VOL. 11, NO. 5, MARCH 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

MEDICAL IMAGE WATERMARKING: RUN THROUGH REVIEW

P. V. V. Kishore[1], M. Siva Srinivasa Rao[2], Ch. Raghava Prasad[1] and D. Anil Kumar[1]
[1]Department of Electronics and Communications Engineering, K. L. University, Green Fields, Vaddeswaram, Guntur - DT., India
[2]Department of Electronics and Communications Engineering, Vignan's University, Vadlamudi, Guntur, India
E-Mail: pvvkishore@kluniversity.in

ABSTRACT

The objective of this paper is to extract the review work related in the field of watermarking focusing exclusively on medical image watermarking. Medical imaging has impacted positively the health care system around the world by helping doctors perform visual diagnostics of the human body. Sharing this information digitally requires copyright protection which is offered using medical image watermarking researchers around the world. This review has two parts. First part embeds knowledge on medical image watermarking and second part extracts the performance of algorithms from the proposed literature to carry out watermarking of medical images. The performance of these methods is compared using normalized cross correlation coefficient and the algorithms were classified into non intelligence and intelligence based watermarking algorithms. This review concludes that intelligence and heuristic approaches for medical image watermarking give informative extracted cover medical images.

Keywords: medical image watermarking, wavelet transforms, lifting wavelets, singular value decomposition, RSA encryption, BAT based optimization, artificial neural networks, intelligence, non-intelligence.

1. INTRODUCTION

Making high quality health care accessible to majority human beings around the globe is a major concern to the administrators, governments and politicians. Traditionally, medicine was practiced until recently on a local basis where the medical practitioner and patient are physically present at the same place. But recent advances in information and communication technologies (ICT) have augmented the number of ways in which healthcare can be distributed to remote parts of the world.

The intermittent developments of Internet and Multimedia Technologies had made possible the duplication of digitally produced information effortless and straightforward. The progression in embedded chip technologies has made it possible to generate, duplicate, broadcast, and dispense digital contents in an unforced manner.

Hence the fortification and enforcement of copyrights for digital media has grown into a critical issue. In the recent past research in computer software design focused on digital watermarking methods to protect internet content. In the midst many health services around the globe are storing and transmitting medical images via internet.

Watermarking digital multimedia [1]-[4] contentshas grown rapidly in the recent past with the advances in internet technology. This watermarking functionality is to hide information, protect the digital copyrights and for content identification of multimedia contents exchanged over the internet.

Internet data travels through unprotected routing switches all over the world. Hence watermarking comes to the rescue for protecting multimedia data that is transmitted through these unsecured servers.

Attacks on security are best characterized by viewing the function of the computer system as a facility of information transfer. In general, normal communication is represented as a flow of information from source to destination. In this process of data transfer, the information can be modified or stolen using various types of attacks.

There are four categories of attacks formulated in literature:

a) **Interruption:** An attack on availability. Information is destroyed or becomes unavailable or unusable.
b) **Interception:** An attack on confidentiality. An unauthorized party gains access to information.
c) **Modification:** An attack on integrity. An unauthorized party not only gains access to, but also tampers with information.
d) **Fabrication:** An attack on authenticity. An unauthorized party inserts counterfeit objects into the system.

These attacks can be divided further two categories, according to the nature of the attacks:

1.1 Active attacks

These attacks involve modification of the data stream or the creation of a false stream and can be subdivided into four categories:

a) **Masquerade:** One entity pretends to be a different entity.
b) **Replay:** The passive capture of a data unit and its subsequent retransmission to produce an illegal effect.
c) **Modification of messages:** Some portion of a genuine message is distorted, or messages are delayed or recorded to produce an illicit effect.

d) **Rejection of service:** One inhibits the standard use or management of communication services.

1.2 Passive attacks

These attacks involve eavesdropping on, or monitoring of, transmission and can be subdivided into two categories:

Release of message contents: An unauthorized party obtains information that is being transmitted.

Traffic analysis: An unauthorized party obtains information useful in guessing the nature of communication by observing the pattern of masked message transmissions.

This research deals with modification and fabrication attacks on medical images. We will look at how to authenticate medical images using watermarking [5].

2. RESEARCH IN DIGITAL WATERMARKING

Watermarks recognize the copyright owner of the file. Watermarks are typically hidden to prevent their discovery and confiscation; they are said to be invisible watermarks [6]. However, visible watermarks [7] can be used and often take the form of a visual pattern superimposed on a cover image.

To embed a watermark W = {w1, w2, w3, w4, …,wn} where, first the basis code is separated into n blocks. Each of these blocks is then represented by w_i and this holds the value either 0 or 1. If w_i is 0, then the block of code it represents will be left unchanged. However, if w_i is 1, then one will look for two statements inside the block and switch them over [8, 9].

The watermark is usually embedded by making changes to the binary code that does not affect the actual contents of the file to a great extent. To decode and extract the watermark, one should have the original binary file [10]. By weighing against the watermarked and original images, the statement controls can be marked and consequently the embedded watermark can be extracted.

This method of watermark embedding and extraction is very simple, but is not resistant to attacks. If the attacker has many different versions of the marked files, then he may detect the watermark and hence be able to remove it [11].

It is complicated to recognize the original from the duplicate when it comes to electronic versions of images. Images copies are identical and it is impossible to tell if it is an original or a copied version. To embed information inside an image one can basically amend some of its characteristics.

Watermarking was first introduced to protect text documents [12]. The text watermarking algorithms popularly include line shift coding [13], various lines inside the document up or down are shifted down by a small fraction according to the codebook. Differential encoding techniques are used in [14], where if a line is shifted the adjacent lines are not moved.

The word shift coding method [15] is based on the same principle as the line shift coding protocol. In feature coding [16], the features are used to hide information and each of these will be marked in the document. Another way of hiding data in text is to use white spaces [17], which can be manipulated so that bits can be stored.

A very simple yet widely used technique for watermarking images [18] is to add a pattern on top of an existing image. Usually this pattern is an image itself - a logo or something similar [19], which distorts the underlying image.

The Least Significant Bit Hiding [20] works by using the least significant bits of each pixel in one image to hide the most significant bits of another. This is achieved by choosing the number of bits to hide the secret image. Increasing the number of bits obviously has a beneficial reaction to the secret image increasing its clarity.

This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. Also, while in this method an image has been hidden, the least significant bits could be used to store text or even a small amount of sound. All you need to do is change how the least significant bits are filled in the host image. However, this technique makes it very easy to find and remove the hidden data [21].

Another way of hiding image data is by way of a direct cosine transformation (DCT) [22-23]. The DCT algorithm is one of the main components of the JPEG compression technique. Hiding via a DCT is useful, as someone who just looks at the pixel values of the image would be unaware that anything is amiss. Also the hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.

While DCT [24] transformations help hide watermark information or general data, they don't do a great job at higher compression levels. The blocky look of highly compressed JPEG files is due to the 8 x 8 blocks used in the transformation process.

Wavelet transformations [25]- [27] on the other hand, are far better at high compression levels and thus increase the level of robustness of the information that is hidden, something which is essential in an area like watermarking. This technique works by taking many wavelets to encode a whole image.

They allow images to be compressed so highly by storing the high frequency "detail" in the image separately from the low frequency parts [28- 30]. The low frequency areas can then be compressed, which is acceptable as they are most viable for compression.

Spread spectrum systems [31] encode data as a binary sequence which sounds like noise, but which can be recognized by a receiver with the correct key. Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium.

Information hiding techniques still suffer from several limitations [32], leaving them open to attack [33] and robustness criteria vary between different techniques. Attacks [34-37] can be broadly categorized, although some attacks will fit into multiple categories.

A digital watermark can be perceived as a visible or invisible detection code that is embedded inside a medical image. Medical image authentication calls for a nonvisible perfectly hidden watermark [38]. Medical image watermarking plays a prominent role in telemedicine applications [39].

Digital watermarks for medical images can be made by hiding patient information to make them unique to a particular patient [40]. Watermark is extracted to prove the authenticity that these medical images belong to a particular patient [41].

3. INTRODUCTION TO MEDICAL WATERMARKING

Medical image watermarking [42]-[45], functions significantly in supporting a patient by conveying his infirmity using medical images through unsecured networks such as the internet to expert doctors around the world. This practice helps to expand the possibility of distantly stationed patients where no expert medical doctor is accessible to increase their disease detection probability. Trafficking medical images through unsecure internet is prone to unwelcome modification to the sensitive contents of the medical images. Medical images contain vulnerable information which is valuable related to the health of the patient [46].

Medical practitioner has to take supreme care to check that the images are not meddled with, before analysing the medical images downloaded from the unsecure internet. For this reason, authentication of medical images such as Ultrasound scans, MRI scans, x-ray and Computer Tomography (CT) scans has to be watermarked. The host medical image can be watermarked with patient information before transmitting on the internet. At the physician's end it has to de-watermark before proceeding for diagnostics.

Medical cover images are watermarked with patient image as watermark which forms an invisible detection code. A medical image watermarking is a perfectly hidden watermarking paradigm as proposed in [47]. The application of medical image watermarking is towards telemedicine applications. In recent years' medical image watermarking is primarily used to hide patient information such as patient's name, age, gender which can uniquely identify a patient [48].

This patient related watermark information is extracted to determine the authenticity of the medical images. As the extracted watermark from the medical image matches the patient data in the doctor's office, it is proved that these medical images belong to a particular patient [49].

There are numerous diverse practices and embedding techniques that facilitate data hiding in a given medical cover image. However, all of the diverse practices and techniques are influenced by a number of requirements so that watermarking can be applied appropriately. The following is a register of major requirements that watermarking techniques have to satisfy: The integrity of the hidden information after it has been embedded inside the cover image must be correct. The secret message must not change in any way, such as additional information being added, loss of information or changes to the secret information after it has been hidden. If secret information is changed during watermarking, it would defeat the whole point of the process.

a) The cover image must remain unaffected or untouched to the naked eye. If the cover image changes considerably, then possibly, a third party may see the information being hidden and therefore could attempt to extract or destroy it.
b) In watermarking, changes in the cover image must have no effect on the watermark.
c) Finally, it is always assumed that the attacker knows that there is hidden information in the cover image.

