East West University

Department of Electronics & Communications Engineering

Fall - 2018

Thesis Title

Watermarked Based Secured Image Processing in Cloud Environment

Submitted by

Sadia Afrin
ID : 2015 - 1 - 55 - 014.

Tahfiza Rahman
ID : 2015 - 1 - 55 - 016.

Supervisor

Mr. Rasel Ahmmed

Lecturer,
Department of Electronics and Communication Engineering,
East West University

Declaration

We hereby declare that we completed our thesis on the topic entitled **"Watermarked Based Secured Image Processing in Cloud Environment"**. We prepared a thesis report & submitted to follow the terms and condition of the **"Department of Electronic and Communication Engineering"**. This paper is required for fulfillment the degree of B.Sc. in Electronic and Communication Engineering.

We claim that the thesis paper along with its literature which is demonstrated in this report are own work.

..... **.....**

Sadia Afrin **&** **Tahfiza Rahman**

ID: 2015-1-55-014 **ID: 2015-1-55-016**

Signature of Supervisor:	**Signature of Chairperson:**
…….	**…….**
Mr. Rasel Ahmmed	**Dr. M. Mofazzal Hossain, PhD**
Lecturer, Department of Electronic and Communication Engineering,	**Professor, Department of Electronic and Communication Engineering,**
East West University, Dhaka,	**East West University, Dhaka, Bangladesh.**

Acknowledgement

First, we are grateful to almighty Allah for blessing us to successfully complete the task. A special thanks with honors to our supervisor Mr. Rasel Ahmmed for giving us his valuable time, guidance, motivating thought and encouragement which lead us to success.

We are also pleased to all our faculty members of ECE department for their guidance and support to complete our graduation degree.

A special thanks to our parents whose encouragement and prayer are always with us.

Thank you all for always supporting us.

Approval

This thesis report ‘Watermarked based secured image processing in cloud environment’ submitted by Sadia Afrin ID: 2015-1-55–014, Tahfiza Rahman ID: 2015-1-55-016, to the department of Electronic and Communication Engineering. East West University is submitted in partial fulfillment of the requirement for the degree of B.Sc. in Electronics and Telecommunications Engineering, under complete supervision of the undersigned.

Approved By:

……

Supervisor

Mr. Rasel Ahmmed

Lecturer,

Department of Electronic and Communication Engineering,

East West University.

Abstract

Watermark is the traditional and reliable data hiding process which remains the most effective security layer in medical technology. It is not much popular in Bangladesh for its less research work and the production process is known to us. Watermark has many Tanique in digital multimedia system. In this work, we collected MRI (Magnetic Resonance Imaging) data for the analysis from literature. These data contain patient's valuable information with their confidentiality or secrecy in biological ingredients and their application on different types of diseases. In our analysis we considered criteria like copy protection, fingerprinting, owner identification, data authentication and watermark attacks. But those data are random data and for our analysis we need to process those data. That's why we have to apply 'MATLAB' as tool for image analysis.

We generated two techniques, one is Least Significant Bit and other one is Visible. We classified them into their most preferable usage and successfully embedded and extracted Using medical MRI data. Finally we have find out most effective results against correspondent attacks. Our research will help patients satisfying a multiplicity of applications in medical information protection, safety and management for a better speed in our daily communicative life.

Contents

Chapter 1

Introduction

With the rapid growth of technology, medical science have started using wireless media for exchanging biomedical information (Electronic Patient Report or hospital logo) for mutual availability of case studies which arises the level of security and authenticity for transmitting biomedical information through the any transmission medium is quite high. All the requirements like level of security can be increased; authenticity of the information can be verified by adding ownership data as the watermark in the original information. This chapter's main objective is to broaden the understanding of healthcare services provided by social media. The reader will be able to understand the means by which medical information is exchanged online and how to interpret this information with some specific examples.

