CHAPTER 1

Introduction

Processing and handling medical data and information by computer systems and transmitting them over fast-paced network infrastructure has become a routine job since large scale employment of low cost computing and networking hardware and software. Presently, medical text and data files and images are stored on disks of medical database systems for quick and reliable storage and retrieval. Furthermore, originally acquired images on films and written data is also digitized and archived for compatibility.

Another impetus is to have complete medical information of patients available in one homogeneous application instead of on several information systems. Medical applications, such as medical diagnosis made by means of telemedicine, and teleconsultation need information and data exchange over an unprotected network. Protection of the uprightness and confidentiality of medical images is a task in the management of patients' medical records. Clandestineness states that unauthorized parties should not be granted to access medical images during transmission. Integrity, on the other hand, implies that images should not be modified in any way during transmission.

The technique used to hide information to a digital cover is known as data hiding (e.g., digital image) for various uses such as copyright protection, hidden communication, content authentication, forensic tracking, etc. The most important requirement of data hiding is that the receiver should be able to extract the exact embedded message from the received marked image. Concurrently, the changes to host image should be invisible, meaning that the visual presentation of marked image should be same as the host one.

Many original and well working data hiding algorithms have been proposed so far, for example, the least-significant-bit (LSB) based method [8], the pixel-value-differencing (PVD) based methods, the transform domain based methods [9], etc. In these algorithms, the information content of host image is permanently and partially or completely distorted and it can't be restored after data extraction. Nonetheless, the recovery of host image itself is quintessential in some applications such as remote sensing, military image processing and management, medical image sharing, archive management, etc.

For all these applications, reversible data hiding provides an ideal and apt solution, since this technique allows one to embed data in such a way that the host image can be exactly reconstructed from the marked content and there is no loss of diagnostic information content of the image at the same time.

The algorithm we used for watermarking will be triangular number generator (TNG) function.

CHAPTER 2

Review of the Literature

Due to the phenomenal growth of the internet in recent times, our attention is drawn towards the need for insuring protection and control of data exchange over the internet. Because of their digital nature, multimedia documents and data can be duplicated, modified, transformed, and disused and transferred easily and quickly.

Exactly identical copies of digital information, be it images, text or audio, can be produced and distributed easily. Digital watermarking is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. The aim of watermarking is to include subliminal information (imperceptible) in a multimedia document to ensure a security service or simply a labeling application. Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. This information can be textual data about the author, its copyright, etc.; or it can be an image itself.

The information to be hidden is embedded by manipulating the contents of the digital data, allowing someone to identify the original owner, or in the case of illicit duplication of purchased material, the buyer involved. These digital watermarks remain intact under transmission/ transformation, allowing us to protect our ownership rights in digital form. Thus, recovering the embedded message is possible even if the document was altered by one or more nondestructive attacks, whether malicious or not.

In practice, a watermarked object may be altered either on purpose or accidentally, so the watermarking system should still be able to detect and extract the watermark. Obviously, the distortions are limited to those that do not produce excessive degradations, since otherwise the transformed object would be unusable.

The attacks could be

- Additive Noise – Through the use of D/A and A/D converters or from transmission errors
- Filtering - Low-pass Filtering, less image degradation, more effect on performance
- Cropping – Attacker is interested in a small portion of the watermarked object
- Compression - Unintentional attack appearing often in multimedia applications while distribution via internet
- Multiple Watermarking - An attacker may watermark an already watermarked object and later make claims of ownership

THERE ARE SOME DESIRABLE CHARACTERISTICS THAT A WATERMARK SHOULD POSSESS

- Imperceptible

An unmarked image is passed through a perceptual analysis block that determines how much a certain pixel can be altered such that the resulting watermarked image is indistinguishable from the original. This takes into account the human eye sensitivity to changes in flat areas and its relatively high tolerance to small changes in edges. If the watermarked image and the original image are perceptually indistinguishable the image is called imperceptible. A watermark is called perceptible if its presence in the marked signal is noticeable like in case of visible watermarking.

- Robustness

The ability of watermark to withstand with the modifications (compression, rotation, noise) is called its robustness. The watermark should be resilient to standard manipulations of unintentional as well as intentional nature. It should be statistically irremovable and should withstand multiple watermarking to facilitate traitor tracing.

- Capacity

The number of bits that can be embedded into the particular cover image with low error visibility is called capacity of watermark. Watermarking capacity is determined by invisibility and robustness requirements.

2.1 CLASSIFICATION OF WATERMARKS

It is not possible to have a universal watermarking algorithm which can cater to the needs of all the applications. So based on the requirements of the application we can classify watermarks with their different properties. Watermarks may be visible, in which case their use is two-fold which includes discouraging unauthorized usage, and also act as an advertisement. However, the focus is on invisible watermarks, as they do not cause any degradation in the aesthetic quality or in the usefulness of the data. They can be detected and extracted later to facilitate a claim of ownership, yielding relevant information as well. Watermarks can also be classified with reference to the level of robustness to image changes & alterations.

They can be divided into 3 main categories:

Fragile, Semi-fragile & Robust. Fragile watermarks are designed to detect even the slightest modifications made to an image. Semi-fragile watermarks are designed to withstand certain legitimate modifications but to detect malicious ones. If the image undergoes severe modifications & degradation, including analog-to-digital & digital-to-analog conversions, cropping, scaling, etc. then a Robust watermark is used.

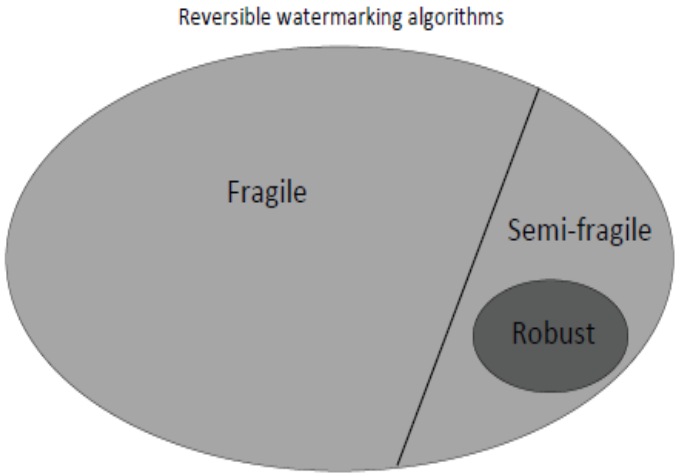

Figure 1: Classification of reversible watermarking algorithms

In the field of medical science, correct diagnosis is a pre-requisite for any successful treatment. In the field of ophthalmology, two factors are of utmost importance when it comes to the diagnosis of eye diseases. First is the successful acquisition of fundus image and second is the successful interpretation of the image. Till date, physical examination by the ophthalmologist is, by far, the only way for the diagnosis of any eye disease. This procedure has two major disadvantages. First being the cost of visit to a doctor, a person with no impairment in vision would not pay a visit to an ophthalmologist, whereas, free/low cost service through an automated process would surely be a breakthrough in early screening of Diabetic Retinopathy patients. Second is the time taken by the ophthalmologist to attend every patient, especially in developing countries where doctor to patient ratio is considerably less. Computers on the other hand provide answers to the above mentioned problems. If the correct algorithms for detection and classification of various diseases are fed into the computer then the screening process can be carried out with high accuracy, making the process fast and cost effective, thus enabling it for widespread application.

Diabetic Retinopathy (DR) is one of the most common diabetic eye disease which occurs in almost 80% of all the patients having diabetes for 10 years or more. Number of people suffering from Diabetes worldwide is 382 million in 2013 and is expected to rise to 592 million in 2035. Hence, the number of people suffering from Diabetic Retinopathy is expected to rise significantly. DR can only be detected by examining the fundus image of the eye or by the physical examination of the ophthalmologist. Diabetic Retinopathy is non reversible in nature i.e. the damage caused to the eye because of DR is permanent. DR can ultimately lead to blindness if not treated at an early stage.

