ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

Prospects of Digital Watermarking in Providing Security, Reliability, and Privacy to Medical Images

Subhrajit Sinha Roy[1], Abhishek Basu[2] and Avik Chattopadhyay[3]

ABSTRACT

Telemedicine is one of the most eminent terms used in the modern e-healthcare system. Digital medical image reports, along with electronic patient records, play a central role in diagnosis from distance. These reports need to be transmitted over an open communication channel with immense security and reliability, so that appropriate diagnosis can be performed. Moreover, the privacy of the patient is required to be preserved. Digital watermarking is one of the most conventional and suitable practices to serve all of these purposes. New challenges appear in the domain of watermarking with the advancement of digital signal processing; consequently, researchers are endowing more efforts to overcome these challenges. In this paper, a survey on medical image watermarking has been done, and the performance of a few state-of-the-art medical image watermarking techniques is compared. This work makes the researchers and the developers familiar with the recent trends, challenges, and scopes in this domain to facilitate them in finding out adequate research directions.

Article information:

Keywords: Comparison, Medical Imaging, Review, Watermarking

Article history:
Received: August 11, 2022
Revised: October 21, 2022
Accepted: February 17, 2023
Published: April 8, 2023
(Online)

DOI: 10.37936/ecti-cit.2023172.249484

1. INTRODUCTION

Electronic healthcare (e-healthcare) system brings in telediagnosis as well as telemedicine to do up the conventional healthcare practices. The word 'telemedicine' comes from the Greek word 'tele' which means distance and the Latin word 'mederi' meaning to cure or to heal. According to the World Health Organization (WHO), it can be described as "the delivery of health care services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment, and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities" [1]. One or more health professionals can get in touch with each other or the patient through telemedicine. This study of 'healing at a distance' [2] was primarily initiated to carry out the purpose of providing healthcare support only in some exigent areas like spacecraft, military services, etc. As per recorded history, the first exchange of medical information was performed in 1930 between Alaska and Australia [3]. With the advancement in information and communication technology (ICT), the scope and the propensity of employing telemedicine have become larger. Moreover, after the Covid-19 pandemic situation, telemedicine turns into an indispensable component of the present healthcare system. Electronic patient records (EPRs) can be transmitted over open network channels in a fast and lucrative way through modern digital ICT. Furthermore, the digital domain offers immense facilitiesfor data manipulation and data augmentation. Consequently, the EPRs could be distorted for being gone through several malicious signal processing attacks like modification, deletion, etc., along with attempts to possess unauthorized access. But, any slightest alteration in EPRs may lead to a false inference as these electronic reports play a central role in telediagnosis. Thus, providing authentication to the EPRs along with the corresponding medical images is of prime concern to the researchers. Tamper detection can be performed

[1,2] The authors are with Department of Electronics and Communication Engineering, RCC Institute of Information Technology, Beliaghata, Kolkata- 700015, India., E-mail: subhrajitkcs@gmail.com and idabhishek23@yahoo.com
[3] The author is with Institute of Radio Physics and Electronics, University of Calcutta, 92 Acharya Prafulla Chandra Road, Kolkata-700009, India., E-mail: avikjoy@yahoo.com

to resolve the problem regarding data authenticity by embedding some copyright information into the EPRs as well as the medical images. Digital watermarking is one of the most suitable and trendy practices to serve the purpose [4].

This paper deals with several digital image watermarking techniques, which can be utilized in secured and authenticated e-healthcare systems. The discussion commences with brief fundamentals on digital watermarking in the next section. Different aspects and applications of watermarking in medical imaging have been explored in the third section. A few of the most recent medical image watermarking techniques, along with a comparative result analysis, are discussed in the fourth and fifth sections, and finally, the discussion is concluded in section six.

2. DIGITAL WATERMARKING

Digital watermarking [5–7] is an art of information hiding, generally to embed some copyright information (known as a watermark) into any multimedia objects (known as cover) in such a way that the hidden data can be extracted from the cover objects without affecting either the watermarks or the covers.

2.1 Attacks on digital watermarking

It is not so easy to identify and classify all the attacks which may be appeared accidentally as well as intentionally during the transmission of data. However, the attacks, related to the domain of digital watermarking, may be sorted broadly into a few major groups [8].

A set of unintentional attacks like linear and nonlinear filtering, resampling, compression, quantization, analog-to-digital conversation and vice-versa, noise addition, etc. are Signal processing attacks, which may degrade the transmitted data quality.

The embedded information may be completely distorted due to some awful geometrical operations like scaling, rotation, translation, cropping, etc. as they intend to resynchronize the watermarked signal, as well as to reduce the channel capacity.

Cryptographic and removal attacks also aim to destroy or remove the hidden information so that the cover can be treated as a copyright-free or unauthentic object.

Apart from these, there are protocol attacks, IBM attacks [8], and some intentional or manual attacks those often cause to find out the flaws of a copyright generating system, as well as to make forgeries by generating fake originals.

2.2 Classifications of digital watermarking

Digital watermarking, i.e. the process of insertion and extraction of the watermark, can be carried out either in spatial [9-10] or in frequency / transform domain [11-13], although some hybrid logics [14-15] have also been developed to get a better result.

This information hiding scheme is applicable for all types of multimedia objects, and hence by the type of the cover object, watermarking can be classified as text [16], image [9-14], audio [17], and video [15]. As per the scope of this paper, image watermarking is the prime concern.

Based on the appearance of the watermark in the cover object, the process can be classified as noticeable or unnoticeable. For instance, an image watermarking technique can be categorized as visible [18] and imperceptible [19]. Dual watermarking techniques are also available and mostly found in the domain of medical image watermarking [20].

From another aspect, the watermarking process can be of three types – robust and fragile. Robustness against the attacks is essential for copyright or authentication [21]; whereas, fragile watermarks are useful for tamper detection [22-23]. Semi-fragile methods provide rigidity to some selective types of attacks only [24].

All types of the above-said watermarking methods can be source based (in identifying the ownership) or destination based (in case of tracing the buyer).

2.3 Applications of digital watermarking

Digital watermarking is applied mainly to serve the function of copyright protection for multimedia objects. A copyright-protected scheme is always reliable for data augmentation and transmission, which are very necessary to meet the increasing demands of subscribers. Other than that, watermarking is also useful in verifying data authenticity, content labeling, tamper detection, source tracking, etc. These facilities, provided by digital watermarking, are utilized in several commercial and non-commercial secured data-transferring and data-storing frameworks. For example, medical imaging, broadcast monitoring in radio or television, digital fingerprinting, digital library or e-resources, and many more digital data capturing, storing, and conveying systems [8, 25].

2.4 Basic features of digital watermarking

The prime objective of digital watermarking is to provide reliability and security to any digital signal without affecting that cover object. To play this role in the new-age digital domain for data transmission, the three major qualities [8], required for any watermarking system are robustness, imperceptibility, and payload or data-hiding capacity.

Robustness: The embedded information should be robust enough to sustain against the attacks, discussed earlier in this section. However, fragile watermarks are often more useful when the intention is to detect any type of tampering attempt.

Imperceptibility: It is more desirable that the embedded information, i.e. the watermark does not

cause any distortion to the cover object. Thus, it is a challenge for the researchers and developers to make the watermark unnoticeable to the human sensing systems.

Payload or hiding capacity: It is defined as the maximum amount of watermarking data that could be embedded into a cover with the assurance of exact recovery.

Except from these three foremost qualities, like any other system implantation, here it is also desired that the execution of the watermarking operation should be made as less complex as possible so that the computational cost becomes justified.

