Journal of Theoretical and Applied Information Technology
10th July 2014. Vol. 65 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY ON WATERMARKING TECHNIQUES, REQUIREMENTS, APPLICATIONS FOR MEDICAL IMAGES

R.LAKSHMI PRIYA[1], V.SADASIVAM[2]
[1]Research Scholar, [2]Principal
Department of Computer Science and Engineering
PSN College of Engineering and Technology, Melathediyoor
Tirunelveli, India-627152
rlpriyajagan@gmail.com, vs_msu@yahoo.com

ABSTRACT

Medical images are often transmitted over insecure channel. Telemedicine enables medical diagnosis and patient care using modern medical equipments. These equipments generate huge volume of data every day. Hence protection of medical image is very crucial. Many approaches like encryption, digital signature, watermarking etc are spotted in the literature. Watermarking in medical images is commonly used for content authentication, effective data distribution and management, storage, security, safe archiving, controlled access retrieval and captioning. The objective of this paper is to present a survey and compare emerging techniques for protection of medical images through watermarking. Various aspects of medical image watermarking are discussed in this paper including classification and performance measures used in recent research. Finally the paper reviews and remarks about the state of the art and compare some recent works on watermarking.

Keywords: *Medical Image Watermarking, DICOM, Electronic Patient Record, Integrity, Authentication, Security, Tamper Localization*

1. INTRODUCTION

In recent years, the sporadic developments of Internet and Multimedia Technologies have facilitated the reproduction of digitally created information simple and easy. The advancements in these technologies have made it possible to create, replicate, transmit, and distribute digital content in an effortless way. Hence the protection and enforcement of intellectual property rights for digital media has become a crucial issue. In recent years the research community and the academicians were focusing on digital watermarking schemes to protect digital content. Among many applications e-health service maintains and transmits medical transcriptions via internet.

Telemedicine is the use of information and communication technologies to provide health care where the patients and participants are separated by geographical distance. A schematic diagram of telemedicine system is shown in Fig. 1. Modern integrated health care systems like Hospital Information System (HIS) and Picture Archiving and Communication System (PACS) provide easy access, manipulation and efficient distribution of medical data [10],[50],[59],[75], [82]. Medical images require strict security in view of its importance in clinical diagnosis, treatment, education and in research. Many hospitals that are geographically dispersed share medical images for e-diagnosis, e-treatment etc. Also HIS and PACS generate huge volume of clinical data like demographic data, images and reports. This huge data acquired should be stored, processed and managed which raises security issues like confidentiality, integrity and authenticity. Wong et al. [95] were one of the first few researchers to address authenticity and integrity of medical image which was published in 1995. But only after 1999 the research on security of medical images got great attention.

Digital watermarking has been proven as a promising technique that can address all security issues [41], [64], [70]. Watermarking technique imperceptibly modifies the cover image with some important information required for diagnosis [8]. The radiologist takes the image and embeds his inference with the help of some embedding algorithm with the patient's electronic record [39] such as name, age, sex etc. Then he stores the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

image in the database where entire historical data are stored. This enables the doctors to view the vital organs, identify blockages and growth and diagnose signs of disease without doing surgery. The doctor can also embed the diagnostic data into the image and ask for second opinion to some other doctor located in some remote area. The second doctor can then embed his own diagnosis data and send back to the first doctor [92], [93].

This paper discusses different applications of Medical Image Watermarking (MIW), study the requirement of MIW, classify MIW into different categories, present the various performance measures found in the literature and also impart different attacks on MIW.

The rest of the paper is organized as follows. Section 2 tends to discuss the various applications of MIW. In section 3 the requirements meant for MIW are elucidated. Section 4 classifies and discusses the different approaches that have been proposed for MIW in the literature. Then section 5 presents the various measures used to evaluate the performance of MIW techniques. Later, various attacks on MIW were also addressed in section 6 which would help the researchers to build robust scheme. Finally, section 7 compares some of the latest work published in last five years and section 8 concludes with directions for future research.

2. APPLICATIONS OF MEDICAL IMAGE WATERMARKING

Medical Image watermarking has been used for different applications [28] like Compact Storage, Saving Bandwidth, Avoiding Segregation, Tamper Proofing, Confidentiality and security, Indexing, Integrity Control, Captioning, Access Control and Origin Identification as discussed below.

Huge amount of medical images are generated every day. Generation and managing the medical data is a challenging task faced by radiologist. In many hospitals electronic patient's record (EPR) and medical images are stored separately. Requirement for memory for storage of images and patient record may increase rapidly. Hence embedding the EPR [55] in the patient's images may save lot of memory [72]. And also if EPR and medical images are stored separately there is a chance for disconnection of patient data and image. Isolation or misplacing of patient data may create a problem in diagnosis which may lead to loss of money as well as life. To avoid segregation of EPR and medical images, Aggeliki Giakoumaki et al. [1] introduced watermarking technique to embed patient data & related information in the image itself. Transmission of multimedia data involves high bandwidth usage. Bandwidth is an important resource in network environment. Integration of EPR and the medical image saves the bandwidth requirement rather than sending EPR separately and medical image separately [74].

Hospital Information Systems (HIS) and Picture Archiving and Communication Systems (PACS) retrieve images based on querying mechanism [19], [37], [49]. As the communication of medical images extends beyond private network, there is a chance for casual or malicious tampering of medical image. Hence confidentiality and security of medical data is of paramount significance in medical data management systems. No patient likes to expose his/her medical report to public. Hence by imperceptibly embedding EPR data with advanced encryption techniques confidentiality and security may be maintained. To detect tampering, fragile watermarking techniques have been proposed. Fragile watermarking techniques embeds watermark that easily gets distorted in case on modification. Such watermarks can be used to authenticate the content. Works based on fragile watermarks even identifies the tampered regions, extent of tampering and even determines whether the data is truthful or not [27], [46].

Digital watermarks embed EPR in the image such that bandwidth and memory are utilized efficiently and effectively. It also provides a mechanism for storage of diagnostics data permanently into the image [13], [56]. Access to the images is made by proper keys only. For this reason watermarking is rising as a prospective tool for access control mechanism since different keys may disclose dissimilar information [6], [33]. Watermarks can also play the role of keywords or indices (e.g., ICD-10 diagnostic codes, image acquisition characteristics, patient demographics etc) for effective retrieval and archiving [9], [43-44], [85]. Watermark can also be used for captioning. Caption or annotation watermarks can be used for providing additional information that is useful for diagnostics. Caption watermark includes health history of patient and diagnostics reports [79]. Digital Signature or physician identification code is used as secret data in many reported works in the literature. In such cases the watermark can be used for origin identification. When watermarking combined with cryptographic technique complete protection is ensured.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. REQUIREMENTS OF MEDICAL IMAGE WATERMARKING

Teleradiology is the transmission of radiological patient images from one location to another for the purposes of sharing studies with other radiologists and physicians [78]. In particular medical image plays a vital role in telesurgery, telediagonosis etc,. Security and privacy protection are critical issues to be considered in teleradiology [20], [68-69]. The security issues that need consideration are Confidentiality, Reliability and Availability.

- Confidentiality: It implies that only the authorized users can have access to the medical data [4].
- Reliability: It signifies two aspects a) Integrity- a proof that the information has not been altered or modified by unauthorized person. b) Authentication-a proof of the information origin and correct patient.
- Availability- It ensures access to medical information by the authorized users in usual conditions of access and exercise.

Security of medical images is very important when images are exchanged via Internet [11]. In such cases, confidentiality and reliability are to be primarily considered. Digital watermarking techniques have the impending to act as a valuable tool for different range of security issues such as confidentiality, origin authentication, ROI protection, integrity and retrieval [23-24]. Watermarking techniques for medical health care applications differs from multimedia applications based on the properties of medical image and purpose of usage. The following requirements are specific to design authentication schemes for medical images.