2.2 STRUCTURE OF A TYPICAL WATERMARKING SYSTEM

Our project uses MATLAB software wherein fundus images are provided as input and images are being screened for different stages of Diabetic Retinopathy. Since macula is primarily concerned, region around the macula is cropped out and image processing algorithms are applied on the cropped images to classify the images into normal and abnormal images. If the image is found to be abnormal then it is further classified into different stages of DR. As already stated, the number of diabetic patients will increase manifold in the coming years and number of ophthalmologists to cater to such a large population of diabetic people are very less. Hence, there is a need of efficient and cost effective automated screening system which can detect DR as early as possible, preferably at non-proliferative stage, so that a large number of patients can be saved from the adverse effects of this disease.

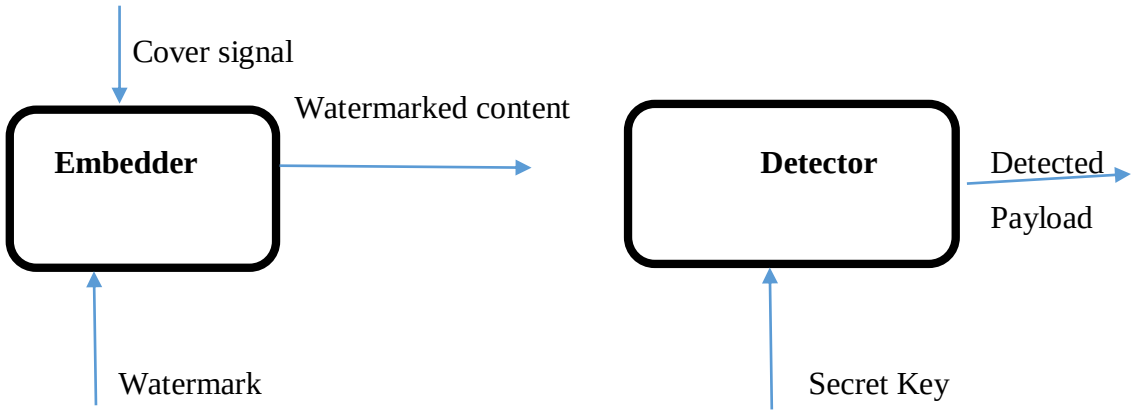

Figure 2: Basic watermarking process block diagram

2.3 REVERSIBLE DIGITAL WATERMARKING

Reversible watermarking techniques are also referred to as reversible or lossless data hiding schemes and were originally born to be related mainly in conditions where the authenticity of a digital image has to be valued and the original content is definitively needed at the extraction side.

It is important to point out that, originally, a high perceptual quality of the watermarked image was not a requirement due to the fact that the original copy was retrievable; hence, other problems such as overflow and underflow caused by the watermarking process were not taken into account either. In addition, by employing reversible watermarking the access to the original content can be controlled, and only the authorized person can access the original content by erasing the watermark while the watermarked content is available to everyone.

Successively, this aspect of these schemes are considered the basis to permit the end user to operate on the watermarked image and to possibly decide to recover the original version at a later time if needed. This flexibility in operation is important within different applications in which reversible watermarking is essential.

Examples of such application are military and satellite imaging, deep space photography, and medical imaging. For instance, in cases where watermarking is deployed on a medical image to secure the privacy of the patients, the physicians or related entities should have access to high quality watermarked medical images to avoid any false or wrong diagnosis that may endanger the health of the patients. Also in most applications, such as data storage and transmission in sensitive fields, it is of great interest to keep the watermark embedded as long as possible in order to continuously protect the information; this means that if the watermark is removed, or at least the part which secures the integrity of the information is extracted, the image is no more protected just like the case of data encryption.

Hence, having high perceptual quality in the marked image while retaining the properties such as reversibility and high capacity is extremely important in reversible watermarking schemes. Reversible watermarking is the method to provide the three mandatory security characteristics in different applications. These characteristics are: Confidentiality, which ensures that only the entitled and eligible users have access to the information; Availability, that is the ability of an information system to be accessible; and Reliability, which is based on the integrity and authenticity of the information. Integrity of the information ensures that the data have not been modified by unauthorized people; authenticity, on the other hand, provides the proof that the information relates to the correct person and issued from the reliable source.

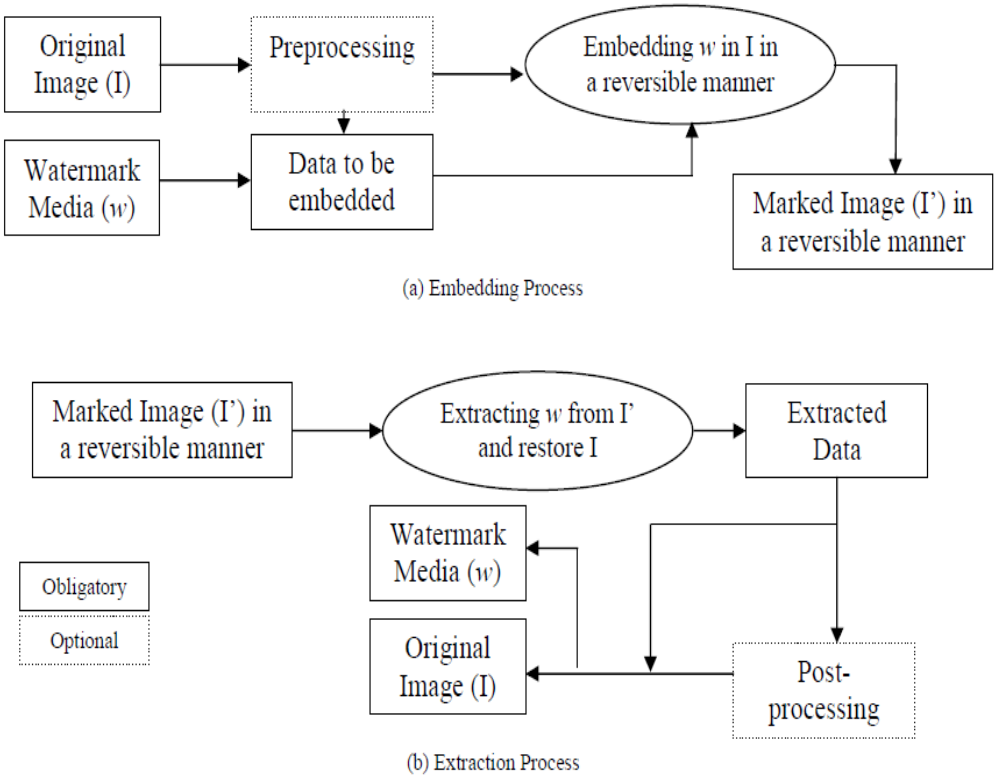

Figure 3: General Framework for Reversible Watermarking (a) embedding process, (b) extraction process.

2.4 MEDICAL IMAGE WATERMARKING

Hiding patient data in the medical image is one of the applications of digital image watermarking. The patient data in the electronic format is called Electronic patient record (EPR). The medical images with EPR attached to them can be sent to the clinicians residing at any corner of the globe for the diagnosis. Thus Medical Image Watermarking plays a vital role in the field of Telemedicine.

2.4.1 ATTACKS ON MEDICAL IMAGES

All patients records, electronic or not, linked to medical secrecy, must be kept confidential. Because of the sensitive nature of the data, the first and the foremost requirement is that any additional information which is being embedded in the medical image must not affect its perceptual quality. Medical image watermarking is done because of mainly two reasons- increase the security, to verify integrity of medical images.

2.4.2 THE ATTACKS ON MEDICAL IMAGES CAN BE BROADLY CLASSIFIED INTO 4 MAIN CATEGORIES

- Interruption: The attack on availability. Information is completely destroyed or becomes unavailable and not usable.
- Interception: The attack on confidentiality. An unauthorized person gets access to the data
- Modification: The attack on integrity. An unauthorized person not only gets access to, but also tampers with information and changes data.
- Fabrication: The attack on authenticity. An unauthorized person inserts counterfeit objects into the data.

