Digital Watermarking for Telemedicine Applications: A Review

Nisreen I.R. Yassin
Engineering Division,
Systems & Information Department,
National Research Centre,
El Buhouth Street, Dokki, Cairo, Egypt

ABSTRACT

Telemedicine is an emerging science that can help in solving the modern global health problems. Exchanging medical images and Electronic Patient Records (EPR) between clinicians, specialists, and radiologists provides a platform for discussing and consulting diagnostic and therapeutic problems. Using Information and Communication Technologies (ICT) in the transmission of medical information for improving healthcare access, diagnosis, and treatment requires various means for security and privacy issues, since, digital information can be easily attacked to be duplicated and manipulated. Digital watermarking is a data hiding technique which used for improving the security of various multimedia applications and extensively investigated to protect the privacy of patients through telemedicine systems. This paper aims to provide a useful preview on telemedicine and the using of digital watermarking in this field.

Keywords

Digital Watermarking, Telemedicine, Data Hiding Techniques, Electronic Patient Record, Security Systems.

1. INTRODUCTION

Recently, achieving the correct medical diagnostic becomes a very difficult decision because of the rapid development of diseases which needs cooperation of several medical organizations. Telemedicine is defined by The American Telemedicine Association (ATA) as “ the use of medical information exchanged from one site to another via electronic communications to improve a patient’s clinical health status, including an increasing variety of applications and services using two-way video, email, smart phones, wireless tools and other forms of telecommunications technology” [1].

The great progress in the health care sector introduces diverse medical imaging means in radiology, hospital information system (HIS), and information management systems in hospitals. Several medical imaging techniques are used in diagnostic decisions such as: Magnetic Resonance Imaging (MRI), Computer Tomography (CT), Ultrasound, and X-Rays [2,3]. Also, the availability of inexpensive high-bandwidth Internet connectivity and the rapidly growing of information and communication technologies have resulted in large opportunities for the creation, access, handle and distribution of digital content by usual individuals. This leads to the emergence of E-Health services which introduce new practices for the professions as well as for the patients by enabling remote access, transmission, and interpretation of the medical images for diagnosis purposes. In addition, telemedicine technology has offered many applications such as remote diagnostics, remote consultation, remote monitoring, and remote operation [4]. This tremendous progress in the field of communication and information technology as well as the telemedicine is accompanied by a host of problems. The main problem is that, the digital content can be copied, manipulated, and redistributed easily at low cost and without loss in fidelity. Exchanging of medical data over the open channels in order to achieve the correct medical diagnostic exposes them to many threats. Also, medical images may pass through various image-information processing systems over the networks, and thereby, the images can be threatened throughout their lifetime in many different ways. Medical information security requires three characteristics [3, 5]: (1) Confidentiality: ensures that only the entitled users have access to the information since some patients do not like to expose their information to the public. (2) Reliability: which includes: (i) integrity: the information has not been modified by non-authorized people. (ii) authenticity: a proof that the information belongs to the correct patient and issued from the right source. (3) Availability: means the access to the information for authorized persons.

Digital watermarking techniques can play an important role in health data management systems to protect the confidentiality of medical data, controlling the access and the retrieval of the data, and maintaining their integrity. A watermark containing medical information such as (patient record, hospital signature, and medical diagnostic) can be embedded into medical images when sharing them through the network. The quality of the medical image is very important in the correct diagnostic process, so extreme care must be considered when watermark embedding process takes place [6]. Another two benefits of using watermarking in telemedicine are: firstly, integration of the patient’s information into its medical image using watermarking is important to avoid detachment or misplacement which means allocating the EPR to a wrong medical image. If EPR and medical image are sent separately from each other, the possibility of detachment increases which affects the quality of the diagnostic process. Secondly, telemedicine requires huge amount of bandwidth, by integrating both the medical images and EPR, memory and bandwidth can be saved [7, 8]. This paper summarizes the applications and problems of telemedicine in section 2. A detailed review on digital watermarking system, requirements, and embedding categories are introduced in section 3. In section 4, a number of recent watermarking techniques for medical images are introduced. Finally, a conclusion for the paper is presented in section 5.

2. TELEMEDICINE

The purpose of telemedicine is to provide clinical support by overcome geographical barriers which means connecting users who are not in the same physical location using various types of ICT. Telemedicine improves health outcomes by allowing many application areas which contribute to facilitate the provision of therapeutic service to the patient and rapid initial treatment to critical situations. Also, there is a set of problems that hinder the spread of telemedicine and prevent benefit from it [9, 10].

2.1 Telemedicine Applications

2.1.1 Home Monitor

home monitoring devices are used to transmit the patient's physiological parameters to the data center such as video interactive combined with video camera, wireless ECG transmission function, wireless auscultation capabilities, broad band cable, satellite communications and digital technology to achieve real-time, two-way high-speed communications.

