J Digit Imaging (2013) 26:326–343
DOI 10.1007/s10278-012-9527-x

A Review of Medical Image Watermarking Requirements for Teleradiology

Hussain Nyeem · Wageeh Boles · Colin Boyd

Published online: 14 September 2012

Abstract Teleradiology allows medical images to be transmitted over electronic networks for clinical interpretation and for improved healthcare access, delivery, and standards. Although such remote transmission of the images is raising various new and complex legal and ethical issues, including image retention and fraud, privacy, malpractice liability, etc., considerations of the security measures used in teleradiology remain unchanged. Addressing this problem naturally warrants investigations on the security measures for their relative functional limitations and for the scope of considering them further. In this paper, starting with various security and privacy standards, the security requirements of medical images as well as expected threats in teleradiology are reviewed. This will make it possible to determine the limitations of the conventional measures used against the expected threats. Furthermore, we thoroughly study the utilization of digital watermarking for teleradiology. Following the key attributes and roles of various watermarking parameters, justification for watermarking over conventional security measures is made in terms of their various objectives, properties, and requirements. We also outline the main objectives of medical image watermarking for teleradiology and provide recommendations on suitable watermarking techniques and their characterization. Finally, concluding remarks and directions for future research are presented.

Keywords Digital watermark · Teleradiology · Security

H. Nyeem (✉)
School of Electrical Eng. and Computer Science,
Science and Engineering Faculty,
Queensland University of Technology (QUT),
GP, O Block, Level 4, Desk 17, GPO Box 2434, Brisbane,
QLD 4001, Australia
e-mail: h.nyeem@qut.edu.au
URL: www.qut.edu.au

W. Boles
School of Electrical Eng. and Computer Science,
Science and Engineering Faculty,
Queensland University of Technology (QUT),
GP, S Block, Level 11, Room 1124, GPO Box 2434, Brisbane,
QLD 4001, Australia
e-mail: w.boles@qut.edu.au
URL: www.qut.edu.au

C. Boyd
School of Electrical Eng. and Computer Science,
Science and Engineering Faculty,
Queensland University of Technology (QUT),
OC, 126 Margaret Street, Level 7, Room 704, GPO Box 2434,
Brisbane, QLD 4001, Australia
e-mail: c.boyd@qut.edu.au
URL: www.qut.edu.au

Introduction

Recent technological advances introduced a radical change in the modern health care sector including medical imaging facilities, hospital information system (HIS), and information management systems in hospitals. Changes in medical imaging facilities in radiology have acquired sufficient reliability and cost-effectiveness that the film-based imaging technology has been shifted to filmless techniques for producing digital images on various devices rather than generating hardcopies. With the use of these digital medical images, in addition, HIS comprising radiology information system (RIS) and picture archiving and communication system (PACS) [1] has facilitated offering various eHealth services. These eHealth services are introducing new practices for the profession as well as for the patients by enabling remote access, transmission, and interpretation of the medical images for diagnosis purposes. This has made easy the widespread use of teleradiology with the potential to improve healthcare access, delivery, and standards, where complex and new legal and ethical issues are also raising.

These issues include image retention and fraud, privacy, malpractice liability, licensing and credentialing, and contracts for PACS, RIS, and teleradiology [2].

In teleradiology, one of the most successful eHealth services at present, security and privacy protection has become a critical issue [3, 4]. In this study, we mainly focus on the teleradiology that essentially captures a broad range of security requirements along with other radiological information management issues including that of its original medical specialty, radiology. When radiology employs the use of imaging to both diagnose and treat disease visualized within the human body, teleradiology has been for a long time understood to be an eHealth service done through remote transmission of the radiology images and information over electronic networks, and the interpretation of the transmitted images for diagnosis purposes [3]. Remote access and transmission of the images and other radiology information, particularly, electronic personal health information (EPHI), expose them to possible tampering or theft with serious ramifications, since they are sensitive and in most cases EPHI are identifiable. Such radiology images and information not only require protection with integrity and high confidentiality but also appropriate management through different healthcare services.

Providing the required security and privacy of the radiology information requires the following: (1) a standard set of security and privacy profile/policy for teleradiology and (2) a set of security measures by which the security principles in the profile are fulfilled. Various national and international legislative rules and directives define the security and privacy requirements of medical information. These requirements are being achieved by different conventional measures, which are thought to be incapable of providing the required security of the electronic radiology information in the PACS/RIS-based teleradiology [5–7]. On the other hand, recent studies show the possibility of using digital watermarking for improving security in teleradiology [8–16].

Digital watermarking has various attractive properties to complement the existing security measures that can offer better protection for various multimedia applications [17]. However, it is particularly important to know the applicability of digital watermarking from every aspect of radiology information requirements and the suitability of that over other (both the existing and developing) similar measures. Although Coatrieux et al. [7, 18] studied the applicability of digital watermarking in medical imaging, a further justification of the watermarking considering the security requirements in teleradiology is still necessary.

The rest of the paper is organized as follows. General security and privacy requirements of, and expected threats for, the medical information from the perspective of different security and privacy profiles/policies are reviewed and presented in section "Security and Privacy Requirements in Teleradiology." The limitations of the conventional security measures to handle those threats are also studied and discussed there in. The section on "Digital Watermarking in Teleradiology" introduces briefly the digital watermarking and its various benefits. Justification over other comparable measures, various properties, objectives, suitable types, and their requirements of watermarking for medical images are also given. Concluding remarks and discussion are given in the section on "Discussion and Conclusions."

Security and Privacy Requirements in Teleradiology

Security and Privacy Standards

Medical information security requirements are generally defined by the strict ethics and legislative rules of the security policy/profile, and concerned entities must adhere to them. There are many widely used guidelines and standards for protecting personal health information. The basic international standard developed for security management of health information is the ISO27799 (Security Management in Health Using ISO/IEC/17799) [19]. The standard itself provides guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO17799/ISO27002. It specifically covers the security management needs in this sector, with respect to the particular nature of the data involved.

Some countries have their own security and privacy policy; for example, USA's Health Insurance Portability and Accountability Act (HIPAA) [20], Code of Federal Regulations number 45 (CFR 45) [21], and Europe's Directive 95/46/EC [22] are expressions of such a constraint. The HIPAA requires all the cover entities (i.e., health plans, health care clearinghouses, and healthcare providers) to take measures to ensure the security of medical images to protect patient's privacy. Directive 95/46/EC states the legislative rules on the protection of individuals with regard to the processing of personal data and on the movement of such data. In addition, the CFR 45 (part 164: security and privacy) includes a set of standards for the protection of sensitive EPHI.

There is no specialized standard similar to HIPAA or CFR 45 in Australia at this time, although it does seem likely that a similar set of standards will eventually be required in the future, if online and electronic health records are to be appropriately protected [23]. As the government regulations in relation to privacy grow throughout the world, it forces the security of medical images to grow also. However, the Australian Law Reform Commission [24] produced the Australian Privacy Law and Practice Report that is a comprehensive review of the Privacy Act of 1988 (Australian Law Reform Commission, 2008). That review incorporates privacy regulations on electronic health information systems.

Besides, the Digital Imaging and Communication in Medicine (DICOM) [25] was conceived in 1983 by a joint committee formed by the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA). Early standards did not gain universal acceptance among manufacturers. In 1993, ACR-NEMA version 3.0 was released, and at this time, the standard was renamed DICOM 3.0. This version of that standard has become universal within radiology and been adopted in other medical fields such as dentistry, pathology, and cardiology [26]. It is now commonly known as simply the DICOM standard, an 18-part document. This standard aims to define a technical framework for application entities involved in the exchange of medical data to adhere to a set of security profiles. DICOM also warrants the inclusion of the imaging information for the electronic health record systems and digital signatures for checking the integrity of medical images.

Medical Information Security Requirements

The standards and their technical frameworks, strict ethics, and legislatives rules, as mentioned above, give rights to the patient and duties to the health professionals. Development and implementation of the security and privacy protection services derived from the standards depends upon the model or infrastructure of the teleradiology and its concerned entities. Two widely used models in today's teleradiology are referred by Ruotsalainen [3] to develop their security requirements. The most common model used in teleradiology is based on offline messaging. The other model incorporates the online delivery of distributed imaging services and allows a radiological information system to be spread over a large distributed area. Irrespective of the communication type (i.e., offline or online), three individual domains, namely: (1) host organization/hospital's PACS/RIS (*domain A*), (2) communication network (*domain B*), and (3) consultant (*domain C*) can be considered from Fig. 1, which are responsible for providing the required security in a teleradiology system. On the other hand, in radiology, security concerns arise only from the domain A (e.g., from acquisition of medical images to storing them in PACS of the same hospital). Therefore, as we mentioned in "Introduction," the security requirements of teleradiology also include the security requirements of radiology.

In an offline model, the security domains are isolated, and communication is made via interfaces whereas online teleradiology maintains communication with a remote consultant allowing access to the local PACS/RIS services of the legacy system [3]. However, based on the technological and organisational models used in teleradiology, their various security requirements can be outlined below [3, 27]:

- All concerned entities/domains (e.g., the PACS/RIS in hospital or clinic, communication network, and consultant/radiologist at distant place) must have the same level of security and protection.
- In all domains, proper authorization process must be employed through various access and user controls, transmission controls, and directive controls.
- Integrity, authenticity, and confidentiality of all radiological information have to be ensured during teleradiology session, consultation process, and information processing, management, and preservation.

The principle of those requirements imposes three mandatory characteristics for security of medical information [7, 27, 28]: confidentiality, reliability, and availability.

