelet transform LSB-substitution	✓	Fragile
Mostafa, et al. [72]	Minimising storage space Reducing distribution overhead Ensuring safety	EPR data	Whole image	DWPT	✗	Robust
Al-Qershi and Khoo [70]	High capacity	Random bit stream	Smooth region Non-smooth region	DE	✓	Fragile
Al-Qershi and Khoo [73]	Authentication Data hiding	EPR data ROI hash message Compressed ROI ROI embedding map ROI blocks	ROI RONI	DE DWT	✓	Robust Fragile
Memon, et al. [3]	Copyright protection Confidentiality Authentication Integrity	Patient's information Doctor's code LSB_s of ROI	ROI RONI	Hybrid	✓	Robust Fragile
Memon, et al. [43]	Authentication	Patient's data Authentication code Hospital logo	RONI	LSB	✓	Fragile

Nambakhsh, et al. [74]	Security Protecting patient's data Avoid mismatching of diagnosis data	ECG signal Patient's ID	Whole image	DWT	✘	Robust
Tan, et al. [39]	Integrity Authentication Tamper detection	Metadata Authentication data Tamper detection data Estimator position	Whole image	Random location signal Estimator	✓	Fragile
Agung and Permana [75]	Tamper detection	Image's LSB_s Authentication data	ROI RONI	LSB	✓	Fragile
Das and Kundu [76]	Security Authentication Save archiving Captioning Controlled access	ROI hash code DICOM metadata Indexing keyword Doctor's code Tamper localisation information	Whole image	LSB	✘	Fragile
Eswaraiah and Reddy [77]	Integrity Tamper detection	Authentication data ROI hash code ROI recovery data	LSB_s of RONI LSB_s of border pixels	LSB	✘	Fragile
Tareef, et al. [12]	Integrity Authenticity	Sparse code of EPR Reshaped ROI	RONI	Sparse coding SVD	✓	Robust
Brar and Kaur [78]	Authentication High capacity	EPR data Hash code	Virtual borders	DE LSB CDCS	✓	Fragile
Parah, et al. [79]	Copyright protection Integrity	Watermark bits EPR data	ROI RONI	DCT	✘	Robust
Roček, et al. [80]	Security Authenticity	Public share Secure share	ROI RONI	DT-CWT LSB	✓	Robust
Parah, et al. [81]	High capacity Content authentication	EPR data Checksum bits Logo bits	Scaled up of original image	PTB conversion ISB bit	✓	Fragile

A second approach can be achieved by inserting the unique identifiers (UIDs) provided by the header of DICOM images which is accompanied by the raw image data. The watermark allows validating the header raw data combination and the source image recovery. Alternative methods involve hiding the full DICOM header but due to some of the metadata are updated each time the image is distributed; only patient information related to the image must be used.

Another technique connects the header with the raw image data by hiding the digital signature of the header. Although this technique reduces the length of the embedded message, the header should be attached to the image when transmitted. On the other hand, integrity control usually implemented by hiding a Digital Signature (DS) or a Message Authentication Code (MAC) of the whole image or some specific features. At the extraction process, the integrity of the image can be verified by comparing between the recomputed DS/MAC and the hidden one [38]. The priority order of authentication and integrity watermarking systems is imperceptibility, robustness and capacity [69].

Several watermarking approaches were proposed to maintain the authenticity and integrity of medical images. Blind reversible watermarking systems established on integer-to-integer wavelet transform technique were introduced by [2, 71]. In these systems, the image is segmented into blocks, and the watermark is inserted into each block by LSB-substitution or bit-shifting technique. The original image can be precisely retrieved at the extraction side since the required information for realising the reversibility such as location map of changeable and unchangeable LSB is also embedded in the image.

Memon, et al. [43] introduced a blind fragile watermarking to ensure the content authentication of CT images. The watermark information, which consists of patient data, hospital logo and authentication code, is embedded in RONI to preserve ROI information and confirm the integrity control. Automatic segmentation technique has been applied instead of drawing a square [82] or ellipse [83] for splitting the ROI and RONI.

Tan, et al. [39] proposed a dual layer reversible watermarking approach to confirm the integrity and authenticity of DICOM images. Firstly, the images were decomposed into 2x2 non-overlapping blocks. Then, one pixel from each block is selected as an estimator, and the other pixels are used for concealing three bits (one bit each). In the first layer, metadata, authentication information and position of the estimator is embedded. In the second layer, tamper detection information is embedded. For tamper localisation, Cyclic Redundancy Check (CRC-16) is calculated and hidden in the same block. The embedding capacity reached

is 0.75bpp. However, this scheme can detect tampered areas it cannot recover the altered region.