1.1 What is Watermarking?

Basically, watermark is a transparent image or text that has been applied to a piece of paper, another image to either protect the original image, or to make it harder to copy the item e.g. money watermarks or stamp watermarks. A transparent watermark is added to a photo by changing the image on the pixel level. The pixels that will make up the resulting watermark is changed more or less in the direction of the watermarking image, if the watermark is 50% transparent, 50% of the RGB (Red, Green & Blue) values are deducted from the original image, and 50% of the RGB values from the watermark are added to the image. There is done a lot of research into adding an invisible watermark to images that is hard to remove. Digital watermarking is the method of embedding data into digital multimedia content [1]. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. Visible Watermarking is that when data embedded as the watermark. This can be a logo or a text that denotes a digital medium's owner. Invisible Watermarking: The data embedded is invisible or, in case of audio content, inaudible. Robust watermarks involve blending signal amplitude with large bandwidth sizes and a short message length [2].Frequency domain capabilities and mixed-domain techniques, when

added to signals, believed to provide the right amount of robustness in order to guard against watermark attacks. Robust watermarks involve blending signal amplitude with large bandwidth sizes and a short message length [2].

1.2 Motivation

Digital watermarking technique may use for protecting the digital intellectual properly to secure of authenticate images and it can also detect the recover illegal changes which made tele radiology images. Digital image watermarking is the practice of hiding secret data into digital medical image. This technique is used to implement schemes and algorithms capable of providing the required security service to telemedicine application [3]. Digital watermarking also can be categorized into visible and invisible, fragile and robust, blind and non-blind with emphasis on authentication rightful ownership and available of the host image respectively. The strength of the embedded watermark and noise are controlled to prevent the image from being used directly regarding to visual properties o the host signal**.**

1.3 Proposed work

In our proposed work, watermark is added in the MRI (Magnetic Resonance Image) using LSB (Least Significant Bit), and also by defining the ROI (Region of Interest) \in the biomedical image. Our proposed method of adding watermark in the ROI of the images is most effectual for those medical images which are resultant of such imaging processes which has image segmentation as one of the essential intermediate part of the process. The efficacy of the proposed method claims robustness against most common attacks. We present an overview of watermarking technology by paying attention to visible and LSB watermarking since it is the usual scheme for authentication. In addition to describing the necessity of watermarking medical data we adopted these procedure. The whole procedure will discuss in details in following chapters.

1.4 Applications of watermarking

Applications of watermarking should contain the following features like security and owner identification is needed. Watermarking can be employed for multiple purposes such as:

1.4.1 Data Authentication

Authentication is the process of identify that the received content or data should be exact as it was sent. There should be no tampering done with it. So for that purpose sender embedded the digital watermark with the host data and it would be extracted at the receivers end and verified. Example like as CRC (cyclic redundancy check) or parity check [4].

1.4.2 Fingerprinting

To assigned a unique identification by storing some digital information in it in the form of watermark is called fingerprinting technique. Detecting the watermark from any illegal copy can lead to the identification of the person who has leaked the original content. Even movies has the watermark having theater identification so if theater identification detected from a pirated copy.

1.4.3 Copy Protection

Copy protect bit prevents Illegal copying by watermarking. This protection requires copying devices to be integrated with the watermark detecting circuitry.

1.4.4 Owner Identification

The application of watermarking to which he developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attackers. So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and removed [4].

1.4.5 Broadcast Monitoring

Broadcasting of TV channels and radio news is also monitoring by watermarking. It is generally done with the Paid media like sports broadcast or news broadcast.

1.4.6 Medical applications

Medical media and documents also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means [4].

1.4.7 Watermark Attacks

Our data faces so many threats so this needed protections from this attacks [1, 2, and 4]. Hereby an introduction has been arranged to view some threats that our data or in our proposed medical data cam face are given below:

- Geometric transformations: Whirl, transference, diverge and resizing image.
- Image Enhancements: Changing contrast, color measure out, sharpening image or text or signal.
- Image Composition : There must be an addition of text, windowing with another image
- Information Reduction: This means cropping an image.
- Multiple watermarking: add second watermark to image that creates a problem of validating the owner information.
- Collusion attacks: Multiple receiving of the same host image.
- Forgery: The same watermark at multiple recipients of different images.

1.5 Summary

In this chapter described the following matters which are effective in point of concerning of the segmentation.