- *Confidentiality*— ensures that only the entitled users have access to the information.
- *Reliability* based on the outcomes of: (1) *integrity*—the information has not been modified by non-authorized people—and (2) *authenticity*—a proof that the

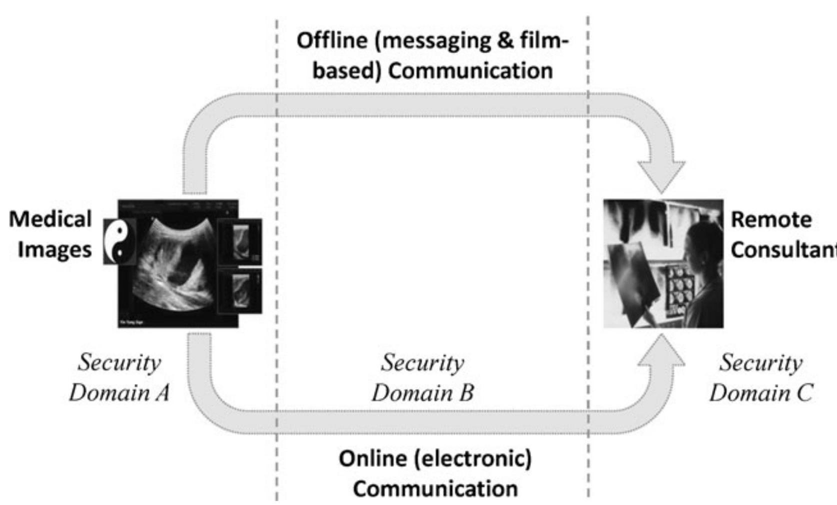

Fig. 1 Teleradiology model

information belongs to the correct patient and issued from the right source.
– *Availability*—warrants an information system to be used in the normal scheduled conditions of access.

On the other hand, the security concept derived from the related standards mentioned in the preceding section can be established through different stages. For example, as outlined by Baur et al. [27], the major stages can be: (1) determination of the appropriate level of security, (2) threat analysis, (3) risk analysis, and (4) establishment of security concept. Determination of the appropriate level of security may include determining security levels of all entities and objects (e.g., IT applications and information sets) linked with the teleradiology system. Threat analysis helps determine the expected threats from the involved objects (e.g., infrastructure, hardware, software, paper-ware). Risk analysis helps quantify the damages for all the identified threats and their occurring frequency. Establishment of security concept deals with either reducing the probability of occurrence of the threats or reducing the damage if an adverse event is unavoidable. This includes selection of suitable measures that reduce the risks to a tolerant level, evaluation of the selected measures, examining the cost–effect relationship as well as analyzing any further risk. All these comprise the security requirements of different domains in teleradiology.

Besides, for computer and network security, various requirements are entitled in different standards such as USA's Federal Information Processing Standards [4] and Germany's *Bundesdaten-schutzgesetz* [27], the general categories of which includes: access control; audit and accountability; certification, accreditation, and security assessment; configuration management; identification, and authentication; media protection; physical and environmental protection; system and communications protection; and system and information integrity. However, as an important aspect of security and risk management in the context of information security [29], we restrict our attention to recognizing the value of information and defining appropriate procedures and protection requirements for the information.

Expected Threats and Conventional Security Measures

Identifying the vulnerability of the system is important to define appropriate procedures or security measures, since the strength of any system is no greater than its weakest link. For example, medical images may pass through various image-information processing systems over the networks, and thereby, the images can be threatened throughout their lifetime in many different ways. A complete protection to those threats means having individual protection mechanisms for each component of the processing system that the images may pass through. With particular attention to the medical information, here we find the suitable measures that provide the required security and privacy services for the information and for the communication services.

Several existing security measures are currently being used such as access control services, firewall, encryption, de-identification services, certification services, etc. Furthermore, the possibilities of new measures such as digital watermarking, digital signature, image hashing, etc. are currently being studied. According to the security requirements discussed in previous section, a review of expected threats and their conventional security measures are summarized in Table 1.

Limitations of the Existing Security Measures

Various existing security measures, as illustrated in Table 1, are being used to protect the medical images and information, and their communications. For example, virtual private network (VPN), firewall, etc., as well as encryption, cryptographic hash function, or their derivatives such as digital signature (DS), machine authentication code (MAC), manipulation detection code (MDC), and perceptual hashing, etc. However, these conventional security measures are considered to have limitations specially in protecting the medical images [6, 7, 13, 18, 30–34], which are summarized in Table 2 and should be properly addressed for the improved security.

Firewall and VPN Among various network security measures, firewalls and VPN are common. Along with intrusion detection systems, antivirus systems, etc., those measures are implemented mainly for protecting the information through securing the communications of a system.

A firewall is usually placed between two networks to act as a gateway, which is a combination of hardware and software that protects the company's network and computers from possible intrusion by hackers from the external network [35]. Canavan [35] described this as a fundamental component of any perimeter defence that can have the following uses: (1) keeping unwanted and unauthorized traffic from passing (in or out); (2) providing an efficient Internet access to internal users; (3) monitoring for and notifying of intrusions and network problems; (4) maintaining logs of all communication activities between two networks effectively, which can be used to identify abnormal events. Canavan also described three principal requirements of an effective firewall: (1) it must act as a door through which all traffic must pass (incoming and outgoing); (2) it must allow only authorized traffic to pass; and (3) it must be immune to penetration or compromise.

However, a firewall by itself does not assure a secure network, and it represents a single point of failure [35]. Firewall, as only a tool, needs proper configuration and regular monitoring. Firewalls that are not properly configured may allow

Table 1 Security requirements of medical information

Security requirement	Threats	Security measures
Confidentiality	Disclosures and re-routing of the information: During transmission (e.g., when an ill-intentioned person intercepts and illicitly copies files and records) In the database (resulting in intrusion, identity usurpation, or Trojan horse virus that keeps an open access through the network)	Encryption of the data Limiting lifetime of data Private communication network (e.g., virtual private network) Access control services (against unauthorized person, illegal copy, identity usurpation, etc.) using smart card, firewall, etc. User control services for authenticating and identifying the user against identity usurpation, etc.
Reliability: integrity and authentication	Illicit destruction, production, and/ modification of the contents of files and records	One-way hash function or robust hash function or digital signature (DS) Encryption of the data File header, audit logs for recording of data transmission Certification of communication partners Access control services for writing, reading, and manipulation of data User control services for authenticating and identifying the user against identity usurpation Software accreditation and use of antivirus and firewall for virus and malicious intrusion Non-repudiation services and e-signing
Availability	File management system disablement, destruction of a hard disk, or a malicious pirate who disrupts or alters surreptitiously the organization or content of the data	Access control services for writing, reading, and manipulation of data User control services for authenticating and identifying the user against identity usurpation Private communication network Software accreditation, and use of antivirus and firewall for virus and malicious intrusion

unauthorized users through. In addition, a denial-of-service attack that effectively shuts down the firewall shuts down the network connection to the outside world [35]. Moreover, a firewall takes time more or less to examine incoming and outgoing traffic, which tends to degrade network performance.

As another significant limitation, firewalls are of no use to track activities on the internal network. While a firewall does make it somewhat more difficult for someone from the outside to get in, the majority of attacks on corporate systems come from the inside, not from the outside [35]. In addition to the threat from inside of an organization, firewalls can be circumvented by outsiders [35]. As a result, critical systems should be configured to monitor logins, failed logins, and all network activity of the internal systems.

A VPN, on the other hand, is a means of transporting traffic in a secure manner over an unsecured network which is achieved by employing some combination of encryption, authentication, and tunnelling [36]. "Tunnelling" refers to the process of encapsulating or embedding one network protocol to be carried within the packets of a second network. There are several different implementations of VPN protocols such as point-to-point tunnelling protocol (PPTP), Internet protocol security (IPSec), secure sockets layer (SSL), secure shell (SSH), etc. Those protocols have different pros and cons from different technical perspective [36]. For example, SSL supports transmission control protocol traffic only; SSL and SSH depend on client port forwarding; some protocols

Table 2 Limitations of existing security measures/tools

Measures/tools	Limitations
Firewall and VPN	Only protect the information up to the point of the internal networks [7]
	Provide a certain level of isolation between the intra-net and internet but are easily bypassed by hackers [7]
Encryption	Probably an efficient tool for secure storage and transmission, but once the sensitive data is decrypted, the information is not protected anymore [7, 13, 33]
	Simply using encryption is no guarantee of confidentiality or secrecy [39].
	The randomness of the data for encrypted files stored on media can be used to distinguish the files from other stored data [39].
File-header	Can be easily usurped by a pirate in the plaintext format
	If encrypted, can be very sensitive to bit errors occurring during storage and transmission [7, 32]
Cryptographic hash function and its derivatives (e.g., DS, MAC, MDC, etc.)	Hash function cannot locate where the images have been tampered [31, 32, 47].
	The security of DS largely depends on the strength of the hash functions used to validate the signatures [30].
	It is possible to generate two datasets with different content but having the same message-digest algorithm 5 (MD5) hash [34].
	Cryptographic hash function is extremely bit sensitive to the input [32, 47].
Perceptual hashing	Perceptual hashing usually requires searching for match and access to a central database, where a large amount of pre-computed perceptual hashes are stored [7].
	Most randomization methods in perceptual hashing are linear, which introduces security flaws as known input/hash pairs can be used to recover a secret key [46].
	Their quantization and encoding stages require the learning of appropriate quantization thresholds.
	The quantizer training as well as the storage of thresholds introduces additional security weaknesses.

use symmetric or weak encryption (e.g., PPTP), and IPSec supports unicast traffic only, etc. However, considering the general perspective of information security, further to firewalls, a VPN can be used to protect the information up to the point of the communication networks.