A watermarking algorithm should be reliable based on the following issues:

a) **Intelligibility:** The most essential prerequisite for any Watermarking scheme shall be such that it is transparent to the end user. The watermarked content should be fragile at the projected user device without frustrating the user.
b) **Protection:** Watermark information can only be available to the sanctioned users. Only approved user shall be able to modify the Watermark content. Encryption is used to prevent illicit access of the watermarked data.
c) **turdiness:** Watermarking must be vigorous enough to endure all kinds for image processing operations, "attacks" or unauthorized access. Any attempt that has a potential to modify the data content is considered as an attack. Sturdiness against attack is a key obligation for Watermarking and the accomplishment of the watermarking algorithm for protection depends on this issue.

Figure-1 shows a simple representation of the generic embedding and decoding process in Medical Image watermarking followed as a part of this work. In this example, a secret patient image is being embedded in a medical cover image obtained from various sources to produce the watermarked image.

There is a growing demand for applications related to watermarking due to the ever increasing storage and sharing of digital media contents around the world on the internet. Watermarking has invaded every multimedia transmission on the internet such as text documents [50],

images [51] and even audio [52] and video data watermarking [53].

Various digital image watermarking schemes are proposed and implemented successfully by researchers around the world on an image in spatial domain [54], transform domain [55] along with encryption techniques which are robust [56], semi-fragile [57]and some are fragile watermarking [58] schemes.

The growing need for medical image watermarking schemes is due to the usage of internet to transfer medical images among expert doctors for advices and case studies.

Medical images can save and are saving human lives around the world. But with sharing comes the fear of hackers. Hackers attack these medical images, modifying their details making the medical image data misleading to a doctor. This point can be better proved by looking at the original and modified medical images as shown in Figure-2(a) and Figure-2(b).

Figure-2(a) is the original MRI image of a patient. When a doctor at a remote location wants a second opinion about the disease, he transmits it to another expert through internet. Figure-2(b) shows the modified medical image by the hackers.

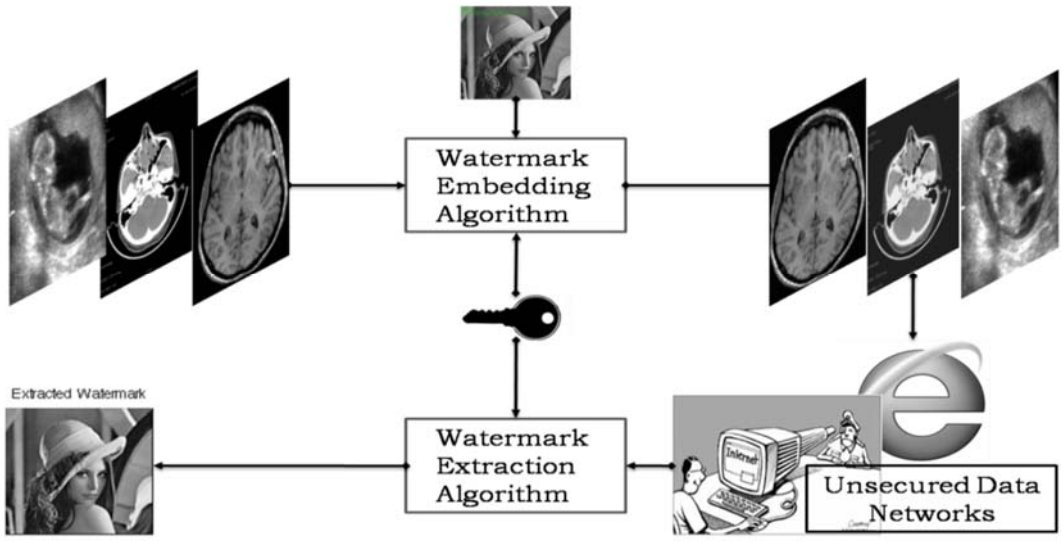
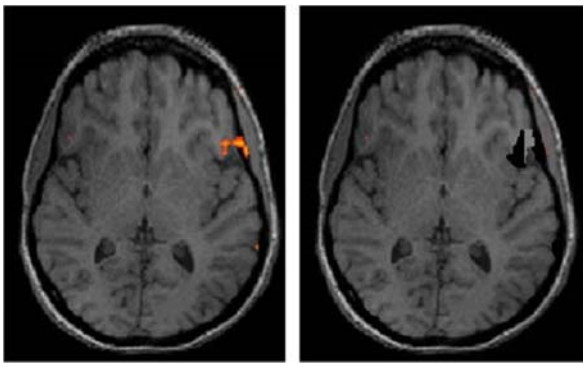
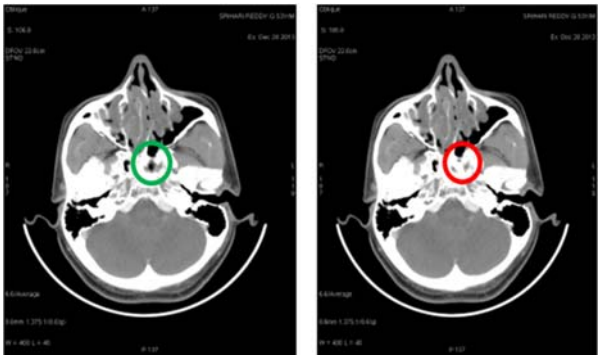


Figure-1. Medical image watermarking and de-watermarking with patient image.



(a) (b)

Figure-2. (a)Original MRI brain image transmitted to the doctor through internet (b) Hacked MRI brain image transmitted to the doctor through internet.



(a) (b)

Figure-3. (a) Original CT brain image transmitted to the doctor through internet (b) Hacked CT brain image downloaded into doctors.

This kind of modifications can sometimes cost a human life. Here there is a need to prevent medical data from hackers and prove the authenticity of the medical images at the receiving doctor's end. Figures 3(a) and (b) shows the original and attacked CT brain image.

In modern medicine it has become a regular practice to send medical images through internet from the diagnostics centre to doctor. The sensitive medical information related to a patient traverse through unsecured networks and databases. This makes the medical images vulnerable to attacks which include tampering of images compromising the patient's information. Figure 4(a) and 4(b) shows the two ultrasound images one original breast cancer image and another tampered ultrasound image of the same patient respectively. Images are courtesy of [12].

Coatrieux*et al* [59] proposed that digital watermarks should be considered as a security tool in order to protect medical records. In the article, the author proposed a new lossless or reversible watermarking approach that allows the embedding of a message within categorical data of relational database. The reversibility property is achieved by adapting the histogram shifting modulation algorithm [60].

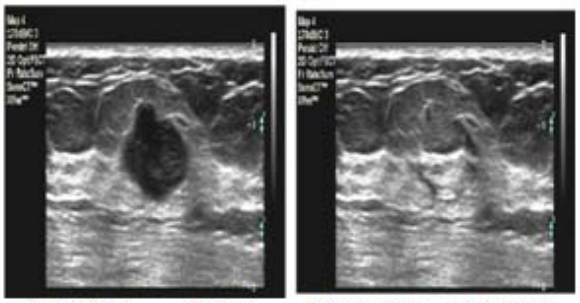


Figure-4(a). Breast Cancer of a patient.

Figure-4(b). Tampered Image of the same patient as Figure-3(a).

Giakoumaki*et al* [61] proposed a wavelet transform-based watermarking, which fulfils the strict requirements concerning the acceptable alterations of medical images. The proposed scheme embeds numerous watermarks helping diverse functionality such as authentication containing doctor's digital signature as a robust watermark, patient's personal and examination related data and a fragile watermark for data integrity control.

Lou *et al* [62] proposed a technique of pixel-value difference expansion, a multiple-layer data hiding technique in spatial domain. It utilizes a reduced difference expansion method to embed the bit stream in the least significant bits (LSBs) of the expanded differences.

Nyeem, H *et al* [63] used least significant bit planes to watermark medical images with patient information. The least significant bit planes were encoded with patient information which least effects the integrity of the visual information present in the medical images.

Eswaraiah*et al* [64] proposed a Region of Interest (ROI) and Least Significant Bit (LSB) based fragile watermarking technique for tamper detection and recovery of medical images. At first, medical image is divided into ROI and NROI. Later, authentication information is inserted into ROI and recovery information into NROI. To increase embedding capacity in ROI, authentication information is compressed using Run Length Encoding (RLE) technique before inserting into ROI. Experimental results reveal that any tampering to ROI of medical image is identified and recovered without any loss.

By using the reduced difference expansion method, we can embed a large amount of data in a medical image whose quality can also be maintained. Moreover, the original image can be restored after extracting the hidden data from the stegno image. Experimental results show that the proposed scheme provides higher embedding capacity at the same level image quality compared with Tai's [65] difference expansion method.

Irany*et al* [66] proposed a high capacity reversible multiple watermarking scheme for medical images based on integer-to-integer wavelet transform and histogram shifting. The novelty of the proposed scheme is that it uses a scalable location map and incorporates efficient stopping conditions on both wavelet levels and different frequency sub-bands of each level to achieve high capacity payload embedding, high perceptual quality, and multiple watermarking capabilities. Results show that the proposed method attains high perceptual quality in higher capacity rates for the medical images.

Lavanya*et al* [67] proposed non region of interest (NROI) based medical image watermarking schemes, where the patient details are embedded in non-ROI region of an image. The encrypted image is divided into non overlapping tiles to identify the region of interest and non-region of interest. In the examination site, examiner embeds patient details in non-ROI [68] of encrypted image using a data-hiding key. With an encrypted image containing patient details, a receiver may first defile and decrypt it using the encryption key and the decrypted version is similar to the original image.