Agung and Permana [75] modified Liew, et al. [84] and Zain and Fauzi [85] approaches by presenting a reversible watermarking technique for detecting the tamper and retrieving the original medical images. The modification based on compressing the original LSBs applying RLE compression technique before encoding it into the RONI section. Firstly, the medical image is separated into ROI and RONI regions. Then, tamper detection and recovery data embedded in ROI, while RONI used to insert the whole LSBs of the image instead of just LSBs of ROI which proposed by Liew, et al. [84] to guarantee the reversibility of the watermarking method.

Das and Kundu [76] developed a blind, fragile and ROI reversible watermarking scheme. The proposed system joins lossless compression and encryption method to hide DICOM metadata, image hash and tamper localisation information into the medical image. Secure Hash Algorithm (SHA-256) was adopted to calculate the hash of the ROI part. This hash is utilised as a message summary to prove the medical image integrity.

Eswaraiah and Reddy [77] proposed a fragile and block based watermarking method for validating the integrity of ROI, identifying the manipulated blocks in ROI and recovering the original ROI region. In this technique, the medical image is segmented into three zones; ROI, RONI and the border region. Then, the hash code of ROI is computed using the SHA-256 method and is hidden in the border pixels. Authentication and recovery information of ROI are inserted into RONI.

Al-Haj [86] suggested an algorithm based on symmetric and asymmetric encryption to ensure confidentiality, integrity and authenticity of the header data, as well as the pixel data of transmitted DICOM images. The pixel data is totally encrypted to realise the confidentiality while integrity and authenticity are guaranteed using digital signatures. A new approach was projected by Roček, et al. [80] by combining the features of reversible, zero and RONI watermarking methods. The basic idea is that the image is segmented into two parts ROI and RONI. The technique merges the zero-watermarking principle in ROI with the high capacity of reversible watermarking in RONI.

3.2.2. EPR Data Hiding Schemes

In order to avoid the detachment between image and patients data as well as to decrease the required storage space, the EPR such as patient name, ID, age, sex, demographic information and diagnosis result can be embedded into the patient image [24]. Hence, the capacity represents a significant requirement. So, the priority order of EPR data embedding is imperceptibility, capacity and robustness [69].

Several watermarking approaches were reported for the aim of EPR data hiding. Mostafa, et al. [72] presented a blind watermarking method for medical image organisation. The proposed system embeds the EPR in the image to minimise the required storage space, reduce distribution overhead and to ensure the safety of the shared data. The EPR is inserted as a watermark into the Discrete Wavelet Packet Transform (DWPT) of the host image. To improve the robustness of the embedding technique, EPR data is coded by applying Bose-Chaudhuri-Hocquenghem (BCH) error correcting code. The drawback of this approach is the low capacity which embeds only one bit in each 4x4 block of pixels. Also, the error correction code decreases the real hiding capacity to be lower than a single bit per 4x4 block.

Nambakhsh, et al. [74] used Electrocardiograph (ECG) signal and patient's ID as dual watermarks to protect patient's data and avoid mismatching diagnosis information. These watermarks are inserted into the grayscale image. The image is decomposed into seven sub-bands implementing dual level DWT. The watermarks are hidden into the two-dimensional wavelet sub-bands using a texture feature extraction process. The evaluation demonstrates that the watermark is robust against several operations. A watermarked image with high quality was achieved for JPEG compressed image up to the quality factor of 85%. Furthermore, the quality of the image tends to degeneration if the size of ECG signal rises. Also, tamper detection which is crucial for medical image authentication is not combined with the proposed scheme.

To increase the embedding capacity for medical images, Al-Qershi and Khoo [73] developed two reversible data hiding approaches based on DE method. The first approach combined Tian [63] technique with Chiang, et al. [87] scheme, and the second method combined Alattar [64] technique with Chiang, et al. [87] scheme. One of the special features of medical images, in comparison to nonmedical images, is the large smooth areas. The proposed scheme divided the image into smooth and non-smooth regions instead of ROI and RONI. For the smooth area, a high hiding capacity technique is utilised. However, DE method is applied to the non-smooth regions.

Parah, et al. [79] presented two different blind methods based on transform domain. The medical images were segmented into ROI and RONI. The digital watermark and EPR data were concealed in both regions in the first technique. In the second algorithm, RONI was utilised to embed the digital watermark and EPR. DCT transform was used to hide the watermark information.