Reversible: Medical images require intactness and good fidelity for diagnostic purpose. Hence it demands recovery of original image without any loss after removing the watermark [98-99]. So the watermarking scheme should be reversible [29], [87]. Barton [7] was the first to propose reversible method. Reversible data hiding assist in recovering the cover media lossless after the hidden data is extracted [5].

Tamper detection: Hospitals, insurance companies and even patients may alter the image for illegal purpose. Therefore the requirement is that when watermark is extracted the system should determine whether the image is tampered or not. In other words tamper detection mechanism facilitates to identify whether the image is authentic or not [61].

Localization: When tampering is detected the scheme should be able to locate and recover the tampered region without any loss. That is the extraction and verification should be clever to reproduce and locate the illegally modified region of the image [42].

Imperceptibility: The watermark should not be noticeable under normal vision to the viewer nor should degrade the visual quality in the image. For medical applications visible watermarks are not encouraged.

Robustness: The watermark should resist attempts that were made to remove or destroy. They are mainly used for content tracking and copyright protection.

Capacity: Capacity describes how many information bits can be embedded. Higher capacity is normally achieved at the expense of other two requirements, imperceptibility and robustness.

Blind Detection: The extraction process should not require the original image and original watermark. This is very important requirement for medical images to guarantee better security [45].

Fragility: The scheme should be sensitive to the attacks, so that the watermark can be easily broken in order to authenticate.

Security: Security implies that the watermarking should be difficult to remove without altering the cover image. It can also be defined as the ability to ensure authenticity and integrity of the watermark under malicious attack.

Time: The time needed for embedding and extraction should be kept small. It should be possible for the doctors to have a fast access to stored images and to make a report.

4. CLASSIFICATION OF MIW

Medical Image Watermarking techniques can be classified into different categories based on Extraction Method, Embedding Domain, Characteristics, ROI Protection, Purpose and Tamper Detection Mechanism

4.1. Extraction method

The extraction process separates the cover data and watermark from the watermarked data. It is used for the verification and validation of the cover data. The extraction process may be carried out with or without the knowledge of the cover data or watermark.

According to the extraction process the MIW can be classified into blind and non blind watermarking. If the extraction process requires the original data or the original watermark, then it is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

called as non blind watermarking, otherwise it is known as blind watermarking. The latter is more suitable for practical applications because the original data or the watermark is often not available at the recipient side.

A non blind, imperceptible and robust hybrid watermarking algorithm for medical images is proposed by Sudeb Das and Malay Kumar Kundu [81]. Contourlet transform is applied to the medical image and then the coefficients are divided into 8×8 non overlapping blocks. Each block is transformed to frequency domain using DCT. EPR is encrypted using Advanced Encryption Standard (AES) using a secret key. It is then concatenated with source authentication information and querying information to form the watermark. BCH (*Bose – Chaudhuri - Hocquenghem*) error correcting code is applied and then the resultant data is scattered. During the extraction phase the original image is required and the other process is exactly the reverse operation as that of embedding. The performance is assessed by using Peak Signal to Noise Ratio (PSNR), Mean Structural Similarity Index Measure (MSSIM), Normalized Correlation (NC) and Bit Error Rate (BER). This technique is more robust to attacks and is imperceptible. However, it requires the original image for detection due to this reason it cannot be applied in real time scenarios.

A blind watermarking technique is proposed by Osamah M.Al-Qershi and Bee Ee Khoo [63]. This method is based on Tian [84] method which aims to increase the hiding capacity. It is a block based algorithm which divides the image into 4×4 non overlapping blocks. Two dimensional Haar Discrete Wavelet Transform is applied to each block [58]. Expandable and non expandable blocks are identified. To each expandable block 16 bits of payload is embedded. First four pixels of each block is used to store embedding map. PSNR and SSIM is used to evaluate the performance of the scheme. The scheme achieves high embedding capacity and high visual quality. However the PSNR value decreases with the increase in capacity which identifies the inverse proportionality between the imperceptibility and capacity.

4.2. Embedding Domain

MIW schemes have been developed in both spatial domains as well as in transform domain. Spatial domain techniques exploit the spatial relationships between pixels. Spatial domain techniques are simple and fast. On the other hand transform domain techniques are more robust to attacks. Few spatial domain and transform domain techniques were discussed in this section.

4.2.1 Spatial Domain Techniques.

Spatial domain watermarking techniques offer number of advantages. These schemes are often fragile and hence mainly used for tamper detection and for content authentication. In spatial domain schemes the watermark is directly embedded by modifying the pixels of the original image without applying any transformation. Hence these schemes are computationally less complex. One such technique proposed by Sudeb Das and Malay Kumar Kundu [80] incorporates ROI protection and tamper detection mechanism. Two different watermarks are embedded in the medical image. One is encrypted EPR/DICOM metadata, keywords, Doctors ID, ROI information and other support information. The second watermark is binary location map, which is used for tamper detection and localization. The watermark is dispersed using one-to-one mapping function. AES, SHA256 and arithmetic coding are used to enhance the security of the system. Performance is measured for images in 7 different modalities in different formats in different bit depth and different sizes. The authors claim that their mechanism achieved superior tamper localization capability, higher capacity and imperceptibility. The method is relatively simple and consumes less time for archiving and retrieval. However two bit planes are used for embedding which results in image degradation.

4.2.2 Transform Domain Techniques.

In transform domain techniques the watermark is embedded after performing transformations such as, Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) etc. The watermark is embedded in the transform coefficients. When compared to spatial domain these techniques offer high security and are robust to attacks. Table 1 shows the strength and weakness of both spatial and frequency domain techniques.

With an intention to increase the robustness a reversible technique based on wavelet transform is proposed by Lingling An et al. [47]. It includes Property Inspired Pixel Adjustment (PIPA), Statistical Quantity Histogram (SQH) shifting and clustering, and Enhanced Pixel-wise Masking (EPWM). PIPA preprocess the image to avoid overflow and underflow. SQH with threshold constraint with k-means clustering is employed to resist unintentional attacks. EPWM is used to balance invisibility and robustness. Experimental results were shown for three different types of images namely, natural images, medical images and synthetic aperture radar image. Results are found to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

be encouraging. Another wavelet based coding method is proposed by Penedo et al. [66] for digital mammography.

A DCT based fragile invertible watermark is proposed by Al-Gindy [3] which is a block based approach applied to medical images. The watermark is a unique 14 decimal digits representing patient's entry date and file ID. The original image is divided into 8×8 sub block and DCT transform is applied to all blocks. For each block one DCT high frequency coefficient is identified and watermark is scrambled randomly using a secret key. The extraction process is exactly the reverse of the embedding process. Performance is measured using PSNR by varying the watermark strength. PSNR of 73dB and 71.5dB is obtained for watermarked and original image. Robustness of the proposed method is evaluated under different attacks.

4.3 Characteristics

MIW can also be classified into two types based on its ability to resist attack; namely, robust and fragile.

4.3.1 Robust Watermark: Robust watermarks are resistant to some image processing operations like, rotation, scaling, cropping etc. Robust techniques assume the transmission channel is lossless. Hence these methods embed watermark in lossless and lossy environment. As a consequence, robust watermarks can be extracted back even after intentional or unintentional attack. Based on the resilient property these watermarks are used for copy protection and copy right protection [60]. Results shows that the method is robust against attack, however the method lacks tamper detection mechanism.

4.3.2 Fragile Watermark: Fragile watermarks are generally used for content authentication. Fragile watermarks cannot resist attacks. It easily gets modified when host image is distorted. So, it is mainly used for integrity verification. Traditionally checksum and pseudo-random numbers are used as fragile watermarks. Latest techniques deploy cryptographic hash function for embedding. Many fragile watermarking techniques are block based technique and authentication code for each block is computed and embedded in the image. Upon reception the code is extracted for each block and compared with known code. If there is mismatch then the image is tampered. Chaw-Seng Woo et al. [14] have proposed multiple watermarks out of which one watermark is fragile used for tamper detection.