To avoid above mentioned attacks while transmission of medical images are watermarked using certain algorithms.

2.5 NEED FOR COMPRESSION

Medical images are acquired and stored digitally especially for grayscale diagnostic imagery which has applications in radiology. These images are of typically large size and also large in number. Efficient compression makes it possible to increase the speed of transmission and reduce the cost of storage. The long term storage and mobile transmission of large size images is prohibitive, no compression is used. A typical size mammogram may be digitized at 2048 x 2048 pixels at 16 Bpp, leading to a file which is over 8 Megabytes in size if no compression is used. For cost-effective wireless transmission, compression must be used to discard some of the redundant image data to meet the mobile bandwidth constraint. This typically involves the use of the widely accepted Joint Picture Experts Group (JPEG) standards. The most commonly used of these is lossy baseline JPEG. Images with slowly varying scene content and high correlation can be compressed efficiently as the image information can be concentrated into few coefficients in the frequency or transform domain. But, here the images we use contain high contrast edges and high levels of detail. More information must be retained in order to effectively reconstruct important picture information. Despite impeccable quality most of the time, lossy compression can introduce false information or artifacts such as ringing and blurring which become apparent at very low bit rates.

2.6 BASIC WATERMARKING ALGORITHM

Least Significant Bit Substitution [Spatial Domain]

The most direct method for watermark embedding would be to embed the watermark into the least-significant-bits of the image and forget about everything else. [10] In this procedure, a smaller object may be embedded many times. Even if most of these are lost due to attacks, a single remaining watermark would be considered a success. It may remain after transformations such as cropping; any addition of noise but lossy compression is likely to degrade the watermark. An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key. To detect the watermark, each key is used to generate its PN sequence, which is then conjoined with the whole image. If the conjoination is high, that bit in the watermark is set to "1", otherwise a "0". The process is then repeated for all the values of the watermark. It improves on the robustness of the watermark to a great extent, but requires several orders more of calculation. It is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions. The benefit is twice; Degradation in smoother regions of an image is more observable to the HVS (humane visual system), and becomes a major target for lossy compression schemes. But it is not possible to identify such region in spatial domain.

2.7 PREVIOUS WORK IN REVERSIBLE WATERMARKING

In the past decade, several reversible watermarking schemes designed for digital multimedia contents have been proposed based on difference expansion (DE) [1] and histogram shifting [11]. Basically, schemes based on DE provide a larger embedding capacity, whereas the visual quality of the stego-image is better for schemes that are based on histogram shifting. In 2003, Tian introduced a reversible, DE-based watermarking scheme [1]. In Tian's scheme, the difference value between two neighboring pixels is calculated and doubled to embed one watermark bit. In 2007, Thodi and Rodríguez [12] proposed a watermarking scheme based on error prediction (PE) to hide the watermark data. In their scheme, a prediction technique is designed to predict the pixel value. Following that, the difference between the current pixel value and its predicted value is computed to embed the watermark data. These two schemes [11, 12] are based on the DE technique to achieve high embedding capacity. However, in such schemes, the pixels may have an overflow or underflow problem, and the visual quality of the stego-image is not very good. To increase the visual quality of stego-images, many researchers have proposed schemes based on the histogram-shifting approach. In 2006, Ni et al. introduced the first histogram-shifting scheme [11]. In their scheme, most of the pixels are shifted by one grayscale value to hide the watermark information. Their scheme achieves stego-images that have high visual quality, but the embedding capacity is limited. In 2009, Kim et al. [14] presented a reversible scheme based on a different histogram-shifting approach to obtain high capacity and imperceptible embedding by dividing the cover image into several sub images. The difference values between the sub-sampled images are calculated. Then, the difference values are shifted to embed more secret data. To further improve Kim et al.'s scheme, in 2010, Li et al. [15] proposed a reversible watermark scheme based on APD. To embed watermark data in Li et al.'s scheme, the difference sequence of pixels is computed.

2.7.1 TIAN'S METHOD

In the field of medical science, correct diagnosis is a pre-requisite for any successful treatment. In the field of ophthalmology, two factors are of utmost importance when it comes to the diagnosis of eye diseases. First is the successful acquisition of fundus image and second is the successful interpretation of the image. Till date, physical examination by the ophthalmologist is, by far, the only way for the diagnosis of any eye disease. This procedure has two major disadvantages. First being the cost of visit to a doctor, a person with no impairment in vision would not pay a visit to an ophthalmologist, whereas, free/low cost service through an automated process would surely be a breakthrough in early screening of Diabetic Retinopathy patients. Second is the time taken by the ophthalmologist to attend every patient, especially in developing countries where doctor to patient ratio is considerably less. Computers on the other hand provide answers to the above mentioned problems. If the correct algorithms for detection and classification of various diseases are fed into the computer then the screening process can be carried out with high accuracy, making the process fast and cost effective, thus enabling it for widespread application.

Diabetic Retinopathy (DR) is one of the most common diabetic eye disease which occurs in almost 80% of all the patients having diabetes for 10 years or more. Number of people suffering from Diabetes worldwide is 382 million in 2013 and is expected to rise to 592 million in 2035. Hence, the number of people suffering from Diabetic Retinopathy is expected to rise significantly. DR can only be detected by examining the fundus image of the eye or by the physical examination of the ophthalmologist. Diabetic Retinopathy is non reversible in nature i.e. the damage caused to the eye because of DR is permanent. DR can ultimately lead to blindness if not treated at an early stage.

2.7 SUMMARY OF LITERATURE REVIEW

This section summarizes the aforementioned schemes in the form of a chart and a table. The reviewed schemes are classified under fragile, semi-fragile, and robust categories in Figure 1. Furthermore, the methodology and algorithm of each method is presented in Figure 3.

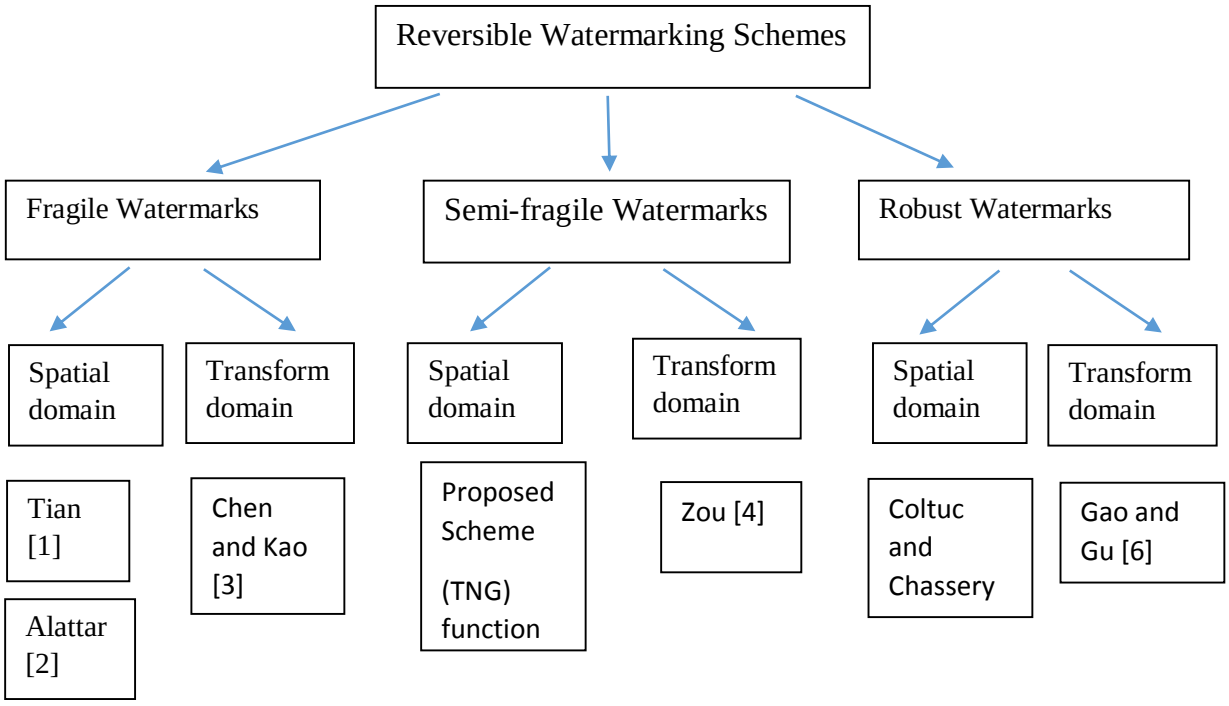

Figure 3: categorization of the significant reversible watermarking schemes.