2.1.2 Emergency Treatment

The first aid and the pre-hospital care are vital to the patients live, so speed and quality of the emergency treatment are very important issues. Wounded vital signs, voice, images could be transmitted to the emergency center via real time transmission using telemedicine system, so doctors can guide the responder to the wounded through the telemedicine system or get ready to do the rescue when the wounded arriving.

2.1.3 Military Application

The modern warfare is implemented in a short period of time under high-tech conditions which resulted in more serious injuries and complex treatment environment. The traditional hierarchical ambulance mode cannot meet these characteristics. Battlefield remote control operation system can be developed using telemedicine technology, where remote surgery and micro-surgery can be done on the wounded using a computer robot controlled by experts.

2.1.4 Telemedicine Education

The latest medical information and treatment techniques can be provided using telemedicine education system to enhance the service level of medical staff. Image of a real-time and interactive simulation class room environments can answer the hospital problems encountered in the diagnosis and treatment activities which can be very useful for young doctors and students.

2.2 Telemedicine Problems

2.2.1 High Cost

The cost of a telemedicine system hardware is very expensive where, real time communication, satellite communication, digital technology, wireless communication, database transmission lines, and online communication are needed.

2.2.2 Low Accuracy of Telemedicine Diagnosis

The consultation experts use the transmitted medical records information to understand, analyze, and judge the situation of the provided medical record. Missing medical information due to delaying communication can affect the accuracy of medical diagnosis.

2.2.3 Security Threats

A lot of security concerns should be given about stealing the patient's privacy. Several existing security techniques are currently being used but these conventional security techniques are considered to have limitations specially in protecting the medical data [11, 12]. Conventional security techniques and their limitations are summarized in table1.

Medical information are very sensitive information, so it needs not only protection with integrity and high confidentiality but also appropriate management through different healthcare services. To prevent the patient's information and medical images from being tampered, watermarking can be used for hiding the EPR inside the medical image. This prevents attackers from easily changing the medical image or the patient information [13].

3. DIGITAL WATERMARKING SYSTEM

Digital watermarking [14] was introduced to provide means for enforcing copyright protection once the use and distribution of digital multimedia data have exploded. Nowadays, digital watermarking is established in many applications [15], one of them is healthcare and medical information systems. Digital watermarking is the process that embeds data called a watermark into an object such that watermark can be detected or extracted later to make an assertion about the object. The basic watermarking system can be described by two functions which are embedding and detection process respectively [16]:

$$E_k(C_o, W) = C_w \tag{1}$$

$$D_k(C_o, C_w, K) = \widehat{W} \tag{2}$$

where, E_k is the embedding function which has two input parameters: the original (host) object C_o, and the watermark W to be embedded using a secret key K. The output from the embedding function is the watermarked data C_w. In the detection function D_k, the original data C_o, the marked and possibly manipulated data C_w, and the secret key K are the requirements for the extraction process. Watermark detector is responsible for extracting or detecting the existence of the watermark. Figure 1 shows a block diagram of the general watermarking framework. To measure the compatibility between the original watermark $W(i,j)$ and the extracted watermark $\widehat{W}(i,j)$, Normalized Correlation Coefficient (NC) can be used as follows:

$$NC = \frac{\sum_i \sum_j W(i,j).\widehat{W}(i,j)}{\sum_i \sum_j W(i,j)^2} \tag{3}$$

NC value is 1 when the original watermark and the extracted watermark are identical and zero if both are different from each other. According to the required application, digital watermarking systems can be classified into (1) Non-blind (private) watermarking systems which require the original data in the detection process. (2) Semi-blind watermarking systems which do not use the original data for detection but use some side information. (3) Blind (public) watermarking systems where the original data cannot be used in the recovery process since it is extremely expensive to maintain a database with all the originals. The only requirement for the extraction process is the watermarked data.

Watermarks can also be classified into (1) robust watermarks which are designed to resist heterogeneous manipulations. All applications which need security of the watermarking systems require this type of watermark. (2) Fragile watermarks which are watermarks with very low robustness. So, this type of watermark can be destroyed even by the slightest manipulations. They can be used to check the integrity of

Table 1. Limitation of conventional security techniques

Conventional Security Technique	Limitations
Encryption	Efficient tool for storage and transmission but after receiving and decrypting, the data is not secure anymore.
File-header (DICOM)	The DICOM file contains medical image, and a separated patient private information stored in header file. This separation can cause mismatch which result in error in diagnosis. The header file can be lost because of any signal processing operations. The intruder can break the confidentiality of patient by access the header file.
Firewall	An isolation tool between the intra-net and internet so, only protects the information up to the point of the internal networks.
Hash function	Takes an arbitrary block of data and returns a fixed-size bit string (hash value), such that an accidental or intentional change to the data will change the hash value. It cannot indicate the location where the images have been tampered. It is bit sensitive to the input.

objects. (3) hybrid watermarking which is a mixture of robust and fragile techniques to provide authentication, integrity verification, and copyright protection simultaneously. (4) Public and private watermarks If the key is known, this type of watermark is referred to as public, and as private watermarks if the key is hidden. (5) Visible or invisible watermarks which can be logos or overlay images in the field of image or video watermarking.