- The basic of watermarking criteria is presented in point of authentication and medical application.
- The different kind of watermark for different image criterion is also clarified with logical view.
- The relevant attacks of the each watermark is presented.

Chapter 2

Literature Review

2.1 Introduction

This chapter concludes about the originate stage of watermark and the story behind its starting point. The idea of hiding data in another media is very old, as described in the case of steganography. Watermark can be found back when a watermark was something that only existed in paper. That time paper was still wet/watery and therefore the mark created by this process is called a watermark. Watermarks were first introduced in Fabriano, Italy, in 1282. Watermarks were created by bending pieces of wire into filigree designs, taken from the French word " filigrane " and secured to the wire mesh. Any design would displace fibers imparting a faint translucent image into the sheet particularly evident when held to the light. It was believed these early watermarks served to identify the work of individual paper makers. This was an extremely arduous activity and wages were earned on a piecework basis.

2.2 History

Originally regarded as almost an art form by the early Italians the watermark soon became synonymous with security. Around 1700 when banknotes first began to appear from the newly founded national and central banks of Europe watermarks were introduced in an attempt to thwart counterfeiting. The invention of the Fourdrinier paper machine in the late 18thCentury created a need to make watermarks on the continuous reel of paper. The dandy roll invented around 1825 was conceived to make an impression by rolling over the surface of the paper whilst in a fluid state displacing fibers and creating the thickness variations necessary to form a watermark. The term digital watermarking first appeared in 1993, when Tirkel et al. (1993).

Visible watermarks are especially useful for conveying an immediate claim of ownership (Mintzer, Braudaway & Yeung, 1997). Invisible watermarks, on the other hand, are more of an aid in catching a thief than for discouraging theft in the first place (Mintzer et al., 1997; Swanson et al., 1998).As watermarking skills developed so more and more complex tonal designs began to appear. These were produced by directly embossing the wire mesh, rather than by attaching designs to the

surface. This method caused the fibers to rearrange themselves into denser areas which appear as the darker parts of the watermark. The use of watermarks now extend from corporate and brand identity through to the creation of highly decorative and innovative products [4]. Their use in the protection of security documents remains as pertinent today as 300 years ago. A genuine watermark cannot be reproduced in any other way than the classic methods on a paper machine.

2.3 Background study (Others work and their limitations)

2.3.1 Visible and Invisible Watermarks

Watermarking is divided into two effective categories: visible and invisible. An example of visible watermarking is presented by television channels, like BBC that has logo visibly superimposed on the corner of the TV picture visible watermark is very simple and equivalent to stamping a watermark on paper. On the other hand invisible watermarking, is a far more complex concept. It is most often used to identify copyright data, like author, distributor, and so forth. Though a lot of research has been done in the area of invisible watermarks, much less has been done for visible watermarks. Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Their main advantage, in principle at least, is the virtual elimination of the commercial value of a document to a would-be thief, without lessening the document's utility for legitimate, authorized purposes [5].

There are different classifications of invisible watermarking schemes because of the enormous diversity of watermarking approaches can be distinguished in terms of watermarking host signal (still images, video signal, audio signal, integrated circuit design), and the availability of original signal during extraction (non-blind, semi-blind, blind). They can be categorized based on the domain used for watermarking embedding process [6]. These are grouped into:

- Spatial domain techniques.
- Transform domain techniques.
- Feature domain techniques.

Recent watermarking techniques described in the literature can be grouped into three main classes. Transform domain methods embed the data by modulating the transform domain signal

coefficients. Spatial domain technique watermark by directly modifying the pixel values of the original image. The transform domain techniques have been found to have the greater robustness, when the watermarked signals are tested after having been subjected to common signal distortions. Feature domain technique takes into account region, boundary and object characteristics. Such watermarking methods may present additional advantages in terms of detection and recovery from geometric attacks, compared to previous approaches.

2.3.2 Spatial Domain Techniques

This section gives a brief introduction to the spatial domain technique to gives some background information about watermarking in this domain. Adding fixed amplitude (PN) sequences to an image is called spatial techniques. PN sequences are used as spreading key when considering the host media as the noise in a spread spectrum system, where the watermark is the transmitted message. PN sequence is used to spread the data bits over the spectrum to hide the data [6].