Encryption In order to protect the privacy and confidentiality of electronic health information, encryption has been a commonly accepted technology in health care sector [37]. In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called *cipher*) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key [38]. The result of the process is encrypted information (called *ciphertext*). There are two types of encryption: symmetric (private/secret key) encryption (e.g., data encryption standard, Rivest Cipher #4- RC4) and asymmetric (public key) encryption (e.g., Diffie Hellman, digital signature algorithm (DSA)).

The strength of the symmetric scheme is largely dependent on the size of the key and on keeping it secret. Generally, the larger the key, the more secure the scheme [39]. Furthermore, symmetric encryption is relatively fast and widely understood. However, the main weakness of this type of encryption is that the key or algorithm has to be shared [39]. In addition, symmetric key provides no process for authentication or nonrepudiation [39]. Here, nonrepudiation is the ability to prevent individuals or entities from denying that a message was sent or received or that file was accessed or altered, when in fact it was. That is why symmetric cryptosystems are not well suited for spontaneous communication over open and unsecured networks [39].

On the other hand, asymmetric encryption uses two keys as opposed to one key in a symmetric system [39]. One of them is kept secret and called private key, while the other is made public and called public key. A message is encrypted with the private key and decrypted with the public key. The advantages of this type of encryption include no secret sharing and providing a means of authentication and nonrepudiation with the help of digital certificates. Unlike symmetric cryptosystem, public key allows for secure spontaneous communication over an open network. Besides, it is more scalable for very large systems than symmetric cryptosystems. Yet, asymmetric encryption is relatively slower and computationally intensive, and requires certificate authority [39].

File Header It is a common practice of appending metadata containing owner ID, size, last modified time, and location of all data blocks, etc., as a header with the data block. The size of this header varies depending on how much header information is to be stored. The DICOM standard allows image information object definitions that a DICOM file not only contains pixel data but also key information about the image [40]. Thus, a single DICOM file contains both a header and all of the image data.

Conventionally, each DICOM medical image is associated with a patient's private data such as patient's name, age, results of examination/diagnosis, time taken, etc. All these private information are recorded into a meta-data or header file, which is appended to the image. The DICOM standard stores the image data and the meta-data separately. Clearly, this is dangerous as the link between the image and the textual information is practically non-existent [41]. For example, for the images with plain-text file-header, the major threat is the violation of the access rights and of the daily logs by the intruder. Hence, breaking of the confidentiality implies that integrity and authenticity of the data cannot be guaranteed anymore [7]. Furthermore, for an encrypted header, the bit error sensitivity may result in loss of header and/raise further complexity in managing the medical images. Thus, at the least, the patients' private data in a DICOM image are at risk of happenings of a mismatch (i.e., linking of meta-data with an incorrect medical image) and of disclosure and loss of header or meta-data in an image undergoing some intentional processing.

Cryptographic Hash Function A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value [32]. The data to be encoded is often called the *message*, and the hashes are sometimes called the *message digest* or simply *digest* [42]. The ideal cryptographic hash function has four main properties [43]: (1) it is easy (but not necessarily quick) to compute the hash value for any given message; (2) it is infeasible to generate a message that has a given hash; (3) it is infeasible to modify a message without changing the hash; and (4) it is infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information security applications, notably in DS, MACs, MDCs, and other forms of authentication [42]. They can also be used for other purposes such that indexing data in hash tables, fingerprinting, detecting duplicate data and accidental data corruption, etc [42]. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes [42]. In addition, most of the existing cryptographic hash function schemes unfortunately remain vulnerable to incidental modifications (i.e., even a one bit change in the input will change the output hashes dramatically) [32]. This severely limits their practical utility in robust content authentication for multimedia applications.

Perceptual Hash Function Perceptual hash functions (or, *robust perceptual hash function*, or simply, *perceptual hashing*) are designated hash functions for multimedia contents. This type of hash function takes a large digital image as input, and with constructing a content descriptor of the input, outputs a fixed length binary vector known as *hash value*. This hash value is required to be invariant under changes to the image that are perceptually insignificant whereas, on perceptually distinct inputs, the hash values need to be approximately independent and hence different with high probability [44]. A good perceptual hash function should have the following properties [45]: (1) *Robust*: Manipulations that do not change the perceptual information should not change the hash value; (2) *Unique*: Perceptually different inputs should have completely different hash values; and (3) *Secure*: It should be very hard to find (forge) perceptually different inputs having similar hash values.

Similar to cryptographic hash functions, perceptual hashing is required to generate different hash values for different inputs. However, here, the definition of difference is changed from bitwise difference to perceptual difference [45]. That is, unlike getting a very different hash value from a single bit change in the input of the cryptographic hash function, perceptual hashes are expected to be different only with the changes in the perceptual content of the input. For instance, the hash value of an image and its JPEG compressed version should be the same for the perceptual hash function, since they have no perceptual difference, although their bit-string representation is completely different [45].

Generally, perceptual hashing consists of feature extraction and randomization that introduces non-invertibility and compression followed by quantization and binary encoding to produce a binary hash output. Most randomization methods are linear, and this introduces security flaws because known input/hash pairs can be used to recover a secret key [46]. Furthermore, the quantization and encoding stages require the learning of appropriate quantization thresholds, and the quantizer training as well as the storage of thresholds that introduce additional security weaknesses.

Moreover, content-based feature extraction methods, developed from a signal processing perspective, are known to be robust but not secure [44]. Kalker [31] described perceptual (or robust) hashing from the perspective of a neural archiving activities using *clever signal processing* and *database techniques*. The former is responsible for extracting essential perceptual features (also referred to as *perceptual hash values* or *hash values* for short), the latter for storing and searching large amounts of pre-computed hash values. Kalker also exemplified with a typical scenario, where a local client (e.g., a mobile phone) is responsible for capturing the content and transmitting the content (possibly only the hash values if the client is equipped with a feature extractor) to a central database. The central database matches the hash values of the unidentified content with the pre-computed hash values, retrieves the best match, and takes appropriate action (e.g., sending an artist name and song title in an SMS message to the requesting client).

Reviewing some key existing security measures as discussed above, it can be said that they are useful in handling the common security problems of the system. Yet, their limitations suggest that they are no longer sufficient to provide the required security of the medical information in teleradiology. Therefore, as the new security problems are arising from the advances of technology and developments of PACS/RIS mentioned in "Introduction," new measures are required to be developed and deployed for the improved security of medical images and EPHI. Hence, studies show that digital watermarking can be promising to facilitate sharing and remote handling of that information in teleradiology in a secure manner [16–18], though a reasonable justification of watermarking applicability for medical images is lacking.

Digital Watermarking in Teleradiology

Watermarking nowadays, while well established in a range of applications [48], is only just beginning to be explored for healthcare and medical information systems [49, 50]. Digital watermarking, basically, is a process that principally permits the adding of information as a 'watermark' into the object, a digital media (e.g., digital image, audio, etc.) such that the watermark can be detected afterward. Generally, digital watermarking consists of three major components: watermark generator, embedder, and detector [51] as shown in Fig. 2. A watermark generator generates desired watermark(s) for a particular application, which are optionally dependent on some keys. Watermark(s) are embedded into the object by a watermark embedder, sometimes based on an embedding key whereas a watermark detector is responsible for detecting the existence of some predefined watermark in the object. It is sometimes desirable to extract a message as well.

In a target application, digital watermarking objectives can deal with mainly two issues. One is to address *security* (e.g., authentication and integrity control of the cover object, confidentiality of the information used in watermark, etc.), and the other is to address *system considerations* (saving memory and bandwidth, avoiding detachment, etc., e.g., annotation of useful information such as electronic patient records (EPR), electronic transaction records (ETR), etc.). Furthermore, based on the processing domain, watermarking schemes can be broadly categorized as (1) spatial domain watermarking and (2) transform domain watermarking. Spatial domain schemes include LSB embedding, spread spectrum technique, etc., and transform domain schemes are based on discrete cosine transform, discrete Fourier transform, and discrete wavelet transforms. Watermarking in spatial and transform domains have different advantages and disadvantages [14, 52], which are illustrated in Table 3 below.

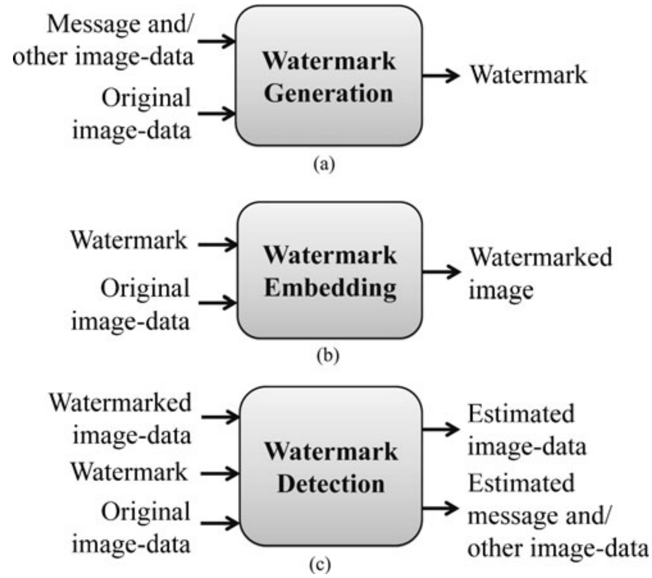

Fig. 2 Fundamental components of digital watermarking: **a** watermark generation, **b** watermark embedding, and **c** watermark detection

Advantages of Digital Watermarking

Watermarking has received much attention recently for medical image applications because of its various attractive attributes [7, 53, 54], which are listed below:

Security and Privacy The fundamental and most attractive property of watermarking is data-hiding capability [55, 56]. The utmost confidentiality can be maintained by hiding the private data into the images. Keeping necessary medical information (e.g., EPR including demographic data, diagnostic results, treatment procedures, etc.) hidden in medical images may provide a better security against malicious tampering, assuming medical images would not be of people's interest without the patient information [15, 57]. Even that which is tampered intentionally or in an unintended manner can be detected and possibly

Table 3 Advantages and disadvantages of watermarking in spatial and transform domains

Types of processing	Advantages	Disadvantages
Spatial domain	Comparatively simple and faster operation	Vulnerable to compression, geometric distortion, and filtering
Transform domain	Compression compatible and robust against many geometric distortions (e.g., rotation, scaling, translation, cropping) and filtering	Comparatively higher computational time and complexity

recovered by using an appropriate watermarking scheme [58, 59]. Hence, Coatrieux et al. [7] outlined three main objectives of watermarking in the medical image applications: *data hiding*, *integrity control*, and *authenticity*, which can provide the required security of medical images. For example, data-hiding objective of watermarking allows inserting meta-data and other information so that the image is more useful or easier to use. Integrity control objective of watermarking ascertains that the image has not been modified in an unauthorized manner. Digital watermarking allows permanent association of image content with proofs of its reliability by modifying [some] image pixel values, independently of the image file format [13]. It can also operate in a stand-alone environment and has a versatile message set. In addition, authenticity traces the origin of an image.

