Wavelet Based Digital Watermarking for Medical Images

1st Amita Joshi
ID - 2019H1030908G
Bits Pilani, Goa Campus
Goa, India

2nd Nishi Singh
ID - 2019H1030108G
Bits Pilani, Goa Campus
Goa, India

3rd Shimoni Sinha
ID - 2019H1030019G
Bits Pilani, Goa Campus
Goa, India

I. Introduction

Digital watermarking have played a very significant role in the field of medical sciences for diagnosis and treatment purposes. Recently due to the development of latest technologies in the areas of communication and computer network, exchange of medical images between hospital has become a common practice. Some of the instances being teleconferences among doctors, distant learning for medical students and so on. For protection of the medical images, digital watermarking has been introduced.

A. Digital Watermarking

Digital watermarking is the hiding of information (the watermark) within the digital data, such that the embedded watermark can be identified or extracted later to produce a confirmation of the validity of data.

Advantages of digital watermarking are: 1) theft protection, 2) certain level of marketing, 3) includes tracking components, and 4) lends credibility. Disadvantages include 1) can interfere with the image, 2) doesn't lead to extra sales, and 3) time consuming process.

For protecting digital images, three categories of water marking has been introduced: 1) robust watermarking, 2) fragile watermarking, 3) semi fragile watermarking and, 4) hybrid watermarking.

Robust watermarking are most difficult to remove from digital content. They are robust against legitimate or illegitimate distortions. They may also be used for copy write protection. Fragile watermarks are easily destroyed by tampering. Thus, they are used for data authentication application. Semi fragile watermarks protect images from illegal modifications. Hybrid watermarking is a combination of fragile and robust methods to achieve authenticity, integrity and ownership protection simultaneously.

B. Drawbacks of current watermarking techniques

1) Region of Interest and Region of Non- Interest Segementation

Medical images can be differentiated into two regions: Region of Interest (ROI) and Region of Non-Interest (RONI). ROI section includes the informative region which is used for diagnostic purposes and must be stored without any distortion. However, RONI usually represents the back background of the image, but occasionally it can contain grey level parts of slight interest. In ROI watermarking, spatial or transform domain techniques is used to hide information. The encoded watermark may be robust or fragile based on the purpose in hand.

To maintain the integrity of medical images that avoids the distortion of image in ROI, watermark embedding in done in RONI. This ensures that informative part of ROI is not distorted.

2) Spatial Domain Techniques

In this method, the watermark is inserted into the cover image by directly modifying the pixel values of the original image. These algorithms are simple, fast and offer high embedding capacity. Also, a small watermark can be hidden several times. Spatial domain techniques may have some benefits, but their main drawback is that they cannot survive against many operation like adding noise and lousy compression methods. Moreover, when discovering the utilized watermarking method, the hidden watermark can be easily altered by an unauthorized user.

With the current algorithms in the medical field, either there was no ROI and RONI segmentation or spatial domain was used for digital watermarking.

C. Mandatory Features of digital image watermarking

The most important features required in medical image watermarking are: 1) Confidentiality, 2) Reliability and, 3) Availability.

Confidentiality indicates that only authorized people have access to the data. This can be accomplished by applying techniques such as encryption, access control and firewall.

Reliability may be decomposed into two aspects: i) integrity which verifies that the information has not been changed, ii) Authentication which ensures that the data belongs to the right patient and is delivered from a verified source. Integrity can be fulfilled by encrypting the images while sharing over the network. Authentication needs measures to discover that confidentiality and/ or the integrity of the data has not been breached.

Availability defines the capability of the authorized users to utilize the information system in the normally scheduled situations of access and practice

D. Final Remarks

Many techniques have been proposed for watermarking the medical images utilizing the spatial and transform domain. The proposed scheme makes use of ROI and RONI segmentation along with the DWT to ensure that all the above mentioned features in section 1E i.e. Confidentiality, Reliability (Authentication and Integrity) and Accessibility are achieved.

The proposed scheme has been implemented in Matlab, as it is a high level technical computing language and interactive environment for algorithm development, data visualization, data analysis, and numerical computation.

II. Literature Survey

[2] Medical images are produced from a wide variety of sources like CT scan, ultrasound and so on. A patient can store his medical image in the form of CD instead of taking a hard copy. However, medical images can be easily tampered and can be used for illegal reasons.