3.1 Requirements of a watermarking system

3.1.1 Perceptual transparency

Watermark embedding must not affect the quality of the underlying host data. A watermark embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark [17, 18]. Perceptual similarity is a measure that determines the similarity level between the original and watermarked images. The most commonly used image similarity index measure is Peak Signal to Noise Ratio (PSNR)[19]:

$$PSNR = 10\log_{10}\frac{max^2}{MSE} \qquad (4)$$

where, max is the possible maximum value of the image. max = 255 for 8 bit gray scale image. MSE is the Mean Square Error between the original and the watermarked image [20]:

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}}\sum_{\mathrm{i}=1}^{\mathrm{M}}\sum_{\mathrm{j}=1}^{\mathrm{N}}[\mathrm{I}(\mathrm{i},\mathrm{j}) - \hat{\mathrm{I}}(\mathrm{i},\mathrm{j})]^2 \qquad (5)$$

where M, N are the size of the image, and $I(i,j), \hat{I}(i,j)$ are the pixel values at location i, j of the original and watermarked images. Larger PSNR means the original and watermarked images are more similar to each other. To have acceptable perceptual value, the PSNR should be greater than 30 dB.

3.1.2 Robustness

There are two major problems when trying to guaranty robustness, the watermark must be still presented in the media after attack and it should be possible for the detector to detect it. Also, when a signal is distorted, its fidelity is only preserved if its perceptually significant regions remains intact, while insignificant regions might be changed greatly with a little effect on fidelity. Basically, attacks are trying to remove the watermark but without destroying the original media so embedding the watermark in significant regions will disturbance the attacker [21]. The robustness can be measured by applying different attacks on the watermarked images and comparing the embedded and extracted watermark by different benchmarks. Robustness is application dependent and it is not necessary that all the applications require robustness against all the operations [22].

3.1.3 Security

The security of watermarking techniques must lie in the choice of a key [23]. The watermarking technique is truly secure if knowing the exact algorithms for embedding and extracting the watermark does not help an unauthorized party to detect the presence of the watermark or remove it [17].

3.1.4 Payload of the watermark

It is the amount of information that can be stored in a watermark and depends on the application. Increasing the watermark payload will affect the fidelity of the system. So, it is very important to make a trade-of between payload and imperceptibility of a watermarking system.

3.1.5 Reversibility

For medical applications, reversibility watermarking is an important issue to recover the original image without any distortion after extracting the watermark bits, in this case, both the watermark information as well as the image itself can be recovered perfectly [24].

3.2 Watermark Attacks

3.2.1 Simple attacks

Attempt to damage the embedded watermark by modifications of the whole image without any effort to identify and isolate the watermark. Examples include frequency based compression, addition of noise, cropping and correction.

3.2.2 Detection-disabling attacks

Attempt to break correlation and to make detection of the watermark impossible. Mostly, they make some geometric distortion like zooming, shift in spatial or temporal direction, rotation, cropping or pixel permutation, removal or insertion. The watermark in fact remains in the cover content and can be recovered with increased intelligence of the watermark detector.

3.2.3 Ambiguity attacks

Attempt to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious which was the first authoritative watermark.

3.2.4 Removal attacks

Attempt to analyze or estimate the watermark, separate it out and discard only the watermark. Examples are collusion attack and de-noising attack.

3.3 Embedding Categories

There are two main categories for embedding the watermark inside digital contents (1) Embedding in spatial domain where embedding and detection of watermark is performed by directly manipulating the pixel intensity values of the digital content such as Least Significant Bit (LSB) embedding, and spread spectrum technique [25]. (2) Embedding in the transform domain where the watermark is embedded by changing the frequency coefficients of the digital content. There are three main transformation based embedding techniques: Discrete Cosine Transform (DCT) [26, 27], Discrete Fourier Transform (DFT) [28, 29], and Discrete Wavelet Transform (DWT) [30, 31]. Watermarking in spatial and transform domains have different advantages and disadvantages which are illustrated in table 2.

