Chapter 2

Review of Medical Image Watermarking Requirements of Teleradiology

2.1 Introduction

The technological advances in communication and digital system reflected radical change in facilitating medical imaging and maintaining hospital information system (HIS), comprising radiology information system (RIS) and picture archiving and communication system (PACS). It introduced new practices for the profession as well as for the patients by enabling remote access, transmission, and interpretation of the medical images used for diagnosis purposes. But it raises new complex and legal ethical issues like image retention and fraud, privacy, malpractice liability, licensing and credentialing, and contracts for PACS and RIS.

Teleradiology is the one of the most successful Health services where the security and privacy protection has become a critical issue [15]. Remote access and transmission of the images and other radiology information, especially in electronic
personal health information (E PHI) is possible to tamper with serious ramifications and in most cases E PHI are identifiable. Such radiology images and information not only require protection with integrity but also require high confidentiality. It also needs appropriate management through different health care services.

The security and privacy of the radiology information requires the following features, (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 systems, which are thought to be incapable of providing the required security for the electronic radiology information in the PACS/RIS based [16] teleradiology. Recent studies reveals the possibility of using digital watermarking for improving security in teleradiology [17]-[21].

2.2 Verification, Validation, and Privacy Requirements in Teleradiology

Medical information security requirements must adhere to strict ethics and legislative rules based on concerned entities. The basic international standard developed for management of health information is ISO27799 (Security Management in Health Using ISO/IEC/17799) [22]. It provides guidance to health organizations and other holders of PHI on how to maintain such information on the basis of standard implementation ISO17799/ISO27002. It specifically covers the care of the patient in terms of reliability, confidentiality, and availability with respect to the particular nature of the data involved.

USA Health Insurance Portability and Accountability Act (HIPAA) [23] and
Europe’s Directive 95/46/EC develop their own verification and privacy policy as per the standards. The HIPAA take measures to ensure the verification of medical images to protect patient’s privacy. Directive 95/46/EC [24] states the legislative rules on the protection of individuals with regard to the processing and communication of personal data EPHI. There is no specialized standard similar to HIPAA but similar set of standards will eventually be required to protect online and electronic health records.

The joint committee formed by the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) developed the standard called Digital Imaging and Communication in Medicine (DICOM) [25] in 1983 for radiology. Early standards did not gain universal acceptance among manufacturers but in 1993, ACR-NEMA version 3.0 was released and the standard was renamed as DICOM 3.0. After that only this version of that standard has become universally accepted within radiology and been adopted in other medical fields such as dentistry, pathology, and cardiology. It is now commonly known as DICOM standard, an 18-part document. This standard aims to define a technical framework for medical application entities that were involved in the exchange of medical data, which satisfy the set of security profiles. For example it adds the patient and specialist information as a header to the medical image. DICOM also warrants the inclusion of the imaging information for the electronic health record systems and digital signatures for checking the integrity of the medical images.

2.2.1 Medical Information Requirements

The development and implementation of the verification, validation, and privacy protection services depend upon the model or infrastructure of the teleradiology and its concerned entities. Two widely used models in today’s teleradiology are referred by Ruotsalainen [15] are offline and online delivery of RIS. In offline, the messages
Figure 2.1: Sharing of Medical Image between Host organization and remote consultant: (a) offline transmission of RIS and (b) online transmission of RIS and medical image films are delivered to the patient and specialist with patient directly as in Fig 2.1a. In online, the patient and the specialist can download the digital medical image and patient information directly from the internet with their authorized user identification as in Fig 2.1b. Irrespective of the communication type (i.e., offline or online), there exist three individual domains namely:

- Host organization/hospital’s PACS/RIS (domain A)
- Communication network (domain B)
- Consultant (domain C) These are responsible for transmitting medical images online with required verification and privacy for a teleradiology system.
<table>
<thead>
<tr>
<th>Security</th>
<th>Threats</th>
<th>Security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>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)</td>
<td>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., and user control services for authenticating and identifying the user against identity usurpation.</td>
</tr>
<tr>
<td>Reliability:</td>
<td>Illicit destruction, production, and modification of the contents of files and records</td>
<td>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, and 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.</td>
</tr>
<tr>
<td>Availability</td>
<td>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</td>
<td>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.</td>
</tr>
</tbody>
</table>
Based on the technological and organizational models used in teleradiology, their various requirements can be outlined in all domains. The requirements such as proper authorization process must be employed through various access and user controls, transmission controls, and directive controls are essential. Integrity, authenticity, and confidentiality of all radiological information should be ensured during teleradiology session; consultation process; and information processing, management, and preservation.

