IJCSN International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014
ISSN (Online) : 2277-5420 www.IJCSN.org
**Impact Factor: 0.274**



# A Survey on Medical Image Watermarking Techniques

**[1] Balamurugan.G, [2] Dr.K.B.Jayarraman, [3] Arulalan.V**

[1, 3] MTECH Student,
Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology,
Pondicherry University, Pondicherry, INDIA

[2] Head of The Department,
Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology,
Pondicherry University, Pondicherry, INDIA

**Abstract -** Medical image watermarking is broadly recognized as a significant technique for enhancing data security, accuracy, authentication, image fidelity and content verification in the recent e-healthcare environment where medical images are stored, retrieved and broadcast over the networks. Medical image watermarking conserves image quality that is necessary for medical diagnosis and treatment. In this paper we highlight the essential needs of medical image watermarking with a review of developments and the significance of watermarking in medical information management**.**

**Keywords -** *Medical image watermarking, authentication, image fidelity, content verification, image quality.*

## 1. Introduction

Medical information system (MIS) in common consists of data about patients, diseases, hospitals, prescriptions and so forth. Hospital information management system (HIMS), picture archiving and communication system (PACS), electronic patient record (EPR), are some of the popular regulations generally referred in health system information management. Medical diagnosis systems are based on images such as CT scans, MRIs, ultrasounds or other image modalities. Information which are obtained from these images are associated with patient information such as study type, hospital logo and ID, machine name & ID, patient name or id, personal data diagnostic findings, and so forth (Raul, Feregrino-Uribe, Gershom, & Trinidad, 2007). The digital imaging, image format and communications in medicine (DICOM), is a commercial standard to storing the medical images in digital format designed by the National Electrical Manufacturers Association (NEMA).

The development of communications has resulted in a digital revolution that has opened new stream for the medical image storing, retrieving and transmitting. Current developments in internet and the growing popularity of the World Wide Web (WWW) have lead to the improved access to the biomedical information. Medical image database management systems help in distribution of patient data among medical practitioners and provide patients with easy access to their own information on health and diagnosis.

### 1.1. Relevance of Medical Imaging Watermarking

Modern health care we can increase the development of infrastructure, but it also increase the importance of privacy, security of information. Research and application of digital watermarking of multimedia has significant importance for protection of ownership rights, authenticity. Studies and application on watermarking has been extended to medical imaging as well, resulting in many implementation schemes since 2000. Watermarking is a sub discipline of data hiding (Miller, & Bloom, 2002), wherein useful retrievable information called watermark is embedded in a cover or host in an invisible way. Digital watermarking also has confirmed to be beneficial in medical imaging (MI) (Coatrieux, Maitre, Rolland and Colorec, 2000). Two main features of watermarking in MI are well familiar:

(i) Meta-data which is embedded as watermark in the images so that the image contains more helpful information with a perfect linking with the patient; and

(ii) Protection of the image is made possible with integrity control (Coatrieux, Lecornu, & Sankur, 2006).

Watermarking has been applied in multimedia with various goals, but it has restrictions in MI for several reasons. In MI, data quality is somewhat critical in nature,

the diagnosis and treatment are the primary goals. Any changes in the data in the MI due to payload of watermark may lead to distortion in image fidelity. So watermark technique should be aim at a reasonable trade-off among its three characteristics:

(i) payload or capacity,
(ii) Robustness against manipulations in general as well as malicious attacks, and
(iii) Imperceptibility or quality.

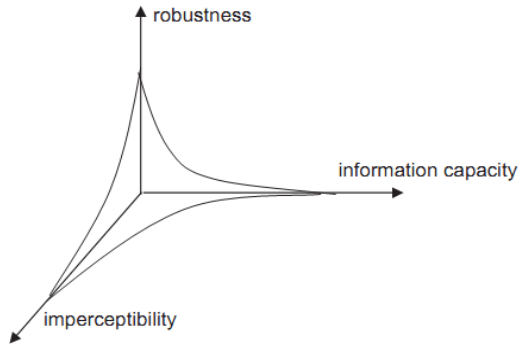


Figure 1: A Trade-Off Among the Features of Watermarking

These tradeoffs are represented in Figure 1. The payload or capacity data which is used as watermark are the data on images themselves, such as patient information, such that the watermark embedded in the medical image which enhances the reliability and assures the accurate linkage of all the information within the image. Thus, Meta data as watermark reduces the chance of incorrect linkage of a patient's data and his medical image.