CHAPTER 3

Database

The images on which watermark would be embedded (cover images) are obtained from Venu Eye Research Centre, Saket, New Delhi. The images are called ophthalmic images and they differ in degradation of some eye characteristic. The images are of dimensions 2240x1488 obtained by software called Amerinex Applied Imaging Aphelion.

Some of the different images:

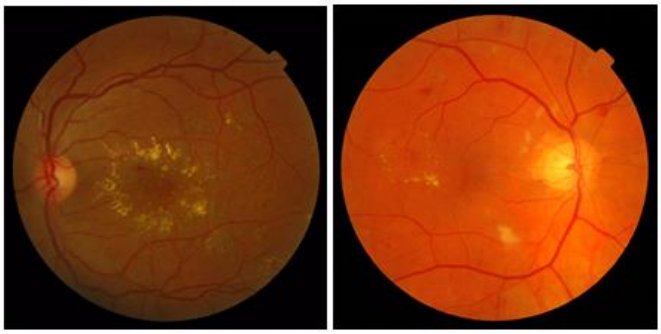

Figure 5: eye fundus images of varying qualities

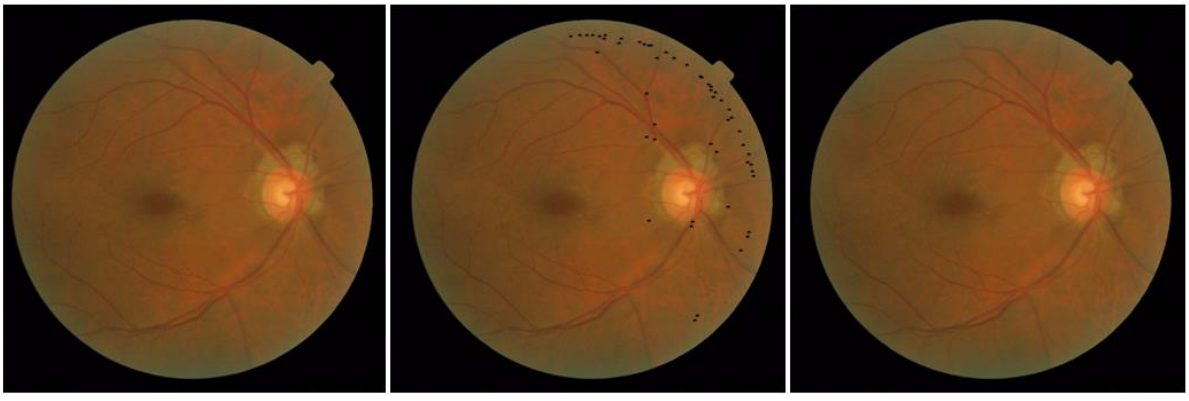

Figure 6: Ophthalmic fundus images varying in pixel densities

The primary goal of the project is to have an automated system for early detection of patients with diabetic retinopathy, a task which requires expertise in the field of Medical sciences, particularly, Ophthalmology watermarked onto the image. It is only the need of an automated system, which necessitates the requirement of an engineer, one with research interest in the field of image processing. Hence, throughout the process of our project, we kept in touch with the Venu Eye Research Centre, Saket, New Delhi. We received immense help and support from the institution. Apart from the data and statistics that were shared by the institution which help us a lot with our project, we were fortunate to get an appointment to personally meet the director of the research centre with our queries on a number of occasions. The learning outcomes of the field visits is immeasurable, we got to understand the perspective of an Ophthalmologist, when he/she diagnoses a patient with Diabetic Retinopathy. Important aspects of the syndrome like, the onset of various abnormalities with the onset of different stages of severity of the disease, factors that are accounted by doctors when they classify the stage of DR, etc. were discussed in those field visits. These aspects are difficult to understand from mere books and journals. A brief description of the outcomes of the field visits has been provided for a better understanding of the disease.

1. The effect of DR on human eye with increasing severity:
    i. Change in vessels: An unusually high number of ripples in a blood vessel's structure. Blood vessels of a normal eye tend to be linear and have no or very little bends. The onset of DR is marked by the presence of ripples in blood vessels of retina.
    ii. Micro-aneurysms: Also known as Red lesions/spots, basically bleeding from blood capillaries. They appear as small dark red spots on a fundus. These leakages are a result of the cracks developed in the capillaries due to the ripples created in the vessels.
    iii. Hemorrhages: Micro-aneurysms blot to form hemorrhages. They appear as red blots on a fundus. All the microaneurysms may not be visible to the naked eye, but, they blot and grow in size to form larger blot of blood.
    iv. Intra Retinal Micro vascular Abnormality (IRMA): Not visible in a fundus image. Ophthalmologists use cameras with depth perception to detect IRMA. This refers

to the uneven protrusions of blood vessels which are hard to detect using a 2-D perception through fundus images.

v. Exudates: When leakage of blood continues at the sites of micro-aneurysms and hemorrhages, supply of blood ceases, as a result protein gets coagulated. They appear as Yellow spots on a fundus.

At this stage, the patient starts experiencing loss of vision. It is very important to understand that going further can lead to two different possibilities, both resulting in complete vision loss.

a. Continue as Non-proliferative: In this case the factor behind vision loss is the proximity of abnormalities to the macula. Hence, a fundus image can be utilized with further image processing to detect this stage.
b. Proliferative: In this case the vision loss is due to Vitreous Humor. Vitreous Humor is the gel filled in between the lens and the retina.

2. Parameters/Features for severity of DR:

   In the Non-Proliferative type of DR, the most significant parameter is the proximity of an abnormality to the macula. Macula is responsible for almost 90% of vision, so any abnormality close to it is a greater threat to vision.

3. Image standards:

   Five different regions can be taken for the retina of a human eye, as shown in the figure below by the 5 thin ovals. The area of retina covered in an image depends on the angle of projection of a camera.

4. Technology vs Ophthalmologist

   Advantages of technology:

   i. Reduce the work load of ophthalmologists, as the chances of DR is high in diabetic patients, and diabetes is a wide spread disease.
   ii. Cost effective, as interference of qualified human resource is not required.
   iii. Time efficient, as patients would not need to wait in queues for their turn for screening.

Constraints and challenges:

i. Ophthalmologists use cameras with 3-D perception, hence a dimension of information is missing for the proposed technology used.

5. Method of treatment:

   The use of LASER is a destructive process, hence it is not used in regions close to the macula. The outer regions are exposed to LASER. As a result the flow of blood/nutrition towards the abnormalities increases and thereby repairs the damage.

All these need to be watermarked onto the image in contention and without any data loss.