Wu et al.[2] proposed a block based method based on DCT for watermarking medical image. It is ROI based. Drawbacks for this method was that the method required more number of calculations to generate recovery data for ROI and embedding it into all blocks of the medical image.

[3] The exchange of medical information over the networks requires content management to index the record information and to provide security and authenticity to the patient's information. The existing research focused on preserving the resolution of the medical images after embedding the watermark without taking into much consideration the robustness of the schemes against different attacks.

Mostafa et al.[3] proposed a methodology that saves the Electronics Patient Record(EPR) in the medical image. This saves the storage space, the transmission overheads and guarantees the security of the information. Watermark embedding is done using the Discrete Wavelet Packet Transform(DWPT). The patent information is coded with an error correcting code, Bose–Chaudhuri–Hocquenghem codes(BCH code), to improve the robustness of the method.

This scheme, however, does not provide us with the reversibility. This means that there is a huge degradation in the quality of the medical image after the watermark embedding. Thus, the watermark recovered does not have high accuracy.

[7] Most of the algorithms proposed have a common problem of security where the watermarks embedded either are not encrypted before embedding or the algorithm used for encryption is weak.

Solanki et al.[7] proposed a watermarking scheme where watermark has been encrypted using RSA algorithm and has been embedded in ROI using DWT.

Drawbacks of this method is that a lot of pre-processing work is required before a watermark can be embedded in the image.

[8] Whenever an image is taken in a hospital, it is stored in a hierarchical manner into Picture Archiving and Communication System(PACS). Through this process of creation and transmission, the integrity of these images, and wider data sets may not be maintained accurately. Therefore the authenticity and integrity of the medical images were at question when they had to be transferred over networks.

Fontani et al.[8] proposed that information is embedded using the DICOM standard, where the digital signature is placed in the header. Digital watermarking be done in such a way that the metadata is robustly linked to the medical image and is not easily distorted. Therefore, they used integer to integer discrete wavelet transform.

The embedding region for the watermark is the whole image making the distortion due then removal of the watermark inevitable. This can lead to wrong diagnosis and various other problems. The methodology proposed is also very fragile to various attacks, this reduces the robustness to a great extent. It also does not propose a viable method to prove the authentication of the image making it more fragile.

[11] Block based watermarking technique proposed in the past few years are detecting the tampered blocks in the watermarked medical image based on average intensity of the blocks. These schemes fail in identifying the changes or tampers in any block if the values of pixels in that block are modified without changing the average value of the block.

Eswaraiah et al.[11] proposed scheme helps in removing these defects. He proposed the scheme in which image is divided into ROI pixels, RONI pixels, and border pixels.. Average and variance of each ROI block are calculated and compared with average and variance of pixels extracted from corresponding RONI block.

The drawback of the proposed method is based on the assumption that the intruders generally try to modify only the significant part (ROI). This method cannot recover original ROI when the RONI and border of the watermarked medical image are attacked or modified by intruders.

[13] In previous methodologies, reversible watermarking is realized by histogram modification. GA algorithm has learning ability for intelligent threshold selection, which controls the effective payload. The experimental results demonstrate that both imperceptibility and robustness are achieved simultaneously for a series of natural images and medical images. However, there is no security feature in this method. Ko et. al. proposed the nested QIM-based method for reversible watermarking, which is targeted for the healthcare information management systems. However, important properties of watermarking algorithm such as the robustness and imperceptibility are not addressed in this scheme, and thus it is not conclusive that the Ko's watermarking method is suitable for medical application.

Baiying et. al.[13] proposed a reversible watermarking method with wavelet transforms and Singular Value Decomposition (SVD). Signature and logo data are inserted by Recursive Dither Modulation algorithm (RDM). Differential Evolution (DE) is explored to design the quantization steps optimally. Good balance of imperceptibility, robustness and capacity is obtained by DE.

The main disadvantage of using the DE algorithm is that the convergence is unstable. Results obtained after SVD is

not always the best for visualization and can also be difficult to interpret.

[14] In most of the previous reported papers, embedding capacity of images is low due to the limited number of peak points present in the cover image. Also, the capability to detect and localise the tamper is one of the most important attributes of any data hiding system. The tamper detection and correction are block based.