### 1.2. Medical Information Assurance

The most important and necessary security features and characteristics recommended are confidentiality, reliability and availability (Raúl et al., 2007; Coatrieux et al., 2006; Coatrieux et al., 2000). Confidentiality means that only the allowed users have access to the information. Reliability is based on integrity and authenticity.

Integrity refers that the information is said to be integral without unauthorized modification, and authenticity is said to be a verification that the information belongs to the actual or truthful patient and originates from the right source (Coatrieux, Lecornu, & Sankur, 2006). There must be a high degree of confidence that the information is accurate ("A beginning to HIPAA," 2001). In MIS, these characteristics are preserved through five security services: availability, authenticity, integrity, confidentiality and non-repudiation.

## 2. Digital Watermarking in Medical Imaging

The role of watermarking in MI is to act as an edge to enhance the protection of content and, without disturbing or corrupting the quality of the data. Its role can also be comprehensive to the traceability from the origin to the destination. DICOM header can contain any metadata but watermark enhances the security of the image, as it is predictable to be a part of the image and at the same time is invisible. Information with access control can be selectively hidden for security reasons. In this medical is classified into two regions namely ROI (region of interest) and the RONI (region of non interest)

### 2.1. Main Watermarking Requirements

Any watermarking algorithm for authentication in MI should have the essential requirements of robustness, payload and imperceptibility. However in terms it is defined, as the quality in terms of perceptibility for human view or examination is of primary significance for medical images, the payload need not be high. It is also implicit that malicious attacks such as planned modification will be kept to a minimum in medical records by scheming access rights. Hence, robustness should be meant at attacks such as compression and data format conversions.

### 2.2. Medical Image Watermarking

Patient ID, name and any other concise particulars such as age, address, hospital logo, image number, doctor's remarks for diagnostic images, etc., can be used as watermarks for MI. DICOM header data can be used as a watermark. However, image as watermark is robust as textual characters are more fragile to attacks such as compression. Security issues is given as follow as for the CIA model.

| Security Requirement | Threats | Security measures |
|---|---|---|
| Confidentiality | Disclosures and re-routing of the information:<br>During transmission (e,, when an ill-intentioned person intercepts and illicitly copies tiles and records)<br>In the database (resulting in intrusion, identity usurpation, or Trojan horse virus that keeps an open access through the network) | Encryption of the data<br>Limiting lifetime of data<br>Private communication network (e,g., virtual private network)<br>Access control services (against unauthorized person, illegal copy, identity' usurpation, etc.) using smart card, firewall.<br>User control services for authenticating and identifying the user against identity usurpation, etc. |
| Reliability | Illicit destruction, production modification of the contents of files and records | One-way hash function or robust hash function or digital signature (DS)<br>Encryption of the data<br>File header, audit logs for recording of data transmission<br>Certification of communication partners |
| Availability | File management system disablement, destruction of a hard disk, or a malicious pirate who disrupts or alters surreptitiously the organization or content of the data | Access control services for writing, reading, and manipulation of data<br>User control services for authenticating and identifying the user against identity usurpation<br>Private communication network<br>Software accreditation, and use of antivirus and firewall for virus and malicious intrusion |

Table1: Security Requirements of Medical Image

## 3. Digital Watermarking - An Introduction

Watermarking is the skill of embedding secret data in other data called cover/host. Files of Multimedia such as audio, video, text and still images can be used as swarm information depending on the media of implementation. Watermark can be plain form or in encrypted text, a pseudo random binary image or a logo that is relevant and related to cover. Watermarking process consists of three levels: generation, embedding and extraction/detection. Watermarking varies from steganography in the intelligence that the embedding information known as watermark is relevant to the host or cover. In steganography, any data can be hidden in the given host. Cryptography improves security as an encrypted watermark is embedded as a substitute of the original watermark. Digital watermarking can be viewed as a

multidisciplinary subject, as the developments in computer vision , digital of image processing, and information theory have stated in a significant development in the theory and applications of watermarking. The concept of watermarking in the industry has been suitably adopted in the digital age and coined as electronic watermark. Cox et al. (2002) and Cox and Miller (2002) founded that "1954" as the birth of the electronic watermark, when a patient was filled for audio watermarking in music to protect his piracy. Since 1993, relevant research and applications have started in multimedia. However, watermarking applications in medical imaging might not progress seriously, as it was consideration that any embedding in medical image might reduce its quality. Since last decade, research in medical imaging under a digital environment highlighted the need for authenticity and security.