3.2.3. Authentication and EPR Data Hiding Schemes

Al-Qershi and Khoo [70] presented a mixture watermarking system to verify ROI authentication, tamper detection and retrieving the tampered region. The DICOM image was segmented into ROI and RONI sections. Patient information and ROI hash message are hidden into ROI part using DE technique. However, tamper detection and retrieval data which contains the location map, the average ROI blocks and a compressed ROI, are inserted into RONI region by implementing a robust scheme based on DWT method. The limitation of this approach is the manual segmentation of ROI. Also, hiding the EPR data, which includes vital and confidential information, in the ROI part by using a fragile watermarking method may not protect it against attacks.

Memon, et al. [3] reported a hybrid method which hides multiple watermarks for ensuring the confidentiality and integrity of medical images. The robust watermark is applied to hide patient data, doctor authentication code and LSBs of ROI into the RONI part to achieve copyright protection, while data integrity was obtained by embedding a fragile watermark into the ROI region. In this scheme, the location map is generated instead of histogram shifting to avoid overflow/underflow. The proposed system allows the simultaneous storing and transmitting the encrypted EPR data which can be removed at the destination without needing of the original image.

Tareef, et al. [12] proposed a recovery algorithm to confirm the integrity and authenticity of the medical images. The developed technique can be utilised for many purposes like EPR data hiding, authentication of the ROI and retrieving the manipulated area. The sparse coding of the EPR data and the reshaped ROI is hidden in the transform domain of the RONI. In the first part of the sparse coding, the patient information was saved along with the image, while the second part was used for verifying the authentication. The hidden sparse coded ROI can be extracted to reconstruct the altered image.

To decrease the storage and communication cost, an efficient reversible watermarking system was presented by Brar and Kaur [78] based on DE technique. The Message Digest 5 (MD5) Algorithm was used to calculate the image hash to provide authentication. EPR data was encoded by utilising Class Dependent Coding Scheme (CDCS) to increase the hiding capacity. The watermarking process is executed utilising pixel difference of virtual borders. Parah, et al. [81] proposed a high capacity reversible watermarking system for medical applications. Pixel to Block (PTB) conversion method was applied to the cover image to guarantee the reversibility. The watermark, which consists of EPR, block checksum and logo bits, was embedded in the patient's image using Intermediate Significant Bit (ISB) substitution for ensuring content authentication at receiver.

4. Evaluation Benchmarks of Watermarking Algorithms

In the digital watermarking scheme, it is necessary to preserve the quality of the images. So, for evaluating both the watermarked image and the watermark itself, two sets of metrics are required; the first set is to measure the quality of the images, while the second set is to evaluate the accuracy of the extracted watermark. Performance comparison of the different approaches that have been discussed in this research regarding these benchmarks is also demonstrated in Table *3*

4.1. Imperceptibility Assessment of Watermarked Image

There are several metrics used to estimate the distortion of watermarked images. Mean Square Error (MSE), PSNR and SSIM index are the most popular metrics utilised for this purpose. The PSNR and MSE metrics measure the error sensitivity variations between the unmodified and modified images while the SSIM metric draws more concern to the structures of these images [88]. In all of the following equations, $N \times M$ is the images dimension, and I, Iw represent the original and the watermarked images, respectively.

4.1.1. Mean Square Error

MSE between the original image and the watermarked image is measured by the *Eq. 10* [13]:

$$MSE(I, I_w) = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i,j) - I_w(i,j))^2 \qquad (10)$$

4.1.2. Peak Signal to Noise Ratio

PSNR is usually utilised to estimate the quality of the original and the watermarked image. A higher PSNR value indicates that both images are more similar to each other [89]. This metric is determined in decibels (dB) *as Eq. 11*:

$$PSNR(I, I_w) = 10 * log_{10} \frac{MAX_I^2}{MSE} \qquad (11)$$

Where: MAX_I represents the largest fluctuation of the input image.

4.1.3. Structural Similarity Index

SSIM evaluates the image quality by measuring the demographic changes between the two images. SSIM can be calculated using *Eq. 12* and takes a value from (−1 to 1) where the value of (1) refers that the compared images being the same [88].

$$SSIM(I, I_w) = \frac{(2\mu_I\mu_{Iw} + c1)(2cov + c2)}{(\mu_I^2 + \mu_{IW}^2 + c1)(\sigma_I^2 + \sigma_{Iw}^2 + c2)} \qquad (12)$$

$$\begin{cases} c1 = (k_1 L)^2 & k_1 = 0.01 \\ c2 = (k_2 L)^2 & k_2 = 0.03 \end{cases}$$

Where: μ_I and μ_{IW} are the average of I and I_w, respectively, σ^2_I and σ^2_{IW} are the variances of I and I_w, respectively. Cov is the covariance of I_w, *c1* and *c2* are variables to stabilise the division with the weak denominator, and L is the dynamic range of pixel values *(L=2^ (number of bits per pixels) -1)*.