4.4. Purpose

The watermarks are embedded into medical image for three purposes. One is for hiding electronic patient's record, second one is integrity verification and the last is for authentication.

4.4.1 EPR hiding watermarks

EPR hiding watermarks aim at reducing the storage space as well as to avoid detachment of image and patients data. When the patient's data and images were stored separately excessive memory is required as well as when transmitted through internet it brings transmission overheads [17-18]. In order to efficiently use the memory and network bandwidth patient's data can be embedded into image. Patient's demographic data, ECG signal, patient name, ID, sex, age, physician identity etc. can be embedded as EPR into the original image [22], [65], [76]. Acharya et al. [73-74] proposed to hide some text and ECG signal. It is first enciphered before embedding it into the patient image. Lou et al. [48] proposed a multi-layer data hiding scheme based on difference expansion. The results are found convincing which maintains quality with higher embedding capacity. Coatrieux et al. [26] proposed a watermarking scheme to hide anonymous patient data in order to verify authenticity of medical image.

ECG signal and patient's ID are used as double watermark [57]. These watermarks are embedded into gray scale Positron Emission Tomography (PET) image. The PET image is decomposed into seven sub-bands using two level dyadic wavelet transform. The watermarks are embedded into the two dimensional wavelet sub-bands using a texture feature extraction algorithm. Evaluation shows that the watermark is robust and resilient when subjected to various attacks. High quality watermarked image is obtained for JPEG compressed image up to quality factor of 85%. However if the size of ECG signal increases the quality tend to decay. And also tamper detection and localization mechanism are not incorporated which is essential for medical image authentication.

4.4.2 Integrity Watermarks

Integrity ensures that the image has not been modified by unauthorized persons. Coatrieux et al. [30] states that integrity verification is an analysis process which asks three main questions? Is the image identical to the original image? If it is not, which parts is untrustworthy? And, what is the motive of tamper? Many techniques for integrity verification have been proposed in the literature which embeds image digest, digital signatures, hash of image etc. Sudeb Das and Malay Kumar Kundu [80] have used SHA256 to ensure the integrity of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the medical image. Coatrieux et al. [30] have addressed all the issues by extracting 3 watermarks for modification detection, tamper localization and to identify the nature of modification. Secure hash and signature of different parts of image is embedded as watermark. Knowledge digest is also used for integrity verification [25]. Similarly many authors have used hash of the image [21], ROI of the image [96] or DICOM header [40], [51] for integrity verification.

4.4.3 Authentication Watermarks

Medical images are of paramount importance for its use in diagnostic, education and research. Fragile watermarks are usually employed for authentication purpose, which identifies the source of the image. Upon reception the legitimate recipients of the marked image can verify the authenticity by checking the presence of source watermark [71], [97], [100]. If the watermarked image is tampered then the embedded watermark is undetectable and the recipient can understand that the image is not trustworthy. Celik et al.[12] introduced a reversible data embedding technique by compressing the quantization residues for image authentication. Zhicheng Ni et al. [101] proposed a lossless semi fragile data hiding scheme for verifying the authenticity of medical image.

Tan et al. introduced a dual layer reversible watermarking technique to ensure authenticity of the image [83]. The images were first decomposed into 2*2 non overlapping blocks. One pixel from each block is chosen as an estimator and other three pixels are used for embedding one bit each. The location of the estimator is kept secure by encrypting its location information using RSA algorithm. In the first layer, patient information, authentication information and location of estimator is embedded. In the second layer, tamper localization information is embedded. For tamper localization CRC-16 is computed and embedded into the same block. The hiding capacity achieved is 0.75bpp. Though this scheme can locate tampered regions it cannot recover the tampered region.

The technique proposed by Marco Fontani et al. [53] embeds the watermark into wavelet transform coefficients. It is a block based techniques which hides secret data only in HH coefficients. LSB technique or p-bit shifting technique is used for embedding. The information about LSB changeable and non changeable is embedded as a location map. Upon extraction the LSB changeable blocks are identified and the watermark is extracted. The method is simple and reversible. But instead of watermarking each image the digital signature of group of images are embedded in a single image. When that particular image is tampered the entire image set cannot be verified.

4.5 ROI protection

A Medical image consists of region of interest (ROI) and region of non interest (RONI). ROI is very significant region which is used by doctors for diagnosis and treatment [2]. Using ROI region for watermarking may distort the pixel in those regions which may consequently lead to misdiagnosis. Hence at most care is given by many authors [52], [54], [91] to preserve the ROI region. So RONI watermarking techniques embed watermarks in regions that do not affect medical diagnosis.

Gouenou Coatrieux et al. [30] with an aim to detect malevolent image alterations and to identify the nature of modification have proposed non significant region watermarking. This method makes use of three watermarks out of which first two are used for modification detection and localization and the third one for detecting the nature of modification. The method first splits the image into region of interest (ROI) and Region of non interest (RONI). Three signatures (H1, H2, and H3) are computed based on ROI and embedded in RONI region. H1 will indicate whether the image is modified or not. H2 is used to identify the tampered location and H3 is to find whether the modification is throughout the whole image or within some region. H3 is calculated based on image moment signature to identify the nature of tamper [34]. This method makes use of multiclass SVM classifier to find the nature of modification. The classifier is able to detect 8 types of modifications, however the method may fail in case of non anticipated modifications. Also the method seems to be highly complex.

In order to avoid compromising diagnostic ability Coatrieux et al. [31] has separated the image into the protection zone and insertion zone. Underlying this idea the medical image is separated into ROI and RONI region. Three signature namely cryptographic hash, single parity and linear block codes are computed for ROI region and are embedded into RONI region. Results show that this technique can detect tamper, However it is assumed that ROI consist of 75% of the image.

Though RONI watermarking leaves the diagnostic information intact, it can be applied only if RONI region exist. Also the embedding capacity may depend on size of RONI.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.6 Tamper detection mechanism

Medical images are easily subject to modification [102]. Hence it is very essential to identify whether tampering has been made on the image. Reversible watermarking technique can implement tamper detection mechanism [32]. Tamper detection mechanism permits to identify the regions of image which have been tampered.

Xiaotoa Guo and Tian-ge Zhuang [96] have proposed a region based lossless watermarking scheme for tamper detection. Hash of the original image is computed and digital signature (DS) is produced based on hash value. Region of embedding is identified by the radiologist such that it does not intersect ROI. Payload comprising patient details is concatenated with DS then encrypted using Rivest Cipher 4 (RC4). Some predefined location is identified and the least significant bits are extracted and ordered sequentially to form bit stream which is then combined with payload and once again encrypted. This is then embedded using difference expansion technique. This scheme achieves high embedded capacity with better visual quality. However if tamper occurs in region of embedding (ROE) then the authentication data may be lost.

Wu et al. [36] has proposed two techniques for tamper detection and recovery. The image is first divided into non overlapping blocks. In the first technique authentication message and recovery message of other blocks is embedded in each block using modulo operation. The second method is ROI based where the recovery information of ROI is embedded in other blocks. If ROI is tampered the approximate image can be obtained from other blocks. The drawback of this work is payload in second method is depended on the size of ROI and also some image may contain multiple ROI which is not considered.

Chiang et al. [16] proposed a mechanism for tamper detection, localization and recovery based on 2 dimensional difference expansion schemes. Before embedding the image is first decomposed into 4*4 block. Two-level DWT transform is used which transforms the smooth blocks into frequency domain. Leaving the uppermost pixel all other pixels of the smooth blocks are transformed to zero. To the rightmost pixel a non-zero value is embedded. All other 14 bits are used for embedding payload. Although the scheme is simple and can accommodate high capacity, the drawback is that the scheme depends on number of smooth blocks.

5 PERFORMANCE MEASURES

In order to measure the performance of the watermarking techniques the following measures were employed in the literature.