CHAPTER 4

Methodology of the Proposed Algorithm

The proposed methodology, as illustrated in the block diagram (Fig 6.) is a comprehensive process that includes the following:

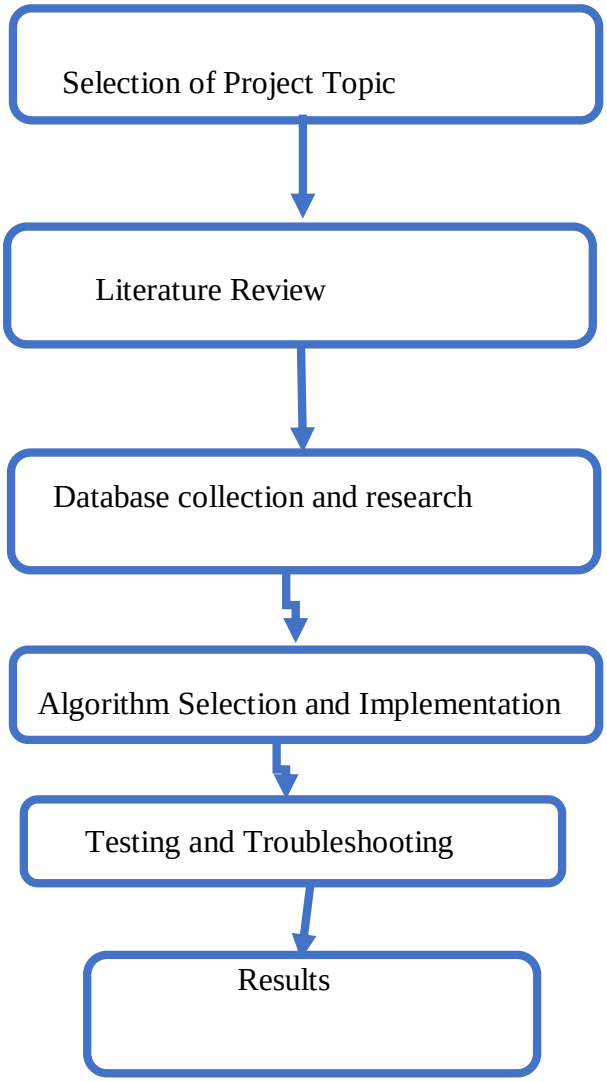

Figure 7. Block Diagram of the proposed method

4.1 IMAGE ACQUISITION

For an image processing application, the input of the system has to be an image with predefined standards. But, since this application is primarily a biomedical application, the input is the fundus of a human eye. Fundus is a Latin term, anatomically referring to the portion of an organ opposite from its opening. Fundus image of an eye is the photograph of the interior surface of the eye, which includes the retinal vessels, optic disk and macula. A typical fundus camera provides an upright, magnified view of the fundus, as shown in Fig 7(a). Since, the quality in terms of resolution, illumination, etc. vary with the device used, hence, the automated system, to be successful must support a range of formats of fundus images as input. However, a typical camera views 30 to 50° of retinal area, with a magnification of 2.5x.

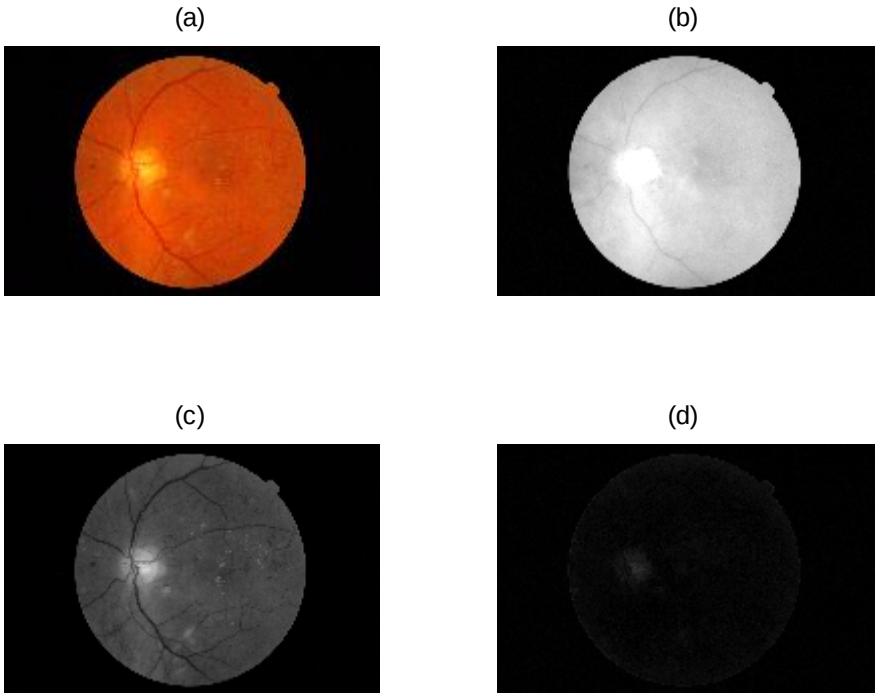

Figure 8. (a) RGB format of a fundus image, (b) Red channel of the image, (c) Green channel of the image, (d) Blue channel of the image

4.2 IMAGE PREPROCESSING

This step is indispensable for most image processing algorithms. Since, the input fundus images can be of varying quality it is important to apply certain pre-processing steps in order to implement generalised detection algorithms on these images. The pre-processing steps used for the proposed algorithm have been discussed in the following sub-sections.

1. *MSB Extraction of Cover image*
2. LSB extraction of Cover image
3. *MSB Extraction of Watermark*
4. *LSB Extraction of the Watermark*
5. *Shifting of Watermark*

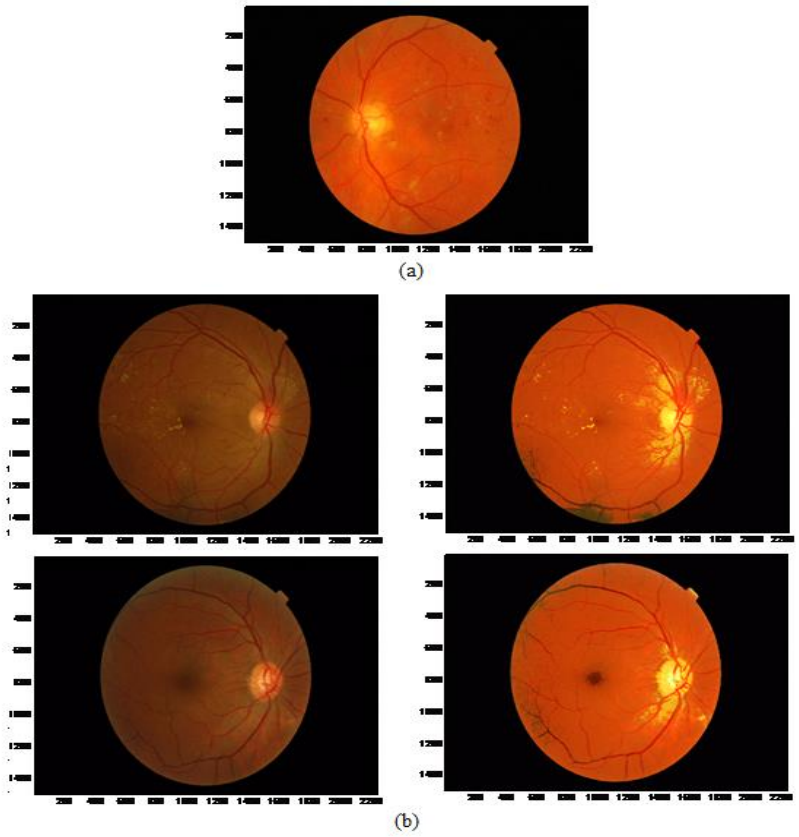

Fig 9. (a) Input Fundus Image (b) Fundus image (left) with corresponding image (right) MSB and LSB extracted images.