4.2. Robustness Evaluation of Extracted Watermark

The following metrics can be applied to measure the reliability and readability of the extracted watermark in the case of logo or binary sequence watermark. In all of the following equations, *W* and *W'* denotes the embedded and extracted watermark, respectively.

4.2.1. Correlation Coefficient

The Correlation Coefficient (CRC) uses to analyse the corresponding between the original and extracted watermark. CRC value ranges from 0 to 1 and can be calculated by *Eq. 13* [90].

$$CRC = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2 * \sum_i \sum_j W'(i,j)^2}} \quad (13)$$

4.2.2. Similarity Measure

Similarity Measure (SIM) also called Similarity Coefficient (SC) can be utilised to gauge the similarity between the concealed and extracted watermarks [90] and can be calculated using *Eq. 14*:

$$SIM = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sum_i \sum_j W'(i,j)^2} \quad (14)$$

4.2.3. Bit Error Rate

Bit Error Rate (BER) metric is described as the ratio between binary patterns that are decoded wrongly and length of the binary sequence. So, the lower is the BER, the better is the efficiency of the embedding scheme [89]. It is defined by *Eq. 15*:

$$BER = \frac{DB}{NB} \quad (15)$$

Where DB is the amount of incorrectly decoded bits and NB is the whole number of bits of the watermark.

4.2.4. Accuracy Ratio (AR)

Accuracy Ratio (AR) also can be used for evaluating the matching between the hidden and extracted watermark. It represents the relation between correct bits and original watermark bits. It can be identified using *Eq. 16* [90].

$$AR = \frac{CB}{NB} \quad (16)$$

Where CB represents the number of correct bits, and NB is the whole number of bits of the original watermark.

Table 4: Performance comparison of various approaches stated in the literature.

Authors	**Image type / No. of images**	**Capacity (C) / Watermark length (L)**	**Results**
Lee, et al. [71]	4 Colour images 6 Grayscale images	Colour: C up to 1 bpp Grayscale: C up to 0.5 bpp	Colour images: PSNR between 33 & 67 dB Grayscale images: PSNR between 32 & 65 dB
Fontani, et al. [2]	2167 DICOM images (CT, MRI, CR)	C up to 0.1 bpp	CT: PSNR between 66 & 84 dB SSIM between 0.999 & 1 MRI: PSNR between 65.5 & 73.8 dB SSIM between 0.982 & 0.999 CR: PSNR between 70 dB & Inf SSIM between 0.999 & 1
Mostafa, et al. [72]	8 Grayscale medical images (CT, MRI, MRA, Radio)	L= 256 Byte	For all modalities: Avg. PSNR around 39.26 dB BER=0
Al-Qershi and Khoo [70]	4 DICOM images (CT, MRI, CR,US)	CT: C= 0.888 bpp MRI: C= 0.2009 bpp CR: C= 0.0808 bpp US: C= 0.3091 bpp	CT: PSNR= 85.50 dB SSIM= 0.9765 MRI: PSNR= 69.71 dB SSIM= 0.9287 CR: PSNR= 65.22 dB SSIM= 0.9977 US: PSNR= 36.71 dB/ SSIM= 0.7708
Al-Qershi and Khoo [73]	16 DICOM images (CT, MRI, US, X-Ray)	CT: C between 0.515 & 0.525 bpp MRI: C between 0.418 & 0.438 bpp US: C between 0.570 & 0.617 bpp X-Ray: C between 0.491 & 0.654 bpp	CT: PSNR between 72.41 & 77.71 dB SSIM between 0.967 & 0.974 MRI: PSNR between 75.6 & 82.34 dB SSIM between 0.946 & 0.961 US: PSNR between 39.02 & 43.93 dB SSIM between 0.944 & 0.991 X-Ray: PSNR between 48.57 & 53.73 dB SSIM between 0.978 & 0.984