Wakatani*et al* [69], proposed a digital watermarking technique by shunning the deformation of the image data in ROI by embedding watermark into areas other than the ROI. Watermark image is compressed by a progressive coding algorithm which is used as the signature information.

Hyung*et al* [70] proposed an embedding algorithm based on ROI. The watermark is embedded into medical image in the neighborhood region where medical information used for diagnosis is negligible. The neighborhood used for diagnosis is called region of interest (ROI) and the watermarking also augments invisibility.

The watermark is the value of bit plane in wavelet transform of the ROI for reliability authentication. The experimental results show that the proposed algorithm can endure productively under attacks.

Adiwijaya*et al* [71] discussed a method of reversible watermarking using a modified LSB and Huffman compression for detecting and recovering the manipulated medical image. The test results show that the proposed system is capable of detecting the attack with an

accuracy of up to 100% and can do the recovery with an accuracy of recovery rate up to 98% for some attacks.

Kongo *et al* [72] utilized the extraordinary superiority of dual tree transform wavelet combined with Bivariate Shrinkage with Local Variance Estimation at the extraction step of the watermark in the medical images. The experimental results showed much improved performance of the proposed technique for DT-CWT in comparison with DWT.

Yaoli Liu *et al* [73] proposed a robust watermarking algorithm for medical image authentication and protection using the visual features of the medical images watermarked with DWT-DCT. The watermarking image is encrypted by Logistic Map to strengthen its security. Simulations show that the algorithm is robust to common and geometric attacks. In the medical image watermarking, the reversible watermarking techniques are gaining enormous attention due to their importance of medical image security and protection [74]. In medical image watermarking techniques based on reversible method, it is possible to remove full watermark information thus leaving original image intact, ready for diagnosis [75].

As illustrated by Navas*et al* [76], medical image watermarking algorithms accounted in literature canbe classified into two classes:

1. Algorithms and Techniques focusing on tamper detection and authentication.

2. Algorithms and methods focusing on electronic patient record (EPR) data hiding.

This paper reviews algorithms and methods focusing on electronic patient Image (EPI) hiding.

EPI data hiding techniques give more significance in hiding watermark in image keeping the imperceptibility very high. The tamper detection methods use the watermarks that localize the changes indicating the location of tampering.

Renaud, K *et al* [77] paper presents details of an authentication system which relies on the user identifying previously drawn Mikons. Mikons are self-drawn icon-like images, meant to depict a message the artist wants to convey at that point in time. These are drawn, at enrolment, using an embedded shock wave component within a browser. At authentication the user identifies his or her own Mikons from challenge sets, each containing one of the user's Mikon and a number of distractor Mikons. The efficacy of Mikons in this setting was investigated by using them in a recognition-based authentication system to authorize users of an online homework system over an eight-month period.

Boucherkha*et al* [78] devised a well-known method to serve image authentication and invisible embedding of patient information. A 128-bit message authentication code (MAC) based on the image digest is created and then this MAC as well as the encrypted patient info is embedded, in a reversible way, at pixels LSBs (Lease Significant Bits) locations, after compressing them.

Chunhua Dong *et al* [79] proposed a zero-watermarking algorithm of the medical image using DCT, which can effectively solve this problem. This algorithm can enhance medical image security, confidentiality and integrity in the application for medical image communications between hospitals. The algorithm combines the visual feature vector of images, encryption technology with the third party authentication, and avoids the selection of ROI to speed up watermarking embedding and extracting. The simulation results demonstrate the algorithm has desired robustness against common attacks and geometric attacks, such as JEPG, rotation, scaling and translation, etc.

Kallel, IF [80] presents different methods developed in image watermarking for verifying the integrity and authenticity of medical images. Lin Gao*et al* [81] proposes a new reversible watermarking scheme based on Integer Discrete Cosine Transform (IntDCT) and Difference Expansion (DE) for watermarking medical images.

Hajjaji, M.A*et al* [82-83] proposed a method that uses JPEG compression for the mixing of medical data. The insertion block is inserted just after the quantization phase. To control identification and eventually the correction (if possible) of the inserted data, we use a series of turbo codes to recover the inserted data, after application of several attacks.

Pradeepkumar, G [84] suggests a comparative performance of digital image watermarking scheme using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) separately [85] and their performance has been measured by using metrics like PSNR, Quality Index and Elapsed time. Initially, the Medical image is decomposed using image transforms like DCT or DWT. Subsequently, the watermark embedding and extraction processes are performed in frequency domain along with LSB substitution algorithm which is in spatial domain.

Jingbing Li et al [86-87] uses a part of sign sequence of DWT-DCT coefficients as the feature vector of images for enhancing the robustness against common attacks and geometric attacks. The watermarking image is scrambled by Arnold transform to enhance its privacy. The experimental results show that the scheme has benefits at visual invisibility and robustness.

Dey, N *et al* [88] presented the entire video of 4D Ultrasound Sound issplit into frames and application of Discrete Wavelet Transformation (DWT), Discrete Cosine Transformation (DCT) followed by Singular Value Decomposition (SVD) make up the watermark embedding technique. Watermark extraction is achieved by applying inverse DWT, inverse DCT and SVD. In this approach the generated peak signal to noise ratio (PSNR) of the original IVUS video signal vs. watermarked signal and the correlation value of the original watermark image and the extracted watermark image have a high acceptable level of imperceptibility and distortion.

Soliman, M.M. *etal* [89-90] considered image watermarking as an optimization problem by utilizing

human visual system (HVS) characteristics and Quantum Particle Swarm Optimization (QPSO) algorithm in adaptive quantization index modulation and singular value decomposition in conjunction with discrete wavelet transform (DWT) and discrete cosine transform (DCT). Experimental results prove the effectiveness of the proposed algorithm that yields a watermarked image with good visual fidelity, at the same time watermark being able to withstand a variety of attacks including JPEG compression, Gaussian noise, Salt and Pepper noise, Gaussian filter, median filter, image cropping and image scaling.

Hsiang-Cheh Huang *et al* [91] proposed the watermarking scheme by predicting the difference between output and input images for making reversible data hiding possible. By carefully selecting prediction coefficients, which are optimized by genetic algorithm, the output image quality can be preserved, while the enhanced amount of embedding capacity can be observed. The author applies the algorithm to medical images for protecting patients' cases from possible human errors incurred. With the training of genetic algorithm, simulation results with our algorithm have demonstrated the enhanced embedding capacity, while keeping the output image quality.

JayanthiV.E. *et al* [92] used biomedical images as watermark is embedded in the regions other than the area of interest so that the diagnosis is not affected. The area of interest of the biomedical image is found out using the K-means segmentation method. Performance of proposed watermarking scheme is robust against various types of attacks such as Affine transform, Gaussian noise, shearing, rotation, median filtering and JPEG compression. This proposed algorithm can be used in Hospital environment.

Jingbing Li *et al* [95] proposed Robust multiple watermarks of medical volume data using 3D DWT-DCT to deal with this problem. The parts of sign sequence of 3D DWT-DCT coefficients are used as feature vector, which is utilized to enhance the robustness against rotation, scaling, translation attacks. The author describes how to obtain the feature vector of medical volume data and embed and extract the multiple watermarks.

Yujia Li *et al* [96] proposed a compressed domain algorithm of robust blind watermarking method for medical volume data, which addressed the problems of authentication and protection of personal information. The scheme obtained the visual feature vectors of medical volume data in DCT compressed domain. Through the concept of zero-watermarking, the algorithm for watermarking for volume data proposed in this paper is robust to geometric attacks. The experimental results demonstrate that the proposed algorithm has good invisibility and robustness.

Shewen Sun *et al* [97] presented a novel color medical image authentication scheme based on QR factorization and dual pseudorandom circular chain (DPCC). The red component and the green component of the color image possess more brightness than the blue one, so QR factorization values of the red component and the green component are used to be the initial values of logistic mapping to generate two watermarks. Then, the least significant bit (LSB) plane of blue component by the watermarks is replaced according to DPCC. Experimental results show that the proposed algorithm is sensitive to malicious attacks on the watermarked image, and can localize the tampered region accurately.

4. MEDICAL IMAGE WATERMARKING: OUR PAST RESEARCH APPROACHES

As mentioned earlier medical image is a primary requirement for communication among medical practitioners through unsecured data networks such as the internet. For an unhealthy person located remotely it is highly impossible to locate an expert doctor to diagnose his medical condition. This difficulty is solved with the help of unsecured internet which acts as a communication link between the remote patient and expert doctor.

The transfer of medical images through unsecured networks makes them visible to unlawful hackers. The theme of this review is to discuss methods to protect the highly vulnerable visible medical images from getting tampered. Protecting medical images using watermarking with patient images for telemedicine application is the central theme of this review.

The paper [134] concentrates on development of a watermarking system that uses transform based features in wavelet domain. Watermarking algorithms proposed in this research are tested with three basic types of cover images namely, magnetic resonance imaging (MRI), computed tomography (CT) and Ultrasound (US). The patient image is used as a watermark.

Therefore, the watermarking system can be used in more real-time environments [98]- [99]. The main challenge in any watermarking system is to preserve the information in the watermarked medical cover image and extract the payload completely at the receiving end with little disturbances even under attacks.

Initially the process was started by the use of wavelet transform [100-102] for medical image watermarking. But seeing the scale of wavelets, it is decided to test different wavelets with multiple levels of decomposition and arrive at a conclusion to judge which type of wavelet at what level best compliments medical image watermarking. Initially, our work involves medical image watermarking process [134] is to identify a novel wavelet and its level along with wavelet coefficients to produce a valid watermark that is immune to attacks when transmitted on open networks. Watermarking in wavelet domain is accomplished with 4 different types of mother wavelets with patient image as watermark.

Watermark extraction procedure involves the transmission of key which in this case is a wavelet component of patient image. A set of measurable parameters are computed that can judge the watermarking algorithm performance for different types of wavelets at different levels.

