International Conference on Multidisciplinary approaches in Social Sciences, Humanities and Sciences
Sri S.Ramasamy Naidu Memorial College, Sattur, Tamil Nadu, India (MASHS-18)
14th December 2018 www.conferenceworld.in ISBN:978-93-87793-61-3

A Survey on Various Aspects of Medical Image Watermarking

Antony Sudha.K [1], MuthuLakshmi.G[2], Cibi Castro.V[3]

[1,3]*Research Scholar, Dept. of CSE, Manonmaniam Sundaranar University, Tirunelveli, India*

[2]*Assistant Professor, Dept. of CSE, Manonmaniam Sundaranar University, Tirunelveli, India*

ABSTRACT - *Medical image data is a central part of diagnostics in today's healthcare information systems. The digital images transferring via internet which will not be secure. Security is the most important issue during transmission of medical images. As the medical images are sensitive so, it is necessary to protect them. Watermarking in medical images is commonly used for content authentication, effective data distribution and management, storage, security etc. This paper presents a survey and analysis of various techniques that are used for protection of medical images through watermarking. Various aspects of medical image watermarking are discussed in this paper including Requirements, classification and performance measures.*

Keywords*: Healthcare information system, medical images, watermarking.*

I. INTRODUCTION

In the digital world all the things are going to be digitalized. Every business area, government and private zones are using the digital image as transferring way for every essential data. The digital images transferring via internet which will not be secure. Therefore there is a need of security for that digital images. Watermarking is also one of the digital image security Technique. Watermarking can increase the security of digital images by inserting special information, called a watermark or hidden data in hidden way. watermarking techniques can be classified based on the different sights. Based on the embedding data concept, the watermarking techniques has the following domains, that is Spatial domain, Transform domain [9]. In Spatial domain the watermark bits directly fixed to the pixels of the cover object. In this methods can be easily modeled. However the embedded watermark can be easily destroyed or can easily be modified by a third person [10][11]. In transform domain, the watermarked image is obtained by embedding the watermark onto the transformed version of the original image [12]. According to human perception, the watermarking techniques are classified into two types. One is visible and another one is invisible watermarking. Visible watermark appears visible to a casual viewer on a careful inspection. Logos are the best example for visible watermarks. Invisible watermarks are used for authentication, integrity verification, and copyright protection. Dual watermark is a combination of visible and an invisible watermark [13]. Invisible watermarks can be classified into four types that are fragile, semi fragile, robust and hybrid. Hybrid watermarking is a mixture of robust and fragile techniques. According to the application the watermarking techniques are divided in two types, namely source based and Destination based.

II. SYSTEM FRAMEWORK FOR WATERMARKING

Watermarking system consists of two processes, Embedding and extraction. In embedding process the watermark fed into the host object in such a way. The host objects like video, audio, text, image, 3Dmesh, etc. The watermark can be name, logo, image, serial number, owner's ID or any other information which shows ownership of the host signal. These signatures are normally converted into a binary sequence before being embedding into the host signal.

- Embedding - Embedding algorithm is used to produce the watermarked image.
- Distribution - To spread the watermarked image.
- Attacks - Alteration of the watermarked image.
- Extraction - To extract the original host object from the watermarked image.
- Detection - To evaluate the accuracy and quality of watermarked images.

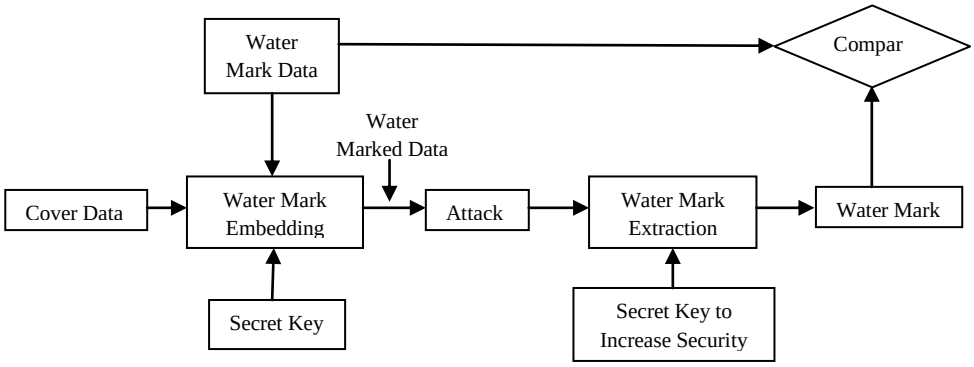

Fig 1. System Framework for watermarking

In embedding process, the cover data and the watermark data enter to the system and according to the embedding algorithm, the watermarked image will be produced. Secret key also inserted to the embedding system for security purposes. If 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. In extraction process to extract the cover data from the watermarked data.

III. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

- Owner Identification - To Show to be valid ownership of the content. A right owner can retrieve the watermark from digital content to prove his ownership.
- Finger Printing - Providing biometric security.
- Copyright Protection - Trace back the source of illegal distribution and duplication of the content.
- Medical Applications - Provide both authentication and confidentiality.
- Secured E-voting system - Provide convert and machine readable layer of security to fight against various issues such as digital counterfeiting, fraud, identity theft etc.
- Source tracking - The watermark is inserted into a digital signal at each point of distribution.

IV. REQUIREMENTS FOR MEDICAL IMAGE WATERMARKING

In the recent digital world, Medical images are often transmitted over insecure channel. Medical images contain sensitive information, and when they are transmitted over the unsecured network, they become vulnerable to corruption by noisy transmission channels and attacks by hackers. Watermarking in the medical field has different practical applications,[14] including telediagnosis, teleconferences among clinicians, and distant learning of medical personnel. Medical image watermarking has been used for Compact Storage, Saving Bandwidth, Avoiding Segregation, Tamper Proofing, Confidentiality and security, Indexing, Integrity Control, Captioning, Access Control. Medical image Watermarking 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. 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 [15] [16]. The following security requirements [1] are needed for medical Image watermarking.

1. Confidentiality means only the authorized users have to access the information.
2. Reliability has two important outcomes: (a) Integrity—the information has not been modified by unauthorized people, and (b) Authentication—a proof that the information belongs indeed to the correct source. Further, the traceability is important components of the reliability and use to trace the information along its distribution.
3. The availability is an ability of information system to be used in the normal scheduled condition of access.

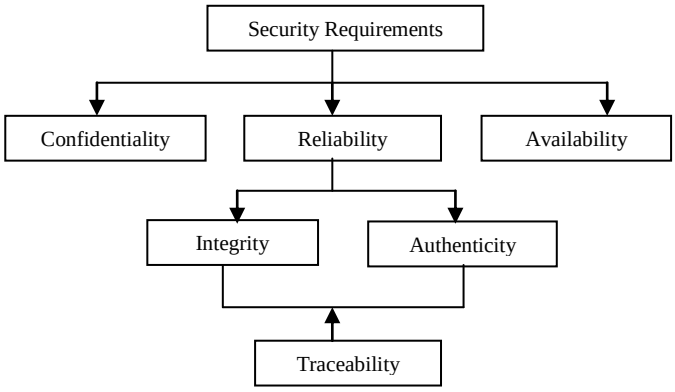

Fig 2. System requirements for EPR

V. CLASSIFICATION OF MEDICAL IMAGE WATERMARKING

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

5.1. Extraction method

The extraction process separates the cover data and watermark from the watermarked data. It issued 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 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.

5.2. 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.

5.3. Characteristics

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

5.4. 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.

VI. PERFORMANCE MEASURES

The Following Analysis are used to measure the performance of the watermarking techniques.

6.1. 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:

$$\text{MSE}(I, I_w) = \text{MSE}(I, I_w) = \frac{1}{mxn} \sum_i^{m-1} \sum_j^{n-1} [I(i,j) - I_w(i,j)]^2 \quad (1)$$

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 versionI_w.

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

Where I and I_w are original image andwatermarked image, MSE is mean squared error. Higher value of PSNR indicates less distortion.

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].

$$wPSNR\ (I, I_w) = wPSNR\ (I, I_w) = 10\log_{10}\left[\frac{Imax^2}{||NVF(Iw(m,n)-I(m,n))||^2}\right] \quad (3)$$

Structural Similarity Index Measure- was used to measure the similarity between the original image and the watermarked image.

Total Perceptual Error- It is calculated from the Watson Metric.

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

$$H\ (I,I_w)=H(I, I_w) =\sum_k p_k \log_{2(pk|qk)} \quad (4)$$

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

6.2. 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. 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.

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

$$NCC=\frac{\sum_x \sum_y w(x,y)w'(x,y)}{\sqrt{(\sum_x \sum_y [w(x,y)^2]).(\sum_x \sum_y [w'(x,y)]^2)}} \quad (5)$$

Here, 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.

6.3. 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.