4.3 PROPOSED SCHEME FOR WATERMARKING

Triangular Number Generator Function

The detailed discussions of extraction and embedding procedures is done in subsections and 2.4 respectively. Unlike the algorithms for DE watermarking proposed in the earlier literatures which select the sub band with the highest energy, this algorithm selects an arbitrary sub band to prevent an intruder or attacker from attacking the highest energy sub band. It also selects the arbitrary coefficients to hide the image watermark. The proposed system applies the concept of a triangular number generating function that encodes a pair uniquely of positive integers into a positive integer as shown in (1). The pattern and arrangement of triangular numbers is shown in Figure 10. Table 1 shows the coded representation of different integer pairs using (1). The first row of the table contains triangular numbers in sequence shown in red faces.

$$T = f(a,b) = [(a+b)^2 + 3a + b]/2 \quad (1)$$

Figure 10: Triangular Numbers

Table 1: Integer Pair representation

a\b	**0**	**1**	**2**	**3**
0	**0**	**1**	**3**	**6**
1	2	4	7	11
2	5	8	12	17
3	9	13	18	24

On applying the steps for extraction from (2) to (4), any number in the table, T can be deterred into a and b exactly, not taking into account the triangular nature, without any additional information. Hence it serves as the best approach for imbibing reversibility.

$$C = \left[\sqrt{8T + 1} - 1\right]/2 \quad (2)$$

where C= a+b

$$a = T - C(C + 1)/2 \quad (3)$$

$$\mathrm{b} = \mathrm{C}(\mathrm{C} + 3)/2 - \mathrm{T} \quad (4)$$

The TNG transform is applied to select the embedding position in the candidate subband. For the watermark of size NxN, the coordinate position (x,y) of the watermark is mapped to (xn,yn) of the candidate subband. This transform not only scrambles the watermark, but also aids in watermark synchronization during extraction. [13]

4.4 Image Quality and Performance Measures

The performance of the watermarking systems can be evaluated by computing various discrete image quality measures on the watermarked images. The various metrics used to determine the closeness of the processed and the original images are discussed in this section. The common metrics used in various image compression and watermarking systems are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). [15] The smaller value of MSE is an indication of good quality of the processed image while a higher value of MSE signifies poor image quality. PSNR is a measure of the image fidelity i.e., a measure of the distortion. A small value of PSNR is an indication of low imperceptibility while a large value indicates a good degree of imperceptibility.

The Structural Similarity Index Measure (SSIM) is used to evaluate the quality of a processed imaged based on its structural similarity with the unaltered image as the reference. Recently, the Universal Image Quality Index (UIQI) measure that takes into account of structural distortions is used as a replacement for MSE and PSNR measures. Our system also uses the Weighted PSNR (WPSNR) and Mean Structural

Similarity Index Measure (MSSIM) metrics to evaluate the perceptual image quality. Further, it evaluates the robustness of the watermark with the Normalized Mean Square Error (NMSE) measure.

Since this paper focuses on reversibility, it is required to ensure that the reconstructed cover images contain less distortions i.e., their fidelity is preserved. Hence, the same metrics discussed above are used to measure the imperceptibility of the watermarked images and the fidelity of the recovered cover images with the original cover images as reference.

4.4.1 Mathematics of PSNR and MSE

For the following implementation, let us assume we are dealing with a standard 2D array of data or matrix. The dimensions of the correct image matrix and the dimensions of the degraded image matrix must be identical.

The mathematical representation of the **PSNR** is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAXf}{\sqrt{MSE}}\right) \quad (5)$$

Equation 5- Peak Signal-to-Noise Equation

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (6)$$

Equation 6 - Mean Squared Error Equation

This can also be represented in a text based format as:

MSE = (1/(m*n))*sum(sum((f-g).^2))

PSNR = 20*log(max(max(f)))/((MSE)^0.5)

Legend:

f: represents the data matrix of original image

g: represents the data matrix of degraded image

m: represents the numbers of rows of pixels of any images

n: represents the number of columns of pixels of any image

$MAX_{f:}$ maximum signal value that occurs in our original image

4.4.2 Motivation for Use as an Image Quality Metric

The mean squared error allows us to compare the real pixel values of our original image to our degraded image for our practical purposes. The MSE describes the average of the squares of the "errors" between our original image and our noisy image. The error is the amount by which the values of the actual image differ from the noisy image.

The proposal is that the higher the PSNR, the better noisy image has been regenerated to match the original image and the better the reconstructive algorithm. This would occur because we wish to reduce the MSE between images with respect the highest signal value of the image.

4.4.3 Closing Notes

When you try to compute the MSE between two identical images, the value will be zero and hence the PSNR will be undefined (division by zero). The main limitation of this metric is that it relies strictly on numeric comparison and does not actually take into account any level of biological factors of the human vision system such as the structural similarity index. (SSIM)[16]

4.5 ALGORITHM IMPLEMENTATION

Watermark embedding and extraction:

Triangular Number Generator (TNG) function is used for the application of algorithm. It is a function as in (1) which uniquely encodes a pair of positive integers (a, b) into a unique number TR. The number TR can be factored back to a and b exactly by applying the extraction procedure. In the watermark extraction and embedding algorithms the proposed systems takes advantage of reversible and blind nature of the TNG.

$$TR = f(a, b) = [(a+b)^2+3a+b]/2 \quad (1)$$

Watermark embedding process is performed by combining *n* number of LSB planes of cover image and the logo image by Eq. 1. As this combination results in an integer whose magnitude value cannot be expressed in n bits, modulo 2^n operation is carried on the obtained integer. While the n bit reminder is concatenated with 8-n bit planes, the quotient is preserved for later use. Secondly, on watermarking extraction procedure, the combination is reconstructed by combining the key and the n LSB planes of the watermarked image. The watermark embedding and extraction algorithms are given in Algorithms, respectively assuming n = 4.

Algorithm for watermark embedding:

Step 1: Extract 4 MSBs and 4 LSBs of original Image to form MSB_T and LSB_T

Step 2: Extract 4 MSBs of Logo Image to form a matrix MSBV and shift it right 4 times

Step 3: Combine LSB_T & shifted MSB_V using TNG function to form matrix T

Step 4: Performing Modulo 16 operation on T to produce remainder and quotient Rem_{TR} and Quo_{TR}, respectively

Step 5: Combining MSB_T and Rem_{TR} to form the watermarked image WMI; preserve as the key Quo_{TR}

Algorithm 2 watermark extraction:

Step 1: Extract 4 MSBs and 4 LSBs of the watermarked image to form MSB_{WMI} and LSB_{WMI}, hence; LSB_{WMI} is Rem_{TR}

Step 2: Multiply key/quotient matrix Quo_{TR} by 16 and add the obtained with LSB_{WMI} to get T

Step 3: Extract the LSB_T and shifted MSB_V from T; Left shift MSB_V>>4 for 4 times to get the watermark

Step 4: join with LSB_T with MSB_{WMI} to get the Cover image

The above algorithms are illustrated for with Fig. 11 and 12, respectively.

Here the thermal Image is the cover Image and the Logo image is the Visual image.