The principle of requirements for security of medical information [26] needs confidentiality, reliability, and availability.

- Confidentiality ensures that only the entitled users have access to the information.
- Reliability based on the outcomes of (a) Integrity the information has not been modified by non-authorized people, and (b) Authenticity a proof that the 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.

The standards mentioned in the preceding section can be established through different stages are stated below,

- Determination of the appropriate verification of all entities and objects (e.g., IT applications and information sets) linked with the teleradiology system
- Threat analysis helps to determine the expected threats from the involved objects (e.g., infrastructure, hardware, software, and paper ware)
- Risk analysis helps to 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 threats or reducing the damages due to unavoidable adverse event.

The requirement 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. Important aspect of privacy and risk management in the context of information is to recognize the value of information and defining appropriate procedures and protection requirements for the information.

2.2.2 Expected Threats and Measures

Identifying the vulnerability of the system is important to define appropriate privacy and risk measures to strengthen the weakest link. For example, medical images transmitted over the networks can be threatened throughout their lifetime in many different ways like ill intentioned person, modification, and so on. Hence, with particular attention, suitable measures have to be evaluated to provide the required security and privacy services for the information and for the communication services. Several existing measures are currently being used such as access control services, firewall, encryption, re identification services, certification services, and so on. The review of expected threats and their conventional measures are summarized in Table 2.1. Furthermore, the possibilities of new measures such as digital watermarking, digital signature, image hashing, and so on. are being studied to fulfill the security requirements as discussed in previous section.

2.3 Limitation of the Existing Verification Measures

Existing measures are being used to protect the medical images and information, and their privacy through communications [27] like virtual private network (VPN); firewall; encryption; cryptographic hash function, or their derivatives such as digital
signature (DS); machine authentication code (MAC), manipulation detection code (MDC); and perceptual hashing.

Firewall and VPN are used for protecting the information through securing the communications of a system. A firewall is placed between two networks, which acts as a gateway to protect the network and computers from possible intrusion by hackers from the external network. The help provided by Firewall are: (1) block unwanted and unauthorized traffic from passing (in or out); (2) providing access to internal users; (3) monitoring intrusions and network problems; and (4) maintaining logs for all communication. The principal requirements of an effective firewall: (1) it must act as a gateway through which all traffic must pass (incoming and outgoing); (2) Allows only authorized traffic to pass; and (3) it acts as immunity against penetration or compromise.

The limitation of firewall is, it does not assure a secure network when representing any single point of failure. The firewall as a security tool needs proper configuration and regular monitoring. If it is not properly configured there is an option to allow unauthorized users and in denial of service attack that effectively shuts down the firewall and the network connection to the outside world. Firewall takes more time to examine incoming and outgoing traffic, which tends to degrade network performance. Firewalls are of no use to track activities on the internal network, threats from inside of an organization, and circumvented by outsiders. To maintain such critical system needs special configuration to monitor logins, failed logins, and all network activity of the internal systems.

A VPN, means transporting of information in a secure manner over an unsecured network achieved by employing some combination of encryption, authentication, and tunneling. *Tunneling* refers to the process of encapsulating or embedding one
network protocol within the packets of another network protocol. VPN protocols are like point to point tunneling protocol (PPTP), Internet protocol security (IPSec), secure sockets layer (SSL), secure shell (SSH), and so on. They are having different pros and cons such as SSL supports transmission control protocol traffic only, whereas SSL and SSH depend on only client port forwarding; PPTP use symmetric or weak encryption; IPSec supports only unicast traffic, and so on. The general perspective of information security based upon firewalls and a VPN can only be used to protect the information up to the point of the communication networks.