5.1 Image Quality Analysis

Watermarking has been proved as a promising technique for providing security, confidentiality and reliability for medical images. Medical image watermarking is used to check the integrity of medical images. The key problem is that, the medical images undergo degradation when secret data is embedded. Generally the requirement is that the images should remain intact and no visible alteration is accepted. No radiologist will accept to use degraded image for processing even though the modification may be slighter. This section discusses the metrics that are used to quantify image degradation.

Mean Square Error (MSE) - compares two images on pixel-by-pixel basis. Mathematically, *MSE* is expressed as:

$$MSE(I, Iw) = \frac{1}{m \times n} \sum_{i}^{m-1} \quad \sum_{j}^{n-1} [I(i,j) - Iw(i,j)]^2$$

Where I is the original image and Iw is the watermarked image both images containing M × N pixels. This measure gives an indication of how much degradation was introduced at a pixel level. The higher the mean square error greater the level of degradation is.

Peak Signal-to-Noise ratio (PSNR) - The visual quality of the embedded images can also be measured using the peak signal-to-noise ratio (PSNR). It is used to measure the distortion between an image I and its watermarked version Iw.

$$PSNR\ (I,Iw) = 10 log_{10}\left(\frac{255^2}{MSE(I,Iw)}\right)$$

Where I and Iw are original image and watermarked image, MSE is mean squared error. Higher value of PSNR indicates less distortion. Chen and Ramabagran [15] have reported that PSNR value between 40-50dB is acceptable. Dalel Bouslimi et al. [21] have claimed that the PSNR value of their method is much above the values pointed out by Chen and Ramabagran [15].

Weighted PSNR - The weighted PSNR is a quality metric that assigns different weights to the perceptually different images regions based on the noise visibility function (NVF) [88-89].

$$wPSNR\ (I, Iw) = 10\ log_{10}\left[\frac{{I_{max}}^2}{\|NVF(I_w(m,n) - I(m,n))\|^2}\right]$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Structural Similarity Index Measure- was used to measure the similarity between the original image and the watermarked image. The value 1 indicates that both images are similar [62], [103].

Total Perceptual Error- It is calculated from the Watson Metric. Lower the value of TPE the better the result [94].

Entropy-The entropy (H) represents the amount of information that is present in the image. The entropy is given by the equation

$H(I,Iw)=\sum_k p_k \ log_{2(p_k|q_k)}$

Where p and q are the probability distribution of I and Iw with k pixel intensities. Entropy of an image is expected to be low for similar image. 0 indicates both images are identical.

5.2 Image Error Analysis

The error in the image can also be utilized to evaluate the quality of the watermarked image. It can be computed by the following measures.

Mean Absolute Error (MAE) - It calculates the absolute pixel by pixel differences in original image and watermarked image [67]. Lower value indicates that the original image and watermark image are close.

Root Mean Square Error (RMSE) - Lower the value of RMSE indicates lower the difference between Original and Watermarked version.

Percentage fit Error (PFE)- It measures the deviation from original image and watermarked image. The value 0 indicates that there is no deviation [86].

Image Error Rate (IER) – It refers to the ratio of the number of the images recovered with errors to the total number of images used for testing.

Bit Error Rate (BER) – It is the ratio of bits received in error to the total number of bits received.

Normalized Cross Correlation (NCC)-The NCC used to verify the robustness of the watermarking systems, by expressing the comparability between extracted watermark and original watermark quantitatively. NCC is defined as

$$NCC = \frac{\sum_x \sum_y W(x,y)W'(x,y)}{\sqrt{(\sum_x \sum_y [W(x,y)^2]).(\sum_x \sum_y [W'(x,y)]^2)}}$$

Where, ***W(x, y)***, ***W'(x, y)*** are the original watermark image and the extracted watermark image respectively. ***NCC*** is a value between 0 and 1. The larger the ***NCC*** value, the higher the watermark robustness.

5.3 Capacity

Bits per pixel- It is used to measure the hiding capacity. It corresponds to how many bits be embedded in a pixel. Higher the hiding capacity lower the quality will be. Capacity, robustness and imperceptibility are in trade off .Higher capacity can be achieved at the expense of either robustness or imperceptibility.

5.4 Complexity Analysis

The average time taken for embedding is calculated. Lower the time taken, the complexity of the system is assumed to be less.

6. ATTACKS ON MIW

Medical images are highly valuable owing to its importance in diagnosis, research and education. Hospital Information System and Picture Archiving and Communication System shares medical images via internet and intranet. When the images are transmitted there is the possibility of attack either intentionally or inadvertently. Intentional attacks are performed to destroy the hidden watermark. Whether the attack is intentional or unintentional they degrade the quality of the image and affect the performance of the system. Hence the watermarking system should be robust enough to survive the attacks. Some counterfeiting attacks that are common for medical images are discussed in this section.

6.1 Cryptographic Attacks

Watermarking is coupled with cryptographic techniques to ensure complete security [20-21]. Some works on joint encryption and watermarking techniques have been proposed in the literature. DICOM, the standard of reference for medical images also allows encryption techniques like triple DES, AES etc,[35]. Hence performance of such joint techniques should be analyzed for cryptographic attacks like known plaintext attack, cipher text only, chosen plain text and on chosen cipher text attacks. Also some attacks aim at cracking the security methods those were employed in watermarking schemes. Example of these attacks includes brute-force search and oracle attack. Brute force search attack aims at finding the embedded secret information whereas oracle attack creates non watermarked signal from watermarked signal [90].

6.2 Geometrical Attacks

Geometrical attacks are based on geometrical transformations, which modify the spatial relationship between the pixels [77]. Some of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

geometrical attacks are rotation, translation, scaling, cropping etc.

6.3 Protocol Attacks

Protocol attacks are based on the idea that the attacker embeds his own watermark in the image and claims that he is the owner of the image and proving it by extracting his own watermark from it [90].

6.4 Watermarking Attacks

Three types of watermarking attacks have been defined by Zhou et al. [104] are given in this segment.

Unauthorized Detection/ Extraction of Messages- In some applications detection of watermark may be a protected action. If an adversary aspires to detect or extract such watermark it is called unauthorized detection or extraction of message.

Unauthorized Embedding Attack- In these attacks an adversary may intend to copy the legitimate watermark from one image to another and may aggravate the ownership authentication process.

Unauthorized Removal Attack- In some cases the original image and extracted image may not match so that it may be rejected. Valid watermark may be present in the rejected image. If someone changes the embedded message, they should also provide a new set of watermarking keys.

Jonathan Blake and Shahram Laifi [38] has identified another watermark attack called unauthorized modification, which is the combination of removal and embedding attack.

7. DISCUSSION

Comparison of some of the research papers published in the last five years is illustrated in Table 2.From the table it is noticed that both spatial domain techniques as well as frequency domain techniques were prominent whose strength and weakness are already discussed. Discrete Wavelet transform is preferred rather than discrete cosine transform and discrete fourier transform. Discrete cosine and discrete fourier transforms are rarely used for medical image watermarking whose applicability to this scenario can be investigated in future. Further, methods based on spatial domain are less complex and provides better visual quality and capacity, while methods based on frequency domain are robust to attack.

Embedding of watermarks in region of non interest (RONI) is proposed with the aim to leave the ROI intact for medical diagnosis. But methods based on ROI protection claims that ROI is only lossless. From the table it is also noted that most recent MIW techniques employ blind extraction method only. And also many of the techniques are block based, which splits the image into non overlapping blocks and computes data on blocks to be used to identify and localize tamper. Different types of data such as patients' data; source information, indexing, and authentication information are embedded as watermarks. It is also noticed that many techniques lacks tamper detection and localization mechanism which is one of the requirement that seeks attention in medical image watermarking. Almost all work listed in Table 2 uses medical images on different modalities. But all these images are grayscale images only. Color medical images such as endoscopic image, digital fundus image etc. are left unaddressed.

Different applications address different characteristics and requirements. Robust watermarking scheme are resistant to attack and provide high security whereas fragile watermarks are easily distorted indicating the tamper. For authentication applications fragile algorithms are preferred. As far as requirements are concerned there exists tradeoff between capacity, imperceptibility and robustness/fragility. Higher capacity can be achieved at the expense of imperceptibility and robustness/fragility.