2.3.3 Transform Domain Techniques

Transformation is first applied to the host data, and then modifications are made to the transform coefficients. This has three parts, including discussions of wavelet based watermarking, DCT-based watermarking and fractal domain watermarking.

2.3.4 Wavelet Decomposition

Video watermarking applications based on a 3-D wavelet transform due to its simple structure. Multi-resolution detection of the digital watermark allows a Gaussian distributed random vector added to high pass bands in the wavelet domain.

2.3.5 Discrete Cosine Transform

Several watermarking algorithms have been proposed to utilize the DCT. However, the Cox et al. (1995, 1997) and the Koch and Zhao (1995) algorithms are the most well-known DCT-based algorithms. Cox et al. (1995) proposed the most well-known spread spectrum watermarking schemes [5, 6].

2.3.6 Fractal Transform-Based

There few references exist for invisible watermarks based on the fractal transform. Restricted amount of binary code can be embedded using this method and fractal analysis is computationally expensive and some images do not have many large self-similar patterns, the techniques may not be suitable for general use.

2.4 Summary

This chapter encapsulates history behinds the origination and previous techniques and their limitations. In this chapter, some of the worthwhile recent research works done on watermark embedding and extraction are discussed to review. Through analysis of the literature, it is found that medical image watermark analysis is one of the most active research areas and enormous research has been done in this area for the last many years.

Chapter 3

Methodology

3.1 Introduction

Medical technology continues the faster motion of innovation in research and healthcare. It plays a crucial role in our life. with the constant pace of progress and increasing amount of digital exchangeable data generates new information security needs. Medical documents and patient's information are also affected. Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of medical documents. In the current state of research, it is difficult to affirm which watermarking approach seems most suitable to ensure an integrity service adapted to MRI images and more general way to health status, preventive health services, treatment and other informative documents. According to human perception watermark can be visible or invisible. Another classification of watermarking procedure is also done as below

1) Robust watermark
    - Generally, it uses as copyright protection and authentication
    - Sustainable to all attacks.

2) Fragile watermark:
    - Purposed for integrity
    - It can be used to localize tempers and also category of tempering.

This procedure can be performed in spatial domain and frequency domain. It is analyzed that frequency domain process are more robust than spatial domain process of watermark. Host data can be any digital multimedia elements like audio, text, image etc [6]. Our scheme indicates the secure process of digitized medical image using LSB technique and visible watermarking.

3.2 LSB Watermarking

The idea of proposed LSB watermarking method, it makes the secure random level of cover image to increase the robustness of the watermarked image. This technique is used for embedding information into a cover image. Typically, in this scheme there is no need to change the whole bit sequence. Only specific bit will get modified and by then a small change of pixel intensity of the colors will occur. The watermarking is done by choosing a subset of image pixels and substituting the LSB of each of the chosen pixels with watermark bits. It is imperceptible by human eyes. LSB watermark can be extract by modifying the changes bits of the watermarked image, as it is a simple watermarking procedure of image. LSB watermark procedure is applicable for multimedia elements as well [7]. The tool used for the execution of this algorithm was MATLAB. The aim of the program is to replace the LSB of the base image with the MSB of the watermark.

Feature of LSB watermarking:

- It is a simple operation.
- Facile to perform.
- It executes the pixel values of the image to be hidden.
- Generates secure random coordinates for robustness of the watermarked image.

This method is quite effective and less complex. For a grayscale bitmap 8-bit Image, it can present 256*256 gray colors. Last two significant bits of each color is encoded which is imperceptible through human eyes. In this proposed method least significant bit of grayscale image will be used for embedding watermark and without losing information of data will recover embedded watermark. Indeed, this approach allows patients to insert data into a set of different types of images (MRI).

Data acquisition:

We have taken MRI (magnetic resonance imaging) that should be hidden by using LSB (Least Significant Bit) whereas only last bit will be change of the grayscale MRI image. To have the

cognizance of medical data in our work we have taken brain MRI images for normal patient, critical patient and abnormal patient. The medical technology has mentioned and previously demonstrate the importance of magnetic resonance imaging. Our brain is the highly specialized organ that controls the human body functions. MRI (magnetic resonance imaging) process is the widely accepted imaging process in brain imaging. We originate the process with brain MRI image as cover image as well as image to be hidden which all have the equal sizes and same resolution. The simulation results of the proposed system are summarized below. First the watermarks were generated and then embedded in the medical images (MRI). After that, the watermark extraction procedure was performed.