3. DATASETS FOR PREDICTION

Generally, medical image watermarking is referred to that particular branch of digital watermarking, where the cover is a medical image, i.e. the image watermarking process that aims to protect medical images. The roles of digital watermarking in medical images are as follows:

(i) Authentication: Digital watermarking suitable for validating the information within a medical image under diagnostic consideration.

(ii) Tamper detection: A fragile or semi-fragile watermark may be utilized for detecting the occurrence of any type of modification or misappropriation that may undermine the integrity of an image report.

(iii) Hiding information: An appropriate watermarking process can embed a large amount of datacontent covertly in a medical cover image with the high certainty of an exact retrieval.

(iv) Copyright protection: Medical images are to be copyright protected not only for the originators (i.e. the pathologies) but also for the doctors and the patient parties for any further requirements to the diagnostic centers.

Reducing storage and bandwidth: Lesser storage will be required for any medical image when the corresponding metadata, i.e. the patient's information and report details are watermarked within that particular image. Besides during transmission, bandwidth can also be reduced as there will be no need to send the metadata separately.

3.1 Quality requirement in medical image watermarking

Medical images are the primary diagnostic documents in the e-healthcare system. Thus, the digital watermarking techniques, employed in medical imaging, should be acquired with some specific qualities to get accomplished with the applicative demands in all aspects [26].

First and foremost, the embedded information must not cause any distortion in the region of interest (ROI) of the medical image, because, any slightest change in ROI may cause an erroneous diagnosis. Hence, any information, embedded into the ROI, must be unnoticeable, i.e., the watermarking process should offer high imperceptibility. It will be more useful if the embedding scheme is capable of distinguishing between ROI and region of noninterest (RONI) so that the watermark information can be kept within the RONI only.

Next, a medical watermarking system must possess enough robustness to protect the embedded diagnostic as well as to authenticate the information from attacks. At the same time, it is also required for the watermark to be sensitive to any kind of alteration in the original image.

The size of the content to be embedded as a watermark often becomes a matter of concern. Thus, another prime quality, required for medical image watermarking, is the ability to hide a large amount of data without affecting the ROI.

Now, robustness and sensitivity are in contrast by nature. Moreover, there are already tradeoffs among robustness, imperceptibility, and hiding capacity. Hence, it is a challenge for the researchers to establish such a watermarking scheme that is precise and justified in all aspects. To deal with this, a good number of medical image watermarking schemes have been developed till date. Some of these have been discussed in this work to depict the scope of digital watermarking in medical imaging.

3.2 Medical image watermarking methods

Image watermarking techniques have been improving day by day with the advancement of digital signal processing. Based on the purposes, the watermarks are made visible or invisible, and robust or fragile. Blind watermarking techniques [27-28], i.e. where the original image is not required in the extraction process, are preferable in the case of medical image watermarking. Similar to conventional digital watermarking techniques, all medical image watermarking methodologies are mainly classified into two parts – spatial domain techniques and transform domain-based techniques, although some hybrid methods are also available.

In the spatial domain, the cover image pixels are directly modified by the watermark information bits/pixels. Least significant bit (LSB) replacement, LSB matching, most significant bit (MSB) replacement, patchwork techniques, correlation-based data embedding, and spread spectrum techniques are some of the most conventional watermarking processes in this domain [20,29-31]. Generally, the lower bit planes of any image pixels are modified to provide high imperceptibility, whereas modifications in higher bit planes are useful in providing improved robustness. Consequently, the MSB modifications are often applied for embedding visible data to serve the purpose of content labeling, and the LSB planes may be used in keeping some fragile information to identify

whether any type of misappropriation has tampered-with the cover or not. However, in most of the recent schemes multiple watermarking or involvement of human visual system (HVS) [32-33], image clustering by means of ROI and RONI and other complementary operations are often found; because the conventional fundamental data hiding techniques are unable to prevail over the incessantly adapted malicious attacks.

The transform domain is preferred more when the prime objective is to provide robustness and security to the image under consideration. Thesetypes of practices are carried on after transforming the input image signals through some apposite signal processing operations like discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), etc. [34-38]. Here, the watermark and the EPR information are embedded by modifying the suitable frequency components of the transformed cover image and after that, corresponding inverse transform(s) is (are) applied to the modified signal to restore the image into the spatial domain. Often modified and/or multiple transformations, singular value decomposition (SVD) are performed to execute hybrid watermarking techniques [39-42]. The concept of region segmentation can be utilized in the frequency domain too [43-44].

The use of biometric images, error-correcting codes, machine learning, and intelligent techniques are also found in some recent works to enhance system efficiency [45-48].

4. RECENT WORKS ON MEDICAL IMAGE WATERMARKING

During the last decade, different advancements have been noticed in the field of medical image watermarking. In 2010, Mustafa *et al.* [28] proposed a packet wavelet transform-based medical watermarking technique to embed EPR data, being encoded through Bose-Chowdhur-Hocquenghem (BCH) code, into the medical images. The average PSNR was found as 39 dB for that scheme. Spread-spectrum-based medical image watermarking was proposed by Kumar *et al.* [49] in 2011. Here, a pair of pseudo-random noise sequences were utilized in embedding and extracting the doctor's signature. This was a robust but non-blind technique. Another spread-spectrum-based technique was introduced by Nakhaie and Shokouhi [50], where the medical image is first segmented into ROI and RONI, and then the watermark information is embedded into the RONI components. This was a frequency domain-based no-reference watermarking process. A lot of medical image watermarking works have been published since 2012.Wavelet-based multiple watermarking technique was proposed for medical images by Pal *et al.* [51] that achieved PSNR upto 41dB. Imperceptibility was improved upto 50dB PSNR by Kannammal *et al.* [52] using the wavelet-based double watermarking technique. DWT was used along with DCT in the hybrid watermarking technique [53], proposed by Umaamaheshvari and Thanushkodi, and PSNR was increased to 57 dB. Robustness was improved by introducing swarm intelligence with an adaptive watermarking technique, developed by Soliman *et al.* [54]. Independent component analysis was performed with DWT by Mangaiyarkarasi and Arulselvi [55]. Wioletta [56] introduced biometric watermarking through Iris code with DWT to improve robustness against different signal processing attacks. Hajjaji *et al.* [57] enhanced imperceptibility to obtain PSNR as high as 57 dB by combining Karhunen Loeve transform with Haar-based DWT. Region-based watermarking with immense hiding capacity was executed through DWT-SVD by Al-Haj and Amer [58]. DWT-SVD combination was also utilized by Gao *et al.* [59], where the cover image itself was considered as the watermark. It provides robustness against geometrical attacks without affecting visual transparency. Zear *et al.* [39] proposed a multiple image watermarking technique that utilized DWT, DCT, SVD, and Hamming error correction code to improve robustness. Image segmentation was also performed to obtain better visual transparency. A.K. Singh [40] attempted to overcome the conflict between robustness and imperceptibility by embedding an encrypted watermark. Here also, DWT, DCT, and SVD were utilized together. Badshah *et al.* [60] implied Lempel-Ziv-Welch lossless image compression in medical image watermarking to obtain better results. Support vector machine-based secured medical image watermarking was proposed by Rai and Singh [61]. DCT-based watermarking was developed by Parah *et al.* [62]. DWT and Schur decomposition-based model was utilized in medical image watermarking by K. Swaraja [63]. Apart from these, there are so many medical image watermarking techniques, developed within the last few decades. However, in this section, a few of the most recent medical image watermarking techniques have been discussed in brief.

This discussion leads to understanding the recent trends and applications of digital image watermarking in the field of medical imaging.