This paper classifies MIW according to various categories. EPR hiding watermarks demand high capacity, authentication watermarks identifies the source of the image whereas integrity watermarks and tamper detection watermarks are concerned with error correction codes.

Performance measures found in the literature were also discussed in this paper. It is seen that many works did not measure the time complexity. Since health care systems were used by doctors in real scenario, it is necessary that time complexity should also be addressed while performing analysis. Some types of attacks on MIW were also given.

8. CONCLUSION

In this survey most important aspects of medical image watermarking such as applications, requirements, classification, image quality measures and attacks in MIW are studied. MIW aims to provide protection of medical images to different health care applications.

Medical image watermarking technique still has not matured and lot of issues is left unasked. Though several techniques have been proposed still the research on MIW has to continue to answer the questions like, Is it possible to devise a scheme which achieves higher imperceptibility without

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compromising capacity. Is it possible to distinguish between malicious manipulation and incidental distortions etc? The answers are not still trivial.

Many watermarking techniques will evolve, but attacks on watermarks as well. It should always be remembered that there exists the tradeoff between robustness, capacity and imperceptibility. Recent innovation and literature has identified many ways to solve the unsolved questions, which when applied intelligently can solve most of the problems. Though the review discussed much information about the medical image watermarking performance evaluation is not done in this work. Future work is planned to present the performance evaluation of existing schemes.

REFERENCES

[1] Aggeliki Giakoumaki, Sotiris Pavlopoulos and Dimitris Koutsouris, "Mulitple Image Watermarking Applied to health Information Management" *IEEE Trans. on Information Technology in Biomedicine*, vol.10, no-4, 2006, pp.722-732.

[2] Akiyoshi Wakatani," Digital Watermarking for ROI Medical Images by using Compressed Signature Image", in *Proc. of the 35th Hawaii Int. Conf. on System Sciences*, 2002, pp. 2043 - 2048.

[3] Al-Gindy, A, "A fragile invertible watermarking technique for the authentication of medical images", in *Proc. of IEEE Int. Symp. on Signal Processing and Info. Tech. (ISSPIT), 2010,* pp.191-195.

[4] Alhaqbani.F and C. Fidge, "Privacy-Preserving Electronic Health Record Linkage Using Pseudonym Identifiers," in *Proc. 10th Int'l Conf. e-Health Networking, Applications and Services*, 2008,pp. 108-117.

[5] Al-Qershi, B.E. Khoo, "Reversible watermarking scheme based on Two-Dimensional Difference Expansion (2D-DE)", in *Proc. Int. Conf. on Computer Research and Development*, 2010,pp. 228–232.

[6] Anderson.R.J and F. A. P. Petitcolas, "On the limits of steganography, "*IEEE Journal Sel. Areas Commun.*, vol. 16, no. 4, May 1998, pp. 474–481.

[7] Barton.J.M, "Method and apparatus for embedding authentication information within digital data", U.S. Patent, Ed., 1997.

[8] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. Journal*, vol. 35, no. 3–4, 1996, pp. 313–336.

[9] Bidgood.W.D *et al.*, "Image acquisition context: Procedure description attributes for clinically relevant indexing and selective retrieval of biomedical images," *Journal of Am. Med. Inform. Assoc.*, vol. 6, no. 1, Jan. 1999,pp. 61–75.

[10] Calcote.S, "Developing a secure healthcare information network on the Internet," *Healthcare Financial Manage.*, vol. 51, no. 1, Jan. 1997, pp. 68.

[11] F. Cao, Huang, X.Q.Zhou, "Medical image security in a HIPAA mandated PACS environment", *Computerized Medical Imaging and Graphics*, vol. 27, no. 2-3, 2003, pp. 185– 196.

[12] Celik MU, Sharma G, Tekalp AM,"Lossless watermarking for image authentication: a new framework and an implementation",*IEEE Trans. on Image Process* ,vol.15, no.4, 2006, pp:1042–1049.

[13] Chao.H.M, C.-M. Hsu, and S.-G. Miaou, "A Data Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 6, no. 1, Mar. 2002, pp. 46–53.

[14] Chaw-Seng Woo, Jiang Du and Binh Pham," Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images", in *Proc. of the ARPS Workshop on Digital Image Computing Pattern Recognition and Imaging for Medical Applications*, 2005, pp.59-64.

[15] Chen.K and T. V. Ramabadran, "Near-lossless compression of medical images through entropy coded DPCM", IEEE *Trans. Med. Imag.*, vol. 13, no. 3, Sep. 1994, pp. 538–548.

[16] Chiang.K.H, K.-C. Chang-Chien, R.-F. Chang, H.-Y. Yen, "Tamper detection and restoring system for medical images using wavelet- based reversible data embedding", *Journal of Digital Imaging,* vol. 21, no.1, 2008, pp. 77–90.

[17] Chou.H.H, Y.-J. Chen, Y.-C. Shiau and T.-S. Kuo, "An effective and efficient compression algorithm for ECG signals with irregular periods", *IEEE Trans.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Biomed. Eng., vol. 53, no.6, 2006, pp. 1198–1205.

[18] Christophe De Vleeschouwer, Jean-François Delaigle, and Benoît Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management", *IEEE Trans. on Multimedia*, vol. 5, no. 1, Mar. 2003, pp. 97-105.

[19] Corboy, W. Tsang, D. Raicu, and J. Furst, "Texture-based image retrieval for computerized tomography databases," in *Proc. 18th IEEE Int. Symp. CBMS'05* , 2005, pp. 593–598.

[20] Dalel Bouslimi, Gouenou Coatrieux and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", *Computer Methods in Biomedicine*, vol.106, no.1, 2012, pp. 47-54.

[21] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", *IEEE Trans. on Information Technology In Biomedicine*, vol. 16, no. 5, Sep. 2012,pp. 891-899.

[22] Feng Bao, Robert H. Deng, Beng Chin Ooi, and Yanjiang Yang, "Tailored Reversible Watermarking Schemes for Authentication of Electronic Clinical Atlas", *IEEE Trans. on Information Technology in Biomedicine*, vol. 9, no. 4, Dec 2005,pp.554-564.

[23] Giakoumaki A, Pavlopoulos S and Koutsouris D, "A multiple watermarking scheme applied to medical image management", in *Proc. of the 26th IEEE-EMBS Ann. Int. Conf. on Eng. in medicine and biology*, 2004, pp 3241–3244.

[24] Giakoumaki, Pavlopoulos and Koutsouris, "Secure and Efficient Health Data Management through Multiple Watermarking on Medical Images", *Medical and Biological Engineering and Computing*, vol. 44, 2006, pp.619-631.

[25] Gouenou Caotrieux, Clara Le Guillou, Jean Michel Cauvin and Christian Roux,"Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images", *IEEE Trans. on Information Technology in Biomedicine*, vol.13, no. 2, Mar. 2009. pp. 158-165.

[26] G. Coatrieux, C. Quantin, J. Montagner, M. Fassa, F-.A. Alla¨ert, and Ch. Roux, "Watermarking medical images with anonymous patient identification to verify authenticity," *Studies Health Technol. Inf.*, vol. 136, 2008, pp. 667–672.

[27] Gouenou Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," in *Proc. of Int. Conf. on IEEE EMBS Information Technology Applications in Biomedicine,* 2000, pp. 250–255.

[28] Gouenou Coatrieux, L. Lecornu, C. Roux, B. Sankur, "A Review of Image Watermarking Applications in Health Care", in *Proc. of IEEE-EMBC Conference*, 2006, pp. 4691-4694.

[29] Gouenou Coatrieux, M. Lamard, W. Daccache, J. Puentes and C. Roux, "A Low distortion and reversible watermark: application to angiographic images of the retina", in *Proc. of the IEEE 27th Annual Conf. of Engineering in Medicine and Biology*, 2005, pp. 2224 - 2227.