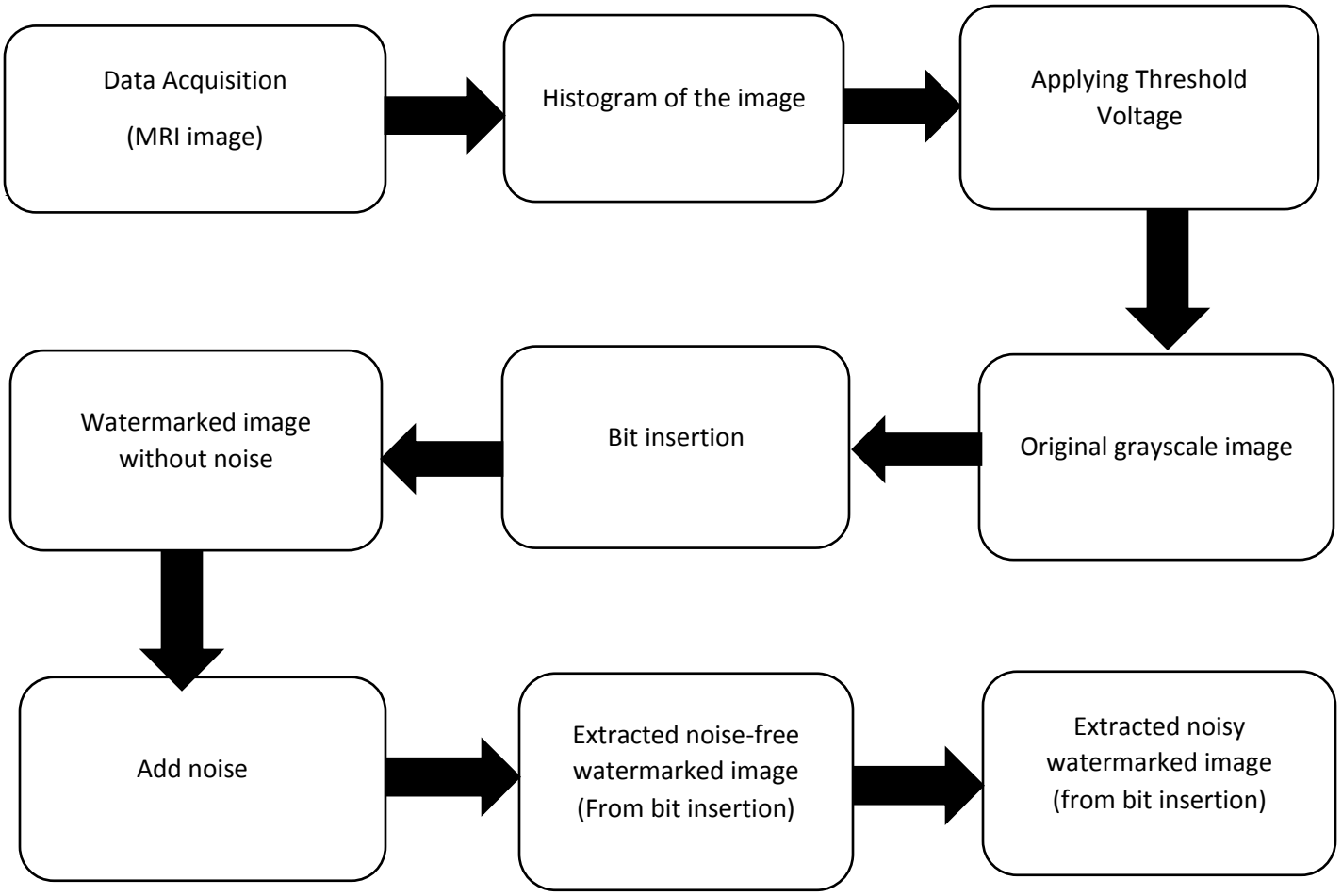


Figure 3.1: Implantation and extraction of watermark using LSB technique.