Avoiding Detachment The data-hiding property of watermarking mentioned above further facilitates annotation of necessary information to avoid detachment. Millions of medical images are being produced in radiology departments around the world, which have immense value to practicing medical professionals, medical researchers, and students [53]. Researches in this field are being accomplished to embed patient data to medical images [55, 60, 61]. If the EPR and the images are separate, the chance of detachment of patient data from the image becomes higher. Misplacing a data will be very crucial in the case of medical image. In order to avoid this misplacing or detachment, watermarking offers necessary data embedding within the image itself.

Indexing Another benefit stems from data-hiding capability of watermarking is indexing, where relevant keywords or indices can be embedded into the images and used for effective archiving and retrieval of the images from databases [53].

Nonrepudiation In teleradiology, distribution of the watermarked images between HISs may cause nonrepudiation problem, where both the involved parties (e.g., hospital personnel and clinician) may repudiate that they did not send the data. Along with other advantages, watermarking is also promising to support nonrepudiation in various multimedia applications [62, 63]. Hence, use of a key-based watermarking system may facilitate nonrepudiation in teleradiology such that both parties could be in safer side where the key used by the hospital could be their logos or digital signatures.

Controlling Access Provision for using keys in watermarking schemes further provides an alternative to access control mechanism, where confidential meta-data can be accessed with the proper authoritative rights given in terms of keys [53, 64].

Memory and Bandwidth Saving Storage space and bandwidth requirements are important decisive factor for small hospitals' financial economy. The memory for storage can be saved to a certain extent in HIS by embedding the EPR in the image [61, 65]. On the other hand, a huge amount of bandwidth is required for the transmission of the image data in teleradiology. The additional requirement of bandwidth for the transmission of the metadata can be avoided if the data is hidden in the image itself. Since the EPR and the image can be integrated into one, bandwidth for the transmission can be reduced in telemedicine applications [53].

Choice of Design and Evaluation Parameters

Watermarking requirements for medical images are mainly defined in terms of security and privacy, fidelity, and computational properties. Hence, *security and privacy requirements* characterize a watermarking scheme to achieve data hiding, integrity control, and authenticity objectives as discussed in previous section. *Fidelity requirements* guarantee that the watermarked medical images are useable for diagnosis and other clinical uses. Besides, the *computational properties* help obtain the cost benefit and feasibility analysis for practical implementation. All these watermarking requirements, on the other hand, define various watermarking design and evaluation parameters in an application scenario. Design parameters help characterize the development of a watermarking scheme, whereas the evaluation parameters help determine the performance of a developing/existing scheme. Typical parameters for watermark generation and embedding include visibility, blindness, embedding capacity, imperceptibility/perceptual similarity, etc. Similarly, blindness, invertibility, robustness, error probability, etc., are the parameters for the detection [66].

Moreover, deploying a watermarking system in medical image applications broadly includes two phases, namely a *development phase* and a *validation phase* as illustrated in Fig. 3. In the development phase, optimum criteria for the necessary design parameters of the system are to be defined properly according to the medical image requirements, since all the design parameters of watermarking frequently influence one another (directly or indirectly) [67]. Similarly, it is also necessary to have a careful consideration on the evaluation parameters, their suitable measures, and the requirements of the medical images in the validation phase, in order to justify the suitability of existing/developing watermarking schemes for medical image application.

The system design and evaluation parameters for image watermarking are mainly associated with its core components: watermark generation, embedding, and detection [66]. Various design and evaluation parameters play an important role in achieving a particular objective in an

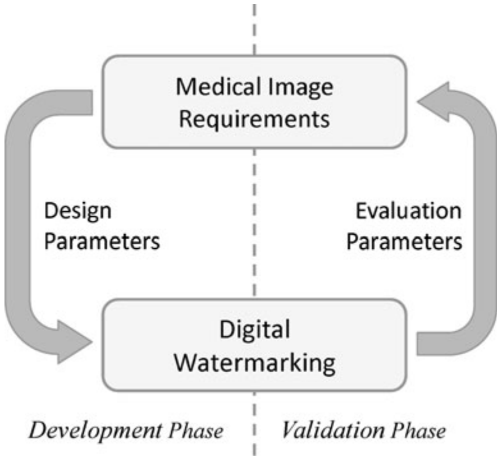

Fig. 3 Interlinking of digital watermarking with medical image applications

application scenario, which has been reviewed for teleradiology application and is discussed in the following.

Visibility Visible watermarking are important in recognition and support of possessing a digital image, where watermarking objectives is mainly to show some necessary information such as logo, icon, courtesy, etc., through the watermarked image. Contrariwise, invisible watermarks are used in digital image applications, where watermarking objectives are to addressing security issues of the images. Like various digital image applications [68–76], invisibility of the watermark appears to be the main interest in the research of medical imaging [8–10, 12, 13, 41, 77–79].

Robustness Robustness is an important parameter for the watermarking detector defined in different ways [80]. Robustness, basically, is defined as the degree of resistance of a watermarking scheme to modifications of the host signal due to either common signal processing, or operations devised specifically in order to render the watermark undetectable [81]. This parameter categorizes watermarking schemes to be *robust*, *fragile*, and *semi-fragile*. In a robust watermarking, a watermark usually carries information regarding the owner in order to validate who the image belongs to (e.g., which person, which institute or organization, etc.). Thus, these watermarking schemes are being used for content authentication purposes in various digital image applications (e.g., copyright protection) [68, 73, 79, 82–86]. Semi-fragile and fragile watermarks are being used to carry much information about itself, its owner's metadata, its distribution, etc., and are thus used for annotation (e.g., hiding ETR or EPR, etc.) [15, 55, 57, 61, 65, 87] and integrity control (e.g., tamper detection and recovery) [8, 59, 88–90].

Blindness Blindness in watermarking refers to the ability of a component function (e.g., watermark generation, detection) to work without any original version of input (e.g., image or watermark, etc.). Non-blindness in watermark generation is important while an original image dependent watermark is required. An original image-dependent watermark is helpful in addressing ambiguity and forgery attacks (e.g., copy attacks) [67]. Here, if the watermark is not dependent on the original image, it can be easily copied to another image or forged to output an invalid watermarked image [91]. Besides, blindness in detection is important, where availability of the original image or watermark at the detector can thwart watermarking objectives. Non-blindness in detection is used sometimes in developing tamper-recovery watermarking schemes, where the recovery of tampered regions is often difficult to achieve from the watermarked image itself.

Embedding Capacity Embedding capacity is generally measured by number of embedding bits. High embedding capacity is a key issue in developing annotation or integrity control watermarking schemes [92], which are generally of fragile or semi-fragile nature to some common image processing. Achieving high embedding capacity often introduces more distortions to a watermarked image and thereby often makes it difficult to preserve high imperceptibility. A robust watermarking used for content authentication purpose requires comparatively lower embedding capacity than that required for annotations purposes of a fragile/semi-fragile watermark [93, 94]. Research shows that LSB embedding techniques offer comparatively higher embedding capacity [13, 95].

Invertibility Invertibility of a watermarking system indicates the detection function to be the inverse of the embedding function. Invertible (or sometimes referred to as *reversible* or *lossless*) watermarking is of special interest in digital image applications where no distortions are allowed in the original image. Therefore, an original image is required to be restored from respective watermarked images by the detector. Invertibility seldom gets interest for non-blind detector since detection itself requires the original image, although developing a blind detector for invertible watermarking is more challenging, especially when a high embedding capacity is desired. Developing this type of watermarking received much attention in medical image applications to avoid any misdiagnosis from distortions in a watermarked image [8, 72, 78].

Perceptual Similarity Perceptual similarity determines the degree of imperceptibility between the original image and its watermarked version, especially in developing an invisible watermarking scheme [67]. Different similarity metrics are used for this parameter such as correlation quality; signal-to-noise ratio (SNR), peak SNR (PSNR), weighted

PSNR, mean square error; structural similarity (SSIM), mean SSIM; and normalized cross-correlation (NCC). In medical image watermarking applications, perceptual similarity must be very high to avoid any risk of misdiagnosis.

Security Security requirements of watermarking include the legitimate access, use, disclosure, disruption, modification, or perusal of the watermarking system. Determining these security requirements in a target application is crucial for the system design, and that can be determined through comprehensive risk management (e.g., examining security policy, access control, physical and environmental security, operation managements, etc.) [96, 97].