Results provide insight into the use of multiresolution wavelet transform [103-104] for medical image watermarking. This procedure identifies the best mother wavelet at a particular decomposition level is suitable for medical image watermarking with patient image watermark.

A new enhanced watermarking method is proposed using lifting wavelet transform (LWT) [104-107] and SVD [108-110] for medical images as opposed to most widely used DWT-SVD [111- 115]. The medical images of patients are watermarked with the image of that particular patient which is extracted at the doctor's end to identification.

Lifting wavelets have distinctive advantage that is explored and is missed in traditional wavelet transform [116]. With lifting wavelets, the inverse transformation is undoing the operations of forward transform which decrease the imaging artefacts during transformation.

Watermarking with lifting scheme of wavelet transform [135] and singular value decomposition (LWT-SVD) is proposed for watermarking different types of medical images such as MRI, CT and US. In this method the singular values of the cover image are modified to create a watermarked medical image.

Experimental results demonstrate that the lifting wavelet transform is a better prospect for medical image watermarking scheme compared to normal discrete wavelet transform [135]. The results prove this fact visually and mathematically by computing psnr and ncc values.

The next medical image watermarking algorithm proposes the use of wavelet coefficients of cover image and RSA algorithm [117] for encryption of patient image. The watermark in this case is a patient image that is first treated with RSA encryption [118-119] with the help of KEY.

The encrypted patient image watermark is then embedded into to the medical image using 2D DWT. But seeing the scale of wavelets, it is decided to test different wavelets with multiple levels of decomposition and arrive at a conclusion that which type of wavelet at what level best compliments medical image watermarking. Finally, the extracted watermark is decrypted using KEY and RSA decryption algorithm.

Experimental results show that the RSA-DWT scheme [139] demonstrates superior protection on unsecured networks compared to normal DWT based watermarking scheme discussed previously. The experimental results prove this fact visually and mathematically by computing various performance metrics [140].

This research proposes to use wavelet transform and artificial neural network back propagation algorithm [120-123] for medical image watermarking. The watermark in this case is a patient image that is embedded into the medical image with the help of KEY.

Here KEY is a position matrix containing positions in the medical image where watermark is embedded. The neural network is trained to find a relation between 3×3 block pixels. This relation will help in reconstruction of the medical cover image after watermark extraction [141].

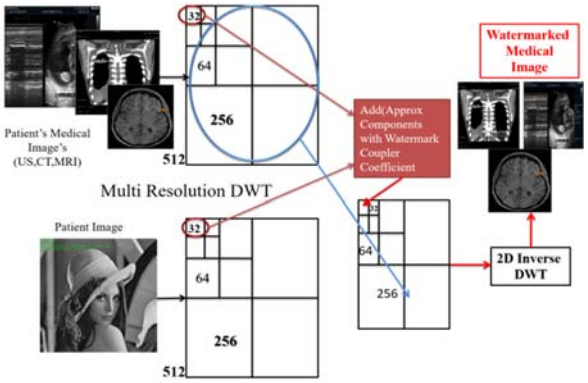


Figure-5. Non-Intelligence based medical image watermarking.

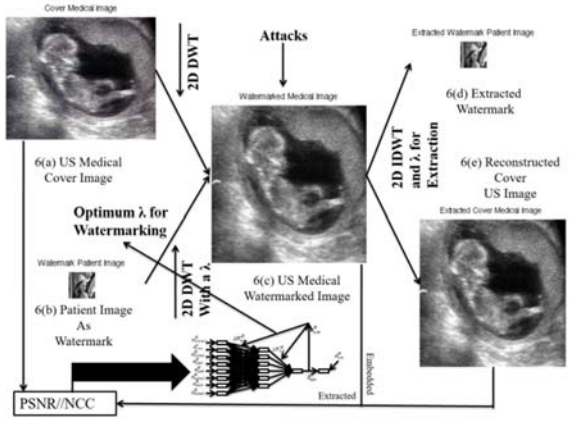


Figure-6. Intelligence based medical image watermarking with artificial neural network controlling the best values of psnr and ncc for embedding.

The patient image watermark is then embedded into to the medical image using 2D DWT. But seeing the scale of wavelets, it is decided to test different wavelets with multiple levels of decomposition and arrive at a conclusion that which type of wavelet at what level best compliments medical image watermarking. Finally, the watermark is extracted using position matrix and trained neural network algorithm [124-126].

This research proposes to use wavelet transform and BAT algorithm proposed by X.-S. Yang and Xin-She Yang [127-128] for medical image watermarking. The medical image is transformed into wavelet domain using a 2D DWT. The type of mother wavelet and level of scaling

are two parameters that are of interest to look for while applying the algorithm.

This patient image watermark is embedded into the medical cover image in transform domain. The extraction process is an inverse algorithm to embedding process. From the watermark embedding and extraction process two performance parameters are computed in the form of peak-signal-to-noise ratio (psnr) and normalized cross correlation (ncc) [129-133].

This procedure of watermarking gives unpredictable outcomes for medical images as cover images, with out of bounds psnr and ncc values. These unpredictable results of watermarking algorithm can be controlled using optimization algorithms such as genetic algorithm (GA), particle swarm optimization (PSO) and ant colony optimization (ANO).

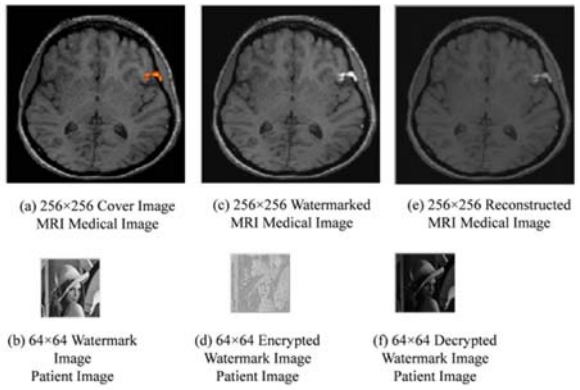


Figure-7. RSA-DWT based non-intelligence medical image watermarking with MRI medical image as cover image (a) MRI Cover image, (b) Patient image as watermark, (c) Watermarked MRI Medical image, (d) Encrypted Medical Image, (e) Reconstructed MRI scan, (f) Extracted patient image.

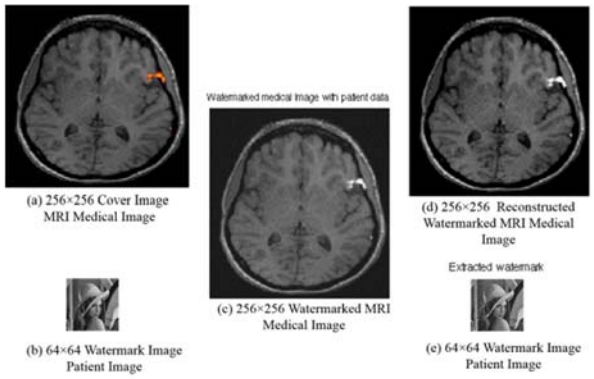
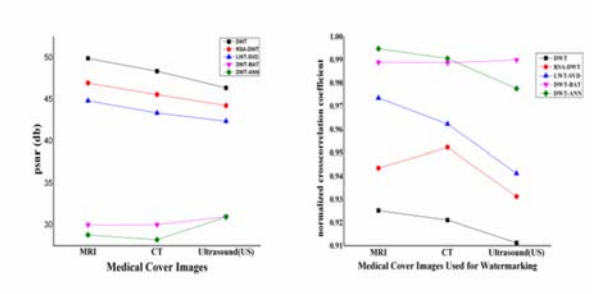


Figure-8. DWT-ANN based intelligent medical image watermarking with MRI medical image as cover image (a) MRI Cover image, (b) Patient image as watermark, (c) Watermarked MRI Medical image, (d) Reconstructed Medical image, (e) Extracted patient Image.

This research uses BAT algorithm [142] for optimizing the psnr and ncc values during watermark embedding and extraction process. The results of simulation show a better performance of BAT algorithm over GA and non-optimization watermarking process for medical images with patient image as watermark.



(a) (b)

Figure-9. (a) psnr and (b) ncc values of intelligent watermarking (DWT-BAT and DWT-ANN) comparedto other non-intelligent algorithms.

The medical image watermarking algorithms can now be classified as intelligence based and non-intelligence based algorithms. The first three algorithms are non-intelligence based, such as DWT, LWT-SVD and RSA-DWT and the last two are intelligence based algorithms which uses Artificial intelligence to reconstruct the watermarked medical images.

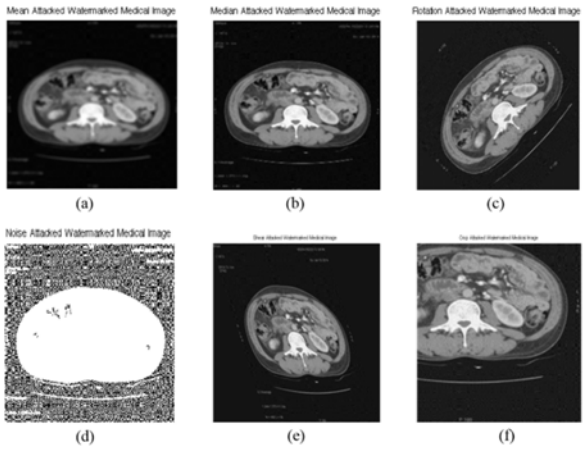


Figure-10. CT watermarked images with DWT-SVD algorithm under attacks (a) Mean Filter, (b) Median Filter, (c) Rotation (45^0), Salt and pepper noise (Var=0.02), (e) Shear (x=1) (f) Crop attack.