Memon, et al. [43]	CT grayscale of 11 patients (60-100 slices each patient)	L between 125 & 600 Byte	PSNR between 52.5 & 69.5 dB
Nambakhsh, et al. [74]	25 PET images	L around 1000 Byte	PSNR greater than 47.43 dB SSIM=0.93
Tan, et al. [39]	4 DICOM images (CT, MRI, US, X-Ray)	L between 9274 & 72690 Byte	Avg. PSNR around 34.8 dB Avg. MSE around 21.5
Agung and Permana [75]	Grayscale US images	C less than 1 bpp	Avg. PSNR around 47.5 dB
Tareef, et al. [12]	10 US images	Not presented	Avg. PSNR around 49.82 dB
Brar and Kaur [78]	Colour & grayscale medical images (BMP&JPEG)	L= 183, 270 & 343 Byte	PSNR between 78.52 & 92.76 dB
Parah, et al. [79]	CT images	L= 256 & 404 Byte	PSNR between 36.71 & 48.29 dB SSIM between 0.96 & 0.99
Roček, et al. [80]	6000 medical images (different modalities & formats)	C between 0.1 & 1 bpp	Avg. PSNR around 81 dB Avg. SSIM around 0.999974
Parah, et al. [81]	Medical & General images	C= 0.75 bpp	Medical images: Avg. PSNR around 46.37 dB Avg. SSIM around 0.9827 General images: Avg. PSNR around 46.37 dB Avg. SSIM around 0.98864

5. Discussion and Conclusions

The necessity of protecting medical images and other patients' data is not only for confidentiality purposes but also to prevent manipulations that might happen by authorised and unauthorised users while using these images. Therefore, there is a need to use a technique for ensuring trust in digital medical workflows. Digital watermarking has been recognised as a favourable approach for ensuring data integrity and authenticity in medical environments. In this paper, we have presented a comprehensive review of medical image watermarking schemes and discussed various issues related to each approach.

Many techniques have been proposed in the literature for watermarking the medical images utilising both spatial and transform domains. These techniques hide the watermark in the whole image or in the images' ROI and RONI by implementing reversible and irreversible methods. In comparison to the transform domain techniques, which are suitable for ownership verification applications, techniques based on the spatial domain are less complex and provide higher capacity and visual quality. However, the spatial domain methods are fragile and cannot survive against many operations making them appropriate for integrity and authentication applications. Also, it is noticed that transform domain schemes based on DCT and DFT are rarely used for medical image watermarking and the majority of the studies prefer the techniques based on DWT due to it is offering an accurate matching of the human visual system.

RONI watermarking systems embed watermarks in regions that are insignificant in medical diagnosis, but they have several drawbacks such as they can be only applied if a RONI exists, the size of the watermark depends on the RONI size and also the ROI may not be protected against malicious attacks. So, applying these methods depends on the image characteristics.

Medical requirements are extremely strict with the quality of medical images and do not allow non-clinical based modification in any way. The irreversible watermarking methods remain subject to acceptance by the radiologists while the original images stay typically favoured for diagnosis purposes. So, the watermarking algorithms applied to medical images should have the ability to retrieve the original non-modified image. Reversible watermarking assures recovering the original image precisely after extracting the embedded watermark successfully. Consequently, the hiding capacity and the number of potential methods that can be performed on medical images have been restricted significantly because of this feature.

In order to apply watermarking to medical information systems, it is fundamental to choose an appropriate and reliable approach. The performance of all watermarking schemes, which have been reviewed in this paper, had been assessed only in terms of perceptibility by utilising physical metrics. PSNR and SSIM benchmarks are the most widely used physical image quality metrics, but they do not take into account all characteristics that are clinically relevant in getting an accurate medical diagnosis [91]. Therefore, this study recommends relating these metrics to the visual/clinical assessment approaches to improve their validity and applicability. This needs expert images' readers to visually evaluate the differences between the original and watermarked images through an objective question set. Also, it is recommended that further work is required for testing the watermarking system regarding image quality in a fully operational PACS where the medical images are archived and retrieved.

References

[1] O. S. Pianykh, *Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide*: Springer Science & Business Media, 2009.

[2] M. Fontani, A. De Rosa, R. Caldelli, F. Filippini, A. Piva, M. Consalvo, *et al.*, "Reversible watermarking for image integrity verification in hierarchical pacs," in *Proceedings of the 12th ACM workshop on Multimedia and security*, 2010, pp. 161-168.

[3] N. A. Memon, A. Chaudhry, M. Ahmad, and Z. A. Keerio, "Hybrid watermarking of medical images for ROI authentication and recovery," *International Journal of Computer Mathematics*, vol. 88, pp. 2057-2071, 2011.

[4] S. C. Liew and J. M. Zain, "Tamper localization and lossless recovery watermarking scheme," in *Software Engineering and Computer Systems*, ed: Springer, 2011, pp. 555-566.

[5] M. L. Richardson, M. S. Frank, and E. J. Stern, "Digital image manipulation: what constitutes acceptable alteration of a radiologic image?," *AJR. American journal of roentgenology*, vol. 164, pp. 228-229, 1995.

[6] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of digital imaging*, vol. 26, pp. 326-343, 2013.