Error Probability Error probability is another important parameter for assessing detection performance of a watermarking scheme. Irrespective of application scenarios, zero error probability is always desirable, although achieving this is practically difficult considering higher degrees of robustness to any distortions [17]. However, like in other digital image applications, keeping the error probabilities lower as much as possible is very important in a medical image application scenario in order to ensure reliable detection. Some of the important and commonly used error probability metrics are *bit error rate*, *false-positive rate*, *false-negative rate*, etc.

Digital Watermarking Versus Other Security Measures/Tools

Digital watermarking has some unique advantages for teleradiology, although few existing security measures/tools may serve its other objectives together, for example, encryption, cryptographic hash function (e.g., MAC, DS, etc.), perceptual hashing, etc. Following our previous discussion on watermarking and other comparable security measures/tools, an extensive comparison among them based on various key properties and requirements of medical image applications is made and presented in Table 4.

As Table 4 illustrates, cryptographic/perceptual hashing has no impact on quality of the host-signal, and is suitable for legacy content, but they are either bit-sensitive (for cryptographic hash functions) or need access to a central database to search for a match with a pre-computed hash (for perceptual hashing), whereas research suggests that a carefully designed watermarking scheme does not alter medical diagnosis [102]. Although watermarking has an impact, more or less, on perceptual quality and difficulties with legacy content, Guo and Zhuang [103] suggested three ways to overcome the distortion induced in images by watermark embedding. They are: (1) defining acceptable range of distortion for watermarking; (2) separating an image into protection zone and insertion zone such as ROI (region of interest) and RONI (region of non-interest); and (3) considering watermarking as an invertible manner to recover the original image at the watermark decoder site. Hence, ROI indicates the region significant for diagnosis and other clinical uses, and RONI indicates the complementary region of ROI, which has lesser or almost no significance in diagnosis.

Defining acceptable range of distortion for watermark embedding through clinical validation is expensive, which is applied by Zain et al. [102]. In contrast, separation of ROI and RONI in medical images is not straightforward and may require the interaction/approval of doctor/radiologist. In addition, making such separation is sometimes very difficult, although it is applied in several watermarking schemes [9, 12, 77]. Besides, developing reversible watermarking is promising for medical image application with taking no risk for sacrificing the diagnostic accuracy, although computational properties may incur additional complexity in different processing domains. Additionally, Coatrieux et al. [104] discussed two limitations of reversible watermarking: (1) It imposes the watermark removal before the diagnosis, and (2) it assumes a secured environment because, once the watermark is removed, the image is not protected anymore like in cryptography. All these suggest that a combination of suitable type of watermarking schemes, where the concept of multiple watermarking stems from, can be developed in order to address the rising security problems of medical images in teleradiology [77, 105–107]. Studies also show that incorporation of asymmetric encryption and lossless compression can help attain additional confidentiality, non-repudiation property, high embedding capacity [15, 103, 108].

Watermarking allows using DS or perceptual hashing for appropriate applications [78, 105, 109, 110]. Watermarking systems have room for employing encryption for the additional confidentiality of metadata (e.g., in generating watermark). Memon et al. [13] proposed a digital watermarking scheme, in which watermark is comprised of patient information, hospital logo, and message authentication code, computed using hash function. To ensure inaccessibility of embedded data to the adversaries, BCH encryption of watermark is performed there. For the same purpose, Li-Qun et al. introduced DSA [111] and digital signature technology based on RSA public cryptosystem [110], integrating reversible digital watermarking with digital signature to form an authentication system.

Furthermore, a few of recent studies show the use of a compression technique for attaining the embedding capacity requirements of watermarking. Nambakhsh et al. [112] presented a watermarking method on several computed tomography (CT) and magnetic resonance (MRI) images, where the original image is compressed using the zero-tree wavelet (EZW) algorithm. Raul et al. [101] used Huffman compression and RC4 method that respectively compress and encrypt the metadata in a blind watermarking scheme. Kundu et al. [15] presented a watermarking scheme that combines lossless data compression and advanced encryption standard

Table 4 Watermarking versus other security measures/tools

Properties and requirements	Digital watermarking	Hash function		Encryption
		Perceptual	Cryptographic	
Objective	Data and copyright protection	Data protection	Data protection	Secure communication
Host-signal/cover-object	Mostly image/audio data	Mostly image data	Plaintext message[a]	Plaintext message[a]
Secret data	Watermark	–	–	Plaintext
Key	Optional	Optional	Optional	Necessary
Input	Generally the watermark and the cover-object/host-signal	Arbitrary block of host-signal	Arbitrary block of host-signal	Arbitrary block of host-signal
Output	Watermarked data	Hash-values/message-digest	Hash-values/message-digest	Ciphertext
Detection type	Blind, semi-blind, non-blind	Non-blind	Non-blind	Blind
Failure	If an invalid watermarked image is detected as valid, or vice versa (e.g., from unauthorized removal or embedding of watermark)	If the message is generated from the hashes, or if another message or perceptual changes in the original gives the same hashes.	If the message is generated from the hashes, or if another message or bit changes in the original gives the same hashes.	If a ciphertext is illicitly de-ciphered
Impact on quality/content of the image	Yes, but can be acceptably reduced/resolved by considering non-region of interest (RONI) or reversible watermarking [14, 98, 99]	No	No	No
Sensitivity to bit error	Low	Low	High	High
Robustness	Can be designed as robust, semi-fragile, fragile	Robust only	Robust only	Robust only
Authentication/integrity check	Yes	Yes	Yes	Yes, but as long as data are encrypted
Tamper localization	Yes (also can suggest for recovery to a certain extent [14])	No	No	No
Annotating metadata (e.g., EPR, ETR, etc.)	Yes, but to a limited capacity	No	No	No
Confidentiality of metadata	Yes (also, for higher confidentiality, encrypted information can be used in generating watermark [57, 100, 101])	No	No	Yes
Database requirement	No, it can operate in stand-alone environment [8, 31]	Yes, for storing pre-computed perceptual hashes [46]	No	No
File-format independent	Yes	–	–	–

[a] Image and audio data can be used, if they are represented as plaintext message

for encryption of medical images. In addition, Sung-Jin et al. [52] proposed an algorithm that utilizes both JPEG 2000 and robust watermarking for protection and compression of the medical image. Thus, depending on the application, a choice for the appropriate mixture of various technologies can be made to devise a suitable watermarking system for teleradiology.

Objectives and Applications of Watermarking for Medical Images

Popularity of Internet has become a boon to patients and low-capital hospitals to utilize the facility to communicate with the clinicians for clinical diagnosis purposes [54], where the security of medical images can presumably be addressed to a considerable extent by inserting a properly selected additional data into medical images through digital watermarking. A digital medical image application is therefore one of the prospective target areas of using digital watermarking. Studies show that various watermarking schemes can be used in teleradiology for (1) origin/content authentication [9, 13, 41, 107, 113–119], (2) EPR annotation [57, 65, 88, 120–122], and (3) tamper detection and recovery of medical images [8, 14, 59, 123, 124]. Some important aspects of medical image watermarking schemes for their different objectives are summarized below.

Origin/Content Authentication Watermarking has received much interest in the research for origin authentication of the medical images. The important details can be stored in images imperceptibly, causing no harm to the ROI of the images. This kind of brief descriptions can be hidden in images immediately after the production of the images in the radiology departments. This can be done by incorporating the watermarking in the different modality machines namely, CT or MRI scanners. The database systems use the mechanisms of granting and revoking privileges and of authorization control to ensure the security of data with the permanent association of the watermark. Our observation suggests the following requirements for this type of watermarking in teleradiology: (1) The watermark should be invisible, blind, and robust; (2) watermark should incorporate the minimum information required for the origin authentication; (3) embedding process must consider the RONI; and (4) proper validation of a watermarking scheme such that the permanent association of the watermark is reliable and safe for diagnosis.

Regarding the validation of a watermarking scheme, although it is required for any scheme to be applied in any application scenario, extra care needs to be taken when the effect of watermark embedding is not recoverable. Hence, the permanent association of such robust watermarking requires compromising few bits, which further warrants determining the acceptable range of distortion. Moreover, this type of watermarking should incorporate the RONI embedding for the reliable clinical uses of medical images, particularly, when used along with a reversible watermarking (to form multiple/sequential/hierarchical watermarking scheme) that assumes a secure environment as mentioned in previous section.

EPR Annotation EPR and other useful medical information annotation are other key objectives for medical image watermarking. Navas et al. [125] suggested three key requirements for EPR data hiding and transmission: (1) The recovery of the EPR should be blind due to the unavailability of the original image; (2) zero bit-error rate (BER) is essential for EPR data; and (3) imperceptibility should not be compromised for any reason. These requirements suggest necessary criteria of a watermarking scheme for medical images to be *invisible*, *blind*, and *reversible*. Such a watermarking scheme can be either *robust* or *semi-fragile*. For higher capacity, the watermarking scheme can be semi-fragile, although it requires defining appropriately the set of necessary operations/processing, to which the scheme needs to be robust or not to be. A bit-error correction technique can be used for attaining zero BER and improving watermarking performance [126, 127]. For additional confidentiality, encryption of the EPR can also be used in watermark generation [127, 128].

Tamper Detection and Recovery (Integrity Control) Medical images in different radiological modalities such as X-rays, ultrasounds, and MRI contain vital medical information that can be tampered with easily available image processing tools. Thus, their protection and authentication seems of great importance, and this need will rise along with the future standardization of exchange of data between hospitals, or between patients and doctors [118]. Integrity of a medical image can be achieved in three levels [129]: (1) *tamper detection*, (2) *tamper localization*, and (3) *possible recovery by approximating the tampered region*. In order to achieve this along with the requirements of medical image needs a watermark to be (1) *fragile and blind* and (2) *reversible or RONI-embedding-based*. Hence, fragile watermarking help locate the tampered region with its fundamental property that a watermark becomes invalid for any malicious or unintentional modifications in the watermarked image.