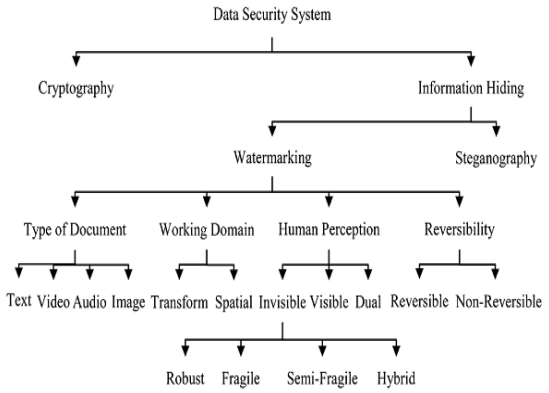


Figure 2. Classification of Data Security System

**According to types of document:**

**Image watermarking**: This is used to cover the special information added on the image and later detect and extract that special information for the author's rights.

**Video watermarking**: This adds watermark in the video stream to organize video applications. It is the expansion of image watermarking. This method needs real time removal and robustness for compression.

**Audio watermarking**: Its application area is one of the most popular and hot issue due to internet music, MP3.

**Text watermarking**: This adds watermark to the PDF, DOC and other text file to avoid the modifications made to the text. The watermark is inserted in the text file as font shape and the space between characters and line spaces.

**Graphic watermarking**: It establishes the watermark to 3D or 2D computer created graphics to show the copyright.

**According to the perceptivity**:

**Visible watermark:** Watermark that is visible in the digital information like printing a watermark on paper, for example television channels, like cartoon, whose symbol is visibly overlaid on the corner of the TV picture.

**Invisible watermarking:** There is an existing technique which can add data into an image which cannot be grasped, but can be hold with the right software.

**According to invisible watermarking:**

**Fragile watermark**: It unclear after slight changes or modification is applied. Fragile watermarks are mostly used for tamper detection.

**Semi fragile watermark**: It supports transformations, but it fails detection after malicious transformations. Normally those are used to detection of malignant transformations.

**Robust Watermark**: It resists a selected class of transformations. It may be used in copy protection applications and also to carry copy and no access control information.

**According to the domain:**

**In Spatial domain:** These domain attentions on altering the pixels of one or two randomly selected images subsets which directly loads the data into the pixels in image. The selected algorithms are SSM, LSB Modulation based technique are used.

**In Frequency domain:** This domain is also known as transforming domain. Principles of certain frequencies are changed from their original. Common used transform domain methods are DWT, DCT and DFT.

### 3.1.1 Implementation of Spatial Domain

The embedding watermark is added in the least significant bit (LSB) of the image pixel. Though these methods are not robust, they are simple and easy to implement and are satisfactory in an attack free environment and lossless compression

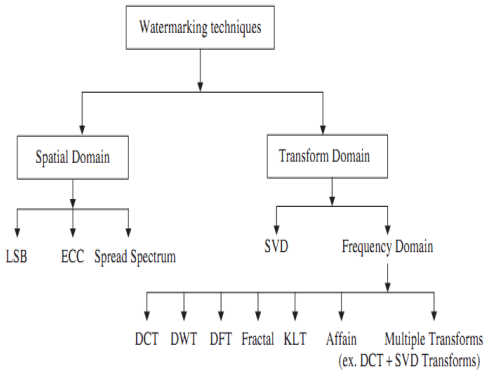


Figure 3 Types of Watermarking Technique Based on Domain

## A. LSB Technique

LSB hides information in the spatial domain. The image is in the form of matrix. Let NxM where N and M are the dimensions of the image and the pixel value is in the position (i, j) is in binary number format. This binary number can be then separated into a most significant bit (MSB) which contains relatively a lot of information and then the least significant bit (LSB) which contains very few information. We can make changes in the value of the LSB without any detectable distortion for the human user for the image is for example in gray scale, therefore we can take the LEAST SIGNIFICANT BIT of an image (the cover image) and change their value of the every pixel within the MSB of another image, that we like to embed in a secret or not detectable way in the cover image.