[7] G. Coatrieux, M. Lamard, W. Daccache, J. Puentes, and C. Roux, "A low distorsion and reversible watermark: application to angiographic images of the retina," in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, 2005, pp. 2224-2227.

[8] K. Pushpala and R. Nigudkar, "A novel watermarking technique for medical image authentication," in *Computers in Cardiology*, 2005, pp. 683-686.IEEE.

[9] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto, "Providing integrity and authenticity in DICOM images: a novel approach," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, pp. 582-589, 2009.

[10] J. Bernarding, A. Thiel, and A. Grzesik, "A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption," *International Journal of Medical Informatics*, vol. 64, pp. 429-438, 2001.

[11] J. Guru and H. Damecha, "Digital watermarking classification: a survey," *International Journal of Computer Science Trends and Technology (IJCST) vol*, vol. 5, pp. 8-13, 2014.

[12] A. Tareef, A. Al-Ani, H. Nguyen, and Y. Y. Chung, "A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding," in *Engineering in Medicine and Biology Society (EMBC), 2014 36th Annual International Conference of the IEEE*, 2014, pp. 5554-5557.

[13] S. M. Mousavi, A. Naghsh, and S. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of digital imaging*, vol. 27, pp. 714-729, 2014.

[14] C. Fung, A. Gortan, and W. G. Junior, "A review study on image digital watermarking," in *The Tenth International Conference on Networks*, 2011, pp. 24-28.

[15] R. Ridzoň, D. Levický, and Z. Klenovičová, "Attacks on watermarks and adjusting PSNR for watermarks application," in *Radioelektronika 2004: 14th international Czech-Slovak scientific conference*, 2004, pp. 27-28.

[16] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modelling: towards a second generation watermarking benchmark," *Signal processing*, vol. 81, pp. 1177-1214, 2001.

[17] M. Durvey and D. Satyarthi, "A review paper on digital watermarking," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 3, pp. 99-105, 2014.

[18] P. Arya, D. S. Tomar, and D. Dubey, "A Review on Different Digital Watermarking Techniques," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, pp. 129-136, 2015.

[19] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, "Properties of digital image watermarking," in *Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on*, 2013, pp. 235-240.

[20] R. Patel and P. Bhatt, "A Review Paper on Digital Watermarking and its Techniques," *International Journal of Computer Applications*, vol. 110, pp. 10-13, 2015.

[21] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," *Information sciences*, vol. 279, pp. 251-272, 2014.

[22] N. Thilagavathi, D. Saravanan, S. Kumarakrishnan, S. Punniakodi, J. Amudhavel, and U. Prabu, "A Survey of Reversible Watermarking Techniques, Application and Attacks," in *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015)*, 2015, p. 37.