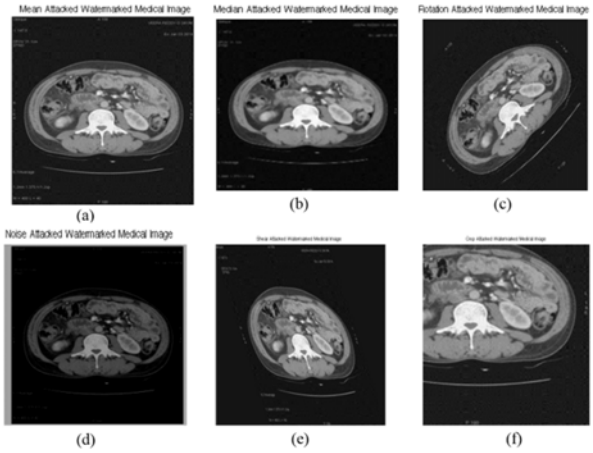


Figure-11. CT watermarked images with DWT-ANN algorithm under attacks (a) Mean filter, (b) Median Filter, (c) Rotation (45^0), Salt and pepper noise (Var=0.02),(e) Shear (x=1) (f) Crop attack.

The primary distinction between the two algorithms can be understood by looking at the Figures 5 and 6. Figure-5 is the embedding procedure for non-intelligence based medical image watermarking and Figure-6 for intelligence based watermarking respectively.

To see this concept in algorithm design that makes a difference in embedding - extraction process without attacks and with attacks, we implemented all the systems in MATLAB R13. Figure-7 shows non-intelligence based RSA-DWT algorithms and Figure-8 shows intelligence based DWT-ANN algorithm respectively. The Figures 7 and 8 display results for MRI medical images as cover images and Lena image as patient image.

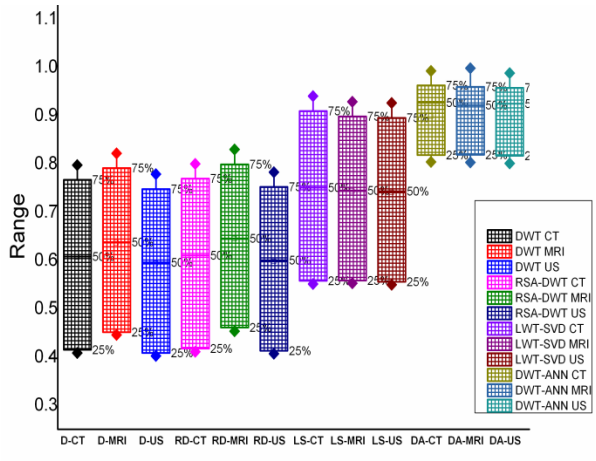


Figure-12. Dynamic range of ncc values of extracted watermarked medical images after attacks for comparing non intelligent and intelligent watermarking algorithms.

Let's compare in Figure 7(c), (d) and (e) with the same indexed terms in Figure-8. We can see that visual quality of intelligent watermarking methods score high when compared to non-intelligent medical imaging algorithms. On the other hand, comparing peak signal-to-noise ratios (psnr) and ncc of Figures 10 and 11 compare results consisting of medical watermarked images extracted at the destination after attacks the two methods for different types of medical images reveals that intelligent image watermarking has superior performance over their non-intelligent contour parts as shown in Figure-9 from non-intelligence and intelligence based medical image watermarking algorithms.

Figures 10 and 11 makes a world of difference to the life of patient in telemedicine applications. Figure-12 shows dynamic range of ncc values of extracted watermarks after the watermarked images were attacked. The figure shows a low dynamic range of ncc values for intelligence based algorithms. This explains why intelligence based algorithms with stand attacks effectively. The lower dynamic range does not give too much space to attack and can reconstruct the lost portions as in case of noise attack in Figure 10(d) and 11(d).

A total of 10 watermarking algorithms were

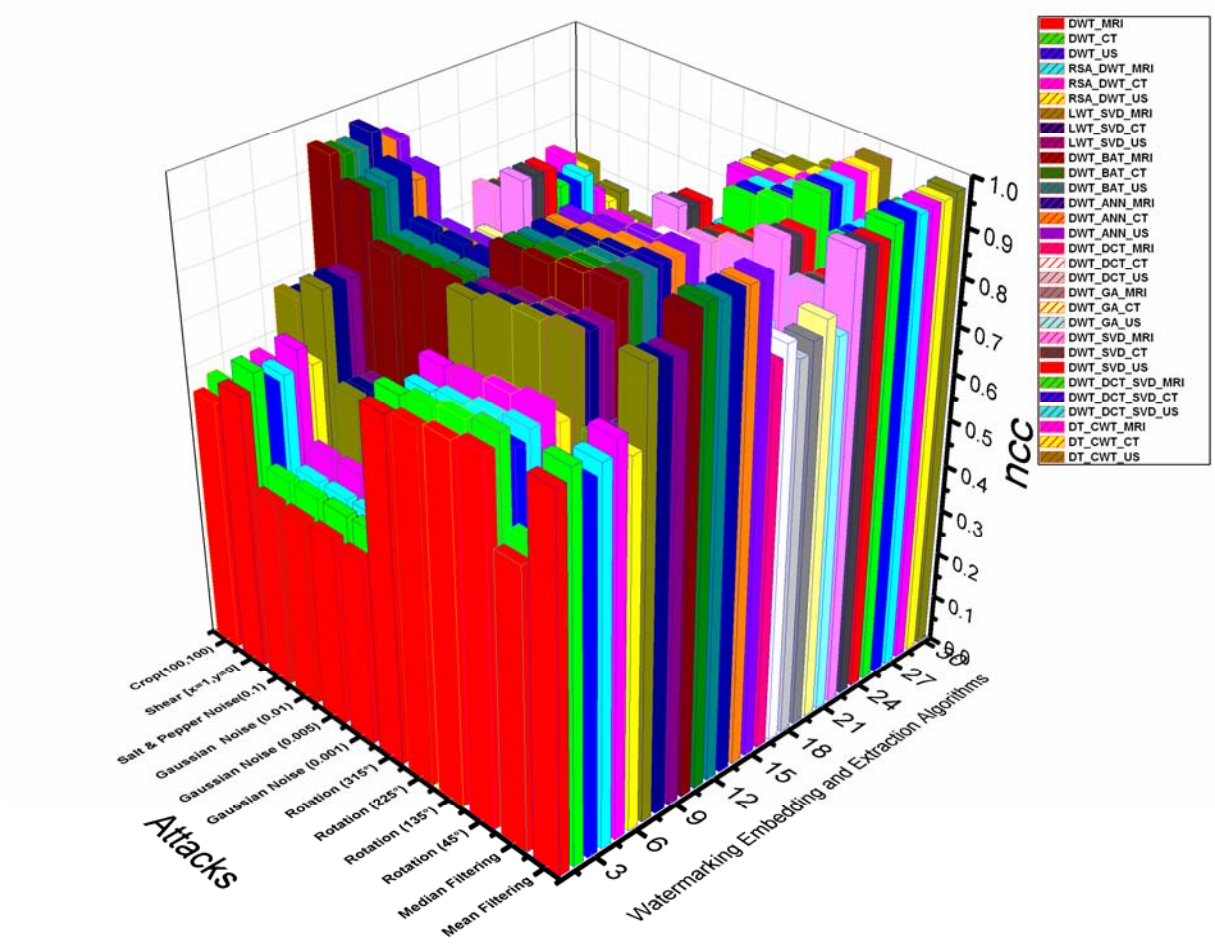


Figure-13. Normalized cross correlation based performance plot for various medical image watermarking algorithms with patient image as payload.

tested for three sets of each containing 20 medical images. These are MRI, CT and US images collected from NRI Medical College and Hospital which are used as cover images. The watermarked image is a Lena image. Normalized cross correlation coefficients for watermarking extraction process under 12 different types of attacks are computed and the values are plotted for ten medical image watermarking algorithms in Figure-13. The Medical image watermarking algorithms used are DWT[134], RSA-DWT [139], LWT-SVD [135], DWT-BAT [149], DWT-ANN [141], DWT-DCT [73], DWT-GA [91], DWT-SVD [111], DWT-DCT-SVD [88] and DT-CWT [72].

Observations on box plot in Figure-8 reveals some interesting performance criterion of watermarking algorithms under attacks. Only intelligence based algorithms perform well under attacks compared to the non-intelligence algorithms. Intelligent watermarking algorithms are neural networks, genetic algorithm and BAT algorithm based methods for watermarking.

5. CONCLUSIONS

This work reviews the watermarking algorithms and in particular medical image watermarking during the past decade. For this review three types of medical images are used such as MRI, CT and Ultrasound images are cover images. Lean image is used as a patient image i.e. as a watermark. A few conclusions were drawn based on this work. Watermarking medical images is of two kinds, ROI and NOR-ROI based in spatial domain. In transform domain DWT is most widely used for medical image watermarking. But only one transform for watermarking fails to withstand attacks. Hence researchers used a combination of algorithms such DWT-DCT, DWT-DCT-SVD etc. for watermarking. But these work observers that this combination fails when the user want to extract and use the cover image, here in this case is a lifesaving medical image. Hence the research started looking towards heuristic and artificial intelligence based approaches to with stand attacks and produce understandable informative cover images. These methods are called intelligent watermarking algorithms. A performance comparison was made based on normalized cross correlation coefficient

between non intelligent and intelligent based medial image watermarking algorithms. From this review we conclude that intelligence based watermarking algorithms are the state of the art in protecting medical information during transit through unsecured data networks.

REFERENCES

[1] J Podilchuk, I. Christine and WenjunZeng. 1998. Image-adaptive watermarking using visual models. IEEE Journal on Selected Areas in Communications. 16(4):525-539.

[2] Hartung, Frank and Martin Kutter. 1999. Multimedia watermarking techniques. Proceedings of the IEEE 87. pp. 1079-1107.

[3] Antonini Marc, et al. 1992. Image coding using wavelet transform. Image Processing, IEEE Transactions on. 12: 205-220.