Shabir et. al.[14] has proposed the usage of Pixel to Block conversion technique (PTB) for high capacity. It is a computationally efficient mechanism for generating cover image from input image. Block checksum computation is used for tamper detection and localization. The main disadvantage is that the watermark embedded in the image is fragile.

[15] In all previous methodologies no medical image watermarking technique has been reported in transform domain which is robust to both the singular attacks as well as to hybrid attacks.

Parah et. al.[15] has presented a robust medical image watermarking system which besides being robust to various singular image processing attacks, has been found robust to different hybrid (two or more simultaneous) attacks. In the paper, two algorithms have been proposed. In the first algorithm, the Electronic Patient Record (EPR) and the watermark is embedded in the whole image. In the second algorithm, the watermark is embedded in the RONI part of the medical image. The proposed techniques have been implemented in DCT domain. 8×8 block wise DCT is computed and DCT coefficients are modified for the embedding purpose.

The disadvantage of embedding in the whole image is that the watermark can distort the medical image to the point where it becomes difficult to recognize the medical image due to distortions. Medical practitioners refuse to diagnose based on images that have been distorted even a little bit.

When watermark is embedded into only RONI part of the image using DCT, the main disadvantage is that there is no protection against picture cropping. One of the main problems and the criticism of the DCT is the blocking effect. In DCT images are broken into blocks 8x8 or 16x16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking effect.

[16] Most of the conventional wavelets convert an image having the integer-valued pixels into floating-point wavelet transform of wavelet domain. Hence, during embedding of watermark, loss of information occurs due to truncation of pixels value which are floating point in nature.

Pandey et. al.[16] proposed a lifting scheme which overcomes the limitation of conventional wavelets by faster and effective execution of the wavelet filtering.

This scheme does not segment the image into two parts ROI and RONI.

[17]The medical image exchange standard (DICOM) offers mechanisms to provide confidentiality for the header data of the image but not for the pixel data, even if it provides mechanisms to achieve authenticity and integrity for the pixel data but not for the header data.

Ali et.al.[17] proposed a scheme that provides a crypto-based algorithm that provides confidentially, authenticity, and integrity for the pixel data, as well as for the header data.

As the algorithm consists of an encryption and signature creation procedure and a decryption and signature verification procedure time taken is more than expected.

[18] In existing system the original image is splitted into blocks using DCT domain, and then Singular Value Decomposition (SVD) on the blocks is applied, which is then followed by DE algorithm. Experimental results show that this scheme maintains a satisfactory image quality and hence the PSNR value is comparatively low for various attacks such as rotation, histogram equalization, cropping and gamma correction.

Al-Haj et. al[18] proposed a scheme to use Discrete Wavelet Transform (DWT). This technique results in higher PSNR value for the possible image processing attacks and hence it provides high level authentication and security as compared to exiting system.

The proposed system is not suitable for any other stronger attacks. Because this may lead to distortion of images and have the possibility of easy retrieval of the hidden information.

[19] Protecting the quality of medical images when transmitted over a network when making sure that there is not much latency involved was an important task. This was not yet taken care of.

Therefore, Soualmi et. al.[19] proposed a combination of DCT transform, Weber descriptors (WDs) and Arnold chaotic map. First the watermark image is scrambled using Arnold chaotic map. Second, the DCT is performed on each medical image block, and the watermark data are embedded in the DCT middle- band coefficients of each block. Finally, a new embedding and extracting technique is proposed, based on WDs without any loss by selecting the right coefficients.

However, in this method the Electronic Patient's Record(EPR) is stored in the Region of Interest(ROI). Using this method, though the robustness is taken care of but the image gets distorted during the extraction process of the watermarked data.

[20] The existing watermark- embedding algorithm with Probabilistic Neural Networks(PNN) depends only on the standard deviations of each coefficient block of the dual-tree complex wavelet transform. Thus, the quality of the watermarked image is degraded after embedding.

Al-Nabhani et. al.[20] proposed an imperceptible and robust blind watermarking algorithm based on the PNN in the wavelet domain. The proposed algorithm focuses on maintaining the invisibility and quality of the watermarked image by selecting the best embedding positions in the block-based wavelet coefficient.

This method is not every efficient under geometric attacks like cropping and so on.

[21] Existing watermarking methods are not compatible with the watermark's ability to resist geometric attacks and be robust at the same time.