4.1 Transform domain-based techniques:

A.K. Singh introduced an error control code to develop a dual watermarking scheme for color medical images in the lifting wavelet transform (LWT) domain using DCT [48]. A secret signature watermark along with the EPR has been kept hidden in the medical cover image to provide enhanced security and reliability to the cover. Before embedding, the watermark and the EPR are encrypted and encoded, respectively, using message-digest (MD5) and BCHerror control code. The cover image has been represented first in YIQ color space and the Y compo-

nent has been decomposed using DWT upto the 3rd level. Then the LH3 and HL3 sub-bands have been transformed using DCT, and finally, into these coefficients, the hiding data have been embedded. The inverse transforms, i.e. IDCT and inverse LWT have been performed to get the YIQ components of the watermarked image, and the final watermarked medical image has been transmitted after being converted into RGB format.

Another dual watermarking scheme for medical images was proposed by H.S. Alshanbari [64]. Here also a robust and a fragile watermark have been used to serve the function of providing ownership information and tamper detection, respectively. According to this proposed algorithm, first, the medical image is considered as a combination of ROI and RONI. The robust watermark (i.e. the ownership information) is embedded in both the ROI and RONI so that the authenticity can be verified from every part of the cover image. To perform the insertion operation of the robust information, first, the 3-level DWT and 1-level DWT are applied, respectively, to the cover image and the watermark image to decompose the images into sub-bands. Then principal components of the cover and watermark were estimated by performing singular value decomposition (SVD), respectively, on the LL3 band of the cover and the LL1 band of the robust watermark. Finally, this embedding process is carried out by modifying the singular values of the cover image through a scaling function and the principal components of the watermark information as obtained before. An inverse SVD and an inverse DWT have been applied consecutively to the modified cover components to restore the watermarked image into the spatial domain. After embedding the ownership information, a robust mark has been generated by compressing the ROI with the Lempel-Ziv-Welch algorithm [64] and then, combining it with a signature information. The signature information has been generated through the hashing algorithm SHA-256 [65]. This way, the robust watermark is formed and inserted into the RONI of the cover image, which is already being modified with the ownership information.

Balasamy and Suganyadevi put a medical image watermarking approach [66] using fuzzy-based ROI selection where the embedding process is performed through DWT and SVD. Here, fuzzification is performed through a hybrid function [66], developed on the basis of the Fuzzy C-means image clustering algorithm [67], to segment the cover image into ROI and RONI. After identifying the ROI, 2-level DWT has been applied to the segmented ROI, followed by SVD operation to the HH2 band. Parallel to this, the watermark has also been transformed using 2-level DWT. A logistic map [66] has been used to encrypt the watermark image and the SVD has been applied to the encrypted HH2 sub-band watermark to generate the key components. These key components are estimated to avoid false positive errors during transmission. The singular values of both the cover and watermark image have been modified using the key components to generate the watermarked components. Then after applying inverse DWT and combining the ROI and RONI, finally the secured medical image information has been made robust against various signal-processing attacks.

A robust watermarking scheme for medical images has been developed in the transform domain by Khare and Srivastava [68].Here to provide enhanced security on the integrity of the cover, homomorphic transform, redundant DWT, and SVD have been utilized together. The purpose of homomorphic transform is to recognize the illumination as well as the reflecting components within the cover. For being inconsistent, the reflecting components are considered suitable for hiding data imperceptibly. In the following steps, the cover image components are divided into different sub-bands through random DWT, and then the singular values are computed for the LH sub-band components corresponding to the reflecting regions through SVD. Same way, redundant DWT and SVD are also applied to find the singular values of the medical watermark components corresponding to the LH sub-band. Watermark embedding is performed by modifying the singular values of the cover with that of the watermark image components using a specific scaling factor. To restore the watermarked image in the spatial domain, the inverses of the respective transforms are applied chronologically, and finally, this medical data is transmitted after being encrypted through 2-D chaotic Arnold transform along with a secret key. For utilizing the said signal transforms, this process offers improved robustness.

Thanki and Kothari [69] show that multilevel security can be achieved for a medical image by embedding a double-sized watermark into it. This is a transform domain-based approach where, finite ridgelet transform (FRT), SVD, and Arnold scrambling have been utilized, respectively, to improve payload, robustness against several attacks like – compression, the addition of noise, filtering, etc., and better security. Here, the secret identifying information of the patient is considered as the watermark, which is to be embedded into the medical image (cover). The cover image was first decomposed into double of its size by applying a hybridization of FRT and SVD. It is because, for any image of size M×N, its corresponding FRT coefficients are obtained in the order of 2M×2N. Parallel to the transformation of the cover image, SVD is applied to the watermark image also, and these singular values of the watermark are embedded into the hybridized transform coefficients of the cover image through an additive operation. Then, the watermarked image is obtained after applying inverse SVD and inverse FRT, consecutively. Finally,

this watermarked image is encrypted using Arnold scrambling, to provide additional protection to the image during transmission over an open communication channel.

In another hybrid watermarking technique, suggested by Swaraja *et al.* [70], DWT, and Schur transform have been employed with Lempel-Ziv-Welch (LZW) lossless data composition algorithm and particle swarm bacterial for-aging optimization (PSBFO) algorithm. Here, the nature of HVS is utilized with computing the edge entropy to determine a more suitable region to make the embedded information discernible. A grayscale 160×240 EPR image, together with a 128×128 color image obtained from the cover ROI is considered as a watermark.LZW is applied to compress the pair of watermarks to improve the payload. RGB cover image is converted to YCbCr form to utilize the Y or luminance components for data insertion, as these are less sensitive to modifications with respect to chrominance (Cb and Cr) components. ROI is kept unchanged so that no ambiguity occurs in diagnosis. 2-level DWT with Schur transform is applied to the RONI portion, and a few suitable non-overlapping blocks in LH2 and HL2 subbands are chosen for data embedding according to visual and edge entropy. In this process, PSBFO plays a central role in optimizing the trade-off between imperceptibility and robustness.

DWT is utilized also in another robust and blind medical image watermarking technique, proposed by Kahlessenane *et al.* [71]. In this approach, the watermark is generated first. The patient's information consists of name, sex, age, and date of birth, along with the date and the time of capturing that particular cover image (i.e. the medical image report) form the watermark as a binary sequence. A fingerprint is generated by performing a hash function through the MD5 algorithm [72] and added to the binary sequence of information to ensure integrity. The embedding process is then initiated to implant this watermark information into the cover image. To generate the watermarked image, the cover image is modified by inserting the computed watermark information into the low-frequency components, containing maximum energy. Based on Haar filtering, DWT is applied here to transform and decompose the cover image into the four different frequency sub-bands. A topological recognition is performed for the LL subband components through the Zig-Zag method to enrich imperceptibility with high robustness, as well as to ensure more effective entropy coding [73]. Finally, the watermarked components are modified by substituting (rather than adding) the watermark components considering some specific conditions proposed for two variants [71].

Kahlessenane *et al.* [74] attempted to find the efficiency of frequency domain watermarking with four different transforms – DCT, DWT, non-subsampled shearlet transform (NSST), and non-subsampled contourlet transform (NSCT). In this proposed method, the cover, i.e. the medical image is watermarked with the image acquisition data together with patient records. Schur decomposition is combined with the transformations every time to decompose the image components into different sub-bands, and the medium band (LH and HL sub-bands in case of DWT) frequency components are selected for embedding watermark data. This allows prevailing over the discrepancy between robustness and imperceptibility. Low-frequency components are chosen for NSST based data embedding approach.