Cryptography has been a commonly accepted technology in health care sector to protect the privacy and confidentiality of electronic health information [28]. In that, the encryption is a process of transforming information to unreadable form called cipher. There are two types of encryption: symmetric (private/secret key) encryption (e.g., data encryption standard, Rivest Cipher RC4) and asymmetric (public key) encryption [e.g., Diffie Hellman, digital signature algorithm (DSA)]. The symmetric encryption is relatively fast but the main weakness of this type of encryption is that the key or algorithm has to be shared. The symmetric key provides no process for authentication or non-repudiation. Asymmetric encryption uses two keys as opposed to one key in a symmetric system kept secret called private key, while the other is made public 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 non-repudiation with the help of digital certificates. Yet, asymmetric encryption is relatively slower due to computationally intensive, and requires certificate authority.

File Header is a common practice of appending metadata containing owner ID, size, last modified time, and location of all data blocks as a header with the data block. The DICOM standard allows the image information with object definitions
and also the key information about the image. DICOM medical image [25] is associated with a patient’s private data such as patient’s name, age, results of examination/diagnosis, time taken, and so on. The DICOM standard stores the image data and the metadata separately. The major threats are the violation of the access rights and of the daily logs by the intruder implies that integrity and authenticity of the data cannot be guaranteed. For an encrypted header, the bit error sensitivity may result in loss of header and raise further complexity in managing the medical images [29]. Hence the patient’s private data in a DICOM image are at risk of happenings of a mismatch of disclosure and loss of header or metadata in an image undergoing some intentional processing. Cryptographic Hash Function takes an arbitrary block of data and returns a fixed-size bit string called hash value, such that an accidental or intentional change to the data will affect the hash value. The data encoded is called message and the hashes are called as message digest or simply digest. The cryptographic hash function has three main properties: (1) Infeasible to generate a message that has a given hash; (2) Infeasible to modify a message without changing the hash; and (3) Infeasible to find two different messages with the same hash. Cryptographic hash functions [30] like DSs, MACs and MDCs can also be used for other purposes for indexing data in hash tables, fingerprinting, detecting duplicate data and accidental data corruption, and so on. It is also called as (digital) fingerprints, checksums, or just hash values. The existing cryptographic hash function schemes remain vulnerable to incidental modifications (i.e., even a one bit change in the input will change the output hashes dramatically) but severely limits their practical utility in robust content authentication for multimedia applications.

Perceptual Hash Function [31] or perceptual hashing takes a large digital image as input. By using a content descriptor, it outputs a fixed length binary vector known as
Table 2.2: Limitation of the Existing Verification Measures

<table>
<thead>
<tr>
<th>Measures/tools</th>
<th>File-header</th>
<th>Cryptographic hash function and its derivatives (e.g., DS, MAC, MDC, etc.)</th>
<th>Perceptual hashing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limitation</td>
<td>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</td>
<td>Hash function cannot locate where the images have been tampered [30]. The security of DS largely depends on the strength of the hash functions used to validate the signatures. It is possible to generate two datasets with different content but having the same message-digest algorithm (MD5) hash [27]. Cryptographic hash function is extremely bit sensitive to the input.</td>
<td>Perceptual hashing usually requires searching for match and access to a central database, where a large amount of pre-computed perceptual hashes are stored. 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. Their quantization and encoding stages require the learning of appropriate quantization thresholds. The quantize training as well as the storage of thresholds introduces additional security weaknesses.</td>
</tr>
</tbody>
</table>
hash value. A perfect perceptual hashing have the following properties: (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 but the definition of difference is changed from bitwise difference to perceptual difference. Perceptual hashing consists of feature extraction and randomization that introduces compression followed by quantization and binary encoding to produce a binary hash output. The linear randomization method introduces security flaws because if the input/hash pairs are known then it can be used to recover a secret key. The storage of thresholds introduces additional security weaknesses. Hence, their limitations suggested that they are no longer sufficient to provide the required security of the medical information in teleradiology. Therefore, new security problems are on the rise due to advances of technology and developments of PACS/RIS mentioned in Introduction. The new security measures are required to be developed and deployed for the improvement in security of medical images and for EPHI. Hence, the studies and illustration in Table 2.2 reveal that the digital watermarking can facilitate sharing and remote handling of medical information in teleradiology in a secure manner. The reasonable justification of watermarking applicability for medical images is lacking.