[4] Wei Z. H., P. Qin and Y. Q. Fu. 1998. Perceptual digital watermark of images using wavelet transform. IEEE Transactions on Consumer Electronics. 44(4): 1267-1272.

[5] Digital Watermarking in Medical Images, A Thesis Submitted for the Degree of Doctor of Philosophy, School of Information Systems, Computing and Mathematics Brunel University, November 2005.

[6] S. Kiran, K.V. Nadhini Sri, J. Jaya. 2013. Design and implementation of FPGA based invisible image watermarking encoder using wavelet transformation. 2013 International Conference on Current Trends in Engineering and Technology (ICCTET). pp. 323-325.

[7] S.Sharma, J.Kaur, S.Gupta. 2013. Improved modified fast Haar Wavelet transformation [MFHWT] based visible watermarking. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).

[8] Zhang Fan, Zhang Hongbin. 2004. Capacity and reliability of digital watermarking. 2004 International Conference on Business of Electronic Product Reliability and Liability. pp. 162-165.

[9] Qing Liu, Jun Ying. 2012. Grayscale image digital watermarking technology based on wavelet analysis. 2012 IEEE Symposium on Electrical and Electronics Engineering (EEESYM). pp. 618-621.

[10] S.Sarkar, K.Senthilkumar. 2012. A highly secured Digital Watermarking Algorithm for Binary Watermark using Lifting Wavelet Transform and Singular Value Decomposition. IET Chennai 3rd International on Sustainable Energy and Intelligent Systems (SEISCON. 2012, 27-29 December) pp.1-5.

[11] M. Steinebach, E.Hauer, P. Wolf. 2007. Efficient Watermarking Strategies. Third International Conference on Automated Production of Cross Media content for multi-channel Distribution, AXMEDIS '07. pp. 65-71.

[12] Xinmin Zhou, Zhicheng Wang, Weidong Zhao, Jianping Yu. 2009. Attack Model of Text Watermarking Based on Communications. 2009 International Conference on Information Management, Innovation Management and Industrial Engineering. pp. 283-286.

[13] Qing Chen, Yufei Zhang, Limin Zhou, Xiaodi Ding, Zhe Fu. 2011. Word text watermarking for IP protection and tamper localization. 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC). pp. 3595-3598.

[14] G.C. Langelaar, R. L. Lagendijk. 2001. Optimal differential energy watermarking of DCT encoded images and video. Image Processing, IEEE Transactions on. 10(1): 148-158.

[15] S. H.Low, N.F. Maxemchuk. 1998. Performance comparison of two text marking methods. Selected Areas in Communications, IEEE Journal on. 16(4): 561-572.

[16] D.J.Coumou, G.Sharma. 2008. Insertion, Deletion Codes with Feature-Based Embedding: A New Paradigm for Watermark Synchronization with Applications to Speech Watermarking. IEEE Transactions on Information Forensics and Security. 3(2): 153-165.

[17] Huijuan Yang, AC.Kot. 2004. Text document authentication by integrating inter character and word spaces watermarking. 2004 IEEE International Conference on Multimedia and Expo, 2004.ICME '04, 30-30. pp. 955-958.

[18] E.C.Chang, M.Orchard. 2000. Geometric properties of watermarking schemes. 2000 International Conference on Image Processing, 2000.Proceedings. pp. 714-717.

[19] Yuanwei Lao, Y.F. Zheng. 2006. Towards Optimal Rate Allocation for Logo Watermarking Using Reversible DWT. 2006 IEEE International Conference on Information Acquisition. pp. 256-261.

[20] Lingna Hu, Lingge Jiang. 2007. Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images. Second International Conference on Communications and Networking in China, 2007.CHINACOM '07, 22-24. pp. 413-416.

[21] Lingna Hu, Lingge Jiang. 2007. Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images. Second International Conference on Communications and Networking in China, 2007.CHINACOM '07, 22-24. pp. 413-416.

[22] Fang Ma, JianPing Zhang, Wen Zhang. 2012. A Blind Watermarking Technology Based on DCT Domain. 2012 International Conference on Computer Science and Service System (CSSS). pp. 397-400.

[23] Shao Feng an, C.Wang. 2009. A computation structure for 2-D DCT watermarking. 52nd IEEE International Midwest Symposium on Circuits and Systems, 2009.MWSCAS '09. pp. 577-580.

[24] Jun Xiao, Ying Wang. 2008. Toward a Better Understanding of DCT Coefficients in Watermarking. Pacific-Asia Workshop on Computation Intelligence and Industrial Application, 2008.PACIIA '08. 2: 206-209.

[25] C.V.Serdean, M.K.Ibrahim, A.Moemeni, M.M.Al-Akaidi. 2007. Wavelet and multiwavelet watermarking. Image Processing, IET. 1(2): 223-230.

[26] Chi-Man Pun. 2007. Image Classification using Wavelet Watermarking Representation. 2007 International Conference on Machine Learning and Cybernetics. 3: 1493-1497.

[27] S.E. El-Khamy, M. Lotfy, R.ASadek. 2003. A block based wavelet watermarking technique for copyright protection and authentication. 2003 IEEE 46th Midwest Symposium on Circuits and Systems. 1: 90-93.

[28] K.M. Parker, J.E. Fowler. 2005. Redundant-wavelet watermarking with pixel-wise masking. IEEE International Conference on Image Processing.ICIP 2005.pp. I685-I688.

[29] Rong Pan, YouxingGao. 2002. A new wavelet watermarking technique. Proceedings of the 4th World Congress on Intelligent Control and Automation. pp. 2065-2069.

[30] Liang Du, Jianjun Zhang, Xinge You. 2009. An image watermarking scheme using new wavelet filter banks. 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, 2009.ASID. pp. 148-151.

[31] J. Mayer. 2011. Improved Spread Spectrum multibit watermarking. 2011 IEEE International Workshop on Information Forensics and Security (WIFS). pp. 1-6.

[32] K. Imabeppu, D. Hamada, M.Unoki. 2009. Embedding Limitations with Audio-watermarking Method Based on Cochlear-delay Characteristics. Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009.IIH-MSP '09. pp. 82-85.

[33] O.O. Khalifa, Y. bintiYusof, A-H. Abdalla, R.F. Olanrewaju. 2012. State-of-the-art digital watermarking attacks. 2012 International Conference on Computer and Communication Engineering (ICCCE). pp. 744-750.

[34] S. Vellaisamy, V. Ramesh. 2014. Inversion attack resilient zero-watermarking scheme for medical image authentication. Image Processing, IET. 8(12): 718-727.

[35] Nikolaidis, S. Tsekeridou, A. Tefas, V. Solachidis. 2001. A survey on watermarking application scenarios and related attacks. 2001 International Conference on Image Processing, 2001.Proceedings. pp. 991-994.

[36] AH. Taherinia, M. Jamzad. 2011. EWA: An exemplar-based watermarking attack. 2011 International Conference on Information Technology and Multimedia (ICIM). pp. 1-5.

[37] AH. Taherinia, M. Jamzad. 2009. A new adaptive watermarking attack in wavelet domain. Multimedia, Signal Processing and Communication Technologies, 2009.IMPACT '09.International. pp. 320-323.

[38] Wong, Ping Wah, and NasirMemon. 2001. Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Transactions on Image Processing. 10(10): 1593-1601.

[39] N. A. Memon, S. A. M Gilani, S. Qayoom. 2009. Multiple watermarking of medical images for content authentication and recovery. IEEE 13th International on Multitopic Conference, 2009.INMIC 2009. pp. 1-6.

[40] AJ.Maeder, B.M. Planitz. 2005. Medical image watermarking for multiple modalities. 2005 34th Proceedings on Applied Imagery and Pattern Recognition Workshop. 6: 160-165.

[41] s. Tachakra, s.t.h.mullett, r.freij and A. sivakumar, 1996. Confidentiality and ethics in telemedicine, Journal of Telemedicine and Telecare. 2(1): 68-71.

[42] G. Coatrieux. 2000. Relevance of watermarking in medical imaging. 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine, Proceedings, IEEE.

[43] Giakoumaki, S. Pavlopoulos, D. Koutsouris. 2004. A Multiple Watermarking Scheme Applied to Medical Image Management. 26th Annual International Conference of the Engineering in Medicine and Biology Society, IEMBS '04. IEEE. pp. 3241-3244.

[44] G. Coatrieux. 2006. A review of image watermarking applications in healthcare. 28th Annual International Conference of the Engineering in Medicine and Biology Society, EMBS'06. IEEE.

[45] Shih, Y. Frank, and Wu.Yi-Ta. 2005. Robust watermarking and compression for medical images based on genetic algorithms. Information Sciences. 175(3): 200-216.

[46] M.T. Naseem, IM. Qureshi, Atta-ur-Rahman, M.Z. Muzaffar,. 2012. Robust watermarking for medical images resistant to geometric attacks. 2012 15th International conference on Multitopic Conference (INMIC). pp. 224-228.

[47] AnandDeepthi and U. C. Niranjan. 1998. Watermarking medical images with patient information. 20th Annual International Conference of IEEE on Engineering in Medicine and Biology Society. pp. 703-706.

[48] Zain M. Jasni, and Abdul RMFauzi. 2006. Medical image watermarking with tamper detection and recovery. 28th Annual International Conference of IEEE on Engineering in Medicine and Biology Society, 2006.EMBS'06. pp. 3270-3273.

[49] K. A. Navas, and M. Sasikumar. 2007. Survey of medical image watermarking algorithms. In: Proc. International Conf. Sciences of Electronics, Technologies of Information and Telecommunications, pp. 25-29.

[50] JalilZunera and Anwar M. Mirza. 2009. A review of digital watermarking techniques for text documents. IEEE International Conference on Information and Multimedia Technology, 2009.ICIMT'09. pp. 230-234.

[51] E.T. Lin and E.J. Delp. 1999. A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS \'99.pp. 274 -278.