A novel watermarking technique was introduced by Ravichandran, *et al.* [33] to offer authentication, consistency, and any type of tamper detection in medical reports. Integer wavelet transform, combined chaotic map, retrieval bit generation, and SHA-256 cryptographic hash function are introduced to meet the goal of this scheme. Here also, the cover image is segmented into ROI and RONI, which are used to embed watermarks assuring data authentication and watermarks providing integrity control, respectively. RONI components related to the LH and HL sub-bands are used in embedding the robust mark information. Authors also claimed that for having less execution time, the approach is supposed to be less complex and suitable for FPGA-based realization.

Recently, Singh *et al.* [75] proposed a region-based hybrid medical image watermarking scheme for robust and secured transmission in the internet of medical things (IoMT). The medical image is partitioned into ROI and RONI. Tamper detection and recovery bits are inserted into the ROI of the cover image. The ROI is watermarked using adaptive LSB substitution. EPR data is compressed using Huffman coding and encrypted using a secret key. QR code of the hospital logo, encrypted EPR, and ROI recovery bits are embedded into RONI using DWT-SVD hybrid transform. The scheme intends to maintain the visual quality of the medical image, robustness of the authentication mark, scope for tamper detection, and security. However, the scaling factor can be optimized.

4.2 Spatial domain-based techniques:

Sinha Roy *et al.* [20] executeda spatial domain-based medical image authentication technique for an automated diabetic retinopathy (DR) test report. The overall process has two wings. In the first section, the retinal area is detected as ROI from the fundus image, and regions of hard exudates are identified, through which the corresponding DR report is generated.Then in the second phase, the authenticity of that report image is put on through a dual watermarking process. A fragile binary watermark is taken to serve the purpose of tamper detection.And a visible robust watermark is implanted into the outside of the

retinal area (i.e. RONI) and made visible for authentication as well as content labeling. The whole process is performed in the spatial domain. This scheme has been experienced with some signal processing attacks to establish the affirmation on the robustness of the visible mark. The fragile watermark is embedded. The invisible watermark is embedded invisibly into some selected blue plane components of the cover image through LSB replacement. It has been shown experimentally that for any kind of further modification in ROI, the authentication mark cannot be recovered.

Konyar and Ozturk [76] have proposed an ECC-based watermarking, where an extra level of security is provided to the watermark by encrypting it through Reed-Solomon (R-S) code before embedding. Initially, an array is formed based on the intensity values of the watermark pixels. Each of the elements in the array is adapted to an 8-bit format. These message bit sequences in the array are then grouped into a few m-bit symbols and substituted by their corresponding decimal values to meet the R-S (n, k) coding criteria. The codeword is achieved from the information polynomial (obtained from the symbol sequences) and the generator polynomial. The encoding is practiced over the Galois field (2^m).The codeword is then embedded into the cover image by modifying the LSB planes of the pixels' luminance values.

Another spatial domain-based reversible watermarking scheme for medical images was proposed by Manikandan and Masilamani [77]. In this approach, the EPR and an authentication code together act as the watermark, to be embedded into the original gray-scale medical images. Considering the size of the image to be watermarked as M×M, an adaptive authentication code sequence of length M^2 is generated from the MSB planes of that particular image using an authentication code generating key and an encryption key. This unique authentication sequence, along with the EPR, forms the watermark. This watermark has been embedded into the gray-scale image through an image scaling-up process and the corresponding watermarked image of size 2M×2M is produced. Hence, it is clear that the intensity values of $3M^2$ number pixels in the output image of this proposed embedding scheme are needed to be approximated based on the original pixel intensities. A set of prescribed rules are then followed to embed the watermark while computing the missing pixel values in the scaled-up output image through adaptive replication of the neighboring pixel intensity values. The experimental analysis of this process has been carried out using a standard dataset of medical images, and the results claim that this novel work is useful to enhance the authenticity of EPRs as well as medical images and can be utilized in automated e-healthcare systems. However, for transmitting these scaled-up images, more channel capacity is required than the conventional watermarked images.

Aiming to the protection of medical image contents along with the watermark, a spatial domain approach was presented by Nagm and Elwan [78]. Here, an encrypted watermark has been synthesized with one of the components of a color medical image, instead of performing conventional watermark embedding. The encryption is carried out to enhance security for the watermark, which is generated by combining different patient-related information (like name, id, etc.) through the dynamic keys, obtained using the SHA-1 algorithm. On the other hand, the color components of the cover image are separated and resized to be apposite for the encoding process. The red and blue planes are considered here as the modified and the pre-modifier components, respectively. This pre-modifier plane is modified with the pre-generated watermark by the AES-128 encryption algorithm. Finally, a bit substitution, performed between the modified and the modifier components in the lower bit planes of every pixel, along with the original green and blue plane components, provides the ultimate watermarked image. This proposed algorithm has been evaluated using the first three bit-planes (starting from LSB) separately, and the experimental results reveal that the 2nd bit-plane is the most suitable for this approach as it offers high visual transparency with improved robustness against some active attacks. In this way, this method, unlike the conventional spatial domain medical image watermarking schemes, shows how the watermark, i.e. the patient information, can be distributed into every pixel irrespective of ROI and RONI to provide high-scale integrity protection without affecting the image quality.

Schur decomposition has been applied with chaotic sequence to embed an encrypted watermark into medical images by Soualmi *et al.* [79]. The watermark is XORed with a binary chaotic sequence to generate the encrypted watermark. Parallel to that the cover is divided into 2×2 non-overlapping sub-blocks, and encrypted through another chaotic sequence, decomposed up into non-overlapping blocks of the same size. Then the encrypted medical image is watermarked with the encrypted watermark by embedding each of the watermark bits to distinct cover image blocks of which weight meet certain criteria. Watermark can be extracted and decrypted through a relative and reverse process using the same chaotic sequences. This is a blind technique as the original cover is not required to retrieve the hidden information.

Apart from these, there are so many watermarking methodologies have already been proposed, and researchers are endowing efforts in developing better methods to provide more security, reliability, and privacy to medical images.

Table 1: *Mathematical expression for the mentioned image quality metrics considering O and E, respectively, as the original and erroneous image signals of size M×N.*

Image Quality Metrics	Mathematical Expressions	Values for two identical images
Peak Signal to Noise Raito (dB)	$\text{PSNR} = 10\log_{10}\frac{MN\times[\max(O(m,n))]^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}[O(m,n)-E(m,n)]^2}$	∞
Normalized Cross-Correlation	$\text{NC} = \frac{\sum_{m,n}(O(m,n)E(m,n))}{\sum_{m,n}(O(m,n))^2}$	1
Structural Similarity Index Measurement	$\text{SSIM} = \frac{(2\mu_I\mu_j)(2\sigma_{IJ}+C_2)}{(\mu_I^2+\mu_J^2+C_1)(\sigma_I^2+\sigma_J^2+C_{12})}$ where μ_I&μ_J are the mean intensity σ_I&σ_J are the standard deviation of the original and distorted image respectively C_1&C_2 are constants σ_{IJ} is the covariance of both the images	1
Bit Error Rate (only for binary images)	$\text{BER} = \frac{\sum_{m,n}\lvert(O(m,n)-E(m,n))\rvert}{M\times N}$	0

Table 2: *Comparison of aforesaid state-of-the-art medical image watermarking techniques.*