If the origin authentication of a medical image is achieved by the robust watermarking, fragile reversible watermarking (in the form of multiple watermarking) can further locate and possibly recover any tampered region of the watermarked image. This will allow the system to control the integrity as well as authentication. In that case, if the watermarking is RONI-based instead of reversible, then the limit of additional distortion must be taken care of. Furthermore, as in EPR annotative watermarking, LSB-embedding-based watermarking schemes for tamper detection and recovery received much interest in the research, since consideration on the embedding capacity is equally important for the both watermarking objectives.

Discussion and Conclusions

Study of security and privacy problems is a continuous process and is mainly influenced by the technological advances in the field. It has been more than a decade since the study of digital watermarking (finding relevance and suitability, and developing of new schemes and their evaluation) has found its way to medical image applications. However, watermarking for medical images is not practically well accepted yet. This reluctance is instigated from the incomplete justification of watermarking applicability for the strict requirements of medical images. In this paper, an extensive investigation is conducted and described in three parts, namely: (1) the security and privacy requirements; (2) conventional security measures and their limitations; and (3) justification of using watermarking for medical images, in teleradiology.

The need for sharing of medical images and information is growing rapidly for improved healthcare access, delivery, and standards. Web services technology has recently been widely proposed and gradually adopted as a platform for supporting systems' integration [130]. The DICOM standard as well as ISO27799 and other government regulations such as HIPAA, CFR 45, Directive 95/46/EC, etc., impose rules as national/international standards to protect individuals' health information, highlighting security and privacy protection requirements. Our study suggested three mandatory characteristics: confidentiality, reliability, and availability that need to be achieved for medical images in teleradiology.

However, a complete solution for various security problems discussed so far is still lacking. Although conventional security measures have their limitations, they cannot be replaced with any individual measure. For example, authentication based on watermarking cannot replace classical cryptographic authentication protocols that protect communication channels [131]. However, well-known cryptographic algorithms can be used to guarantee the privacy, authenticity, and integrity of messages embedded in multimedia content, where there is no cryptographic solution for the threat of unauthorized watermark removal [132]. To this, other conventional security measures may still be required, while watermarking complements the security of multimedia data. Especially, watermarking provides a great prospect for teleradiology because it functions as a communication tool with the authenticity of the origin/sender, nonrepudiation, detection of data tampering, memory and bandwidth saving, integrity of the image, and so on.

We observed that the general requirement for any medical image watermarking implies that watermarking needs to be *invisible* and *blind*, whereas, *robustness*, *reversibility*, and *RONI embedding* as well as other design parameters must be taken into consideration according to the objectives dictated by the application scenario. Although it is not identified as a general requirement, a prior clinical validation of a watermarking scheme may always be subjected to its medical image application irrespective of the type and properties of watermark(s). As a result, any permanent or temporary modification due to watermark embedding may remain reliable and safe for diagnosis.

In teleradiology, the primary objective of a watermarking scheme for medical images should be authentication (e.g., origin or content). EPR annotation and integrity control (or, tamper detection and recovery) can be a further goal(s) to form a multiple watermarking scheme. Thereby, a properly designed multiple watermarking scheme may have the potential intelligence to address the rising problem in teleradiology. Although the concept of multiple watermarking scheme is not new, their applicability in teleradiology naturally requires more explicit consideration on the performance evaluations and security analysis, including overall computational complexity, speed, and cost–benefit analysis.

Finally, without considering and characterizing, the required design and evaluation parameters systematically may pose serious flaws and may render a watermarking scheme ultimately useless for the application. Therefore, this study recommends a systematic development of multiple watermarking schemes and their complete assessment through defining the parameters properly such that they can offer a better complementary solution for achieving improved security in teleradiology. Hence, a suitable generic watermarking model and a point of reference for benchmarking is recommended as another milestone to be addressed in future research.

References

1. Hyung-Kyo L, Hee-Jung K, Ki-Ryong K, Jong-Keuk L: Digital watermarking of medical image using ROI information. In: Enterprise networking and computing in healthcare industry, 2005. HEALTHCOM 2005. Proceedings of 7th International Workshop on, 2005, pp. 404–407
2. Al-Damegh SA: (22 March). Emerging issues in medical imaging (Indian J Med Ethics.2005 Oct-Dec;2(4) ed.) [Online]. Available: http://www.ijme.in/134co123.html
3. Ruotsalainen P: Privacy and security in teleradiology. European Journal of Radiology 73:31–35, 2010
4. Prior F, Ingeholm ML, Levine BA, Tarbox L: Potential impact of HITECH security regulations on medical imaging. In: 2009 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society. EMBC 2009, 3–6 Sept. 2009, Piscataway, NJ, USA, 2009, pp. 2157–60
5. Kobayashi LOM, Furuie SS: Proposal for DICOM multiframe medical image integrity and authenticity. Journal of Digital Imaging 22:71–83, 2009
6. Cao F, Huang HK, Zhou XQ: Medical image security in a HIPAA mandated PACS environment. Computerized Medical Imaging and Graphics 27:185–196, 2003
7. Coatrieux G, Maitre H, Sankur B, Rolland Y, Collorec R: Relevance of watermarking in medical imaging. In: Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference on, 2000, pp. 250–255
8. Tan C, Ng J, Xu X, Poh C, Guan Y, Sheah K: Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. Journal of Digital Imaging 24:528–540, 2011
9. Memon NA, Chaudhry A, Ahmad M, Keerio ZA: Hybrid watermarking of medical images for ROI authentication and recovery.

International Journal of Computer Mathematics 88:2057–2071, 2011
10. Lin PL, Hsieh C-K, Huang P-W: A hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recognition 38:2519–2529, 2005
11. Chang C-C, Fan Y-H, Tai W-L: Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recognition 41:654–661, 2008
12. Al-Qershi OM, Khoo BE: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. Journal of Digital Imaging 24:114–125, 2011
13. Memon NA, Gilani SAM, Ali A: Watermarking of chest CT scan medical images for content authentication. In: Information and Communication Technologies, 2009. ICICT '09. International Conference on, 2009, pp. 175–180
14. Liew SC, Zain JM: Reversible medical image watermarking for tamper detection and recovery. In: Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, 2010, pp. 417–420
15. Kundu MK, Das S: Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding. in Pattern Recognition (ICPR), 2010 20th International Conference on, 2010, pp. 1457–1460
16. Coatrieux G, Lecornu L, Sankur B, Roux C: 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
17. Cox I, Miller M, Bloom J, Fridrich J, Kalker T: Digital watermarking and steganography, 2nd edition. Elsevier, Burlington, 2007
18. Coatrieux G, Maitre H, Sankur B: Strict integrity control of biomedical images. In: Security and watermarking of multimedia contents III, January 22, 2001–January 25, 2001, San Jose, CA, United states, 2001, pp. 229–240
19. (27 March 2012). ISO 27799:2008, Health informatics—information security management in health using ISO/IEC 27002 [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=41298
20. The Health Insurance Portability and Accountability Act (HIPAA) [Online]. Available: http://www.hhs.gov/ocr/privacy/index.html
21. Code of Federal Regulations-Title 45, subtitle A—Dept. of Health and Human Services, part 164—Security and Privacy [Online]. Available: http://www.access.gpo.gov/nara/cfr/waisidx_10/45cfr164_10.html
22. Directive 95/46/EC of the European Parliament and of the Council [Online]. Available: ec.europa.eu/justice/policies/privacy/…/dir1995-46_part1_en.pdf
23. (09 October 2011). Holistic, or full of holes? PCI, HIPAA and experiences in implementing secure computing systems [Online]. Available: http://www.dotsec.com/Links%20-%20health.html
24. (03 October 2011). Australian Law Reform Commission [Online]. Available: http://www.alrc.gov.au/
25. DICOM, Part 15: security and system management profiles, PS 3.15-2009 [Online]. Available: ftp://medical.nema.org/medical/dicom/2009/
26. Turner JE, Bhacchu DS et al. (May 2002): Beginners guide to PACS. In: MDA Evaluation Report, ed London: PACSnet, Bence-Jones Offices, St. Georges's Hospital
27. Baur HJ, Engelmann U, Saurbier F, Schroter A, Baur U, Meinzer HP: How to deal with security issues in teleradiology. Computer Methods and Programs in Biomedicine 53:1–8, 1997
28. Epstein MA, Pasieka MS, Lord WP, Wong STC, Mankovich NJ: Security for the digital information age of medicine: issues, applications, and implementation. Journal of Digital Imaging 11:[d]33–44, 1998
29. Jahangiri A: Training: information security [Online]. Available: http://www.alijahangiri.org/documents/Information-Security.htm
30. Goldwasser S, Bellare M: (07 October). Lecture notes on cryptography [Online]. Available: http://cseweb.ucsd.edu/~mihir/papers/gb.pdf
31. Kalker T: Issues with digital watermarking and perceptual hashing. Proc. SPIE 4518:189, 2001
32. Paar C, Pelzl J: Hash functions: understanding cryptography. ed: Springer Berlin Heidelberg, 2010, pp. 293–317
33. Zhou XQ, Huang HK, Lou SL: Secure method for sectional image archiving and transmission. In: Medical imaging 2000: PACS Design and Evaluation: Engineering and Clinical Issues, 15–17 Feb. 2000, USA, 2000, pp. 390–9
34. Xiaoyun Wang DF, Xuejia Lai, Hongbo Yu: (2004). Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD [Online]. Available: http://eprint.iacr.org/
35. Canavan JE: Chapter 12: firewalls. In: Fundamentals of network security, ed Boston, London: Library of Congress Cataloging-in-Publication Data, Artech House
36. Canavan, J. E. Chapter 11: virtual private networks. In: Fundamentals of network security, ed Boston, London: Library of Congress Cataloging-in-Publication Data, Artech House.
37. Stine K, Dang Q: Encryption Basics. Journal of AHIMA 82:44–47, 2011
38. (01 September 2011). Encryption [Online]. Available: http://en.wikipedia.org/wiki/Encryption
39. Canavan JE: Chapter 3: encryption, digital signatures, and certification authorities. In: Fundamentals of network security, ed Boston, London: Library of Congress Cataloging-in-Publication Data, Artech House
40. DICOM, Part 3: information object definitions [Online]. Available: ftp://medical.nema.org/medical/dicom/2009/09_03pu3.pdf
41. Wong MLD, Goh AWT, Chua HS: Medical image authentication using DPT watermarking: a preliminary attempt. Forensics in Telecommunications, Information and Multimedia 8:42–53, 2009
42. (06 October 2011). Cryptographic hash function [Online]. Available: http://en.wikipedia.org/wiki/Cryptographic_hash_function
43. Lafourcade P, Alexandre C, Florian M: (1st Semester 2010/2011, 03 October). Lecture note 05-security models: symmetric encryption, [Online]. Available: http://www-verimag.imag.fr/~plafourc/teaching/Master_Pro_2010_2011/Lecture_Note10/Lecture_Note_05.pdf
44. Evans BL (12 November 2011). Image Hashing Research [Online]. Available: http://users.ece.utexas.edu/~bevans/projects/hashing/
45. (3 October 2011). Perceptual hashing [Online]. Available: http://isis.poly.edu/projects/percephash
46. Voloshynovskiy S, Koval O, Beekhof F, Pun T: Conception and limits of robust perceptual hashing: towards side information assisted hash functions. In: Media forensics and security, January 19, 2009–January 21, 2009, San Jose, CA, United states, 2009, p. The Society for Imaging Science and Technology (IS and T); The International Society for Optical Engineering (SPIE)
47. Preneel B: Analysis and design of cryptographic hash functions (PhD Thesis) [Online]. Available: http://homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf, 2003
48. Digital watermarking services & applications. Available: http://www.digitalwatermarkingalliance.org/membership.asp
49. Liew SC, Zain JM: Experiment of tamper detection and recovery watermarking in PACS. In: Computer Research and Development, 2010 Second International Conference on, 2010, pp. 387–390
50. Que D, Wen X, Chen B: PACS model based on digital watermarking and its core algorithms. In: MIPPR 2009-Medical Imaging, Parallel Processing of Images, and Optimization Techniques: 6th International Symposium on Multispectral Image Processing