4. LITERATURE REVIEW

Different types of watermarking methods have been proposed in literature to provide the security services required for telemedicine applications. A hybrid algorithm which is based on Particle Swarm Optimization (PSO) is proposed in [32]. In the embedding process, the host image and the watermark are decomposed using DWT. Then, DCT is applied to the LL band of both images. PSO is applied to the DCT block of the host image to find the global best intensities to embed the watermark. A PSO algorithm is described and images from the Digital Imaging and Communications in Medicine (DICOM) link are used in the simulation process. The relation between the PSNR and the PSO different levels with and without attacks is discussed. Ali Al-Haj et al in [33] proposed a multiple watermarking scheme used for achieving security of medical images transmitted over public networks. Blind watermarking scheme based on embedding a watermark into the Region-Of-Non Interest (RONI) of the medical image using DWT and Singular Value Decomposition (SVD) to provide confidentiality and authenticity has been presented. Also, integrity is provided by embedding a fragile watermark into the Region Of Interest (ROI) of the medical image based on block level spatial domain scheme. LSBs of ROI blocks are replaced by fragile watermarks which are Pseudo Noise (PN) sequences to implement the tamper localization functionality. Those LSBs are saved and embedded into the HH sub-band of RONI block as a robust watermark. Another two robust watermarks are embedded, the first one is a hospital logo which is embedded in the HL sub-band, and the second one is a patient information watermark which is embedded in the LH sub-band. In the embedding process, a single watermark bit is embedded into upper element of the diagonal matrix of each sub-band SVD of medical image RONI block. The algorithm was evaluated using gray-scale medical images of three modalities which are MRI, Ultrasound, and X-ray. The experimental results showed the effectiveness of the algorithm in providing the authenticity, integrity and tamper localization requirements with PSNR greater than 32.9232 dB. In [34] DFT based watermarking method is proposed to avoid detachment of medical images from their corresponding EPR data. The watermark pattern is produced by combining DICOM metadata and encryption techniques. The Race Integrity Primitives Evaluation Message Digest RIPEMD-160 is applied to the EPR data of the DICOM metadata. The result is converted to binary representation and divided into two blocks. The watermark is the xor operation result between these two blocks. The original DICOM image is resized and transformed into magnitude and phase components using DFT. To avoid wrong medical diagnostics, the integrated optical density, which describes the appearance of an image, is obtained to indicate a suitable watermark strength for embedding process. The watermark is embedded into the magnitude of the middle frequency components in the DFT domain. The receiver operating characteristics curves are plotted to show the desirable detachment detection performance of the proposed method.. The experimental results showed the effectiveness of the algorithm in avoiding perfectly the detachment problem with PSNR greater than 49 dB.

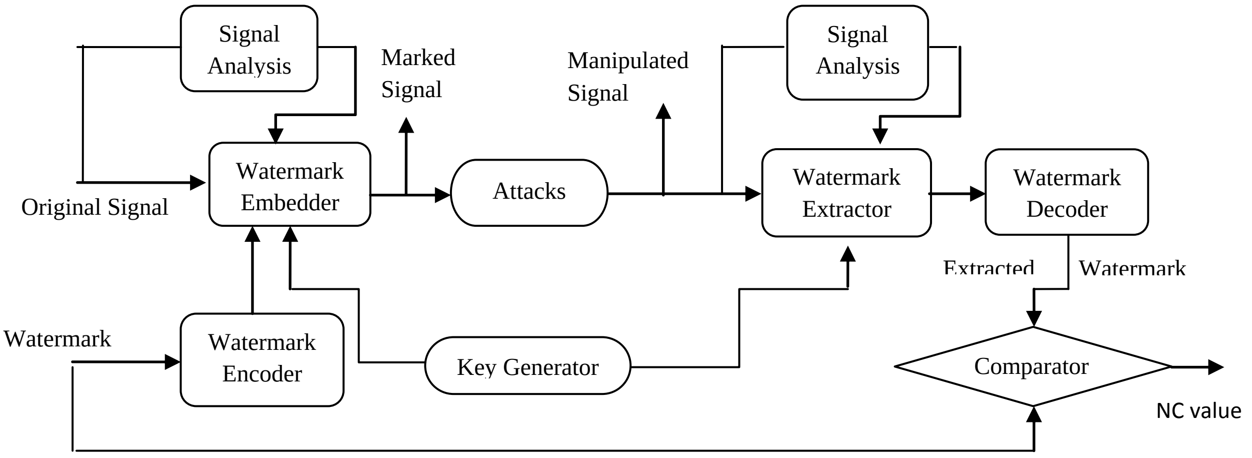

Fig 1: Watermarking system framework

Table 2 Comparison between watermarking embedding domains

Process domain	Advantage	Disadvantage
Spatial domain	Fast & simple, high capacity, and may overcome cropping attacks.	Weak against noise, compression, filtering and geometric attacks.
Frequency domain	Robust against many signal processing operations, and geometric distortions. Has compression compatibility.	Higher processing time and higher complexity.