Method	Domain (with Type)	Type and Size of Cover Image	Type and Size of Watermark	Payload (bits/ pixel)	Remarks on imperceptibility	Remarks on robustness
Singh, 2019 [48]	Transform (Robust)	Color Image (512×512)	Gray Image(64×64), and text watermark of 80 characters	0.0425	PSNR = 30.42 dB NC = 0.9757	Moderate
Swaraja *et al.*, 2020 [70]	Transform (Robust)	Color Image (1024×1024)	Gray Image (160×240) Color Image (128×128)	0.668	PSNR = 35.84 dB	High
Konyar and Ozturk, 2020 [76]	Spatial (Semi-fragile)	Gray Image (480×480)	Gray Images with different resolutions	0.79	PSNR = 41.85 dB, SSIM = 0.9335 (for 0.79 bpp) PSNR = 46.26 dB, SSIM = 0.9858 (for 0.33 bpp)	Robust to salt and pepper
Thanki and Kothari, 2020 [69]	Transform (Robust)	Gray Image (128×128)	Binary Images (256×256)	2	PSNR = 47.6473 dB, NC = 0.9176 (for binary logo) PSNR = 44.0248 dB, NC = 0.91176 (for sample patient information)	High
Alshanbari , 2020 [64]	Transform (Dual)	Gray Image (480×680)	Gray Image (60×60)	0.088	PSNR = 48.67 dB (after robust watermarking) PSNR = 48.14 dB (after Dual watermarking)	Moderate
Balasamy and Suganyadevi, 2020 [66]	Transform (Robust)	Gray Image (512×512)	Gray Image (64×64)	0.125	PSNR = 54.26 dB	Moderate, better with Fuzzy logic
Khare and Srivastava, 2020 [68]	Transform (Robust)	Gray Image (512×512)	Gray Image (128×128)	0.5	PSNR = 57.29 dB SSIM = 0.9995 NC= 0.9997	High
Sinha Roy *et al.*, 2020 [20]	Spatial (Dual)	Color Image (536×356)	Visible: 4221 bits Invisible: 4096 bits	0.044	PSNR = 60 dB SSIM = 0.9998	Moderate
Manikandan and Masilamani, 2020 [77]	Spatial (Robust)	Image having $4M^2$ number of pixels	Image having $3M^2$ number of bits	0.75	PSNR = ∞ SSIM = 1	Poor

Table 2 cont.: *Comparison of aforesaid state-of-the-art medical image watermarking techniques.*

Method	Domain (with Type)	Type and Size of Cover Image	Type and Size of Watermark	Payload (bits/ pixel)	Remarks on imperceptibility	Remarks on robustness
Ravichandran *et al.*, 2021 [33]	Transform (Robust)	Gray Image (256×256)	Approx. 146800 bits including text and binary images	2.24	PSNR = 48.81 dB NC = 0.9999 SSIM = 0.9944	Poor
Nagm and Elwan, 2021 [78]	Spatial (Robust)	Color Image (512×512)	Binary Image (512×512)	0.33	PSNR = 55.41 dB, SSIM = 0.9995 (for LSB approach) PSNR = 49.9081dB, SSIM = 0.9985(for Bit2SB approach) PSNR = 43.8138dB, SSIM = 0.9908 (for Bit3SB approach)	Robust to intentional attacks
Kahlessenane *et al.*, 2021 [71]	Transform (Robust)	Gray Image (512×512)	43,690 bits for Variant 1 32,768 bits for Variant 2	0.167 (Variant 1) 0.125 (Variant 2)	PSNR = 74.47 dB, SSIM = 1 (for variant 1) PSNR = 74.16 dB, SSIM = 1 (for variant 2)	High
Kahlessenane *et al.*, 2021 [74]	Transform (Robust)	Gray Image (1024×1024)	Binary Image (1024×1024)	1	PSNR = 42.85 dB, SSIM = 0.9998, NC = 0.9923 (for NSST–Schur method) PSNR = 44.98 dB, SSIM = 0.9998, NC = 0.9947 (for NSCT–Schur method) PSNR = 49.20 dB, SSIM = 0.9998, NC = 0.9995 (for DWT–Schur method) PSNR = 47.98 dB, SSIM = 0.9997, NC = 0.9989 (for DCT–Schur method)	High
Singh *et al.*, 2022 [75]	Transform (Dual)	Gray / Color Image (512×512)	Binary EPR (64×64) Binary hospital logo (64×64)	0.03125 (gray image) 0.01042 (color image)	PSNR = 45.95 dB, SSIM = 0.9195 (for gray image) PSNR = 47.42 dB, SSIM = 0.9505 (for color image)	High
Soualmi *et al.*, 2022 [79]	Spatial (Semi-fragile)	Gray Image (256×256)	Binary Image (128×128)	0.25	PSNR = 66.84 dB SSIM = 0.94	Robust to image compression

Table 3: *Detailed study on robustness of the aforesaid state-of-the-art medical image watermarking techniques against different geometrical, noise and compression attacks.*

Method	Scaling Attack	Salt & Pepper Attack	Gaussian Noise	Histogram	JPEG Compression Attack
Singh, 2019 [48]	BER= 0 NC=0.8491	BER=0 NC=0.8077	BER=0 NC=0.8984	BER=24 NC=0.5882	BER=0 NC=0.9837
Swaraja *et al.*, 2020 [70]	PSNR = 34.34 dB NC = 0.96	PSNR = 33.87 dB NC = 0.98	PSNR = 33.25 dB NC = 1	PSNR = 35.68 dB NC = 0.94	PSNR = 35.23 dB NC= 0.99
Thanki and Kothari, 2020 [69]	NC = 0.9564 (For Binary Logo) NC = 0.9415 (For Sample Patient Information)	NC=0.9940 (For Binary Logo) NC= 0.9480 (For Sample Patient Information)	NC = 0.9694(For Binary Logo) NC = 1.0000 (For Sample Patient Information)	-	NC=0.9859(For Binary Logo) NC=0.9988(For Sample Patient Information)
Alshanbari, 2020 [64]	NC=0.8352 [for (0.5,2)] NC=0.8662 [for (2,0.5)]	-	-	-	NC=0.8341 (with QF=90) NC=0.7354 (with QF=70) NC=0.7226 (with QF=50)
Balasamy and Suganyadevi, 2020 [66]	-	NC=0.89(Without Fuzzy logic) NC=0.924 (With Fuzzy logic)	NC=0.991 (Without Fuzzy logic) NC=0.997(With Fuzzy logic)	NC=0.937(Without Fuzzy logic) NC=0.956(With Fuzzy logic)	-

Table 3 cont.: *Detailed study on robustness of the aforesaid state-of-the-art medical image watermarking techniques against different geometrical, noise and compression attacks.*

Method	**Scaling Attack**	**Salt & Pepper Attack**	**Gaussian Noise**	**Histogram**	**JPEG Compression Attack**
Khare and Srivastava, 2020 [68]	NC=0.9991 SSIM= PSNR=48.7725 dB	NC=0.9998 SSIM=0.9782 PSNR=42.3179dB	NC=0.9988 SSIM=0.8470 PSNR=35.3514 dB	NC=0.9979 SSIM=0.7422 PSNR=16.7729 dB	NC=0.9997 SSIM=0.9886 PSNR=45.6184 dB (QF=90)
Sinha Roy *et al.*, 2020 [20]	SSIM=0.8013 PSNR=15.6dB	-	SSIM=0.5178 PSNR=12.72 dB	-	SSIM=0.8366 PSNR=22.2 dB
Manikandan and Masilamani, 2020 [77]	-	BER=0.036	-	BER=0.094 PSNR=14.264 dB) SSIM=0.607	-
Kahlessenane *et al.*, 2021 [71]	NC=0.91135	NC=0.9678	NC=0.9614	NC=0.9736	NC=0.9205
Kahlessenane *et al.*, 2021 [74]	NC=0.7475 (For DWT) NC=0.7793 (For DCT) NC=0.8917 (For NSST) NC=0.8122 (For NSCT)	NC=0.8936 (For DWT) NC =0.9141 (For DCT) NC=0.9294 (For NSST) NC=0.8741 (For NSCT)	NC=0.9733 (For DWT) NC=0.9412 (For DCT) NC=0.9922 (For NSST) NC=0.9914 (For NSCT)	NC= 0.8555(For DWT) NC= 0.8607(For DCT) NC= 0.9274 (For NSST) NC= 0.8607 (For NSCT)	NC=0.9617 (For DWT) NC=0.9854 (For DCT) NC=0.9699 (For NSST) NC=0.9430 (For NSCT)
Singh *et al.*, 2022 [75]	BER= 0.02 NC= 0.8315	BER= 0.016 NC= 0.8538	-	BER= 0.016 NC= 0.8871	BER= 0.015 NC= 0.99
Soualmi *et al.*, 2022 [79]	BER = 0.57 NC = 0.53	BER = 0.005 NC = 0.97	BER = 0.49 NC = 0.48	BER = 0.500 NC = 0.500	BER = 0.008 NC = 0.865