[30] Gouenou Coatrieux,Hui Huang, Huazhong Shu,Limi Luo and Christian Roux," A Watermarking based Medical Image Integrity Control System and an Image Moment Signature for Tampering Characterization", *IEEE Journal of Biomedical and Health Informatics*, vol.17, no.6, Nov. 2013, pp.1057-1067.

[31] Gouneou Coatriex, Henri Maitre and Bulent Sankur," Strict Integrity Control of Biomedical Images", in *Proc. of SPIE Security and Watermarking of Multimedia Contents III*, vol. 4314, 2001, pp. 229-240.

[32] Guo X and Zhuang TG," Lossless watermarking for verifying the integrity of medical images with tamper localization ," *Journal of Digital Imaging* , vol.22, no.6, 2009, pp.620-628.

[33] Hartung.F and M. Kutter, "Multimedia watermarking techniques," in *Proc.of IEEE Int.Conf.*, vol. 87, no. 7, Jul. 2006, pp. 1079–1107.

[34] H. Huang, G. Coatrieux, H. Z. Shu, L. M. Luo, and C. Roux, "Medical image tamper approximation based on an image moment signature," in *Proc. Int. Conf. e-Health Networking Applications and Services (Healthcom)*, 2010, pp. 254–259.

[35] http://medical.nema.org. *Digital Imaging and Communications in Medicine (DICOM) Standard*, DICOM. (2006).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[36] JefferyH.K Wu,Ruey-Feng Chang, Chi-Jen Chen, Ching-Lin Wang, Ta-Hsun Kuo, Woo Kyung Moon and Dar-Ren Chen," Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique", *Journal of Digital Imaging*, vol. 21, no.1, Mar. 2008, pp. 59-76.

[37] Johnson.N.F, "In search of the right image: Recognition and tracking of images in image databases, collections, and the internet," *Technical Report, CSIS-TR-99-05- NFS, Center for Secure Information Systems*, George Mason University, Fairfax, VA, USA, April 1999.

[38] Jonathan Blake and Shahram Latifi," Digital Watermarking Security", *Defence Science Journal*, vol. 61, no. 5, Sep 2011, pp. 408-414.

[39] Kaihara.S, "Realization of the computerized patient record: Relevance and unsolved problems," *Int. Journal on Med. Inform.*, vol. 49, no. 1, Mar. 1998, pp. 1–8.

[40] L. Kobayashi and S. Furuie, "Proposal for DICOM multiframe medical image integrity and authenticity," *Journal of Digital Imag.*, vol. 22, no. 1, 2009, pp. 71–83.

[41] Kong.X and R. Feng, "Watermarking medical signals for telemedicine," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 3, Sep. 2001, pp. 195–201.

[42] Kuo-Hwa Chaing,,Kuang-che Chang – Chien, Ruey-Feng Chang and Hsun-Yen Yen, "Tamper Detection and Restoring System for Medical Images Using Wavelet-based Reversible Data Embedding", *Journal of Digital Imaging*, vol. 21, no. 1, Mar. 2008, pp. 77-90.

[43] Lehmann.T.M, B..B.Wein, J.Dahmen, J. Bredno, F.Vogelsang, andM.Kohnen, "Content-based image retrieval inmedical applications:Anovelmulti-step approach," in *Proc. SPIE, Storage Retrieval Media Databases*, vol. 3972, 2000, pp. 312–320.

[44] Lehmann.T.M, B. B. Wein, and H. Greenspan, "Integration of content based image retrieval to picture archiving and communication systems," in *Proc. Medical Informatics Europe, MIE 2003*, May 2003.

[45] Li.C.T and F.M.Yang, "One dimensional Neighbor forming Strategy for Fragile Watermarking", *Journal of Electronic Imaging*, vol. 12, no.2, 2003, pp. 284-291.

[46] Lin.E.T and E. J. Delp, "A review of fragile image watermarks," in *Proc. of ACM Multimedia Security Workshop*, Oct. 1999, pp. 47–51.

[47] Lingling An, Xinbo Gao, Xuelong Li, Dacheng Tao, Cheng Deng, and Jie Li," Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking", *IEEE Trans. on Image Processing,* vol. 21, no. 8, Aug. 2012, pp. 3598-3611.

[48] Lou.D.C, M.-C. Hu and J.-L. Liu, "Multiple layer data hiding scheme for medical images," *Comput. Stand. Interfaces,* vol. 31, no.2, 2009, pp. 329-335.

[49] Loupias.E, N. Sebe, S. Bres, and J. M. Jolion, "Wavelet-based salient points for image retrieval," in *Proc.of Int. Conf. on Img. Proc. ICIP*, vol. 2, Sep 2000, pp. 518–521.

[50] Louwerse.K, "The electronic patient record: The management of access— Case study: Leiden University Hospital," *Int. J. Med. Inform.*, vol. 49, no. 1, Mar. 1998, pp. 39–44.

[51] Luiz Octavio Massato Kobayashi, Sergio Shiguemi Furuie and Paulo Sergio Licciardi Messeder Barreto, "Providing Integriry and Authenticity in DICOM Images: A Novel Approach", *IEEE Trans. on Information Technology in Biomedicine*, vol.13, no.4, Jul. 2009, pp. 582-589.

[52] Malay Kumar Kundu and Sudeb Das," Lossless ROI Medical Imaga Watermarking Technique with Enhanced Security and High Payload Embedding", in *Proc. of IEEE Int. Conf. on Pattern Recognition,* Aug. 2010, pp. 1457-1460.

[53] Marco Fontani, Alessia De Rosa, Roberto Caldelli, Francesco Filippini, Alessandro Piva, Matteo Consalvo, Vito Cappellini,"Reversible Watermarking for image integrity verification in hierarchical PACS", in *Proc. of 12th ACM workshop on Multimedia and Security*, Sep. 2010, pp. 161-168.

[54] Memon.N and S. Gilani, " NROI watermarking of medical images for content authentication," in *Proc. of IEEE Int. Conf. Multitopic Conference,* Dec 2008, pp. 106 –110.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[55] Meyer.F.D, P. A. Lundgren, G. D. Moor, and T. Fiers, "Determination of user requirements for the secure communication of electronic medical record information," *Int. J. Med. Inform.*, vol. 49, no. 1, Mar. 1998, pp. 125–130.

[56] Miaou.S.G, C.-M.Hsu, Y.-S. Tsai, and H.-M. Chao, "A Secure Data Hiding Technique with Heterogeneous Data Combining Capability for Electronic Patient Records," in *Proc. 22nd Ann.. Int. Conf. IEEE EMBC*, vol. 1, Jul 2000, pp. 280–283.

[57] Mohammad-Saleh Nambakhsh, Alireza Ahmadianb and Habib Zaidi," A contextual based double watermarking of PET images by patient ID and ECG signal", Computer Methods and Programs in Biomedicine, vol. 104, no. 3, Dec. 2011, pp. 418-425.

[58] Mohanty.S, "Digital Watermarking: A Tutorial Review ," *Master Project Report*, Dept. of Electrical Engineering, India, Institute of Science, Bangalore, India, 1999.

[59] Munch.H, U. Englemann, A. Schroter and H.P. Meinzer, "The integration of medical images with the patient record and their web based distribution", *Journal. Acad. Radiol*. ,vol.11, no.6, 2004, pp. 661–668,.

[60] Mwangi.E, "A geometric attack resistant image watermarking scheme based on invariant centroids," in *Proc. IEEE Int. Symp. Signal Proc. Inf. Tech.*, 2007, pp. 190–193.

[61] Ni R, Ruan Q, Zhao Y, "Pinpoint authentication watermarking based on a chaotic system", *Forensic Sci. Int Journal* ,vol. 179, no.1, 2008, pp. 54–62.