Following are the described steps are used to perform LSB
1. Select the cover image and the watermark image
2. Select number of bits of the cover image so that it can able to maintain the quality of the image. Image quality depends only on number of bits. If more bits are selected then it will depreciate the quality of the image.
3. Insert the MSB (most significant bits) of watermark or secrete image in LSB (least significant bits) of cover image.

For Example let us consider a grid for 3 pixels of a 24-bit image can be as follows:
(10110110 11111100 00110100)
(11011110 101100101 01101011)
(01010101 010111001 10110000)
When the number 302, which binary representation is 100101110 is embedded into the least significant bits of this part of the image, the resulting grid is as follows:
(10110111 11111100 00110101)
(11011111 10100100 01101011)
(01010101 01011101 10110000)
For detecting/extracting watermarking we examine through the image, get the least significant bits according the bits were used to store the secret image. The bits removed now become the most significant bits of secrete image.
For above example 100101110 is secrete image.

## B. SPREAD SPECTRUM (SS) WATERMARKING

In spatial domain, Spread spectrum (SS) watermarking using binary watermark is discussed in details in the following section. Various steps for watermark embedding are described as follows:

**Step1: Image Partitioning**
The cover image is in use as F, where F = {Fij, 1 i Flength, 1 j Fwidth}, while Fij ∈ {0, 1, 255}, Flength is the image length and Fwidth the width of image. Now we separate the cover image into (m x m) blocks which is non-overlapping, where m = 4, 8, 16, 32 etc. Suppose we call them as Hij, where 'i' is the number of rows and 'j' is the number of columns.

**Step 2: Formation of message vector**
The message image is taken as W, where W = {Wij, 1 I Wlength, 1 j Wwidth}, while Wij ∈ {0, 1}, Wlength is the image length and Wwidth the width of image. We divide the watermark image into (L x L) none overlapping blocks, where L = 2, 4, 8, 16 etc. We call them as Qij.

**Step 3: Formation of compare bit**
The MSB plane of 2-D pixel values of Hij is transformed to 1- D strings. This forms the string1. Another binary string, string2 is created using the bit values of the binary watermark image. An extended binary string is made by integrating the redundancy (repeating each bit 16 times).
Now, the set of the strings produced from the cover image and the watermark image are contrast with one another. If there occurs more than 50% positional match of the bits in the above form matrix, a bit '1' is assigned for the string otherwise bit '0'. Bit '1' indicates in-phase condition of two strings while out of phase condition is denoted by bit '0'. We obtain the vector S LxL from the PN (Pseudo Noise) sequence generated from the polynomial defined for an exacting image length over which the message would be embedded. S = {s1, s2, s3, sLxL}, si ∈ {0, 1}. The vector Z is created by zi = 2sj – 1, where zi ∈ {1,-1}. If there are equal numbers of zeroes and ones are at hand in S then the vector Z will be a vector with zero mean. We have to Generate 4 PN (Pseudo Noise) codes of length (n x n), where n = 4, 8, 16 etc.

**Step 4: Watermark Embedding**
We now embedded the cover image with the watermark image using the Spread Spectrum (SS) watermarking scheme.
The rule is given as:

Fe = F + KS if bj = '0'
Fe = F - KS if bj = '1'

Where Fe = Embedded image in spatial domain. F = Cover image. K = Modulation Index. S = PN code.

Watermark Image **Extraction & Message Decoding.**

The watermark extraction process requires the sets of PN matrices (S) that were used for data embedding. Various steps for watermark decoding are described as follows:

**Step 1: Image partitioning**
The traditional image R may be tampered with noise for which the brightness of the image can vary. The established image R is separated into 8x8 non overlapping

blocks, suppose R* ij where, i is number of rows and j is number of column.

**Step 2: Correlation calculation**
Correlation values between the watermarked image matrix and each code pattern of the set (S) are calculated.
We have a total of (Mm.Nm) (equal to the number of watermark bits) correlation values (ri) where i=1, 2… Mm.Nm. The decision rule for the decoded watermark bit is as follows:

(1) For ri _ 0, the extracted bit is 0
(2) For ri < 0, the extracted bit is 1.