A spread spectrum watermarking algorithm for telemedicine applications is proposed in [35]. The scheme embedded a medical text watermark into horizontal and vertical sub-bands coefficients of the first, second and third level DWT of the medical cover image. Each character of the text watermark is converted to binary format using ASCII codes. Bose, Chaudhuri, and Hocquenghem (BCH) codes are implemented on the binary watermark to enhance bit error rate (BER) performance of the extracted watermark. A pair of PN sequences is generated corresponding to each bit of text watermark. These PN sequences are embedded into selected wavelet coefficients in column wise operation. The selection is done by thresholding the coefficient values present in each column. Embedding the watermark bits is done as follows:

$$W = \begin{cases} V + kX & if \;\; b = 0 \\ V - kX & if \;\; b = 1 \end{cases} \qquad (6)$$

where V is wavelet coefficient column vector of the cover image, W is the wavelet coefficient vector after watermark embedding, k is the gain factor, X is the PN sequence vector and b is the message bit that has to be embedded. The experimental results were carried out using MR images and the length of the embedded watermark was 381 bits. The performance of the extracted watermark is analyzed with and without BCH coder. The maximum PSNR value achieved by the proposed method is 49.12 dB. Embedding a watermark signal into Electro-myogram (EMG) signal for tele-monitoring applications is presented in [36].The EMG signal is a perceptive diagnostic tool which is used for detection of various muscle related diseases by measuring and recording the muscle electrical signal. EMG is done to find out the diseases that damages muscle tissue, nerves, or the junctions between nerves and muscles. For embedding a binary watermark image, EMG signal is converted to the largest possible square 2-D signal and decomposed into four sub-bands using Stationary Wavelet Transformation (SWT). Two

blind watermarking mechanisms based on spread spectrum are described. A comparative study of EMG features between the original and watermarked EMG signal is introduced. The experimental results showed that the achieved PSNR is greater than 16.4344 dB.

K. Anusudha et. al introduced a method for protecting the patient information in which this information is embedded as a watermark in the DWT of the medical image [37]. The hospital logo was used as a reference image to extract the EPR without the need of the original image, so that the scheme is blind. Two sub-bands with middle energy were selected out of four bands of the DWT of the medical image in which energy is computed as :

$$E = \frac{1}{nxn} \sum_{i=0}^{n} \sum_{j=0}^{n} c^2(i,j) \qquad (7)$$

Where E is the energy of a wavelet sub-band of size nxn, and $c(i,j)$ is the DWT coefficient. The selected sub-bands $b_{r,k}$ and a reference image R_k whose size is equal to sub-band size are divided into blocks where k is the block number. The embedding process is done using the following equation:

$$\hat{b}_{r,k} = \begin{cases} b_{r,k} + \alpha.R_k & if \;\; w = 0 \\ b_{r,k} - \alpha.R_k & if \;\; w = 1 \end{cases} \qquad (8)$$

Where α is the impact factor, and w is the watermark bit. For extracting the EPR, the correlation coefficient value between the reference image block and the corresponding watermarked sub-band block is computed. The watermark bit is 0 if correlation value is greater than or equal 0 else it is 1. Performance of the proposed method was tested for four modalities of medical images: MRA, MRI, and CT. The proposed scheme is tested against some common attacks as well as PSNR and NC are calculated in each case.

N. Venkatram et al proposed a medical image watermarking scheme based on Rivest, Shamir and Adleman (RSA) algorithm which is used to generate a key and encrypt the patient image that is the watermark and 2D discrete wavelet transform which is used for watermarking of the encrypted patient image watermark into a medical image [38]. The paper presented for the RSA algorithm which is widely used in secure communications. Prime numbers are selected randomly between 1 and 200 for every new encryption of patient image. The encrypted patient image and the key are saved with the watermarked medical image for decryption. Different levels of DWT decomposed medical image are tried. The encrypted watermark is embedded into the medical image as follows:

$$I'(i,j) = I(i,j) + (2\sigma + \delta)(2w^e(k) - 1) \qquad (9)$$

Where $I'(i,j)$ is the watermarked DWT coefficient, and $I(i,j)$ is the original DWT coefficient. σ is the ratio of standard deviation of wavelet coefficient block and the maximum standard deviation of all the coefficient blocks. δ is a fixed embedding watermark strength which is fixed at 0.05 in the proposed scheme. $w^e(k)$ is the encrypted patient image watermark at k^{th} position. To identify authentication of the medical image, firstly, the encrypted watermark patient image is extracted from the received medical image. Secondly, the watermark patient image is decrypted using the saved key. The equation used for watermark extraction process is as follows:

$$W^{e'}(i,j) = \frac{2(I'(i,j) - I(i,j))}{(2\sigma + \delta) + 1} \qquad (10)$$

Where, $W^{e'}(i,j)$ is the extracted watermark patient image which encrypted with RSA. $I'(i,j)$ is the received watermarked medical image at ith and jth location. $I(i,j)$ is the original cover image that is received with the transmitted watermarked image. The results are produced for three types of medical images (CT, MRI, US) with one patient image watermark using four wavelets (haar, db, symlets, bior) at four different levels(1,2,3,4). The smallest achieved PSNR is 46.3454db for US cover image.