and Pattern Recognition, October 30, 2009–November 1, 2009, Yichang, China, 2009, pp. Natl. Lab. Multi-spectral Inf. Process. Technol.; Huazhong University of Science and Technology; National Natural Science Foundation of China; China Three Gorges University
51. Li Q, Memon N: Security models of digital watermarking. In: Sebe N, Liu Y, Zhuang Y, Huang T Eds. Multimedia content analysis and mining. vol. 4577, ed: Springer Berlin/Heidelberg, 2007, pp. 60–64
52. Lim SJ, Moon H-M, Chae S-H, Chung Y, Pan SB: JPEG 2000 and digital watermarking technique using in medical image. In 3rd IEEE International Conference on Secure Software Integration Reliability Improvement, SSIRI 2009, July 8, 2009 - July 10, 2009, Shanghai, China, 2009, pp. 413–416
53. Das S, Kundu M: Effective management of medical information through a novel blind watermarking technique. Journal of Medical Systems, pp. 1–13
54. Navas KA, Sasikumar M: Survey of medical image watermarking algorithms. Presented at the 4rth International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SETIT), TUNISIA, 2007
55. Chao H-M, Hsu C-M, Miaou S-G: A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Transactions on Information Technology in Biomedicine 6:46–53, 2002
56. Fallahpour M, Megias D, Ghanbari M: High capacity, reversible data hiding in medical images. In: Image processing (ICIP), 2009 16th IEEE International Conference on, 2009, pp. 4241–4244
57. Ulutas M, Ulutas G, Nabiyev VV: Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of Systems and Software, vol. (in press), Corrected Proof, 2012
58. Luo H, Yu F-X, Chen H, Huang Z-L, Li H, Wang P-H: Reversible data hiding based on block median preservation. Information Sciences 181:308–328, 2011
59. Wu JHK, Chang R-F, Chen C-J, Wang C-L, Kuo T-H, Moon WK, Chen D-R: Tamper detection and recovery for medical images using near-lossless information hiding technique. Journal of Digital Imaging 21:59–76, 2008
60. Jianguo Z, Jianyong S, Yuanyuan Y, Chenwen L, Yihong Y, Jin J, Weihua C, Kun S, Guozhen Z: Image-based electronic patient records for secured collaborative medical applications. In: 2005 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 31 Aug.-3 Sept. 2005, Piscataway, NJ, USA, 2006, p. 3pp
61. Münch H, Engelmann U, Schröter A, Meinzer HP: The integration of medical images with the electronic patient record and their web-based distribution1. Academic Radiology 11:661–668, 2004
62. Cheung S-C, Chiu DKW, Ho C: The use of digital watermarking for intelligence multimedia document distribution. Journal of Theoretical and Applied Electronic Commerce Research 3:103–118, 2008
63. Zhou W, Rockwood T, Sagetong P: Non-repudiation oblivious watermarking schema for secure digital video distribution. In: Multimedia Signal Processing, 2002 IEEE Workshop on, 2002, pp. 343–346
64. Fridrich J: Applications of data hiding in digital images. In: Proceedings of Fifth International Symposium on Signal Processing and its Applications, 22–25 Aug. 1999, Brisbane, Qld., Australia, 1999, p. 9 vol.1
65. Navas KA, Archana Thampy S, Sasikumar M: EPR hiding in medical images for telemedicine. In: Proceedings of World Academy of Science and Engineering and Technology, 2008
66. Nyeem H, Boles W, Boyd C: Developing a digital image watermarking model. In: Digital Image Computing Techniques and Applications (DICTA), 2011 International Conference on, Noosa, Queensland, Australia, 2011, pp. 468–473
67. Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T: Models of watermarking. In: Digital watermarking and steganography (second edition), ed Burlington: Morgan Kaufmann, 2008, pp. 61–103
68. Deng C, Gao X, Li X, Tao D: A local Tchebichef moments-based robust image watermarking. Signal Processing 89:1531–1539, 2009
69. Ganic E, Eskicioglu AM: Robust DWT-SVD domain image watermarking: embedding data in all frequencies. presented at the Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, Germany, 2004
70. Liu J-L, Lou D-C, Chang M-C, Tso H-K: A robust watermarking scheme using self-reference image. Computer Standards & Interfaces 28:356–367, 2006
71. Nikolaidis N, Pitas I: Robust image watermarking in the spatial domain. Signal Processing 66:385–403, 1998
72. Pan W, Coatrieux G, Cuppens N, Cuppens F, Roux C: An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform. In: 2010 32nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC 2010), 31 Aug.-4 Sept. 2010, Piscataway, NJ, USA, 2010, pp. 4740–3
73. Qi X, Qi J: A robust content-based digital image watermarking scheme. Signal Processing 87:1264–1280, 2007
74. Rey C, Dugelay JL: Blind detection of malicious alterations on still images using robust watermarks. In: Secure Images and Image Authentication (Ref. No. 2000/039), IEE Seminar on, 2000, pp. 7/1–7/6
75. Simitopoulos D, Koutsonanos DE, Strintzis MG: Robust image watermarking based on generalized radon transformations. Circuits and Systems for Video Technology, IEEE Transactions on 13:732–745, 2003
76. Wong PW, Memon N: Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Transactions on Image Processing 10:1593–1601, 2001
77. Badran EF, Sharkas MA, Attallah OA: Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images. In: 2009 National Radio Science Conference, NRSC 2009, March 17, 2009 - March 19, 2009, New Cairo, Egypt, 2009
78. Guo X, Zhuang T-G: A region-based lossless watermarking scheme for enhancing security of medical data. Journal of Digital Imaging 22:53–64, 2009
79. Shih FY, Wu Y-T: Robust watermarking and compression for medical images based on genetic algorithms. Information Sciences 175:200–216, 2005
80. Nyeem H, Boles W, Boyd C: On the robustness and security of digital image watermarking. In: IEEE/IAPR International Conference on Informatics, Electronics & Vision (ICIEV) 2012 (accepted)
81. Tefas A, Nikolaidis N, Pitas I: Chapter 22—image watermarking: techniques and applications. In: Al B Ed. The Essential Guide to Image Processing, Secondth edition. Academic, Boston, 2009, pp 597–648
82. Nezhadarya E, Wang ZJ, Ward RK: Robust image watermarking based on multiscale gradient direction quantization. IEEE Transactions on Information Forensics and Security 6:1200–1213, 2011
83. Lie WN, Chang LC: Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification. IEEE Transactions on Multimedia 8:46–59, 2006
84. Jen-Sheng T, Win-Bin H, Yau-Hwang K: On the selection of optimal feature region set for robust digital image watermarking. Image Processing, IEEE Transactions on 20:735–743, 2011
85. Bi N, Sun Q, Huang D, Yang Z, Huang J: Robust image watermarking based on multiband wavelets and empirical mode