[23] O. M. Al-Qershi and B. Khoo, "Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images," in *Proceedings of International Conference on Medical Systems Engineering (ICMSE)*, 2009, pp. 829-834.
[24] R. Priya and V. Sadasivam, "A survey on watermarking techniques, requirements, applications for medical images," *Journal of Theoretical and Applied Information Technology*, vol. 65, pp. 103-120, 2014.
[25] A.-N. Yahya, H. A. Jalab, A. Wahid, and R. M. Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," *Journal of King Saud University-Computer and Information Sciences*, vol. 27, pp. 393-401, 2015.
[26] S. P. Mohanty, K. Ramakrishnan, and M. Kankanhalli, "A dual watermarking technique for images," in *Proceedings of the seventh ACM international conference on Multimedia (Part 2)*, 1999, pp. 49-51.
[27] P. Jain and A. S. Rajawat, "Fragile watermarking for image authentication: survey," *International Journal of Electronics and Computer Science Engineering*, vol. 1, pp. 1232-1237, 2012.
[28] J. M. Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 7, pp. 19-28, 2007.
[29] A. B. Dehkordi, S. N. Esfahani, and A. N. Avanaki, "Robust LSB watermarking optimized for local structural similarity," in *2011 19th Iranian Conference on Electrical Engineering*, 2011, pp. 1-6.
[30] Z. Wenyin and F. Y. Shih, "Semi-fragile spatial watermarking based on local binary pattern operators," *Optics Communications*, vol. 284, pp. 3904-3912, 2011.
[31] J. D. Chang, B. H. Chen, and C. S. Tsai, "LBP-based fragile watermarking scheme for image tamper detection and recovery," in *Next-Generation Electronics (ISNE), 2013 IEEE International Symposium on*, 2013, pp. 173-176.
[32] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on circuits and systems for video technology*, vol. 16, pp. 354-362, 2006.
[33] M. Kaur and R. Kaur, "Reversible watermarking of medical images: Authentication and Recovery-A Survey," *Journal of Information and Operations Management*, vol. 3, p. 241, 2012.
[34] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain," *Optik-International Journal for Light and Electron Optics*, vol. 125, pp. 428-434, 2014.
[35] M. Ali and C. W. Ahn, "An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain," *Signal Processing*, vol. 94, pp. 545-556, 2014.
[36] A. K. Kaushik, "A novel approach for digital watermarking of an image using DFT," *Int JElectronComp Sci Eng*, vol. 1, pp. 35-41, 2012.
[37] S. Tyagi, H. V. Singh, R. Agarwal, and S. K. Gangwar, "Digital watermarking techniques for security applications," in *Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), International Conference on*, 2016, pp. 379-382.
[38] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A review of image watermarking applications in healthcare," in *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, 2006, pp. 4691-4694.
[39] C. K. Tan, J. C. Ng, X. Xu, C. L. Poh, Y. L. Guan, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, pp. 528-540, 2011.
[40] G. Coatrieux, H. Maitre, and B. Sankur, "Strict integrity control of biomedical images," in *Photonics West 2001-Electronic Imaging*, 2001, pp. 229-240.
[41] F. Y. Shih and Y. T. Wu, "Robust watermarking and compression for medical images based on genetic algorithms," *Information Sciences*, vol. 175, pp. 200-216, 2005.
[42] G. Coatrieux, J. Montagner, H. Huang, and C. Roux, "Mixed reversible and RONI watermarking for medical image reliability protection," in *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*, 2007, pp. 5653-5656.
[43] N. A. Memon, S. A. M. Gilani, and A. Ali, "Watermarking of chest CT scan medical images for content authentication," *International Journal of Computer Mathematics*, vol. 88, pp. 265-280, 2011.
[44] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," ed: Google Patents, 2001.
[45] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in *Proc. EUSIPCO*, 2000, pp. 533-536.
[46] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Transactions on Multimedia*, vol. 5, pp. 97-105, 2003.

[47] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, "Reversible watermarking: current status and key issues," *IJ Network Security,* vol. 2, pp. 161-170, 2006.
[48] W. Pan, G. Coatrieux, J. Montagner, N. Cuppens, F. Cuppens, and C. Roux, "Comparison of some reversible watermarking methods in application to medical images," in *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*, 2009, pp. 2172-2175.
[49] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: an overview and a classification," *EURASIP Journal on Information Security,* vol. 2010, p. 2, 2010.
[50] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," in *International Workshop on Digital Watermarking*, 2004, pp. 115-124.
[51] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE transactions on image processing,* vol. 14, pp. 253-266, 2005.
[52] M. Arsalan, S. A. Malik, and A. Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images," *Journal of Systems and Software,* vol. 85, pp. 883-894, 2012.
[53] V. Fotopoulos, M. L. Stavrinou, and A. N. Skodras, "Medical image authentication and self-correction through an adaptive reversible watermarking technique," in *BioInformatics and BioEngineering, 2008. BIBE 2008. 8th IEEE International Conference on*, 2008, pp. 1-5.
[54] C. De Vleeschouwer, J. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," in *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*, 2001, pp. 345-350.
[55] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," in *Multimedia Signal Processing, 2004 IEEE 6th Workshop on*, 2004, pp. 211-214.
[56] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition,* vol. 41, pp. 3582-3591, 2008.
[57] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing,* vol. 89, pp. 1129-1143, 2009.
[58] A. Khan and S. A. Malik, "A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection," *Information Sciences,* vol. 256, pp. 162-183, 2014.
[59] Y. M. Cheung and H. T. Wu, "A sequential quantization strategy for data embedding and integrity verification," *IEEE transactions on circuits and systems for video technology,* vol. 17, pp. 1007-1016, 2007.
[60] M. J. Saberian, M. A. Akhaee, and F. Marvasti, "An invertible quantization based watermarking approach," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008, pp. 1677-1680.
[61] L. T. Ko, J. E. Chen, Y. S. Shieh, H. C. Hsin, and T. Y. Sung, "Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems," *Computational and mathematical methods in medicine,* vol. 2012, 2012.
[62] L. T. Ko, J. E. Chen, Y. S. Shieh, M. Scalia, and T. Y. Sung, "A novel fractional-discrete-cosine-transform-based reversible watermarking for healthcare information management systems," *Mathematical Problems in Engineering,* vol. 2012, 2012.
[63] J. Tian, "Reversible data embedding using a difference expansion," *IEEE transactions on circuits and systems for video technology,* vol. 13, pp. 890-896, 2003.
[64] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in *Proceedings IEEE International Conference on Image Processing. Barcelona, Spain,* 2003, pp. 501-504.
[65] A. M. Alattar, "Reversible watermark using difference expansion of quads," in *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'04)*, 2004, pp. 377-380.
[66] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *Image Processing, IEEE Transactions on,* vol. 13, pp. 1147-1156, 2004.
[67] D. M. Thodi and J. J. Rodriguez, "Prediction-error based reversible watermarking," in *Image Processing, 2004. ICIP'04. 2004 International Conference on*, 2004, pp. 1549-1552.
[68] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *Image Processing, IEEE Transactions on,* vol. 16, pp. 721-730, 2007.
[69] K. Navas and M. Sasikumar, "Survey of medical image watermarking algorithms," in *Proc. Internation Conf. Sciences of Electronics, Technologies of Information and Telecommunications*, TUNISIA, 2007, pp. 25-29.
[70] O. M. Al-Qershi and B. E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images," *Journal of digital imaging,* vol. 24, pp. 114-125, 2011.
[71] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Transactions on Information Forensics and Security,* vol. 2, pp. 321-330, 2007.