Table 4: *Detailed study on the robustness of the aforesaid state-of-the-art medical image watermarking techniques against different image filtering attacks.*

Method	**Median Filtering Attack**	**Sharpening Attack**	**Low Pass Filtering**	**Average Filtering**
Singh, 2019 [48]	-	-	BER=0 NC=0.9546	-
Swaraja *et al.*, 2020 [70]	-	-	-	-
Thanki and Kothari, 2020 [69]	NC =1.0000 (For Binary Logo) NC = 0.9564 (For Sample Patient Information)	NC =1.0000(For Binary Logo) NC = 0.9516 (For Sample Patient Information)	NC=0.9501(For Binary Logo) NC= 0.8704 (For Sample Patient Information)	-
Alshanbari, 2020 [64]	NC=0.79195	NC=0.7627	NC=0.77823	NC=0.7023
Balasamy and Suganyadevi, 2020 [66]	- NC= 0.53	NC = 0.972 (Without Fuzzy logic) NC=0.989 (With Fuzzy logic)	NC=0.901(Without Fuzzy logic) NC=0.954(With Fuzzy logic)	- NC = 0.530
Khare and Srivastava, 2020 [68]	NC=0.9984 SSIM=0.9788 PSNR=38.8434 dB	NC=0.9998 SSIM=0.9967 PSNR=46.1375 dB	NC=0.9986 SSIM=0.9968 PSNR=46.4164 dB	-
Sinha Roy *et al.*, 2020 [20]	SSIM=0.9234 PSNR=18.5 dB	-	SSIM=0.9587 PSNR=21.3 dB	-
Manikandan and Masilamani, 2020 [77]	BER = 0.417 PSNR =37.194 dB SSIM=0.983	BER = 0.336	BER=0.236 PSNR=39.840 dB SSIM=0.994	BER=0.472 PSNR= 29.084 dB SSIM= 0.948

Table 4 cont.: *Detailed study on the robustness of the aforesaid state-of-the-art medical image watermarking techniques against different image filtering attacks.*

Method	Median Filtering Attack	Sharpening Attack	Low Pass Filtering	Average Filtering
Kahlessenane *et al.*, 2021 [71]	-	NC=0.9878	-	NC=0.9623
Kahlessenane *et al.*, 2021 [74]	-	NC=0.7173 (For DWT) NC=0.7693 (For DCT) NC=0.8784 (For NSST) NC=0.7644 (For NSCT)	-	NC=0.9567 (For DWT) NC=0.8854 (For DCT) NC=0.9574 (For NSST) NC=0.9179 (For NSCT)
Singh *et al.*, 2022 [75]	BER= 0.03 NC= 0.8874	BER=0.11 NC= 0.9741	BER= 0 NC= 0.9999	-
Soualmi *et al.*, 2022 [79]	BER= 0.48 NC= 0.53	-	-	BER = 0.490 NC = 0.530

5. PERFORMANCE ANALYSIS FOR THE AFORESAID METHODS

It is already mentioned earlier in this paper that imperceptibility, robustness, and payload are the three major parameters, considered in measuring the qualities of any image watermarking scheme. A good number of image quality metrics [80-81] are available for the quantitative evaluation of imperceptibility and robustness. Among these, peak signal-to-noise ratio (PSNR), normalized cross-correlation (NC), structural similarity index measures (SSIM), and bit error rate (BER) (used in the case of binary images/watermarks only) are some of the most commonly used metrics. The mathematical expressions for these aforementioned metrics are given in Table 1.

Considering the watermarked image as the noisy image, imperceptibility is computed by means of quality metrics with respect to the original cover images. Imperceptibility, offered by different schemes discussed in the previous section, is compared in Table 2.

In the time of assessment of robustness, the original watermark and the extracted watermark from the received image are considered as the original and noisy image, respectively. A number of test attacks are deliberately applied to the watermarked images before extraction of the watermark to verify how robust the hidden information is against the implicated attacks. A comparative study on the robustness of the watermarking schemes, considered in this survey, is performed in Table 3 and Table 4.

Payload is measured as the ratio of the total number of embedded bits to the total number of cover image pixels.

6. CONCLUSIONS

In this paper, the distinct features of digital image watermarking have been recalled to show how these can be utilized in providing security and reliability to the medical images and corresponding EPRs. A good number of different existing state-of-the-art medical image watermarking technologies have been discussed in detail to understand the recent trends of work in this domain. A comparative study of these methodologies shows how the three major qualities (imperceptibility, robustness, and payload) are optimized according to the purposes. This discussion also spans over introducing several hybrid models to offer enhanced privacy to the EPRs during transmission on open communication channels. The basic requirements and processes regarding medical image watermarking are briefed here with some recent works in such a way that the scopes for further research or development could be derived from it.

References

[1] WHO, *A health telematics policy in support of WHO's Health-For-All strategy for global health development: report of the WHO group consultation on health telematics*, 11–16 December, Geneva, 1997. Geneva, World Health Organization, 1998.

[2] E. M. Strehle and N. Shabde, "One hundred years of telemedicine: does this new technology have a place in paediatrics?," Archives of Disease in Childhood, Vol. 91, no. 12, pp. 956–959, 2006.

[3] M. Z. Karen, "Telemedicine: History, Applications, and Impact on Librarianship," US National Library of Medicine National Institutes of Health, 1996.

[4] A. Anand, A. K. Singh, "Watermarking techniques for medical data authentication: a survey," *Multimedia Tools and Applications*, vol. 80, pp. 30165–30197, 2021.

[5] S. Bhattacharya, "Survey on digital watermarking – a digital forensics and security application," *International Journal of Advanced Re-*

search in Computer Science and Software Engineering, vol. 4, no. 11, pp. 1–7, 2014.

[6] S. Borra, R. Thanki, and N. Dey, "Digital Image Watermarking: Theoretical and Computational Advances," *CRC Press*, 2018.

[7] S. Sinha Roy, A. Basu, and A. Chattopadhyay, "Intelligent Image Watermarking for Copyright Protection," *Intelligent Multi-modal Data Processing*, pp. 69–96, 2021.

[8] S. Sinha Roy, A. Basu and A. Chattopadhyay, *Intelligent Copyright Protection for Images*, 1st Ed., New York, USA, CRC, Taylor and Francis, 2019.

[9] S. Sinha Roy, A. Basu, A. Chattopadhyay, *et al.*, "Hardware execution of a saliency map based digital image watermarking framework," *Multimedia Tools and Applications*, vol. 80, pp. 27245–27258, 2021.

[10] S. Kumar and B. K. Singh, "Entropy based spatial domain image watermarking and its performance analysis," *Multimedia Tools and Applications*, vol. 80, pp. 9315–9331, 2021.