[52] Boney Laurence, Ahmed H. Tewfik and Khaled N. Hamdy. 1996. Digital watermarks for audio signals. The Third IEEE International Conference on Multimedia Computing and Systems. pp. 473-480.

[53] Wolfgang Raymond B., Christine I. Podilchuk and Edward J. Delp. 1999. Perceptual watermarks for digital images and video. Proceedings of the IEEE. 87(7): 1108-1126.

[54] Shih, Y. Frank, and Wu. Scott YT. 2003. Combinational image watermarking in the spatial and frequency domains."Pattern Recognition. 36(4): 969-975.

[55] Tao Peining and Ahmet M. Eskicioglu. 2004. A robust multiple watermarking scheme in the discrete wavelet transform domain. Optics East.International Society for Optics and Photonics.

[56] Nikolaidis Nikos and Ioannis Pitas. 1998. Robust image watermarking in the spatial domain. Signal processing. 66(3): 385-403.

[57] Lu, Zhe-Ming, et al. 2003. Semi-fragile image watermarking method based on index constrained vector quantisation. Electronics Letters. 39(1): 35-36.

[58] E.T. Lin and E.J. Delp. 1999. A Review of Fragile Image Watermarks. Proceedings of the Multimedia and Security Workshop at ACM Multimedia\'99. pp. 35-39.

[59] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec. 2000. Relevance of watermarking in medical imaging. 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. pp. 250-255.

[60] G. Coatrieux, E. Chazard, R. Beuscart, C. Roux. 2011. Lossless watermarking of categorical attributes for verifying medical data base integrity. Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE. pp. 8195-8198.

[61] Giakoumaki S. Pavlopoulos and D. Koutouris. 2003. A medical image watermarking scheme based on wavelet transform. In Engineering in medicine and biology society, 2003.Proceedings of the 25th annual international conference of the IEEE. pp. 856-859.

[62] Lou, Der-Chyuan, Ming-Chiang Hu, and Jiang-Lung Liu. 2009. Multiple layer data hiding scheme for medical images. Computer Standards & Interfaces. 31(2): 329-335.

[63] H. Nyeem, W. Boles, C. Boyd. 2013. Utilizing Least Significant Bit-Planes of RONI Pixels for Medical Image Watermarking. 2013 International Conference

on Digital Image Computing: Techniques and Applications (DICTA). pp. 1-8.

[64] R. Eswaraiah, E.S. Reddy. 2014. A Fragile ROI-Based Medical Image Watermarking Technique with Tamper Detection and Recovery. 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT). pp. 896-899.

[65] Tai, Wei-Liang, Chia-Ming Yeh and Chin-Chen Chang. 2009. Reversible data hiding based on histogram modification of pixel differences. IEEE Transactions on Circuits and Systems for Video Technology. 19(6): 906-910.

[66] Irany Behrang Mehrbany, Xin Cindy Guo and Dimitrios Hatzinakos. 2011. A high capacity reversible multiple watermarking scheme for medical images. 2011 IEEE 17th International Conference on Digital Signal Processing (DSP). pp. 1-6.

[67] Lavanya A. and V. Natarajan. 2012. Watermarking patient data in encrypted medical images. Sadhana. 37(6).

[68] Inoue H., Miyazaki A., Yamamoto A. and Katsura T. 1998, October. A digital watermark based on the wavelet transform and its robustness on image compression. 1998 International Conference on In Image Processing, ICIP 98, 2: 391-395.

[69] WakataniAkiyoshi. 2002. Digital watermarking for ROI medical images by using compressed signature image. IEEE 35th Annual Hawaii International Conference on System Sciences, 2002.HICSS. pp. 2043-2048.

[70] Hyung-Kyo Lee, Hee-Jung Kim, Seong-Geun Kwon, Jong-Keuk Lee. 2005. ROI Medical Image Watermarking Using DWT and Bit-plane. 2005 Asia-Pacific Conference on Communications. pp. 512-515.

[71] Adiwijaya P.N., FaoziyahF.P., PermanaT.AB., Wirayuda U.N. Wisesty. 2013. Tamper detection and recovery of medical image watermarking using modified LSB and Huffman compression. 2013 Second International Conference on Informatics and Applications (ICIA). pp. 129-132.

[72] R.M. Kongo, L. Masmoudi, N. Idrissi, N. Hassanain, M. Cherkaoui, A. Roukhe. 2012. A medical image watermarking scheme based on dual-tree wavelet transform. 2012 Second International Conference on Innovative Computing Technology (INTECH). pp. 144-152.

[73] Yaoli Liu, Jingbing Li. 2012. The medical image watermarking algorithm using DWT-DCT and logistic.2012 7th International Conference on Computing and Convergence Technology (ICCCT). pp. 599-603.

[74] H. Trichili, M. Bouhlel, N. Derbel and L. Kamoun. 2002. A new medical image watermarking scheme for a better telediagnosis, Proceedings of IEEE International Conference on Systems, Man and Cybernetics, Yasmine Hammamet, Tunisia. pp. 557-560.

[75] B. Macq, and F. Dewey. 1999. Trusted Headers for Medical Images, DFGVIIII-DIIWatermarking Workshop, Erlangen, Germany.

[76] K.A, Navas, M. Sasikumar, S. Sreevidya. 2007. A Benchmark for Medical Image Watermarking. 14th International Workshop on Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. pp. 237-240.

[77] K. Renaud. 2009. Web Authentication Using Mikon Images. Privacy, Security, Trust and the Management of e-Business, 2009.CONGRESS '09.World Congress on. pp. 79-88.

[78] S. Boucherkha, M. Benmohamed. 2006. A Multi-Tier Architecture to Safely Share Digital Medical Images. International Conference on Dependability of Computer Systems, Dep Cos-RELCOMEX '06, pp. 319-326.

[79] Chunhua Dong, Huaiqiang Zhang, Jingbing Li, Yen-wei Chen. 2011. Robust zero-watermarking for medical image based on DCT. 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT). pp. 900-904.

[80] IF.Kallel, M. Kallel, M.-S.Bouhlel. 2006. A Secure Fragile Watermarking Algorithm for medical Image Authentication in the DCT Domain. Information and Communication Technologies.ICTTA '06. 2nd, pp. 2024-2029.

[81] Lin Gao, TiegangGao, Guorui Sheng, Yanjun Cao, Li Fan. 2012. A new reversible watermarking scheme based on Integer DCT for medical images. 2012 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR). pp. 33-37.

[82] M.AHajjaji, E.-B.Bourennane, A .Mtibaa, G. Ochoa-Ruiz. 2013. A digital watermarking algorithm based on quantization of the DCT: Application on medical imaging. 2013 International Conference on Control,

Decision and Information Technologies (CoDIT). pp. 372-377.

[83] M.AHajjaji, A. Mtibaa, E. Bourennane. 2011. A Watermarking of Medical Image-New Approach Based On Multi-Layer Method. 33-41, International Journal of Computer Science Issues, 8(4).

[84] G. Pradeepkumar, S. Usha. 2013. Effective watermarking algorithm to protect Electronic Patient Record using image transform. 2013 International Conference on Information Communication and Embedded Systems (ICICES). pp. 1030-1034.

[85] Umaamaheshvari and Dr. K. Thanushkodi. 2011. An Effective Watermarking Scheme for Medical Images Using Hybrid Transform (DCT-DWT). Vol. 5.2011 in IJCSES.

[86] Jingbing Li, Chunhua Dong, Mengxing Huang, Yong Bai, Huaiqiang Zhang. 2012. The medical images watermarking using DWT and Arnold. 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE). pp. 27-31.

[87] Chunhua Dong, Jingbing Li, Yen-wei Chen. 2012. A DWT-DCT Based Robust Multiple Watermarks for Medical Image. 2012 Symposium on Photonics and Optoelectronics (SOPO). pp. 1-4.

[88] N. Dey, P. Das, AB. Roy, A. Das, S.S. Chaudhuri. 2012. DWT-DCT-SVD based intravascular ultrasound video watermarking. 2012 World Congress on Information and Communication Technologies (WICT). pp. 224-229.

[89] M.M. Soliman, A .ellaHassanien, H.M. Onsi. 2012. An adaptive medical images watermarking using Quantum Particle Swarm Optimization. 2012 35th International Conference on Telecommunications and Signal Processing (TSP). pp. 735-739.

[90] Z. Shaomin and J. Liu. 2009. A novel adaptive watermarking scheme based on human visual system and particle swarm optimization. Information Security Practice and Experience, Lecture Notes in Computer Science, LNCS. 5451, pp. 136-146.

[91] Hsiang-Cheh Huang, Ting-Hsuan Wang, Yueh-Hong Chen, Jui-Pin Hung. 2013. Prediction-Based Reversible Data Hiding for Medical Images with Genetic Algorithms. 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp. 5-8.

[92] V.E. Jayanthi, V.M. Selvalakshmi, V. Rajamani. 2009. Digital watermarking robust to geometric distortions in biomedical images. 2009 International Conference on Control, Automation, Communication and Energy Conservation, 2009.INCACEC 2009, pp. 1-6.

[93] Ping Dong, Jovan G. Brankov and Yongyi Yang. 2005. Digital Watermarking Robust to Geometric Distortions. IEEE Trans. Image Processing. 14(12).

[94] M. Kutter and F. A. P. Petitcolas. 1999. A fair benchmark for image watermarking systems. Electronic Imaging '99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA, 25(27 January 1999).The International Society for Optical Engineering.

[95] Jingbing Li, Yong Bai, Wencai Du, Yen-wei Chen. 2011. 3D DWT-DCT based multiple watermarks for medical volume data robust to geometrical attacks. 2011 International Conference on Electronics, Communications and Control (ICECC). pp. 605-609.

[96] Yujia Li, Jingbing Li. 2013. The robust medical volume data watermarking based on DCT compressed domain. 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC). pp. 2209-2212.