2.4 Digital Watermarking in Teleradiology

Digital watermarking is a process that principally hides information as a ‘watermark’ into the digital media (e.g., digital image, audio, etc.). It consists of three major components: watermark generator, embedder, and detector as shown in
Fig 2.2. A watermark generator generates desired watermark that is embedded into the object by a watermark embedder using a key and the watermark detector detects the existence of watermark in the digital media. Its main issues address security in terms of authentication and integrity control of the cover object, confidentiality of the information used in watermark, and the other is to address the system considerations like saving memory and bandwidth, and avoiding detachment, for example, annotation of useful information such as electronic patient records (EPR), electronic transaction records (ETR), and so on. Digital 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, and so on, whereas 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 which are illustrated in Table 2.3. Watermarking was initiated to use for medical image applications due to its various attractive attributes [32], which are listed below: Security and Privacy. The confidentiality of medical image can be maintained by hiding the private data into the images. Hiding the necessary medical information (e.g., EPR including demographic data, diagnostic results, treatment procedures, etc.) in medical images may provide a better security against malicious tampering [33]. If it is tampered intentionally or in an unintended manner then that can be detected and possibly recovered by using an appropriate watermarking scheme. The three main objectives of watermarking in the medical image applications to provide required security for medical images are (1) data hiding, (2) integrity control, and (3) authenticity. It can be done by hiding personnel identification with diagnosis information of the patient [34].

Avoiding Detachment: Researches in this field are being accomplished to embed patient data to medical images. If the EPR and the images are separate then there is a higher chance of detachment of patient data from the image. Misplacing of a patient data will be a very critical issue in the case of medical image. In order to avoid this misplacing or detachment, watermarking [35] offers necessary data embedding within the image itself.

Indexing: The relevant keywords or indices and personnel identification can be embedded into the images and that can be used to index the image of the particular patient. It can be used for effective archiving and retrieval of the images from databases [32].
Non repudiation: In teleradiology, key-based watermarking system may facilitate non-repudiation service [36] in teleradiology. Both the parties must be approved to access the patient data and such medical data should be in safer side. It can be done by using the key shared by the hospital which could be their logos or digital signatures and the patient.

Controlling Access Provision for using keys in watermarking schemes provides an access control mechanism where the confidential metadata can be accessed with the proper authoritative rights given in terms of keys [32].

Memory and Bandwidth Saving: Storage space and bandwidth requirements are important decisive factor for small hospitals to save the financial economy. On other hand, The memory for storage can be saved to a certain extent in HIS by embedding the EPR in the image. On the other hand, a huge amount of bandwidth can be reduced by reducing the number of documents. It is required for the transmission of the image data in teleradiology by integrating the EPR with the image reduces the bandwidth limit for the transmission, which can further be reduced in telemedicine applications [32][35].

2.5 Choice of Design and Evaluation Parameters

Watermarking requirements for medical images are mainly defined in terms of security and privacy, fidelity, and computational properties. All these requirements define various watermarking design and evaluation parameters in an application scenario. Design parameters help to characterize the development of a watermarking scheme, whereas the evaluation parameters help to determine the performance of developing new scheme from existing scheme. Evaluation parameters for watermark generation and embedding include visibility, blindness, embedding
capacity, imperceptibility/perceptual similarity, and so on. Similarly, blindness, invertible, robustness, error probability, and so on are the parameters for the detection.

The system design and evaluation parameters for image watermarking are associated with its core components such as watermark generation, embedding, and detection as shown in Fig 2.2. The design and evaluation parameters [37] play an important role in achieving a particular objective in an application scenario. It has been reviewed and discussed for teleradiology application as follows.

Visibility/Invisibility: Visible watermarking is important in recognition and support of possessing a digital image. The main objective of this type of watermarking is mainly to show some necessary information such as logo, icon, courtesy, and so on through the watermarked image to verify the copyright. Contrariwise, invisible watermarks are used in digital image applications [38]-[43]; their watermarking objectives are to address the security issues of the images. In various digital image applications, invisibility of the watermark appears to be the main interest in the research of medical imaging security [44][45].

Robustness is an important evaluation parameter defined as the degree of resistance of a watermarking scheme from modifications of the host signal in order to render the watermark undetectable. This parameter is used to categorize watermarking schemes to be robust, fragile, and semi-fragile. The robust watermarking is usually for copyright protection, whereas semi-fragile and fragile watermarks are being used for annotation (e.g., hiding ETR or EPR, etc.) and integrity control (e.g., tamper detection and recovery) [46]-[53].