[62] Osamah M.Al-Qershi and Bee Ee Khoo," Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images", *Journal of Digital Imaging*, vol. 24, no. 1, 2011, pp. 114-125,

[63] Osamah M.Al-Qershi and BeeEeKhoo, "Two-dimensional difference expansion (2D-DE) scheme with a characteristics-based threshold", *Signal Processing*, vol. 93, no.1, Jan. 2013, pp. 154–162.

[64] Osborne.D, "Embedded Watermark for Image Verification in Telemedicine", *PhD thesis, University of Adlaide*, 2005.

[65] Pan.W, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens and C. Roux, "Medical image integrity control combining digital signature and lossless watermarking", in *Proc. of Int. Conf. Data privacy management and autonomous spontaneous security, LNCS*, vol. 5939, 2010, pp. 153–162.

[66] Penedo.M, W. A. Peraman, P. G. Tahoces, M. Souto, and J. J. Vidal, "Embedded wavelet region-based coding methods applied to digital mammography," in *Proc. IEEE Int. Conf. Image Process.*, vol. 3, Sep. 2003, pp. III-197–200.

[67] Planitz.B and A. Maeder, "Medical image watermarking: A study on image degradation," in *Proc. Australian Pattern Recognition Society (APRS)*, Feb.2005, pp.3-8,.

[68] Poonkuntran.S, R.S.Rajesh, P.Eswaran, "Reversible, Multilayered Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding", in *Proc. IEEE Int. Adv. Computing Conf. (IACC 2009)*, pp. 2583-2587, Mar 2009, ISBN: 978-981-08-2465-5.

[69] Poonkuntran.S, R.S.Rajesh, P.Eswaran, "Wavetree Watermarking : An Authentication Scheme for Fundus Images", in *Proc. IEEE Int. Conf. on Emerging Trends in Computing*, Jan 2009, pp.507-511.

[70] Puech.W and J. M. Rodrigues, "A new crypto-watermarking method for medical images safe transfer," in *Proc. 12th Eur. Signal Process. Conf.*, Sep 2004, pp. 1481–1484.

[71] Queluz.M.P, "Authentication of digital images and video:Generic models and a new contribution," *Signal Process.: Image Commun.*, vol. 16, no. 5, pp. 461–475, Jan. 2001.

[72] Rajendra Acharya, Deepthi Anand, Subbanna Bhat and Niranjan," Compact Storage of Medical Images with Patient Information", *IEEE Trans. on Information Technology in Biomedicine*, vol.5, no.4, Dec. 2001, pp. 320-323.

[73] Rajendra Acharya, Niranjan,Iyengar, Kannathal, Lim Choo Min," Simultaneous Storage of Patient Information with Medical Images in the frequency Domain", *Computer Methods and Programs in Biomedicine*, vol. 76, no.1, 2004, pp. 13-19.

[74] Rajendra Acharya, Subbanna Bhat, Sathish Kumar and Lim Choo Min," Transmission and storage of medical Images with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Patients Information", *Computers in Biology and Medicine*, vol. 33, no.4, 2003, pp. 303-310.

[75] Robinson.G.P, H. D. Tagare, J. S. Duncan, and C. C. Jaffe, "Medical image collection indexing: Shape- based retrieval using KD-trees," *Comput. Med. Imag. Graph.*, vol. 20, no. 4, 1996, .pp. 209–217.

[76] Rodrigues.J.M, W. Puech, and C. Fiorio, "Lossless crypto-data hiding in medical images without increasing the original image size," in *Proc. 2nd Int. Conf. Adv. Med. Signal Inf. Process.*, Sep 2004, pp. 358–365.

[77] Rodriguez Colin Raul, et al," Data Hiding Scheme for Medical Images", in *Proc. of the 17th International Conference on Electronics, Communications and Computers, CONIELECOMP '07.*, Feb. 2007, pp.32.

[78] Ruotsalainen," Privacy and security in teleradiology". *European Journal of Radiology*, vol. 73, no.1, 2010, pp. 31-35.

[79] Shaw.S, "Overview of Watermarks, Fingerprints, and Digital Signatures", JISC Technology Applications Programme (JTAP), Aug. 1999, Available: http://www.jisc.ac.uk/uploaded_documents/jtap-034.doc

[80] Sudeb Das and Malay Kumar Kundu," Effective management of medical information through ROI-lossless fragile image watermarking technique", *Computer Methods and Programs in Biomedicine*, vol.111, no.3, 2013, pp. 662-75.

[81] Sudeb Das and Malay Kumar Kundu," Hybrid Contourlet-DCT based Robust Image Watermarking Technique Applied to Medical Data Management", in *Proc. of 4th Int. Conf. on Pattern Recognition and Machine Intelligence*, 2011, pp. 286-292.

[82] Tagare.H.G, C. C. Jaffe, and J. Dunkan, "Medical image databases: A content-based retrieval approach," *Journal of Am. Med. Inform. Assoc.*, vol. 4, no. 3, May 1997, pp. 184–198.

[83] Tan,C.K., Ng,C., Xu,X., Poh C.L., Yong, L. G. and Sheah, K., "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, no.3, June 2011, pp. 528-540.

[84] Tian J, "Reversible data embedding using a difference expansion", *IEEE Trans. Circ. Syst. Video Technol,* vol. 13, no.8, 2003 ,
a. pp.890–893.

[85] Traina.C, A. J. M. Traina, R. R. Santos, and E. Y. Senzako, "A support system for content-based medical image retrieval in object oriented databases," *Journal of Med. Syst.*, vol. 21, no. 6, 1997, pp. 339–352.

[86] Viswanathan.P and P. Venkata Krishna, "A Joint FED Watermarking System using Spatial Fusion for Verifying the Security issues of Teleradiology", *IEEE Journal of Biomedical and Health Informatics*, Early Access.2013.

[87] Viswanathan.P and P. VenkataKrishnn," Cryptographic Text Watermarking Medical image system with Reversible property", *Int. Journal on Information Processing*, vol. 5, no. 3, 2011, pp. 74-80.

[88] Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proc. Int. Workshop Inf. Hiding*, Oct 1999, pp. 211–236.

[89] Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgartner, and T. Pun.,"Generalized watermarking attack based on watermark estimation and perceptual remodulation", in *Proc. SPIE 3971, Security and Watermarking of Multimedia Contents II*, 358, 2000.

[90] Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, and J. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," *IEEE Communications Magazine*, vol. 39, no.8, 2001, pp. 118–126.

[91] Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modelling: Towards a second generation watermarking benchmark," *Signal Process.*, vol. 81, no. 6, Jun. 2001, pp. 1177–1214.

[92] Walton.S, "Information Authentication for a Slippery New Age", *Dr. Dobbs Journal*, Vol. 20, No. 4, 1995, pp. 18-26.

[93] Wang.P, "A Public Key Watermark for Image Verification and Authentication", in *Proc. of Int. Conf. on Image Processing (ICIP'98)*, 1998, pp. 425-429.

[94] Watson.A.B, "DCT quantization matrices visually optimized for individual images", in *Proc. SPIE HumanVision, Visual*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Processing and Digital Display IV, vol. 1913, Sep. 1993, pp. 202–216.

[95] S. T. C. Wong, M. Abundo, and H. K. Huang, "Authenticity techniques for PACS images and records," *Proc. SPIE*, vol. 2435, 1995, pp. 68–79.

[96] Xiaotoa Guo and Tian-ge Zhuang, "A Region based Lossless Watermarking Scheme for Enhancing Security of Medical Data", *Journal of Digital Imaging,* vol. 22, no. 1, Feb. 2009, pp. 53-64.

[97] Yang.H and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," *IEEE Signal Process. Lett.*, vol. 13, no. 12, Dec. 2006, pp. 741–744.

[98] Zain.J.M, L. P. Baldwin, and M. Clarke," Reversible watermarking for authentication of DICOM images" In *Proc. of IEEE Int. Conf. in Medicine and Biology Society,* vol 2, 2004, pp. 3237–3240.