Liu et. al.[21] proposed multi-watermarking algorithm.First, the visual feature vector of the medical image was obtained by dual-tree complex wavelet transform and discrete cosine transform (DTCWT-DCT). Then using henon map chaotic encryption technology, the security of the watermark information is strengthened.

The physician don't get to decide the Region of Interest(ROI) of the medical image which might affect the diagnosis.This method is more efficient for coloured medical images.

III. System Model

Sender sends the watermarked image that has the watermark encoded by a secret key. Watermark consists of patient's information, doctor's information, diagnostic information of that patient, least significant bits (LSB) of ROI part of the medical image and logo that is additionally stored to check integrity.

Fig. 1. System Model

The receiver receives the watermarked medical image and removes the watermark by using an extraction algorithm and uses the same key to decode the watermark that had been embedded in the watermarked image.

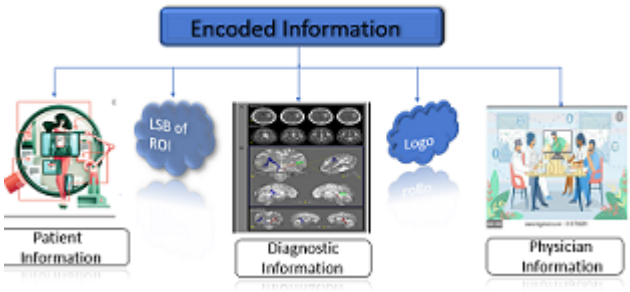

Fig. 2. Information encoded in the watermark

IV. Problem Statement

Watermarking technology has recently evolved in medical image watermarking as it can be used to hide the patient's information and then extract back the information using certian private key. Watermark content embedding into a medical image is a crucial task. It is because of the requirement of confidentiality, reliability and availability for proper diagnostic and extraction of watermark content. Not only the Electronic Patient Record (EPR) data but logo is also required for the authntication of medical image.

Various papers were proposed to hide the patient's information in the medical image. Some of them suggested using spatial domain as it required less calculations in the embedding process. Fontani et. al[8] proposed that DICOM standard be used in embedding, where the digital signature is paced in the header. Shabir et. al[14] proposed the usage of pixel to block conversion technique for high capacity embedding. Some papers suggested an embedding process that was very robust but lacked reversibility.

Watermarking techniques that used spatial domain for embedding data have the disadvantage that it deals with the image plane itself, whereas the frequency domain deals with the rate of pixel change. It also lacks robustness and can be easily attacked by geometric attacks. Discrete Cosine Transform(DCT) when used for watermarking medical image is more time-consuming as it requires a number of calculations to generate recovery data and also embedd it into blocks of medical image. When a medical image has not been segmented into Region of Inerest (ROI) and Region of Non-Interest (RONI) and instead medical data has been embedded into the whole image leads to high distortion of the ROI part of the medical image. Due to high distortion, medical practitioners would refuse to diagnose based on that medical image.

Therefore, we require a watermark technique that provides us a more robust watermark that can be embedded with compromising the quality of the medical image and is less time consuming and requires less computing power.

In this paper, wavelet based digital watermarking is proposed. Here, three level Digital Wavelet Transform (DWT) along with the BCH coding makes the scheme more undetectible and robust against a variety of attacks. Three level DWT is applied on the RONI region of the medical image which generates different frequency sub-bands (LL, LH, HL, HH) after every level of decomposition. The encoding of the image is done in the non-overlapping blocks of the LL subband. After embedding the watermark, we perform three level Inderse DWT transform toget the watermarked medical image.

V. Proposed Solution

1) Watermark Embedding Scheme

The physician segments the medical image into Region of Interest (ROI) and Region of Non-Interest (RONI) depending on the information that he wants to collect for the medical diagnosis.

In Region of Interest (ROI) part of the image, a fragile watermark is introduced using LSB algorithm. The LSB algorithm introduces the watermark in the image by changing the Least Significant Bits of the grey scale image.

The original LSB bits of the ROI part along with patient information, doctor's information, diagnostic information and logo are first encoded using secret key and then embedded into the RONI region of the image as a robust watermark.

The RONI region is first divided into N X N blocks and then subjected to a 3-level Discrete Wavelet Transform (DWT). After this, the robust watermark generated from above is

inserted into the image. The image is then subjected to 3-level Inverse Discrete Wavelet Transform (IDWT) to bring it back to spatial domain. Finally, the ROI and RONI regions are combined to get the watermarked image that is to be sent to the receiver.