Embedding Capacity is a general metric to measure the number of embedding bits. Higher embedding capacity is a key issue in developing annotation or
integrity control watermarking schemes. Achieving higher 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 annotation purposes of a fragile/semi fragile watermark [54]. Research shows that the LSB embedding techniques offer comparatively higher embedding capacity.

Invertible (or sometimes referred to as reversible or lossless) watermarking is of retaining the original image from respective watermarked images by the detector. Developing this type of watermarking received much attention in medical image applications to avoid any misdiagnosis from distortions in a watermarked image [43].

Perceptual Similarity determines the degree of imperceptibility of the watermark in the watermarked image. It is evaluated between the original image and its watermarked version used only for developing an invisible watermarking scheme [37]. 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.

Verification and privacy 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.) [55].

Error probability is another important parameter for assessing detection
performance of a watermarking scheme. Zero error probability considers higher degree of robustness to any distortions [37] in a medical image application scenario in order to ensure reliable detection. The important and commonly used error probability metrics are bit error rate, false-positive rate, false-negative rate, and so on.

2.6 Digital Watermarking Vs other Measures and Tools

Table 2.4: Watermarking vs other measures and tools

<table>
<thead>
<tr>
<th>Properties and requirements</th>
<th>Digital watermarking</th>
<th>Hash function</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Perceptual</td>
<td>Cryptographic</td>
</tr>
<tr>
<td>Objective</td>
<td>Data and copyright protection</td>
<td>Data protection</td>
<td>Data protection</td>
</tr>
<tr>
<td>Host-signal/cover-object</td>
<td>image/audio data</td>
<td>image data</td>
<td>Plain text message</td>
</tr>
<tr>
<td>Secret data</td>
<td>Watermark</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Key</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Input</td>
<td>Generally the watermark and the cover-object/host-signal</td>
<td>Arbitrary block of host-signal</td>
<td>Arbitrary block of host-signal</td>
</tr>
<tr>
<td>Output</td>
<td>Watermarked data</td>
<td>Hash-values/message digest</td>
<td>Hash-values/message digest</td>
</tr>
<tr>
<td>Detection type</td>
<td>Blind, semi-blind, non-blind</td>
<td>Non-blind</td>
<td>Non-blind</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Properties and requirements</th>
<th>Digital watermarking</th>
<th>Hash function</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Perceptual</td>
<td>Cryptographic</td>
</tr>
<tr>
<td>Failure</td>
<td>Invalid watermarked image is detected as valid, or vice versa (e.g., from unauthorized removal or embedding of watermark)</td>
<td>If the message is generated from the hashes, or if another message or perceptual changes in the original gives the same hashes</td>
<td>If the message is generated from the hashes, or if another message in the original gives the same hashes</td>
</tr>
<tr>
<td>Impact on quality/content of the image</td>
<td>Yes, but can be acceptably reduced/resolved by considering non region of interest (RONI) or reversible watermarking</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sensitivity to bit error</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Robustness</td>
<td>Can be designed as robust, semi-fragile, fragile</td>
<td>Robust</td>
<td>Robust</td>
</tr>
<tr>
<td>Authentication/integrity check</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tamper localization</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Confidentiality of metadata</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Database requirement</td>
<td>No, it can operate in stand-alone environment</td>
<td>Yes, for storing precomputed perceptual hashes</td>
<td>No</td>
</tr>
</tbody>
</table>
Watermarking and other comparable security measures and tools for teleradiology are based on various key properties and requirements of medical image applications as presented in Table 2.4. It illustrate, cryptographic/perceptual hashing, which is suitable for legacy content, but they are either bit-sensitive (for cryptographic hash functions) or need access to a central database for precomputed hash (for perceptual hashing). It has no impact on quality of image, whereas research suggests that a carefully designed watermarking scheme does not alter medical diagnosis [56].

The three ways to overcome the distortion induced in images by watermark embedding are as follows: (1) Defining embedding method with less rate of modification to provide acceptable range of distortion, (2) Image is separated into protection zone and insertion zone such as ROI (region of interest) and RONI (region of non interest), and (3) Reversible watermarking to recover the original image.