Umaamaheshvari et al. [39] presented Independent Component Analysis (ICA) and Ridgelet transform for watermarking baby scan image. ICA is used to project the cover image into a basis with its components as statistically independent as possible. Ridgelet transform is a good method for enhancing edges and reducing noise. Ramesh et al. [40] used DWT to protect the copyright of digital signature of medical images. The watermark is embedded into the high frequency HL and LH sub-bands. The watermark digital signature is processed into a checked board image with black and white squares before embedding process. The robustness of this algorithm is tested using different filtering techniques. Hajjaji et al. presented an approach for watermarking medical images using the techniques of Code Division Multiple Access (CDMA), DWT and Error Correcting Code (ECC) [41]. This algorithm embedded 1536 bits in different types of images (Echographic, and IRM) and achieved good results in terms of watermarked image quality where the smallest obtained PSNR is 30 db for both tested images. Also, the robustness against JPEG compression and Gaussian noise attacks showed good results. Kumar et al. [42] proposed a high capacity scheme to be used in telemedicine applications. Their algorithm is based on Haar wavelet transform of radiological images. Spread spectrum is used for embedding medical information into radiological images based on pseudo-random sequence pairs. Two watermark images were embedded into host CT scan image. The effect of varying gain factor, DWT levels, and watermark size was discussed. Hajjaji et al. [43] proposed a watermarking algorithm based on LSB of medical images to check the security issues of patient data sharing. Harris corner detector is used for selecting the important feature points in the medical image. Secure Hash Algorithm (SHA) is used to generate the hospital signature then the massage is coded by turbo coding in order to be robust against different attacks. The number of embedded medical watermark bits were 425 without turbo coding.

5. DIGITAL WATERMARKING ADVANTAGES

Digital watermarking has many features that make them superior to other traditional means of security protection in the fields of copyright protection and telemedicine. The advantages of digital watermarking are summarized as follows:

5.1 Security capabilities

Confidentiality in telemedicine applications can be achieved by hiding medical information or EPR into different modalities of medical images. At the receiver side, the EPR must be recovered without need for the original image, and it must be recovered with zero bit error rate. Embedding capacity is very important issue in telemedicine such that high embedding capacity is required as well as preserving high imperceptibility. Trade off between embedding capacity and imperceptibility should be considered. Error correction codes can be used to recover EPR free from errors. Reliability of medical information is essential and can be achieved by appropriate watermarking scheme. Even if the medical information is tampered while exchanged over networks, digital watermarking can be used to detect the tamper , localize the tamper , and finally recover the tamper.

5.2 Avoiding detachment

Hiding capability of digital watermarking is used to avoid misplacement or detachment problem. EPR or patient information is vital for the process of diagnosis and treatment. If EPR and its image modality are transmitted separately then detachment possibly occur and wrong diagnosis and treatment takes place. In order to avoid this situation, embedding EPR into its corresponding image using watermarking is a good solution.

5.3 Memory and bandwidth saving

Telemedicine applications require huge amount of bandwidth to transmit millions of medical images and EPRs around the world between hospitals and medical centers. Also, unlimited memory for storage these images and EPRs is reason to block the spread of this technology. Reducing bandwidth and memory storage can be done by integrating EPRs into corresponding medical images using appropriate digital watermarking techniques.

6. CONCLUSIONS

Telemedicine is a very essential science which can contribute in disease control through the deployment of diagnosis and treatment operations in remote locations. In this paper, a comprehensive review on telemedicine and medical image watermarking has been introduced. Applications and problems of telemedicine have been described in details. The main problem is the security of EPR before, during, and after its transmission over the network. Different issues in digital watermarking system have been introduced such as requirements, attacks, and embedding domains. Different medical watermarking schemes have been demonstrated. By comparing watermarking with conventional security tools, watermarking can overcome limitations of conventional tools so it is an effective way to ensure the protection of medical information, as well as ensure the quality of diagnosis and treatment. In addition, integrating watermarking with other conventional security tools can ensure more of confidentiality, and reliability for telemedicine system. Such as using encryption and watermarking to provide an effective control access mechanism. Also, DICOM meta-data can be inserted as a watermark into its DICOM image then recovery of the text meta-data after possibly different signal processing operations. Using different machine learning techniques in watermarking medical images can offer a good opportunity to preserve the quality of the medical image which is essential for diagnosis process by controlling watermark embedding factor as well as identifying the best locations to embed EPR into medical image. A study of watermarking based on machine learning techniques can be considered for future work.