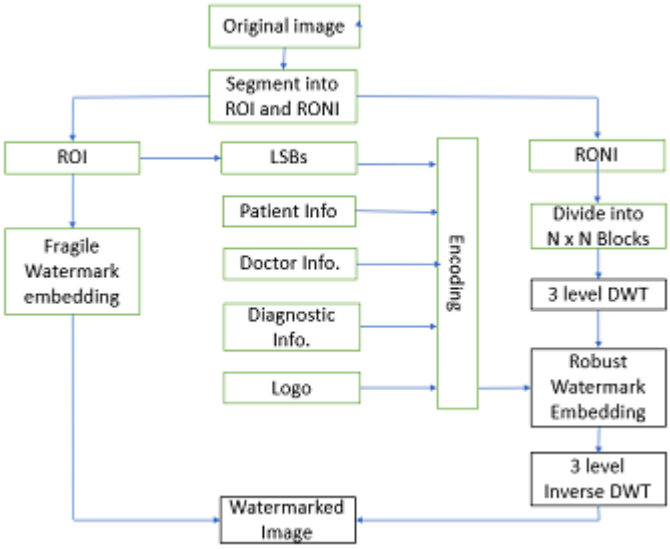

Fig. 3. Embedding Process.

2) Watermark Extraction Scheme

The watermarked image received from the sender is divided into Region of Interest (ROI) and Region of Non-Interest (RONI) part.

The RONI part is divided into N X N blocks and then subjected to 3-level Discrete Wavelet Transform (DWT). The robust watermark is then extracted and is decrypted to get back patient information, doctor's information, diagnostic information and logo along with the Least Significant Bits of the ROI region. The doctor's information is used to check the authenticity of the image and the logo is used to check the integrity of the image.

In the ROI part, the fragile watermark is extracted to check the integrity of the image and the least significant bits extracted from the robust watermark is used to replace the bits in the ROI part to get back the original non-distorted image.

The RONI part is again subjected to 3-level Inverse Discrete Wavelet Transform (IDWT) and then combined with the ROI part to get back the original image.

The effectiveness of the above scheme has been validated in Matlab simulations.

VI. Security Analysis

Security analysis of our proposed work has been done by considering these parameters: confidentiality and reliability.

Confidentiality has been achieved by generating two keys. The first key is a 256 X 256 matrix that has been used to embed information at the first level of DWT decomposition. This key has been generated by combining RONI part of image (converted into matrix form) and a random matrix of size 256

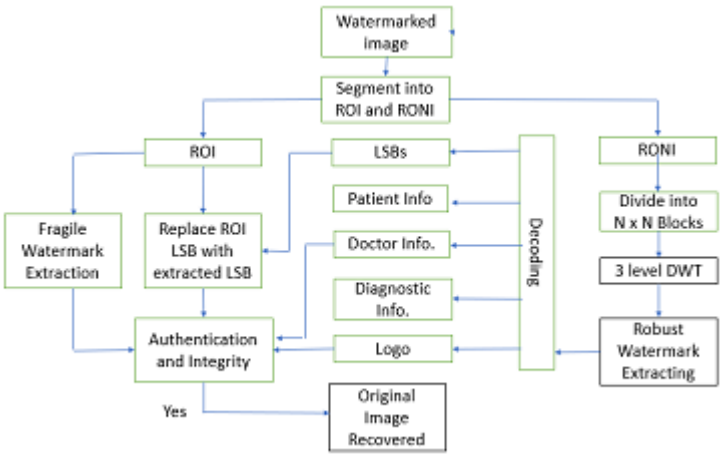

Fig. 4. Extracting Process.

X 256 that has been separately generated. The second key is a 128 X 128 matrix that has been created from the key that has been computed above.

Reliability has been divided into two parts: Integrity and Authentication. Integrity has been achieved by embedding a logo image along with all the information that needs to sent with the medical image as part of watermark. Whenever the watermarked image is been tampered with, the extracted logo will show some level of distortion. This will tell the receiver that the image has been tampered with and will therefore provide integrity to the image. Authentication has been provided by storing patient's information and doctor's information as part of watermark.