[11] B. Ram, "Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform," *International Journal of Advancements in Research and Technology*, vol. 2, no. 4, 2013.

[12] W. Xiang–yang, L. Yu–nan, L. Shuo, *et al.*, "A new robust digital watermarking using local polar harmonic transform," *Journal of Computers and Electrical Engineering*, vol. 46, pp. 403–418, 2015.

[13] K. Fares, K. Amine and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik*, vol. 208, no. 164562, 2020.

[14] A. Susanto, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hybrid Method using HWT-DCT for Image Watermarking," *International Conference on Information Technology for Cyber and IT Service Management (CITSM)*, Denpasar, 2017.

[15] J. Sang, Q. Liu and C-L. Song, "Robust video watermarking using a hybrid DCT-DWT approach," *Journal of Electronic Science and Technology*, vol. 18, no. 2, 100052, 2020.

[16] N. S. Kamaruddin, A. Kamsin, L. Y. Por and H. Rahman, "A Review of Text Watermarking: Theory, Methods, and Applications," *IEEE Access*, vol. 6, pp. 8011-8028, 2018.

[17] G. Hua, J. Huang and Y. Q. Shi, "Twenty years of digital audio watermarking – a comprehensive review," *Signal Processing*, vol. 128, no. 222–242, 2016.

[18] S. -k. Yip, O. C. Au, C. -w. Ho and H. -m. Wong, "Lossless Visible Watermarking," *2006 IEEE International Conference on Multimedia and Expo*, Toronto, ON, Canada, pp. 853-856, 2006

[19] T. J. Anumol, V. A. Binson, and S. Rasheed, "FPGA Implementation of Low Power, High Speed, Area Efficient Invisible Image Watermarking Algorithm for Images," *International Journal of Structural Engineering(IJSE)*, vol. 4, no. 8, 2013.

[20] S. Sinha Roy, A. Basu and A. Chattopadhyay, "Secured Diabetic Retinopathy Detection through Hard Exudates," in *Proc. Research and Applications in Artificial Intelligence. Advances in Intelligent Systems and Computing*, Springer, Singapore, vol. 1355, 2021.

[21] V. S. Verma and R. K. Jha, "An Overview of Robust Digital Image Watermarking," *IETE Technical Review*, vol.32, no. 6, pp. 479-496, 2015.

[22] Z. Wujie, Y. Lu, W. Zhongpeng, *et al.*, "Binocular visual characteristics based fragile watermarking scheme for tamper detection in stereoscopic images," *International Journal of Electronics and Communications*, vol. 70, no. 1, pp. 77–84, 2016.

[23] Z. Zhang, H. Yao, Z.Xiang, and Fang Cao, "Self-Embedding Watermarking Algorithm Under High Tampering Rates," *IETE Technical Review*, vol. 38, no. 1, pp. 17-25, 2021.

[24] X. Yu, C. Wang and X. Zhou, "Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images," *Future Internet*, vol. 9(4), no. 56, 2017.

[25] A. Rashid, "Digital Watermarking Applications and Techniques: A Brief Review," *International Journal of Computer Applications Technology and Research*, Vol. 5, no. 3, pp. 147-150, 2016.

[26] A. K. Singh, B. Kumar, G. Singh and A. Mohan, "Medical image watermarking techniques: a technical survey and potential challenges," *Medical image watermarking*, Springer, Cham, pp. 13–41, 2017.

[27] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3669–3697, 2017.

[28] S. A. K. Mostafa, N. El-sheimy, A. S. Tolba, *et al.*, "Wavelet packets based blind watermarking for medical image management," *Open Biomedical Engineering Journal*, vol. 4, pp. 93–98, 2010.

[29] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285–287, 2006.

[30] H. Xu, J. Wanga and H. J. Kim, "Near–Optimal Solution to Pair Wise LSB Matching Via an Immune Programming Strategy," *Information Sciences*, vol. 180, no. 8, pp. 1201–1217, 2010.

[31] D. N. Tran, H-J. Zepernick and T. M. C. Chu., "LSB Data Hiding in Digital Media: A Survey," *EAI Endorsed Transactions Review Arti-*

cle/EAI.EU on Industrial Networks and Intelligent Systems, vol.9, no.30, 2022.

[32] A. Basu, T. S. Das, and S. K. Sarkar, "Robust Visual Information Hiding Framework Based on HVS Pixel Adaptive LSB Replacement (HPALR) Technique," *International Journal of Imaging and Robotics*, vol. 6, pp. 71–98, 2011.

[33] D. Ravichandran, P. Praveenkumar, S. Rajagopalan, *et al.*, "ROI-based medical image watermarking for accurate tamper detection, localisation and recovery," *Medical & Biological Engineering & Computing*, vol.59, pp. 1355-1372, 2021.

[34] A. Anand, A. K. Singh, "Watermarking techniques for medical data authentication: a survey," *Multimedia Tools and Applications*, vol. 80, pp. 30165–30197, 2021.

[35] H. V. Singh and A. Rai, "Medical image watermarking in transform domain," *Smart Innovations in Communication and Computational Sciences*, vol. 851, pp. 485–493, 2018.

[36] Z. Xia, X. Wang, W. Zhou, *et al.*, "Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms," *Signal Process*, vol. 157, pp. 108–118, 2018.

[37] J. Liu, J. Li, J. Ma, *et al.*, "A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon map," *Applied Sciences*, vol. 9, no.4, pp. 1–23, 2019.

[38] A. K. Singh, M. Dave and A. Mohan, "Multilevel encrypted text watermarking on medical images using spread-Spectrum in DWT domain," *Wireless Personal Communications*, vol. 83, no. 3, pp. 2133–2150, 2015.

[39] A. Zear, A. K. Singh and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools and Applications*, 2016.

[40] A. K. Singh, "Improved hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools and Applications*, vol. 76, pp. 8881–8900, 2016.

[41] S. Priya, B. Santhi, P. Swaminathan and J. Raja Mohan, "Hybrid transform based reversible watermarking technique for medical images in telemedicine applications," *Optik*, vol. 154, pp. 655–671, 2017.

[42] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," *Multimedia Tools and Applications*, vol. 78, pp.17027–17049, 2019.

[43] Z. Cui, W. Qi, Y. Liu and J. Guo, "Research on Region Selection Strategy for Visible Watermark Embedding," *IETE Technical Review*, vol. 38, No. 1, pp. 5-16, 2021.

[44] Y. Liu, X. Qu and G. Xin, "A ROI-based reversible data hiding scheme in encrypted medical images," *Journal of Visual Communication and Image Representation*, vol. 39, pp. 51–57, 2016.

[45] W. Wójtowicz, "Biometric watermarking for medical images–example of IRIS code," *Technical Transactions*, pp. 409–416, 2013.

[46] M. Vafaei, H. Mahdavi-Nasab and H. Pourghassem, "A new robust blind watermarking method based on neural networks in wavelet transform domain," *World Applied Sciences Journal*, vol. 22, no. 11, pp. 1572–1580, 2013.

[47] A. K. Singh, B. Kumar, S. K. Singh, *et al.*, "Multiple watermarking technique for securing online social network contents using Back propagation neural network," *Future Generation Computer Systems*, vol. 86, pp. 926–939, 2018.

[48] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," *Multimedia Tools and Applications*, vol. 78, pp. 30523–30533, 2019.

[49] B. Kumar, H.V. Singh, S.P. Singh and A. Mohan, "Secure spread spectrum watermarking for telemedicine applications," *Journal of Information Security*, vol. 2, pp. 91–98, 2011.