[97] Shewen Sun, Song Wei, Cong Wang. 2009. DPCC and QR factorization-based color medical image authentication algorithm. International Conference on Image Analysis and Signal Processing, 2009.IASP 2009, pp. 81-84.

[98] P. Suapang, S. Yimmun, A. Puditkanawat. 2011. Web-based Medical Image Archiving and Communication System for Teleimaging. 2011 11th International Conference on Control, Automation and Systems (ICCAS), pp. 172-177.

[99] Su Jin Lee, Moon Hae Kim. 2002. KoMIPS: A Web-based medical image processing system for telemedicine applications. TENCON '02.Proceedings.2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. pp. 569-572.

[100] D. Osborne, D. Rogers, J. Mazumdar, R. Coutts, D. Abbott. 2002. An Overview of Wavelets for Image Processing for Wireless Applications. Proceedings of SPIE: Smart Structures, Devices and Systems, University of Melbourne, Australia. 4935: 427-435.

[101] P. V. V. Kishore and P. Rajesh Kumar. 2012. A Video Based Indian Sign Language Recognition System (INSLR) Using Wavelet Transform and Fuzzy Logic. IACSIT International Journal of Engineering and Technology. 4(5).

[102] P. V. V. Kishore. 2011. Video Audio Interface for Recognizing Gestures of Indian Sign. International Journal of Image Processing (IJIP). 5(4): 479-500.

[103] Ming-Shing Hsieh, Din-Chang Tseng, Yong-Huai Huang. 2001. Hiding digital watermarks using multiresolution wavelet transform. Industrial Electronics, IEEE Transactions on. 48(5): 875-882.

[104] Jianyong Huang, Changsheng Yang. 2004. Image digital watermarking algorithm using multiresolution wavelet transform. 2004 IEEE International Conference on Systems, Man and Cybernetics. pp. 2977-2982.

[105] S. Sarkar, K. Senthilkumar. 2012. A highly secured Digital Watermarking Algorithm for Binary Watermark using Lifting Wavelet Transform and Singular Value Decomposition. IET Chennai 3rd International on Sustainable Energy and Intelligent Systems (SEISCON 2012). pp. 1-5.

[106] K. Loukhaoukha, J.-Y. Chouinard. 2009. Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification. 11th Canadian Workshop on Information Theory, 2009.CWIT 2009. pp. 177-182.

[107] Li Lizong, GaoTiegang, GuQiaolun, Bi Lei. 2010. A Verifiable Copyright-Proving Scheme Based on Lifting Wavelet Transformation. 2010 Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI). pp. 68-72.

[108] K. Ghaderi, F. Akhlaghian, P. Moradi. 2013. A new robust semi-blind digital image watermarking approach based on LWT-SVD and fractal images. 2013 21st Iranian Conference on Electrical Engineering (ICEE). pp. 1-5.

[109] Andrews C. Harry, C. Patterson. 1976. Singular Value Decomposition (SVD) Image coding. IEEE Transactions on Communications. 24(4): 425-432.

[110] AB. Jeng, Li-Chung Chang, Hong-Jhe Li. 2010. Exploring better parameter set for singular value decomposition (SVD) hashing function used in image authentication. 2010 International Conference on Machine Learning and Cybernetics (ICMLC). pp. 2600-2604.

[111] Li Qiang, Chun Yuan and Yu-ZhuoZhong. 2007. Adaptive DWT-SVD domain image watermarking using human visual model. IEEE 9th International Conference on Advanced Communication Technology.

[112] YavuzErkan and ZiyaTelatar. 2007. Improved SVD-DWT based digital image watermarking against watermark ambiguity. Proceedings of the 2007 ACM symposium on applied computing. ACM.

[113] Li, Guohui. 2007. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. 2007 IEEE International Conference on Multimedia and Expo.

[114] Yin, Cheng-qun. 2007. Color image watermarking algorithm based on DWT-SVD. 2007 IEEE International Conference on Automation and Logistics.

[115] B. Jagadeesh, S.S. Kumar, K.R. Rajeswari. 2009. A Genetic Algorithm Based Oblivious Image Watermarking Scheme Using Singular Value Decomposition (SVD). First International Conference on Networks and Communications, 2009.NETCOM '09. pp. 224-229.

[116] Sweldens. 1998. The lifting scheme: A construction of second generation wavelets. SIAM Journal on Mathematical Analysis. 29(2): 511-546.

[117] Boscher Arnaud, Robert Naciri and Emmanuel Prouff. 2007. CRT RSA algorithm protected against fault attacks. Information Security Theory and Practices.Smart Cards, Mobile and Ubiquitous Computing Systems.Springer Berlin Heidelberg. pp. 229-243.

[118] Barrett Paul. 1987. Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. Advances in cryptology-CRYPTO'86. Springer Berlin Heidelberg.

[119] 2002. Washington, C. Lawrence, and Wade Trappe, Introduction to cryptography: with coding theory. Prentice Hall PTR.

[120] S.N. Sivanandam, M. Paulraj an Introduction to Neural Networks, Vikhas Publications Company Ltd. India. 2003.

[121] J.S. Bhalla, A. Aggarwal. 2013. A novel method for medical disease diagnosis using artificial neural networks based on backpropagation algorithm. Confluence 2013: 4th International Conference on Next Generation Information Technology Summit. pp. 55- 61.

[122] AL. Paul, P.C. Byrne. 1990. An efficient learning algorithm for the backpropagation artificial neural network. Southeastcon '90.Proceedings.IEEE, 63a 1: 61-63.

[123] M. I El Adawy, M.E. Aboul-Wafa, H. A Keshk, M. M. El Tayeb. 2002. A SOFT-backpropagation algorithm for training neural networks. Radio Science Conference, 2002.(NRSC 2002).Proceedings of the Nineteenth National. pp. 397-404.

[124] Shi-chun Mei, Ren-hou Li, Hong-mei Dang, Yun-kuan Wang. 2002. Decision of image watermarking strength based on artificial neural-networks. 9th International Conference on Neural Information Processing, 2002.ICONIP '02, pp. 2430-2434.

[125] T.Schmidt, H. Rahnama, A.Sadeghian. 2008. A review of applications of artificial neural networks in cryptosystems. Automation Congress, 2008.WAC 2008.World, September 28 2008-October. pp.1-6.

[126] A.Al-Gindy. 2010.A fragile invertible watermarking technique for the authentication of medical images. 2010 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp. 191-195.

[127] X.-S. Yang. 2010. A New Metaheuristic Bat-Inspired Algorithm, in: Nature Inspired Cooperative Strategies for Optimization (NISCO 2010) (Eds. J. R. Gonzalez et al.), Studies in Computational Intelligence, Springer Berlin, 284, Springer. pp. 65-74.

[128] Xin-She Yang and Amir H. Gandomi. 2012. Bat Algorithm: A Novel Approach for Global Engineering Optimization, Engineering Computations. 29(5): 464-483.

[129] YufengZheng, Edward A. Essock, Bruce C. Hansen, Andrew M. Haun. 2007. A new metric based on extended spatial frequency and its application to DWT based fusion algorithms. International Journal of Information Fusion. 8(2): 177-192.

[130] A.M.L. Lanzolla, G. Cavone, M. Savino, M. Spadavecchia. 2011. Analysis of influence parameters on image quality in ultrasound examination", Proc. of MeMeA, Bari, Italy, pp. 238-240.

[131] Z. Wang, A.C. Bovik. 2002. A universal image quality index. IEEE Signal Process.Lett. 9(3): 81-84.

[132] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli. 2004. Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. 13(4): 600-612.

[133] Zhou. W, A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity. IEEE Trans. on Img. Processing, 13(4): 600-612.

[134] N. Venkatram, L.S.S. Reddy, P.V.V. Kishore. 2014. Medical Image Watermarking using Wavelet Transform for Telemedicine Applications. CiiT International Journal of Digital Image Processing, ISSN 0974-9586, (IF 1.352). 6(1): 6-15.

[135] N. Venkatram, L.S.S. Reddy, P.V.V. Kishore. 2014. Blind Medical Image Watermarking using Lifting Wavelet Transform and Signgular Value Decomposition for Telemedicine Applications. WSEAS Transactions on Signal Processing, Greece, Print ISSN: 1790-5052, E-ISSN: 2224-3488, 10: 281-300.

[136] Voloshynovskiy S. Pereira, T. Pun, J.Eggers and J. Su. 2001. Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE Communications Magazine. 39(8): 118-126.

[137] Voloshynovskiy S., Pereira, V. Iquise and T. Pun. 2001. Attack modelling: Towards a second generation watermarking benchmark. Signal Process. 81(6): 1177-1214.

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

[139] N. Venkatram, L.S.S. Reddy, P.V.V. Kishore. 2014. Rsa-Dwt Based Medical Image Watermarking For Telemedicine Applications. Journal of Theoretical and Applied Information Technology (JATIT), ISSN: 1817-3195/ ISSN: 1992-8645. 65(2).

[140] N. Venkatram, L.S.S. Reddy, P.V.V. Kishore. 2014. Rsa-Dwt Based Medical Image Watermarking For Telemedicine Applications. IEEE Conference on Networks and Communications, August 19-20, Vignan University.

[141] P.V.V. Kishore, K.SaiPrajwal, M.Kamal Mohan, S. Koteswarao. 2015. Medical Image Watermarking with ANN in wavelet Domain. IEEE International conference on Electronics, Computing and Communication Technologies, CONECCT-2015, 10-11, IIIT Bangalore, India.

[142] P.V.V. Kishore, P.DheerajSrivathsav, M.Manikanta, N. Venkatram, L.S.S. Reddy, Goutham. E.N.D, D.Kimila Devi, A.S.C.S. Sastry. 2015. Medical Image Watermarking with Psnr Optimization in Wavelet Domain Based On Bat Algorithm. Journal of Theoretical and Applied Information Technology (JATIT), ISSN: 1817-3195/ ISSN: 1992-8645, 81(2).