All the information that needs to be sent across to the receiver as part of watermark has been encoded by BCH encoder. BCH encoder creates a BCH code that are cyclic error correcting codes that are constructed using polynomials over a finite field (also called Galois field). One of the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors. Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes, using small low-power electronic hardware.

A. Security Attacks

To check the security level of the proposed solution, we are checking our system by attacking it with few security attacks.

- Gaussian Noise - Gaussian noising is a process that adds a noise signal to an image in order to deliberately corrupt the image, hence reducing its visual quality.
- Salt and Pepper Attack - Salt and Pepper noise has a very different probability distribution function to Gaussian noise. Salt and Pepper noise represents itself as randomly occurring white and black pixels in an image.

- Median Filtering Attack - Median Filtering is an image processing technique which aims at reducing the presence of noise in an image, hence enhancing the image quality. The theoretical reason behind the use of Median Filter to attack watermarks is based upon the property that the watermark signal possesses when it resides in its host. Any watermark signal can be considered as a small varying signal inside its host. The strength of this signal is equivalent to most noise in any image capture equipment. Since a Median Filter removes noise presence, it is expected that any watermark signal present in the image will also be affected or removed.
- Gaussian Smoothing Attack - Gaussian Smoothing shares many common properties with other smoothing processes such as Median Filtering. It is an image processing technique which aims at reducing the presence of noise in an image to improve its quality. The reason behind the use of the Gaussian Smoothing process to attack watermarks is similar to that of the Median Filter. The difference between Gaussian Smoothing and Median Filtering lies on the way the smoothing is carried out. A Gaussian Smoothing filter is a low pass frequency filter whereas Median filter is a replacing a pixel value by the weighted average of the intensity levels in the neighborhood defined by the filter mask.
- Flip transform - Flip the image matrix row or column based on parameter.
- Modification - Modify some of the bits of the watermarked image so that the data stored in it has changed.
- Scale Transform - Change the size of the watermarked image so that the image pixel information changes.

VII. Performance Analysis

In the digital watermarking scheme, it is necessary to preserve the quality of the images. So, for evaluating the watermarked image,we need to know the accuracy of the extracted watermark. The results can be shown against the following benchmarks:

1) Peak Signal to Noise Ratio (PSNR): PSNR is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.The higher the PSNR values indicate that the watermarked image is very similar to the original image.
2) Signal to Noise Ratio (SNR): SNR is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise.
3) Mean Squared Error (MSE): MSE measures the average of the squares of the errors—that is, the average squared difference between the estimated values and the actual value.

COMPARISON	PSNR	MSE	SNR
Al Nabani et al [20]	60.63 dB	0.00754	48.67 dB
Soualmi el al [19]	43.76 dB	0.010923	28.79 dB
Al Qershi et al [6]	85.5 dB	0.002781	72.18 dB
Our Proposed Scheme	98.58 dB	0.001193	86.199 dB

Fig. 5. Performance Analysis

VIII. Conclusion

The necessity of protecting medical images and other patients' data is not only for confidentiality purposes but also to prevent manipulations that might happen by authorised and unauthorised users while using these images.Many techniques have been proposed in the literature for watermarking the medical images utilising both spatial and transform domains.Studies prefer the techniques based on DWT due to it is offering an accurate matching of the human visual system.Medical requirements are extremely strict with the quality of medical images and do not allow non-clinical based modification in any way.Our proposed solution tries to meet all the criterion mentioned in the problem statement.The future scope of this work is to make it more attack resistant. We need to apply some techniques apart from the BCH encoding to improve the robustness of the image.

References

[1] Lee, Sunil and Yoo, Chang and Kalker, Ton. (2007). Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform. Information Forensics and Security, IEEE Transactions on. 2.321-330.10.1109/TIFS2007.905146.

[2] Wu, J.H.K., Chang, R., Chen, C. et al. Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique. J Digit Imaging 21, 59–76 (2008).

[3] Ahmed, Salwa and El-Sheimy, Naser and Tolba, Ahmad and Abdelkader, Fadia and Elhindy, Hisham. (2010). Wavelet Packets-Based Blind Watermarking for Medical Image Management. The open biomedical engineering journal. 4. 93-8. 10.2174/1874120701004010093.

[4] Chiang, K., Chang-Chien, K., Chang, R. et al. Tamper Detection and Restoring System for Medical Images Using Wavelet-based Reversible Data Embedding. J Digit Imaging 21, 77–90 (2008).