[72] S. A. Mostafa, N. El-Sheimy, A. Tolba, F. Abdelkader, and H. M. Elhindy, "Wavelet packets-based blind watermarking for medical image management," *The open biomedical engineering journal*, vol. 4, p. 93, 2010.
[73] O. M. Al-Qershi and B. E. Khoo, "High capacity data hiding schemes for medical images based on difference expansion," *Journal of Systems and Software*, vol. 84, pp. 105-112, 2011.
[74] M. S. Nambakhsh, A. Ahmadian, and H. Zaidi, "A contextual based double watermarking of PET images by patient ID and ECG signal," *Computer methods and programs in biomedicine*, vol. 104, pp. 418-425, 2011.
[75] B. Agung and F. P. Permana, "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 on*, 2012, pp. 167-171.
[76] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Computer methods and programs in biomedicine*, vol. 111, pp. 662-675, 2013.
[77] R. Eswaraiah and E. S. Reddy, "ROI-based fragile medical image watermarking technique for tamper detection and recovery using variance," in *Contemporary Computing (IC3), 2014 Seventh International Conference on*, 2014, pp. 553-558.
[78] A. S. Brar and M. Kaur, "High capacity, reversible data hiding using cdcs along with medical image authentication," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, pp. 49-60, 2015.
[79] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: a robust medical image watermarking system for E-healthcare," *Multimedia Tools and Applications*, pp. 1-35, 2015.
[80] A. Roček, K. Slavíček, O. Dostál, and M. Javorník, "A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters," *Biomedical Signal Processing and Control*, vol. 29, pp. 44-52, 2016.
[81] S. A. Parah, F. Ahad, J. A. Sheikh, and G. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," *Journal of Biomedical Informatics*, 2017.
[82] H. K. Lee, H. J. Kim, K. R. Kwon, and J. K. Lee, "ROI medical image watermarking using DWT and bit-plane," in *Communications, 2005 Asia-Pacific Conference on*, 2005, pp. 512-515.
[83] N. A. Memon and S. Gilani, "NROI watermarking of medical images for content authentication," in *Multitopic Conference, 2008. INMIC 2008. IEEE International*, 2008, pp. 106-110.
[84] S. C. Liew, S. W. Liew, and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery with Run Length Encoding compression," *World Academy of Science, Engineering and Technology*, vol. 72, pp. 799-803, 2010.
[85] J. M. Zain and A. R. Fauzi, "Medical image watermarking with tamper detection and recovery," in *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, 2006, pp. 3270-3273.
[86] A. Al-Haj, "Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images," *Journal of digital imaging*, vol. 28, pp. 179-187, Apr 2015.
[87] K. H. Chiang, K. C. Chang-Chien, R. F. Chang, and H. Y. Yen, "Tamper detection and restoring system for medical images using wavelet-based reversible data embedding," *Journal of Digital Imaging*, vol. 21, pp. 77-90, 2008.
[88] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, pp. 600-612, 2004.
[89] K. Heylen and T. Dams, "An image watermarking tutorial tool using Matlab," in *Proc. of SPIE*, 2008, pp. 1-12.
[90] V. S. Jabade and D. S. R. Gengaje, "Literature review of wavelet based digital image watermarking techniques," *International Journal of Computer Applications*, vol. 31, pp. 28-35, 2011.
[91] C. H. McCollough, M. R. Bruesewitz, and J. M. Kofler Jr, "CT dose reduction and dose management tools: overview of available options 1," *Radiographics*, vol. 26, pp. 503-512, 2006.