[50] A. A. Nakhaie and S. B. Shokouhi, "No reference medical image quality measurement based on spread spectrum and discrete wavelet transform using ROI processing," in *Proceedings of 24th Canadian Conference on Electrical and Computer Engineering*, pp. 121–125, 2011.

[51] K. Pal, G. Ghosh and M. Bhattacharya, "Biomedical image watermarking in wavelet domain for data integrity using bit majority algorithm and multiple copies of hidden information," Am. J. Biomed. Eng., Vol.2, no. 2, pp. 29–37, 2012

[52] A. Kannammal, K. Pavithra and S. SubhaRani, "Double watermarking of DICOM medical images using wavelet decomposition technique," *European Journal of Scientific Research*, vol. 70, no. 1, pp. 46–55, 2012.

[53] A. Umaamaheshvari and K. Thanushkodi, "High performance and effective watermarking scheme for medical images," *European Journal of Scientific Research*, vol.67, no. 2, pp. 283–293, 2012.

[54] M. Soliman, A. E. Hassanien, N.I. Ghali and H. M. Onsi, "An adaptive watermarking approach for medical imaging using swarm intelligent," *International Journal of Smart Home*, vol.6, no.1, pp. 37–50, 2012.

[55] P. Mangaiyarkarasi and S. Arulselvi, "Medical image watermarking based on DWT and ICA for copyright protection," *Recent Advancements in System Modelling Applications*, vol. 188, pp. 21–33, Springer, New York, 2013.

[56] W. Wioletta, "Biometric watermarking for medical images – example of Iris code," *TECHNICAL*

TRANSACTIONS, vol. 1-M, no. 5, pp. 409–416, 2013.

[57] M. A. Hajjaji, E.-B. Bourennane, A. B. Abdelali and A. Mtibaa, "Combining Haar wavelet and Karhunen Loeve transforms for medical images watermarking," *BioMed Research International*,pp. 1–15, 2014.

[58] A. Al-Haj and A. Amer, "Secured telemedicine using region-based watermarking with tamper localization," *Journal Digit Imaging*, vol. 27, no. 6, pp. 737–750, 2014.

[59] L. Gao, T. Gao, G. Sheng and S. Zhang, "Robust medical image watermarking scheme with rotation correction," *Intelligent Data analysis and its Applications*, vol. 2, pp. 283–292, Springer, New York, 2014.

[60] G. Badshah, S.-C. Liew, J. MdZain and M. Ali, "Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique," *Journal of Digital Imaging*, vol. 29, no. 2, pp. 216–225, 2016.

[61] A. Rai and H.V. Singh, "SVM based robust watermarking for enhanced medical image security," *Multimedia Tools and Applications*, vol. 76, pp. 18605–18618, 2017.

[62] S. A. Parah, J. A. Sheikh, F. Ahad, *et al.*, "Information hiding in medical images: a robust medical image watermarking system for E-healthcare," *Multimedia Tools and Applications*, vol. 76, pp. 10599–10633, 2017.

[63] K. Swaraja, "Medical image region based watermarking for secured telemedicine," *Multimedia Tools and Applications*, vol. 77, pp. 28249–28280, 2018.

[64] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools and Applications*, vol. 80, pp. 16549–16564, 2020.

[65] F. Mendel, N. Pramstaller, C. Rechberger and V. Rijmen, "Analysis of step-reduced SHA-256," *International Workshop on Fast Software Encryption*, pp. 126-143, Springer, Berlin, Heidelberg, 2006.

[66] K. Balasamy and S. Suganyadevi, "A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD," *Multimedia Tools and Applications*, vol. 80, pp. 7167–7186, 2021.

[67] M. N. Ahmed, S. M. Yamany, N. Mohamed, *et al.*, "A modified fuzzy C-means algorithm for Bias field estimation and segmentation of MRI data," in *IEEE Transactions on Medical Imaging*, vol. 21, no. 3, pp. 193-199, March 2002.

[68] P. Khare and V. K. Srivastava, "A Secured and Robust Medical Image Watermarking Approach for Protecting Integrity of Medical Images," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, pp. e3918, 2020.

[69] R. Thanki and A. Kothari, "Multi-level security of medical images based on encryption and watermarking for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, pp. 4307–4325, 2021.

[70] K. Swaraja, K. Meenakshi and K. Padmavathi, "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine," *Biomedical Signal Processing and Control*, vol. 55, no. 101665, 2020.

[71] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, " A DWT based watermarking approach for medical image protection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 2931–2938, 2021.

[72] X. Zheng and J. Jin,"Research for the application and safety of MD5 algorithm in password authentication," *2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*, Chongqing, China, pp. 2216-2219, 2012.

[73] S. Basheera, D. BhanuPrakash and P. Naganjaneyulu, "Blind medical image watermarking technique for secure recovery of hidden data," *International Conference on Digital Image Processing and Information Technology*, Tamil Nadu, India, pp. 185-192, 2011.

[74] F. Kahlessenane, A. Khaldi, R. Kafi, *et al.*, "A robust blind medical image watermarking approach for telemedicine applications," *Cluster Computing*, vol. 24, pp. 2069–2082, 2021.

[75] P. Singh, K. J. Devi, H. K. Thakkar and K. Kotecha, "Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT," *IEEE Access*, vol. 10, pp. 8974-8993, 2022.

[76] M. Z. Konyar and S. Ozturk, "Reed Solomon Coding-Based Medical Image Data Hiding Method against Salt and Pepper Noise," *Symmetry*, vol. 12, no. 899, 2020.

[77] V. M. Manikandan and V. Masilamani, "A novel image scaling based reversible watermarking scheme for secure medical image transmission," *ISA Transactions*, vol. 108, pp. 269-281, 2020.

[78] A. Nagm and M. Safy Elwan, "Protection of the patient data against intentional attacks using a hybrid robust watermarking code," *PeerJ Computer Science*, vol. 7, 2021.

[79] A. Soualmi, A. Alti and L. Laouamer, "A novel blind medical image watermarking scheme based on Schur triangulation and chaotic sequence," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 1, 2022.

[80] M. Kutter and F.A.P. Petitcolas, "A fair benchmark for image watermarking systems," *Journal*

of Electronic Imaging, vol. 9,no. 4, pp. 445-455, 2000.

[81] S. Sinha Roy, S. Saha and A. Basu, "A Generic Testing Architecture for Digital Watermarking," Proc. FRCCD-2015, pp. 50-58, 2015.

Subhrajit Sinha Roy received his B. Tech. and M. Tech degree in Electronics and Communication Engineering from Maulana Abul Kalam Azad University of Technology in year 2012 and 2015, respectively. He is pursuing his Ph.D. (Tech.) from the Institute of Radio Physics and Electronics, University of Calcutta, Kolkata, India. At present he is also an Assistant Professor in the department of Electronics and Communication Engineering at RCC Institute of Information Technology, Kolkata, India. His field of interest spans digital image processing, Multimedia Copyright protection technique, FPGA based system design, Low cost system implementation.

Abhishek Basu received his Ph. D. (Engg.) from the ETCE Department, Jadavpur University, India in 2015. He is currently an Assistant Associate Professor with the RCC Institute of Information Technology Kolkata, India. He is a fellow of IETE. His research interests include Multimedia copyright protection, digital image processing, VLSI IP protection technique, FPGA based system design, low power VLSI design, and embedded system design.

Avik Chattopadhyay received his Ph. D. (Tech.) from the Institute of Radio Physics and Electronics, University of Calcutta, Kolkata, India in 2013. He is currently an Assistant Professor with the Institute of Radio Physics and Electronics, University of Calcutta, Kolkata, India. His research interests include study of post-CMOS devices for low power VLSI applications, designing of FPGA- based systems, multimedia security, and image processing.