Histogram:

Histogram provides useful information about an image demonstrated by graph analysis. It signifies the pixel intensity distribution of an image. High contrast image manifest the evenly spaced histogram. Since contrast of an image is revealed by histogram, low contrast image like grayscale image will not have much clear distribution of pixel intensity levels. Histogram varies with pixel intensity, color contrast. Photoshop has extensive histogram display tools in MATLAB. Histogram of a monochrome image with L possible gray levels f = 0 1 L-1 possible Gray levels, f=0, 1, ..., L-1.

P (l) = n1 / n,

- n is the number of pixels with gray level l
- n1 is the number of pixels with gray level l.
- P is the total number of pixels in the image

The histogram of an image shows us the distribution of grey levels in the image massively useful in image processing or in other words the image histogram provides a global description of the visual appearance of the image. An image from MRI scan is composed of gray level intensity values in the pixel spaces. The gray level intensity values depend on the cell concentration in the volume scanned. A darker region indicates the presence of some abnormality.

Threshold Voltage:

Thresholding endeavors to consider an intensity value of gray level image that creates division among intensity values. It performs division by determining pixel group with intensity greater than the threshold into one division and other pixels into another division.

This technique is characterized based on image space region that has the capabilities of transforming a color image into binary image. Proper threshold value to allocate image pixels into different regions and foreground from background.

For application of thresholding based segmentation technique, it is required to apply the correct threshold values in order to achieve proper segmentation results, otherwise results are poor.

Bit insertion:

In this scheme images are 256*256 Pixels by 8 bit per pixel gray scale image. Simple approach to embedding information in a graphical **image** file. Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel values Least Significant Bit (LSB) modifications. Kurah and McHugh's proposed an algorithm to embed in the LSB and it was known as image downgrading. Least Significant Bit insertion is an example of the less predictable or less perceptible. This section explains how this works for an 8-bit grayscale image and the possible effects of altering such an image. If we use a grayscale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255.

Noise effect:

The normalized correlation coefficient (NCC) is used to measure the similarity between the cover image and the watermarked image. There are different types of distortion **(Salt and Paper Noise, Gaussian Noise, Poisson Noise, Speckle Noise)** to the watermarked image and the error is calculated by Mean Square Error (MSE). The traditional error measuring techniques are mainly MSE and Peak Signal to Noise Ratio (PSNR). These are widely used because they are simple to calculate and are independent of viewing conditions and individual observers. At the embedding section we added Gaussian noise that creates a difference to the output of the entire process.

Noise effects image bit substitution and creates visual distinguish between the cover image and watermarked image. Noise is impermissible and gives inappropriate results comparing with the extracted image.

3.3 Visible watermarking

Visible watermark is another technique of embedding watermark into an object or digitized image to help to protect the owner's right to that object. It commonly used in applications such as photograph catalogs, allowing the viewer to see what the image is like before ordering a good

copy. A visible logo or label is placed at the corner of the image or overlays a transparent pattern over the image. This renders the viewed mage useless for reproduction or commercial use.

In medical field, it is required to provide integrity, ownership of documents and maintain confidentiality of patient and hospital data. It continues to play a vital role in various medical applications. In medical applications, documents must be kept without any loss of information that is, watermark should not introduce visible distortion in the image.

Feature of visible watermarking:

- Easiest ways to prove authentication.
- Lossless property is used to ensure the signal fidelity
- Since embedded part is visible the original watermark is available and helps for the recovery of the original host image from the watermarked image.

Medical imagery field need assurance of security, authenticity and manage capacity of diagnostic information of patient. For this reason, visible watermark method keeps pace with demand. In this scheme we propose a visible watermarking which actually carries the ownership of medical data and perceptible to human naked eyes.