7. REFERENCES

[1] American Hospital Association, “The Promise of Telehealth for Hospitals, Health Systems and their Communities”, Trend Watch, January 2015.

[2] G. Coatrieux, L. Lecornu, B. Sankur, and Ch. Roux, “A Review of Image Watermarking Applications in Healthcare”, Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS '06, pp. 4691-4694, 2006.

[3] H. M. Chao, C. M. Hsu, and A.-G. Miaou, “A Data Hiding Technique with Authentication, Integration and Confidentiality for Electronic Patient Records”, IEEE

Transactions on Information Technology in Biomedicine, vol. 6, issue 1, pp. 46-53, March 2002.

[4] Elek Dinya, Tamás Tóth, “Health Informatics: e-HEALTH and TELEMEDICINE”, Institute of Health Informatics, Semmelweis University, February 4, 2013.

[5] K. A. Navas, S. A. Thampy, and M. Sasikumar, “ ERP Hiding in Medical Images for Telemedicine,” in Proceedings of the World Academy of Science and Technology, vol. 28, 2008.

[6] S. C. Rathi and V. S. Inamdar, “Medical Images Authentication through Watermarking Preserving ROI”, Health Informatics International Journal (HIIJ), vol. 1, no. 1, August 2012.

[7] Coatrieux G, Maitre H, Sankur B, Rolland Y, Collorec R, “Relevance of watermarking in medical imaging”, Information Technology Applications in Biomedicine, pp. 250–255, 2000.

[8] Navas KA, Sasikumar M, “Survey of medical image watermarking algorithms”, Presented at the 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SETIT), Tunisia, 2007.

[9] World Health Organization, “Telemedicine: opportunities and developments in Member States: report on the second global survey on e-Health”, 2009.

[10] Ming-gang Wang, Ying-jun Mao and Wei Li, ”The Application of Telemedicine Technology”, Lecture Notes in Electrical Engineering, Springer 2014.

[11] Paar C, Pelzl J, “Hash functions: understanding cryptography”, Springer Berlin Heidelberg, pp. 293–317, 2010.

[12] Hussain Nyeem, Wageeh Boles, Colin Boyd, “ A Review of Medical Image Watermarking Requirements for Tele-radiology”, Society for Imaging Informatics in Medicine, September 2012.

[13] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital watermarking, Morgan Kaufmann Publishers, Sans Francisco, CA, USA, 2004.

[14] O. Findik, I. Babaoglu, and E. Ulker, “A Color Image Watermarking Scheme Based on Hybrid Classification Method: Particle Swarm Optimization and k-nearest Neighbor Algorithm,” In: Optics Communications, vol. 283(24), pp. 4916-4922, 2010.

[15] Digital watermarking services & applications. Available:http://www.digitalwatermarkingalliance.org/membership.asp

[16] M. Arnold, M. Schmucker, and S. D. Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”, Artech House computer Security Series, 2003.

[17] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, “Multimedia data-embedding and watermarking technologies,” Proceedings of the IEEE, vol. 86, issue 6, pp. 1064-1087, June 1998.

[18] M. Ishtiaq, M. A. Ja-ar, M. A. Khan, Z. Jan, and A. M. Mirza, “Robust and Imperceptible Watermarking of Video Streams for Low Power Devices,” Communication Computer Information Science, vol. 61, pp. 177-184, 2009.

[19] A. N. Netravali and B. G. Haskell, Digital Pictures: Representation, Compression, and Standards, Plenum, New York, 1995.

[20] M. K. Thakur, V. Saxena, and J. P. Gupta, “A Performance Analysis of Objective Video Quality Metrics for Digital Video Watermarking,” in Proceeding of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 12_17, Chengdu, China, July 9-11, 2010.

[21] P. Singh and R. S. Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks,” International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, issue 9, March 2013.

[22] A. M. Al-Haj, Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications, Hershey, New York, 2010.

[23] J. Fridrich and M. Goljan, “Comparing Robustness of Watermarking Techniques,” in Proceeding of Electronic Imaging '99, The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents, vol. 3657, pp. 214-225, San Jose, CA, January 25-27, 1999.

[24] Kaur M, KAUR R, “Reversible watermarking of medical images authentication and recovery- a survey”, Journal of Information and Operations Management, vol. 3, Issue 1, pp. 241– 244, 2012.