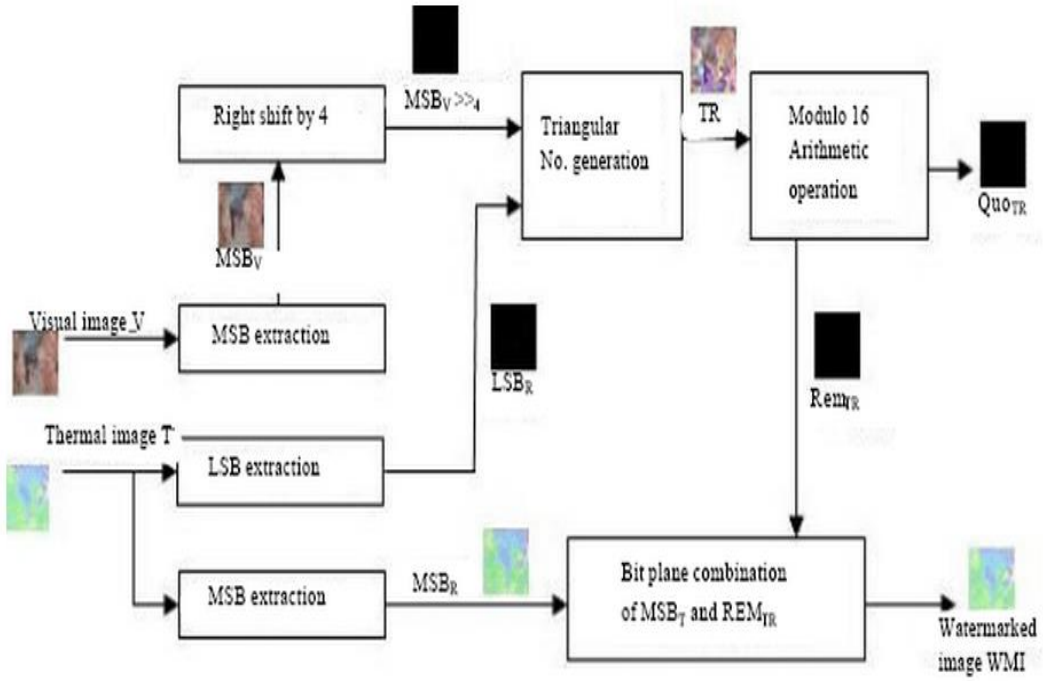

Figure 11 Watermark Embedding

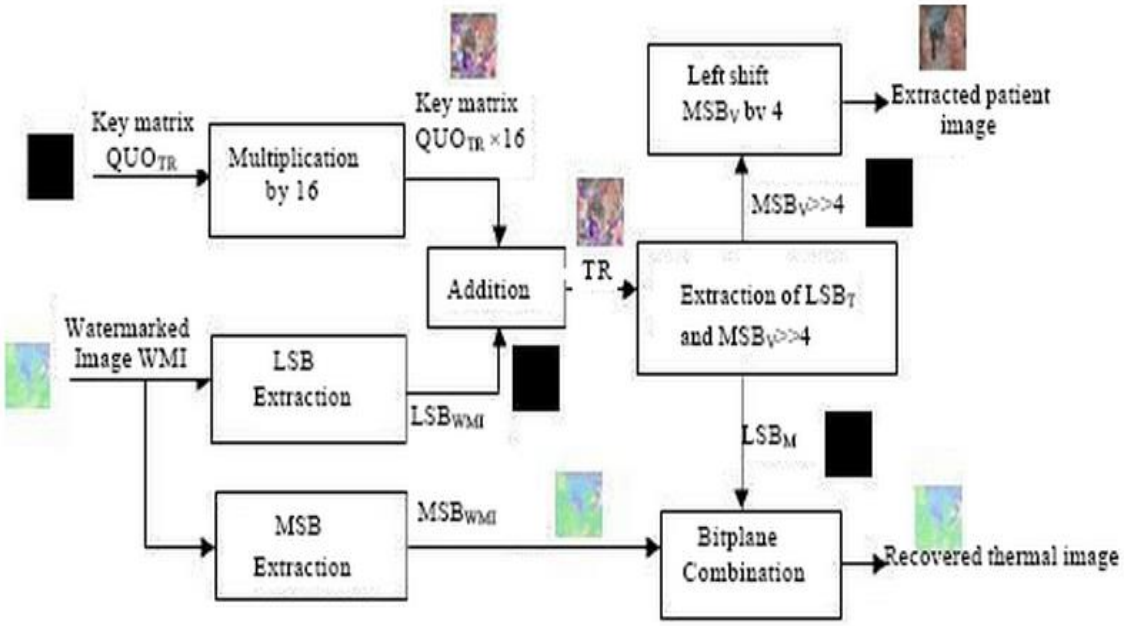

Figure 12: Watermark Extraction

This gives the complete understanding of the embedding and extraction process and working in the same manner we embed and extract watermarked image on several cover images which we have a database from Venu eye research Clinic.