The watermark embedding having acceptable range of distortion is expensive, which is applied by Zain et al., [56] for clinical decision. The separation of ROI and RONI in medical images should not be done directly without the interaction or approval of the doctor or radiologist. It has been applied in several watermarking schemes but found very difficult to separate. Besides, Reversible watermarking is a promising method for taking no risk for sacrificing the diagnostic accuracy to medical image application, but may incur additional complexity in different processing domains. The two limitations of reversible watermarking: (1) It imposes removal of embedded watermark after the extraction or before the diagnosis and (2) Once the watermark is removed, the image is not protected anymore like in cryptography. All these suggested that the concept of multiple watermarking systems is needed to address the rising security problems of medical images in teleradiology [57]. It also shows that incorporation of asymmetric encryption system and lossless compression can help in attaining additional confidentiality, non-repudiation property, and high
embedding capacity. The requirement of digital watermarking is compared with other approaches for solving all the security issues of teleradiology as illustrated in Table 2.4.

The encryption with watermarking is employed to provide additional confidentiality of metadata (e.g., in generating watermark) in which patient information, hospital logo, and message authentication code computed using hash function are used as watermark. To ensure inaccessibility of embedded data to the adversaries, the BCH encryption watermarking and DSA based on RSA public cryptosystem with reversible digital watermarking are used. The few recent studies suggested that the use of a compression technique for attaining the embedding capacity is the needed requirement of watermarking.

2.7 Objectives and Applications of Watermarking for Medical Images

A digital medical image application is therefore one of the prospective target areas of using digital watermarking [58]-[60]. Studies show that various watermarking schemes can be used in teleradiology for (1) origin/content authentication, (2) EPR annotation, and (3) tamper detection and recovery of medical images. Some important aspects of medical image watermarking schemes for their different objectives are summarized below.

Origin/Content Authentication: The important details can be hidden in images with imperceptibility and without causing harm to the ROI. It ensures the origin and content authentication of the images. The above observation suggests the following requirements for watermarking in teleradiology: (1) The watermark should be invisible, blind, and robust. (2) The watermark should incorporate the minimum
information required for the origin authentication. (3) The embedding process must consider the RONI. (4) The proper validation of a watermarking scheme required such that the permanent association of the watermark is reliable and safe for diagnosis.

EPR Annotation: Three key requirements for EPR data hiding and transmission are (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. For higher capacity, the watermarking scheme can be semi-fragile, although it requires defining appropriate set of necessary operations or 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 for improving watermarking performance with quality. For additional confidentiality, encryption of the EPR can also be used during watermark generation.

Tamper Detection and Recovery (Integrity Control): Integrity of a medical image can be achieved in three levels (1) tamper detection, (2) tamper localization, and (3) possible recovery by approximating the tampered region. In order to achieve this without affecting the basic requirements of medical image, the watermarking scheme should be (1) fragile and blind and (2) reversible or RONI based embedding. Fragile watermarking help to locate the tampered region with its fundamental property such that a watermark becomes invalid for any malicious or unintentional modifications in the watermarked image. Tamper detection and recovery received much interest in the research of LSB embedding based watermarking schemes, since consideration on the embedding capacity is equally important for both watermarking objectives.

2.8 Summary

The learning of verification and privacy problems is a continuous process due to
influence of technological advances in the teleradiology. The study of requirement and finding relevance, suitable new schemes, and their evaluation is used to develop its way to medical image applications. It is investigated from the applicability for the strict requirements of medical images described in three parts, namely: (1) the verification and privacy requirements; (2) conventional 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 used for availability in online sharing. The DICOM standard as well as ISO27799 and other government regulations such as HIPAA, CFR 45, Directive 95/46/EC, and so on, impose rules as national/international standards to protect individuals health information, highlighting verification and privacy protections. Three mandatory characteristics are confidentiality, reliability, and availability that need to be achieved for medical images to verify the issues for teleradiology.

The complete solution for various verification and privacy problems for teleradiology discussed so far is still lacking. Conventional measures have their limitations but they cannot be replaced with any individual measure. 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. Watermarking complements the security of multimedia data, which provides a great prospect for teleradiology because it functions as a communication tool with the authenticity of the origin or sender, non-repudiation, detection of data tampering, memory and bandwidth saving, integrity of the image, and so on. The general requirement for any medical
image watermarking implies that watermarking needs to be invisible and blind. 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.

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. 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. Multiple watermarking schemes and their complete assessment through defining the parameters properly show 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.