**Step 3:** Substring decoding MSB plane of the individual blocks of watermarked image or its indistinct version is picked up and a set of 1D string Pi= {P1, P2, P3, P4} is generated from the 8x8 block. Bi-phase demodulation scheme is used in this stage. Based on the value of the extracted bit in the decoded watermark, the string either remains unchanged (if detected bit is '1') or goes together (if detected bit is '0'). Each and every string obtained in the above process is used to get back the binary watermark (bit redundancy). Binary detection is then applied for each substring based on the majority decision rule i.e. if more than 50% symbols are '1' in a sub substring, decision for decoding is '1', otherwise '0'. The embedded binary digits produces from the substrings are then converted to the pixel (each pixel of watermark image is represented by single bit) and binary watermark image is obtained.

3.1.2. Frequency Domain Techniques

In Frequency domain the secret information are hidden in the lower or middle frequency portions of the protected image, since the higher frequency portion is more likely to be concealed by compression. But how to choose the fine frequency portions of the image for watermark is another important and complicated topic. Various frequency domain techniques are as follows:-

## 4. Discrete Cosine Transform (DCT) Based Technique

DCT (discrete cosine transform) domain watermarking can be classified into two main functions namely Global DISCRETE COSINE TRANSFORM watermarking and Block based DISCRETE COSINE TRANSFORM watermarking. One of the first algorithms which are presented by Cox et al used global DCT method to embed a robust watermark in the perceptually significant bit of the Human Visual System (HVS). Embedding in the perceptually significant portion of the image has its own benefits because most compression functions eradicate the perceptually insignificant portion of the image. In spatial domain it denotes the LSB. Conversely in the frequency domain it represents the high frequency components. It is a method which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with various amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. It is very secure to JPEG compression, since JPEG compression itself uses DCT. However, DCT methods lack resistance to strong geometric deformation.

## 5. Discrete Fourier Transformation (Dft) Based Technique

It is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks. DFT uses complex numbers, while DCT uses just real numbers. Ruanaidh et al. proposed a DFT watermarking scheme in which watermark is embedded by modifying the phase information within the DFT. It has been shown that phase based watermarking is robust against image contrast operation. Later Ruanaidh and Pun showed how Fourier Mellin transform could be used for digital watermarking. Fourier Mellin transform is similar to applying Fourier Transform to log-polar coordinate system for an image. This scheme is robust against geometrical attacks. Simulations imply that magnitude DFT survives sensible compression which can be attributed to the fact that mainly practical compression schemes try to maximize the PSNR. Hence using magnitude DFT is a way to develop the hole in most practical compression schemes.

## 6. Discrete Wavelet Transform (Dwt) Based Technique

Dwt-based methods allow good spatial localization and have multi resolution characteristics, which are similar to the human visual system. Also this approach shows robustness to low-pass and median filtering. However, it is not robust to geometric transformations. If watermarking techniques can develop the characteristics of the human visual system (HVS), it is possible to hide watermarks with more energy in an image, which makes watermarks more robust. From this point of view, the dwt is a very gorgeous transform, because it can be used as a computationally efficient version of the frequency models for the hvs. For instance, it is said to be that the human eye is less sensitive to noise in high resolution dwt bands and in the dwt bands having an orientation of 45° (i.e., hh bands). Furthermore, dwt image coding, are included in the forthcoming image compression standards, such as jpeg2000 .thus dwt decomposition can be exploited to make a real-time watermark application. Many approaches apply the basic schemes described at the beginning of this section to the high resolution dwt bands, lh, hh, and hl .a huge number of algorithms

operating in the wavelet domain has been proposed till date.