CHAPTER 5

Experimental Results

5.1 COMPARISION OF INPUT IMAGE, WATERMARKED IMAGE AND REGENERATED IMAGE

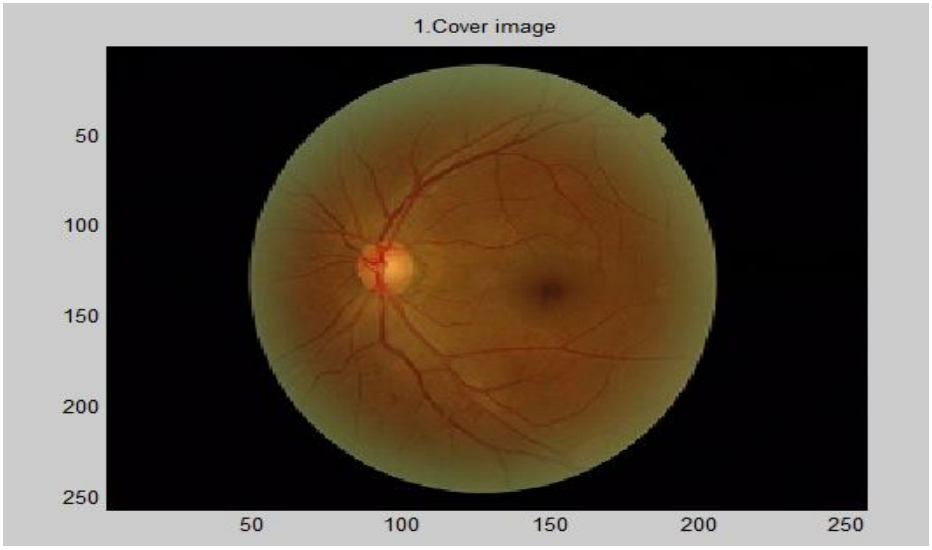

Figure 13: Input Cover Image

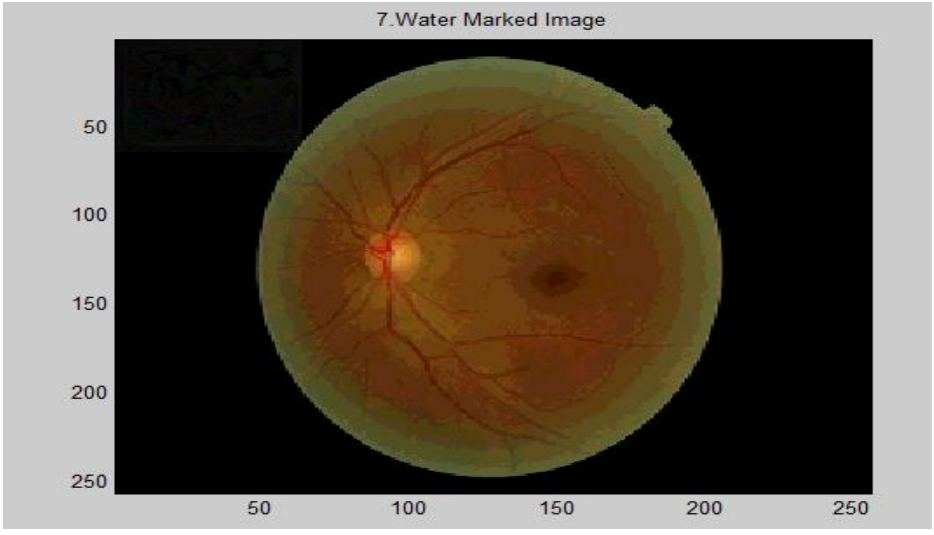

Figure 14: Watermarked Image

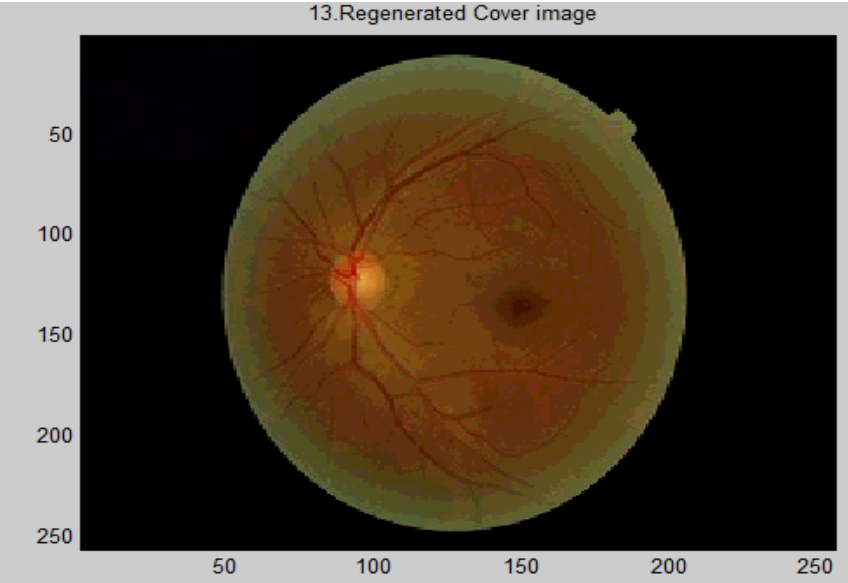

Figure 15: Regenerated Cover Image

5.2 COMPUTATION TIME FOR DIFFERENT WATERMARK SIZES

TABLE 2

Comparison of Computation Time

SAMPLE	COMPUTATION TIME for 64x64 watermark (seconds)	COMPUTATION TIME for 128x128 (seconds)
Sample 1	35.104453	38.566743
Sample 2	36.563452	39.667324
Sample 3	34.459954	38.452264
Sample 4	36.554673	40.956783

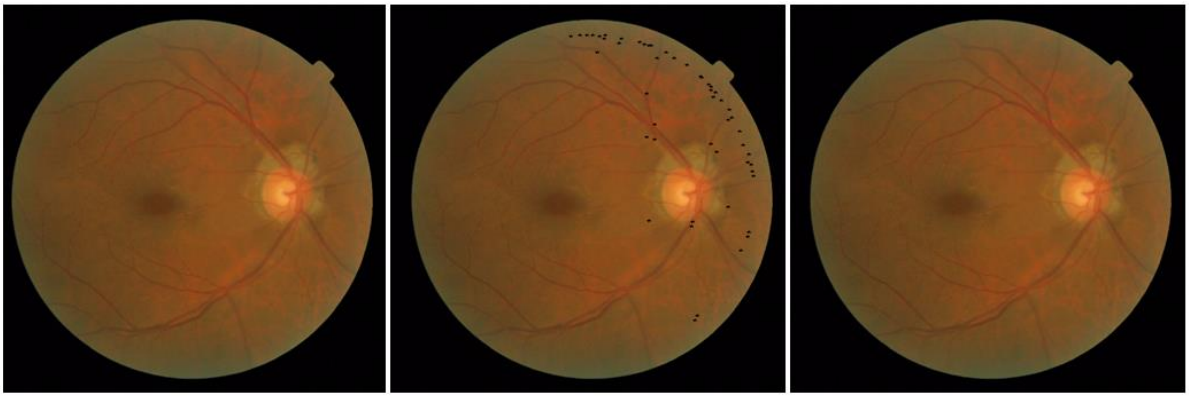

Fig 16. Sample image 1, (Left) Input cover, (Center) Watermarked image, (Right) Regenerated Image

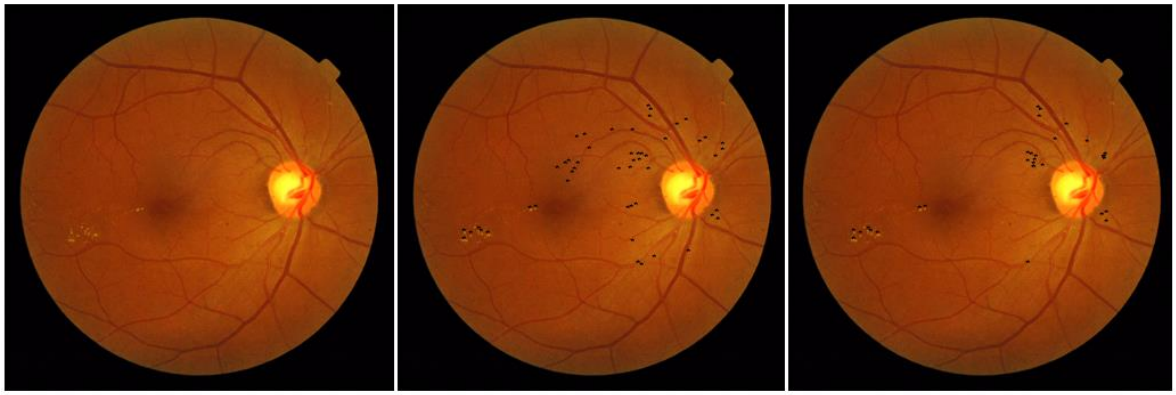

Fig 17. Sample image 2, (Left) Input cover, (Center) Watermarked image, (Right) Regenerated image

Fig 18 Sample image 3, (Left) Input cover, (Center) Watermarked image, (Right) Regenerated image

Fig 19. Sample image 4, (Left) Input cover, (Center) Watermarked image, (Right) Regenerated image

5.3 PSNR VALUE OF SELECTED SAMPLE IMAGES

The algorithm was successfully implemented and positive results for PSNR were obtained which can be seen from the Table 3.

For the sample image 1, the PSNR value for 64x64 sized watermark is 32.4343 and for 128x128 sized watermark PSNR is 32.2159.

TABLE 3

PSNR value for 128x128 and 64x64 watermark

SAMPLE	PSNR (64x64)	PSNR (128x128)
Sample 1	32.4343	32.2159
Sample 2	32.4543	32.2365
Sample 3	32.7674	32.4326
Sample 4	32.3978	32.1094

CHAPTER 6

Conclusion

This thesis examines a novel high capacity reversible multiple watermarking scheme applicable to all environments where security and privacy are the main concerns, such as medical record protection and archiving. The motivation of this project is to improve digital medical watermarking performance in different aspects to better serve the multimedia communication and its related problems. The designed and developed scheme benefits from three important and quintessential properties in the watermarking area: high capacity, reversibility, and multiple watermark embedding capability. It uses the Triangular number generator function to create the necessary embedding space in the sub-bands of the host image. The proposed scheme is tested on natural and medical images in instances where single or multiple watermarks are embedded showing significant improvement in data hiding capacity and visual quality of the marked image. The proposed scheme is then compared to four seminal methods, each exploiting different techniques; the obtained results show significant enhancement in performance that satisfies the criteria of high fidelity and data payload for digital watermarks.

This method also produces significantly high values of PSNR for all sample images and the difference between PSNR values for sample images with 64x64 and 128x128 watermark was very less. This indicates that this method is suitable for reversibly watermarking ERP to medical especially ophthalmic images without degradation of the diagnostic information content of the medical image.

CHAPTER 7

Future Work

The research basis of this project thesis can be extended in to two major directions. First, each of the proposed methodologies can be improved and enhanced in order to better serve the applications and purposes they are developed and designed for, also the work can be changed to address other applications where privacy and security properties are required. Furthermore, the proposed frameworks can be developed to offer added properties and features so they can be engaged in applications for which the proposed schemes with current properties are not suitable for.

The Structural Similarity (SSIM) index can be employed as a replacement of PSNR as the measure to evaluate the performance of the proposed reversible watermarking scheme.

The security layer used in the scheme can be modified such that embedding conditions and parameters are merged with encryption algorithm.

Also the proposed method can be adjusted to suit other purposes in applications where semi- fragile reversible data hiding is needed. The modifications can even be taken to the point of applying the scheme to video content.