[99] Zhang.X, S. Wang, Z. Qian and G. Feng, "Reversible fragile watermarking for locating tampered blocks in JPEG images", *Signal Processing* , vol. 90, no.12, 2010, pp.3026–3036.

[100] Zhao.X, A. T. S. Ho, H. Treharne, V. Pankajakshan, C. Culnane, and W. Jiang, "A novel semi-fragile image watermarking, authentication and self-restoration technique using the slant transform," in *Proc. Int. Conf. Intel. Inf. Hiding Multimedia Signal Process.*, vol. 1, 2007, pp. 283–286.

[101] Zhicheng Ni,Yun Q.Shi, Nirwan Ansari,Wei Su,Qibin Sun and Xiao Lin," Lossless Image Data Hiding Designed for Semi Fragile Image Authentication", *IEEE Trans. on Circuits and Systems for Video Technology*, vol.18, no.4, Apr. 2008, pp. 497-510.

[102] Zhou XQ, Huang HK and Lou SL," Authenticity and integrity of digital mammography images," *IEEE Trans Med Imag*, vol. 20, no.8, 2001, pp.784–791.

[103] Zhou.W, A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", *IEEE Trans. on Img. Processing*, vol.13, no.4, 2004, pp. 600–612.

[104] Zhou.X, W. Zhao, Z. Wang, and L. Pan, "Security theory and attack analysis for text watermarking", in *Proc of Int. Conf. on E-Business Inf. System Security,* 2009, pp. 1-6.

Journal of Theoretical and Applied Information Technology
10th July 2014. Vol. 65 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

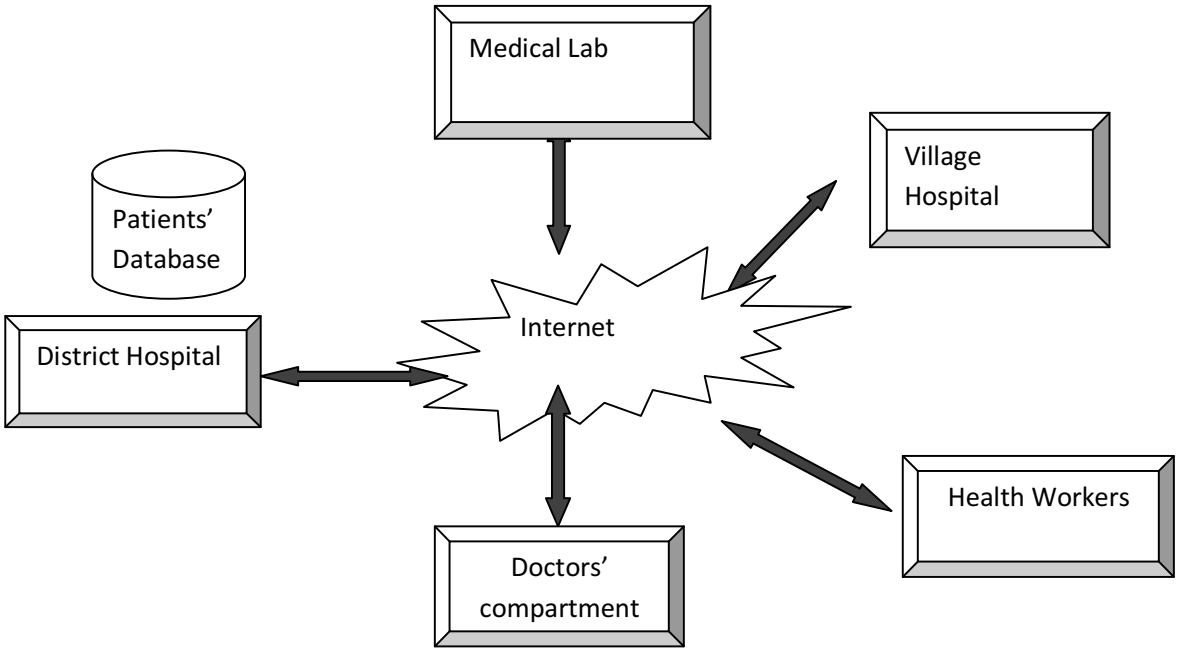

Figure.1- SCHEMATIC DIAGRAM OF TELEMEDICINE SYSTEM

Table 1- COMPARISON BETWEEN SPATIAL DOMAIN AND FREQUENCY DOMAIN

Factors	Spatial Domain	Frequency Domain
Strength	-Fast -High capacity -Low computation cost -High quality	-Robust to JPEG Compression/JPEG 2000 Compression
Weakness	-Low security -Sensitive to image manipulations	-High Computational cost -Sensitive to filtering/geometrical attacks -Low capacity

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2-PERFORMANCE COMPARISON

Author(year)	Objective	Domain	ROI	Extraction	Tamper Detection	Block Based	Nature of Watermark	Image Type/No on images	Result
Sudeb Das & Malay Kumar Kundu [80] (2013)	Authentication, integrity and data hiding	Spatial	Yes	Blind	Yes	Yes 3*3	Electronic Health Record	430 images in 7 modalities	Avg. PSNR between 43.5-44.8 dB Capacity: 0.89-0.39 bpp for ROI size of 5-30%. Avg WPSNR:43.6-44.8 Avg MSSIM:0.87-0.97 Total PerceptualError (TPE):0.02-0.09
Viswanathan & Venkatakrishna [86] (2013)	Confidentiality Availability Reliability	Spatial Encryption and biometric	Yes	Blind	No	No	ROI Or Copyright data	DICOM	PSNR: 45-62dB Capacity: 1bpp
Gouenou Coatrieux et al. [30] 2013	Integrity verification	Spatial	Yes	Blind	Yes	Yes 64*64 or 128*128	ROI Signature	MRI-120 images Xray(162-mammograms) CT-200 abdomen images Ultrasound(Echo) of vein-52 images	Detection rate of multiclass classifier is shown under 8 types of attacks.
Dalel Bouslimi et al. [20] (2012)	Reliability	Spatial & encryption	No	Blind	No	Yes	DS/Image Authentication code	100 US	PSNR: 49.36dB Capacity :1bpp.
Dalel Bouslimi et al. [21] (2012)	Reliability	Spatial Encryption	No	Blind	No	Yes	Hash of Image	100 Ultrasound images 200 PET images	PSNR: 53.9dB-60.15dB
Mohammed Saleh Nambaksh et al. [57] (2011)	Authentication EPR hiding	Frequency (Wavelet)	No	Blind	No	No	ECG Signal Patient Data	25 PET images	PSNR:48.33dB Capacity:0.25bpp
Al-Gindy [3] (2010)	Authentication	Frequency (DCT)	Yes	Blind	No	Yes 8*8	Patient entry date & file ID	Medical image	PSNR:73dB
Marco Fontani et al. [53] (2010)	Reliability	Frequency (Wavelet)	Yes	Blind	No	Yes	Digital Signature of the image	2167 images in MRI, CT, CR and Mammogram	PSNR:66-84dB

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Osamah M.Al-Qershi et al. [62] (2011)	Authentication and data hiding	Frequency (Wavelet)	Yes	Blind	Yes	Yes 16*16	Patient's data, Authentication data	MR US CT CR	PSNR MR-69.7dB US-36.3dB CT-85.5dB CR-65.2dB
Sudeb Das & Malay Kumar Kundu [81] (2011)	Authentication Integrity	Frequency	No	Non Blind	No	Yes 8*8	EPR	Abdomen CT CT Head MRI Brain US	MSSIM Abdomen CT-0.87 CT Head-0.95 MRI Brain-0.97 US-0.93
Malay Kumar Kundu & Sudeb Das [52] (2010)	Authentication	Spatial domain	Yes	Blind	Yes	No	EPR	Abdomen CT Brain CT Brain MRI US, CT	MSSIM-0.99
Gouenou Coatrieux et al. [25] (2009)	Reliability	Frequency (DCT)	No	Blind	No	Yes 2*2	Knowledge Digest	Endoscopic image 750 color images	PSNR:42.36dB