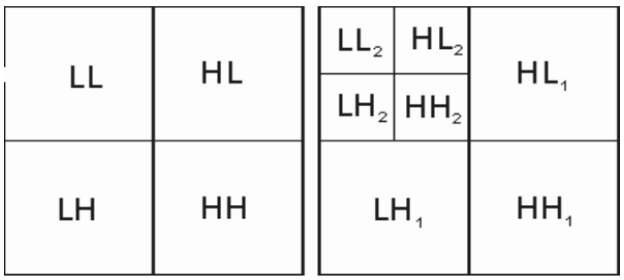


Figure 3, 1-scale and 2-scale 2-dimemsional discrete wavelet transform

## 7. Integer Wavelet Domain Watermarking

Beside DFT, DCT and DWT, we have also worked the state-of-art Integer Wavelet Transform (IWT) due to some amount of reasons. The detailed conversation for selecting the IWT is given as under Most conventional DWT based fragile or semi-fragile watermarking schemes description in the literature have three shortcomings

- Insecurity. The schemes used only one wavelet base to perform the DWT. Once the algorithm was stolen by an attacker, the hidden information bits may be exposed or changed easily.
- Low robustness to JPEG.
- High computational complexity.

Compared to DCT, DWT has less computational cost. But in the case of images having large size, it is still a problem when DWT applied to a whole image. A feasible method to improve security is to choose a wavelet base from a set of appropriate wavelet bases by parameters. If the parameter space is large enough, it is impossible for the attacker to get the useful information thus guarantees an extra security. Meerwald et al. Proposed for the first time to use the parameterized wavelet transform in fragile watermarking. Integer wavelet transform allows building the lossless wavelet transform which is important for fragile watermarking.

## 8. Optimization Techniques Image Watermarking

### 8.1. Singular Value Decomposition (SVD)

Singular value decomposition is one of the most influential numerical analysis tool used to evaluate matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as original matrix. SVD transformation conserves both one-way and non-symmetric properties, frequently not obtainable in DCT and DFT transformations. Wie Cao et.al developed SVD in DT-CWT domain. Using this SVD, the digital image processing has benefits like the size of the matrices from SVD transformation is not fixed and can be a square or a rectangle; singular values in a digital image are less affected if general image processing is performed and singular values contain intrinsic algebraic image properties. The singular values of the host image are customized to embed the watermark image by employing multiple singular functions. Watermark is embedded and extracted by correcting the value between selected coefficients and actual output trained by support vector regression. SVD factorization is done on different non-overlapping blocks by taking wavelet transform.

### 8.2. Independent Component Analysis (ICA)

Independent component analysis is newly developed technique for image watermarking. ICA is applied to compute statistically independent transform coefficients where watermark is embedded. The main advantage of this technique is that on one hand, each user can define its own ICA-based transformation. These transformations act as a private-key. An orthogonal watermark is urbanized to blindly detect it with a simple matched filter. ICA consists of projecting a set of components on to another statistically independent set. This method assumes multiple-input multiple- output model and has been successfully applied to image watermarking. ICA assumes watermarked image as a mixture of original image and watermark. The mixture image can be separated to estimate this watermark. Although ICA is utilized to detect and extract the watermark, they are still susceptible to geometric deformation attack. To embed logo watermarks, the original image is decomposed by Redundant DWT and watermarks are embedded into middle frequency at LH and HL sub bands.

### 8.3. Artificial Neural Network (Ann)

An artificial neural network (ANN) is a mathematical model or computational model that is enthused by the structure and/or functional aspects of biological neural networks. A neural network consists of an interconnected group of artificial neurons, and it processes information using a connectionist approach to computation. They are frequently used to model complex relationships between inputs and outputs Chuan-Yu Chang et. al. introduced copyright authentication for images with a full counter-propagation neural network (FCNN). Most attacks do not corrupt the quality of detected watermark image as FCNN has storage and fault tolerance. Chen Yong Qiang developed an optimal image watermark algorithm using synergetic neural network. Quan Liu et. al. designed and realized meaningful digital watermarking algorithm based

on Radial Basis Function (RBF) neural network. RBF Neural network is worked to simulate human visual system to determine watermark embedding intensity.

### 8.4. Support Vector Machine (SVM)

SVM is a new machine learning method introduced by Vapnik. SVM has been effectively applied to numerous classification and pattern recognition problems. SVM is maintained to lead enhanced generalization properties. In recent years, SVM has been used for digital watermarking. SVMs are easier and improved to use than traditional neural network models. The design of SVM is to build a mapping model from input data to output data which are also defined as features for input data and targets for output data. There are two data sets in classification, i.e., training data and testing data. Each training data contains several features and one target. After SVM learns using the training data, SVM can produce a model to calculate the corresponding target of the test data.