[5] Al-qershi, Osamah and Khoo, Bee Ee. (2011). High capacity data hiding schemes for medical images based on difference expansion. Journal of Systems and Software. 84. 105-112. 10.1016/j.jss.2010.08.055.

[6] Al-qershi, Osamah and Khoo, Bee Ee. (2009). Authentication and Data Hiding Using a Reversible ROI-based Watermarking Scheme for DICOM Images. World Academy of Science, Engineering and Technology. 38.

[7] Solanki, Neha and Malik, Sanjay. (2014). ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security. International Journal of Modern Education and Computer Science. 6. 40-48. 10.5815/ijmecs.2014.10.06.

[8] Fontani, Marco and De Rosa, Alessia and Caldelli, Roberto and Filippini, Francesco and Piva, Alessandro and Consalvo, Matteo and Cappellini, Vito. (2010). Reversible watermarking for image integrity verification in hierarchical PACS. MM and Sec'10 - Proceedings of the 2010 ACM SIGMM Multimedia and Security Workshop. 161-168. 10.1145/1854229.1854259.

[9] Nambakhsh, Mohammad-Saleh and Ahmadian, Alireza and Zaidi, Habib. (2010). A contextual based double watermarking of PET images by Patient ID and ECG Signal. Computer methods and programs in biomedicine.

[10] Das, Sudeb and Kundu, Malay. (2013). Effective Management of Medical Information through ROI-Lossless Fragile Image Watermarking Technique. Computer Methods and Programs in Biomedicine. 111. 662-675. 10.1016/j.cmpb.2013.05.027.

[11] Eswaraiah, R and Reddy, Edara. (2014). Medical Image Watermarking Technique for Accurate Tamper Detection in ROI and Exact Recovery of ROI. International journal of telemedicine and applications. 2014. 984646. 10.1155/2014/984646.

[12] Tan, Chun and Ng, Jason and Xu, Xiaotian and Poh, Chueh Loo and Guan, Yong and Sheah, Kenneth. (2010). Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability. Journal of digital imaging : the official journal of the Society for Computer Applications in Radiology. 24. 528-40. 10.1007/s10278-010-9295-4.

[13] Baiying Lei, Ee-Leng Tan, Siping Chen, Dong Ni, Tianfu Wang, Haijun Lei. (2014). Reversible watermarking scheme for medical image based on differential evolution, ISSN 0957-4174.

[14] Shabir A. Parah, Farhana Ahad, Javaid A. Sheikh, G.M. Bhat. (2017). Hiding clinical information in medical images: A new high capacity and reversible data hiding technique, Journal of Biomedical Informatics, Volume 66, ISSN 1532-0464.

[15] Parah, S.A., Sheikh, J.A., Ahad, F. et al. Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl 76, 10599–10633 (2017).

[16] Pandey, m k and Parmar, Girish and Gupta, Rajeev and Sikander, Afzal. (2019). Lossless robust color image watermarking using lifting scheme and GWO. International Journal of System Assurance Engineering and Management. 10.1007/s13198-019-00859-w

[17] Ali, Musrrat and Ahn, Chang Wook and Pant, Millie. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik. 125. 428-434. 10.1016/j.ijleo.2013.06.082.

[18] Al-Haj, Ali. (2014). Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. Journal of digital imaging. 28. 10.1007/s10278-014-9734-8.

[19] Soualmi, Abdallah and Adel, Alti and Laouamer, Lamri. (2018). A New Blind Medical Image Watermarking Based on Weber Descriptors and Arnold Chaotic Map. Arabian Journal for Science and Engineering. 43. 10.1007/s13369-018-3246-7.

[20] Al-Nabhani, Yahya and Jalab, Hamid and Wahid, Ainuddin and Md. Noor, Rafidah. (2015). Robust Watermarking Algorithm for Digital Images Using Discrete Wavelet and Probabilistic Neural Network. Journal of King Saud University - Computer and Information Sciences. 27. 10.1016/j.jksuci.2015.02.002.

[21] Liu, Jing and Li, Jingbing and Ma, Jixin and Sadiq, Naveed and Bhatti, Uzair and Ai, Yang. (2019). A Robust Multi-Watermarking Algorithm for Medical Images Based on DTCWT-DCT and Henon Map. Applied Sciences. 9. 700. 10.3390/app9040700.