[25] R. Chandramouli and N. Memon, “Analysis of LSB Based Image Steganography Techniques,” in Proceedings International Conference on Image Processing, vol. 3, pp. 1019-1022, Thessaloniki, Greece, 7-10 October, 2001.

[26] E. Chrysochos, V. Fotopoulos, A. Skodras, “Robust Watermarking of Digital Images Based on Chaotic Mapping and DCT,” in Proceedings of the16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, 25-29 August, 2008.

[27] A. G. Bors and I. Pitas, “Image Watermarking using Block Site Selection and DCT Domain Constraints,” Optical Express, pp. 512-523, 1998.

[28] A. D. Roza, M. Barni, F. Bartolini, V. Capalini, and A. Piva., “Optimal Decoding of Non-additive Full Frame DFT Watermarks“, Proceedings of the 3rd Workshop on Data Hiding, 2006.

[29] V. Solachidis and I. Pitas, “Circularly symmetric watermark embedding in 2-D DFT domain,” IEEE Transactions on Image Processing, vol. 10, no. 11, pp. 1741-1753, 2001.

[30] P. Loo, “Digital Watermarking using Complex Wavelets,” in Signal Processing and Communication Laboratory, Department of Engineering, University of Cambridge, 2002.

[31] D. Kundur and D. Hitzinakos, “A Robust Digital Image Watermarking Method using Wavelet-based Fusion,” in Proceedings of International Conference on Image Processing, Washington DC, USA, 1997.

[32] Anusudha Krishnamurthi1, N. Venkateswaran2, and J. Valarmathi3,”Swarm Optimization Based Dual

Transform Algorithm for Secure Transaction of Medical Images", The Advances in Intelligent Systems and Computing series, vol. 328, pp. 483-491, Springer 2015.

[33] Ali Al-Haj, Alaa' Amer," Secured Telemedicine Using Region-Based Watermarking with Tamper Localization Secured Telemedicine Using Region-Based Watermarking with Tamper Localization", Journal of digital imaging, Vol. 27, pp. 737–750 ,May 2014.

[34] Manuel Cedillo-Hernandez, Francisco Garcia-Ugalde, Mariko Nakano-Miyatake, Hector Perez-Meana," Robust watermarking method in DFT domain for effective management of medical imaging", Signal, Image, and Video processing Journal, Volume 9, Issue 5, pp 1163-1178, July 2015.

[35] Amit Kumar Singh, Basant Kumar, Mayank Dave, Anand Mohan," Robust and Imperceptible Spread-Spectrum Watermarking for Telemedicine Applications", Proceeding of The National Academy of Sciences, Volume 85, Issue 2, pp 295-301, India 2015.

[36] Nilanjan Dey, Goutami Dey, Sayan Chakraborty and Sheli Sinha Chaudhuri, "Feature Analysis of Blind Watermarked Electro-myogram Signal in Wireless Tele-monitoring", Concepts and Trends in Healthcare Information Systems Volume 16 of the series Annals of Information Systems, pp 205-229, September 2014.

[37] K. Anusudha , N. Venkateswaren, "Energy Based Wavelet Domain Medical Image Watermarking", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014.

[38] N. venkatram, l. s. s. reddy, p. v. v.kishore, ch.shavya, "RSA-DWT based medical image watermarking for telemedicine applications", journal of theoretical and applied information technology31st.,vol. 65, no.3, July 2014.

[39] A. Umaamaheshvari and K. Thanushkodi, "Digital Image Watermarking Based on Independent Component Analysis and Ridgelet Transform," International Journal of Computer Science and Network Security, IJCSNS, vol. 11, no. 4, April 2011.

[40] S. M. Ramesh and A. Shanmugam, "An Efficient Robust Watermarking Algorithm in Filter Techniques for Embedding Digital Signature into Medical Images Using Discrete Wavelet Transform", European Journal of Scientific Research, vol. 60, no.1,pp. 33-44, 2011.

[41] M. A. Hajjaji, A. Mtibaa, and E. B. Bourennane, "Watermarking of Medical Image: New Approach Based On Multi-Layer Method," International Journal of Computer Science Issues, IJCSI, vol. 8, issue 4, no. 2, July 2011.

[42] B. Kumar, A. Anand, S. P. Singh, and A. Mohan, "High Capacity Spread-Spectrum Watermarking for Telemedicine Applications," World Academy of Science, Engineering and Technology, vol. 79, 2011.

[43] M. A. Hajjaji, A. Mtibaa, and E. B. Bourennane, "A Watermarking of Medical Image: Method Based "LSB", Journal of Emerging Trends in Computing and Information Sciences, vol.2, no. 12, December 2011.