### 8.5. Genetic Algorithm **(GA)**

Genetic watermarking based on transform-domain techniques. A genetic algorithm is a search heuristic used for optimization. It generates solution using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. In each generation, the fitness of every entity in the population is evaluated, multiple individuals are stochastically selected from the current population (based on their fitness), and modified (recombined and possibly randomly mutated) to form a new population. Commonly, the algorithm end when either a maximum number of generations have been produced, fitness level has been reached for the population. In case of watermarking, the singular values (SVs) of the host image are customized by multiple scaling factors to embed the watermark image. Modifications are optimized using GA to obtain the highest possible robustness without losing the transparency.

## 9. Conclusion

We provided a clear view about the use of watermarking technique in medical image processing. We explained the type of watermarked technique based on domain, such as spatial and frequency domain. Spatial domain consists of various techniques, LSB and Spread Spectrum similarly in frequency domain, DFT, DWT, DCT and SVD. We produced a literature survey on medical image watermarking based on resent researches with various optimization techniques from inter-domain which can also be applied on upcoming researches in medical image watermarking domain.

## Reference

[1] Planitz, B. P. and Madre, A. J. (2005, February 12). Medical image watermarking: A study on image degradation. Proceedings of the Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC 2005), pp. 3–8.

[2] Planitz, B. P. (2006, July). Medical image watermarking. CT/MRI&PACS/CR/DR, 28–30 July, Gold Coast, Australia.

[3] Puech, W. and Rodrigues, J. M. (2004). A new crypto-watermarking method for medical images safe transfer. Proceedings of 12th European Signal Processing Conference EUSIPCO'04, pp. 1481–1484.

[4] Raúl, R. C., Feregrino-Uribe, C., Gresham de, J., and Trinidad, B. (2007). Data hiding scheme for medical images. 17thInternational Conference on Electronics, Communications.

[5] Rodrigues, J. M., Puech, W., and Fiorio, C. (2004). Lossless crypto data hiding in medical images without increasing the original image size. MedSIP 2004. 2nd Medical Image and Signal Processing, pp.358–365

[6] Mahmoud El-Gayyari, ―Watermarking Techniques Spatial Domain Digital Rights Seminar ©‖, Media Informatics University of Bonn Germany.

[7] Jahnvi Sen, A.M. Sin, K. Hemachandran,‖ AN ALGORITHM FOR DIGITAL WATERMARKING OF STILL IMAGES FOR COPYRIGHT PROTECTION‖, Jahnvi Sen et al / Indian Journal of Computer Science and Engineering IJCSE).

[8] G. Coatrieux, L. Leone, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'‖A Review of digital image watermarking in health care‖.

[9] Edin Muharemagic and Bork Firth ―A Survey of watermarking techniques and applications‖ 2001.

[10] Guo X, Zhuang TG: A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22(1):53–64,2009

[11] Zain J, Baldwin L, Clarke M: Reversible watermarking for authentication of DICOM images, in Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society pp 3237–3240,2004

[12] Hanhan AHAM: Digital image watermarking, in Faculty of Engineering Electrical Engineering

Department. AN-Najah National University, 2011.

[13] Yang B, Schmucker M, Funk W, Busch C, Sun S: Integer DCT-based reversible watermarking for images using compounding technique. Proc SPIE 5306:405–415, 2004

[14] Celik MU, Sharma G, Tekalp AM, Saber E: Lossless gneralized-LSB data embedding. IEEE Trans Image Process 14(2):253–266, 2005

[15] Li J, Du W, Bai Y, Chen YW: 3D-DCT based zero-watermarking for medical volume data robust to geometrical attacks, in Wireless Communications and Applications. In: Sénac P, Ott M, Seneviratne A Eds. Springer Berlin: Heidelberg, 2012, pp 433–444.

[16] Gung BWR, Adiwijaya, Permian FP: Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression, in Communication, Networks and Satellite (Commentate), 2012 IEEE International Conference. pp 167–171, 2012.

[17] Do MN, Vetter M: The contoured transform: an efficient directional multi resolution image representation. Image Process IEEE Trans 14(12):2091–2106, 2005

[18] Viswanathan P, Krishna PV: Fusion of cryptographic watermarking medical image system with reversible property, in Computer Networks and Intelligent Computing. In: Venugopal KR, Patnaik LM Eds. Springer Berlin: Heidelberg, 2011, pp 533–540