6.4. Complexity Analysis

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

Table 1. Performance comparison for medical image watermarking techniques

Author (year)	Objective	Domain	Technique	Watermark Image	Result
S.Priya R.Varatharajan Gunasekaran [1] (2018)	Security	Transform domain	DWT -DCT	Scrambled Images	PSNR : 53 – 56.49dB
Abdulazim shehap Mohamed [7] (2018)	Authentication	Spatial domain	SVD	Generated from host images	PSNR : 50.97 & 51.03dB
Aditi Zear, Amit kumar singh [2] (2016)	Security	Transform domain	DWT,DCT & SVD	Signature and Symptoms text	PSNR : 43.95dB
Rohini srinivastava, Basant kumar [6] (2016)	Security and storage	Transform domain	JPEG Compression using DCT	Logo	PSNR : 36.23dB CPU time 1.31sec
N.H.Ghazali, Azizah [4] (2015)	Data hiding	Spatial domain	Fibonacci decomposition and Knight's Tour algorithm	Hospital's logo	PSNR :88.63 dB SSIM : upto 2.0 bpp
Conghuan ye ,zengg [5] (2015)	Security and efficiency	Spatial and encryption	Encryption (JFF) Scheme based on GoL and DNA	Finger printing	Information Entropy H=7.9860

Suraj kumar singh , varun P.Gopi , P.Palanisami [3] (2014)	Security	Spatial domain	DES & RNS	Natural images	MSE value of zero & PSNR value of infinite
Muhammd Arsalan [8] (2012)	Reversible data hiding	Transform domain	GA-RevWM based on GA & IWT	Generate from host images	PSNR :42.8 - 44.6 SSIM : 0.9855-0.9862
Qershi [17] (2011)	Authentication and data hiding	Transform domain	DE , DWT	EPR	PSNR : 69.26dB

VII. CONCLUSION

In this survey gives detailed information about digital image watermarking such as System framework, Applications and also gives most important aspects of medical image watermarking such as Requirements, classification, Performance measures. Medical image watermarking aims to provide protection of medical images to different healthcare applications. Though the review discussed some information about the medical image processing.

REFERENCES

[1] S. Priya, R. Varatharajan, Gunasekaran,"Paillier homomorphic cryptosystem with poker shuffling transformation based water marking method for the secured transmission of digital medical images" Personal and Ubiquitous Computing, Springer-Verlag London Ltd., part of Springer Nature 2018.

[2] Aditi Zear, Amit Kumar Singh, Pardeep Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine" , DOI 10.1007/s11042-016-3862-8, Springer Science+Business Media New York 2016.

[3] Suraj Kumar Singh, Varun P. Gopi, P. Palanisamy,"Image Security using DES and RNS with Reversible Watermarking", 2014 International Conference on Electronics and Communication System (lCECS - 2014).

[4] N. H. Ghazali, Azizah Abd Manaf, G. Sulong,"High Capacity Watermarking Technique for MedicalImages Using Fibonacci Decomposition", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 2 (2015) pp. 3431-3437.

[5] Conghuan Ye, Zenggang Xiong, Yaoming Ding, Xueming Zhang, Guangwei Wang, and Fang Xu,"Joint Fingerprinting/Encryption for Medical Image Security", International Journal of Security and Its ApplicationsVol.9, No.1 (2015), pp.409-418.

[6] Rohini Srivastava , Basant Kumar, Amit Kumar Singh, Anand Mohan , "Computationally efficient joint imperceptible image watermarking and JPEG compression: a greencomputing approach", Multimed Tools Appl (2018) 77:16447–16459 DOI 10.1007/s11042-017-5214-8.

[7] Abdulaziz Shehab , Mohamed Elhoseny , Khan Muhammad ,Arun Kumar Sangaiah , Po Yang, Haojun Huang, And Guolin Hou,"Secure and Robust Fragile Watermarking Scheme for Medical Images",Digital Object Identifier 10.1109/ACCESS.2018.2799240.

[8] Muhammad Arsalan, Sana Ambreen Malik, Asifullah Khan,"Intelligent reversible watermarking in integer wavelet domain for medical images", 0164-1212/$ – see front matter © 2011 Elsevier Inc. All rights reserved. doi:10.1016/j.jss.2011.11.005.

[9] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, Senior member, ieeemultiple image watermarking applied to health information management. IEEE Trans. Inf. Technol. Biomed. 10(4), 722–732 (2006).

[10] Zain JM, Clarke M: Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. Int J Comput Sci Netw Secur 7(9):19–28, 2007.

[11] Wu N-I, Hwang M-S: Data hiding current status and key issues. Int J Netw Secur 4(1):1–9, 2007.

[12] Heylena K, Dams T: An image watermarking tutorial tool usingmatlab. Mathematics of Data/Image Pattern Recognition, Compression, and Encryption with Applications XI, Proc. of SPIE 2008. 7075, 70750D: p. 1–12.

[13] S.P. Mohanty, Watermarking of digital images, M.S. Thesis, Indian Institute of Science, India,1999.

[14] 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.

[15] 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.

[16] 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.

[17] Al-Qershi OM, Khoo BE: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. J Digit Imaging 24(1):114–125, 2011.