decomposition. IEEE Transactions on Image Processing 16:1956–1966, 2007
86. Agarwal P, Prabhakaran B: Robust blind watermarking of point-sampled geometry. Information Forensics and Security, IEEE Transactions on 4:36–48, 2009
87. Shan H, Kirovski D, Min W: High-fidelity data embedding for image annotation. Image Processing, IEEE Transactions on 18:429–435, 2009
88. Hasan YMY, Hassan AM: Tamper detection with self-correction hybrid spatial-DCT domains image authentication technique. In: 2007 IEEE International Symposium on Signal Processing and Information Technology, 15–18 Dec. 2007, Piscataway, NJ, USA, 2007, pp. 369–74
89. Lee T-Y, Lin SD: Dual watermark for image tamper detection and recovery. Pattern Recognition 41:3497–3506, 2008
90. Zain JM, Fauzi ARM: 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
91. Holliman M, Memon N: Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. IEEE Transactions on Image Processing 9:432–441, 2000
92. Al-Qershi OM, Khoo BE: High capacity data hiding schemes for medical images based on difference expansion. Journal of Systems and Software 84:105–112, 2011
93. Fan Z, Hongbin Z: Digital watermarking capacity and reliability. In: e-Commerce Technology, 2004. CEC 2004. Proceedings. IEEE International Conference on, 2004, pp. 295–298
94. Yu N, Cao l, Fang W, Li X: Practical analysis of watermarking capacity. In: Communication Technology Proceedings, 2003. ICCT 2003. International Conference on, 2003, pp. 1872–1877 vol.2
95. Smitha B, Navas KA: Spatial domain—high capacity data hiding in ROI images. In: Signal Processing, Communications and Networking, 2007. ICSCN '07. International Conference on, 2007, pp. 528–533
96. Uttridge I, Bazzana G, Gemma D, Heiler J, Giuchi M, Geyres S: Evaluation of the security of distributed IT systems through ITSEC/ITSEM: experiences and findings. In: Information systems security, ed: Chapman & Hall, Ltd., 1996, pp. 405–416
97. ISO/IEC 27001:2005. Available: http://www.iso.org/iso/catalogue_detail?csnumber=42103
98. Zain JM, Baldwin LP, Clarke M: Reversible watermarking for authentication of DICOM images. In: Conference Proceedings—26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC 2004, September 1, 2004 - September 5, 2004, San Francisco, CA, United states, 2004, pp. 3237–3240
99. Coatrieux G, Montagner J, Huang H, Roux C: 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
100. Piva A, Barni M, Bartolini F, De Rosa A: Data hiding technologies for digital radiography. Vision, Image and Signal Processing, IEE Proceedings 152:604–610, 2005
101. Raul RC, Claudia FU, Trinidad-Bias GJ: Data hiding scheme for medical images. In: Electronics, Communications and Computers, 2007. CONIELECOMP '07. 17th International Conference on, 2007, pp. 32–32
102. Zain JM, Fauzi ARM, Aziz AA: Clinical assessment of watermarked medical images. Journal of Computer Science 5:857–863, 2009
103. Guo X, Zhuang T-G: A lossless watermarking scheme for enhancing security of medical data in PACS. In: Medical Imaging 2003: PACS and Integrated Medical Information Systems: Design and Evaluation, February 18, 2003–February 20, 2003, San Diego, CA, United States, 2003, pp. 350–359
104. Coatrieux G, Lamard M, Daccache W, Puentes W, Roux C: A low distortion 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
105. Giakoumaki A, Pavlopoulos S, Koutsouris D: Multiple image watermarking applied to health information management. Information Technology in Biomedicine, IEEE Transactions on 10:722–732, 2006
106. Osborne D, Abbott D, Sorell M, Rogers D: Multiple embedding using robust watermarks for wireless medical images. In: 3rd International Conference on Mobile and Ubiquitous Multimedia, MUM 2004, October 27, 2004 - October 29, 2004, College Park, MD, United States, 2004, pp. 245–250
107. Memon NA, Gilani SAM, Qayoom S: Multiple watermarking of medical images for content authentication and recovery. In: 2009 IEEE 13th International Multitopic Conference, INMIC 2009, December 14, 2009–December 15, 2009, Islamabad, Pakistan, 2009, p. Muhammad Ali Jinnah University; University of Engineering and Technology; Institute of Electrical and Electronics Engineers; Pakistan Science Foundation; Nayatel (Micronet Broadband Group of Companies)
108. 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. vol. 5939, J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and Y. Roudier, Eds., ed: Springer Berlin/Heidelberg, 2010, pp. 153–162
109. Pan W, Coatrieux G, Cuppens-Boulahia N, Cuppens F, Roux C: Medical image integrity control combining digital signature and lossless watermarking. In: 4th International Workshop on Data Privacy Management, DPM 2009, and 2nd International Workshop on Autonomous and Spontaneous Security, SETOP 2009, September 24, 2009 - September 25, 2009, St. Malo, France, 2010, pp. 153–162
110. Li-Qun K, Yuan Z, Xie H: A Medical image authentication system based on reversible digital watermarking. In: Information Science and Engineering (ICISE), 2009 1st International Conference on, 2009, pp. 1047–1050
111. Li-Qun K, Yuan Z, Xie H: Watermarking image authentication in hospital information system. In: Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference on, 2009, pp. 1–4
112. Nambakhsh MS, Ahmadian A, Ghavami M, Dilmaghani RS, Karimi-Fard S: A novel blind watermarking of ECG signals on medical images using EZW algorithm. In: Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE, 2006, pp. 3274–3277
113. Smith JP: Authentication of digital medical images with digital signature technology. Radiology 194:771–4, 1995
114. Viswanathan P, Venkata Krishna P: Text fusion watermarking in medical image with semi-reversible for secure transfer and authentication. In: Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on, 2009, pp. 585–589
115. Pushpala K, Nigudkar R: A novel watermarking technique for medical image authentication. Computers in Cardiology 2005:683–686, 2005
116. Lin C-H, Yang C-Y, Chang C-W: Authentication and protection for medical image. In: 2nd International Conference on Computational Collective Intelligence - Technologies and Applications, ICCCI 2010, November 10, 2010 - November 12, 2010, Kaohsiung, Taiwan, 2010, pp. 278–287

117. Lim YS, Feng DD: Multiple block based authentication watermarking for distribution of medical images. In: 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, ISIMP 2004, October 20, 2004 - October 22, 2004, Hong Kong, China, Hong kong, 2004, pp. 631–634
118. Fotopoulos V, Stavrinou ML, Skodras AN: 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
119. Ahmed F, Moskowitz IS: A semi-reversible watermark for medical image authentication. In: Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Transdisciplinary Conference on, 2006, pp. 59–62
120. Guoxia S, Huiqiang S, Xinghua S, Shuzhong B, Ju L: Combination independent content feature with watermarking annotation for medical image retrieval. In: Innovative Computing, Information and Control, 2007. ICICIC '07. Second International Conference on, 2007, pp. 607–607
121. Navas KA, Thampy A, Sasikumar M: A novel technique for EPR hiding in medical images for telemedicine. In: 4th Kuala Lumpur International Conference on Biomedical Engineering 2008, Biomed 2008, June 25, 2008–June 28, 2008, Kuala Lumpur, Malaysia, 2008, pp. 703–706
122. Wu M, Liu B: Data hiding in binary image for authentication and annotation. IEEE Transactions on Multimedia 6:528–538, 2004
123. Huang H, Coatrieux G, Shu HZ, Luo LM, Roux C: Medical image tamper approximation based on an image moment signature. In: 2010 12th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom 2010), 1–3 July 2010, Piscataway, NJ, USA, 2010, pp. 254–9
124. Jun-Chou C, Chin-Chen C: Detection and restoration of a tampered medical image. In: Medical Imaging and Augmented Reality. Second International Workshop, MIAR 2004. Proceedings, 19–20 Aug. 2004, Berlin, Germany, 2004, pp. 78–85
125. Navas KA, Nithya VS, Rakhi R, Sasikumar M: Lossless watermarking in JPEG2000 for EPR data hiding. In: 2007 IEEE International Conference on Electro/Information Technology, 17–20 May 2007, Piscataway, NJ, USA, 2007, pp. 697–702
126. Zinger S, Jin Z, Sankur B: Optimization of watermarking performances using error correcting codes and repetition. Presented at the CMS'2001: Communications and Multimedia Security, 2001
127. Nayak J, Bhat PS, Kumar MS, Rajendra Acharya U: Reliable transmission and storage of medical images with patient information using error control codes. In: IEEE INDICON 2004 - 1st India Annual Conference, December 20, 2004 - December 22, 2004, Kharagpur, India, 2004, pp. 147–150
128. Machkour M, Khamlichi YI, Afdel K: Data security in medical information system. In: Multimedia Computing and Systems, 2009. ICMCS '09. International Conference on, 2009, pp. 391–394
129. Huang H, Coatrieux G, Montagner J, Shu HZ, Luo LM, Roux C: Medical image integrity control seeking into the detail of the tampering. In: Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE, 2008, pp. 414–417
130. Dickson KWC, Patrick CKH, Vivying SYC, Eleanna K: Protecting the Exchange of Medical Images in Healthcare Process Integration with Web Services. In: System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference, 2007, pp. 131–131
131. Fridrich J, Goljan M, Du R: Invertible authentication. San Jose, CA, USA, 2001, pp. 197–208
132. Cox I, Doërr G, Furon T: Watermarking is not cryptography. In: Digital Watermarking. vol. 4283, Y. Shi and B. Jeon, Eds., ed: Springer Berlin/Heidelberg, 2006, pp. 1–15