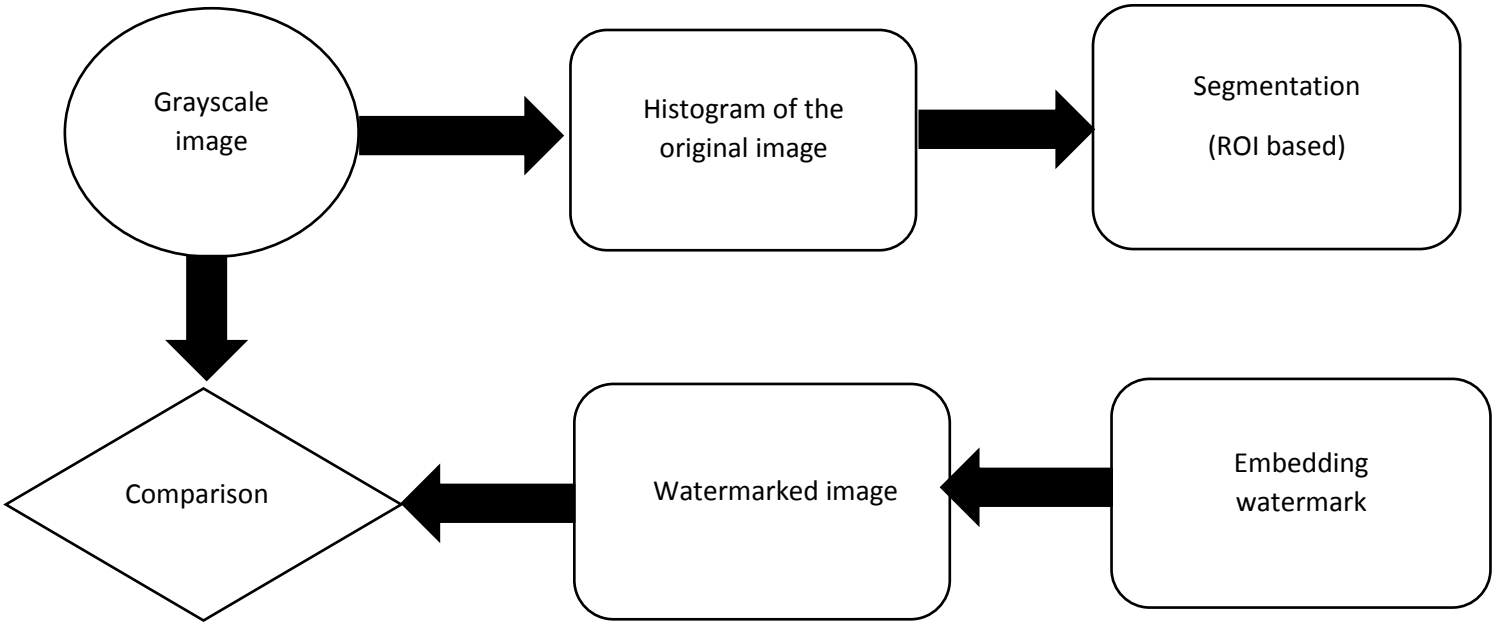


Figure 3.2: Generation of visible watermark

Embedding process of visible watermark:

In this step we take a forward move to segment the image based on important part that provides useful information of diagnoses. Image segmentation divides images into different regions and simplifies the image in more meaningful, informative, feasible. Segmentation can be performed in various techniques as below

- Thresholding
- Edge detection
- Region-growing methods

ROI (region of interest):

Region-based watermarking methods separate medical images into two parts: region-of-interest (ROI) and region-of-non-interest (RONI). The ROI of the image contains the significant information that the physicians utilize for the diagnosis. It is also the region whose integrity must be strictly controlled since the modification of even one bit may not be tolerated. On the other hand, the RONI of the image does not contribute to the diagnosis process and thus can be used for robust watermark insertion. After identifying the RONI, data is hidden within that region using watermark embedding. As data is hidden within less informative region, distortion of that region of the image due to watermark embedding does not cause any loss in the diagnostic.

3.4 Summary

In image watermarking techniques, the main consideration is the evaluation of the robustness and effectiveness of the watermarking method through measurement of the impact of different attacks upon the watermarked image. Based on the watermarking method used, the image may be robust against a specific group of attacks. This section gives an overall vision on different groups of attack that may be used by invaders to remove the watermark from the watermarked image. In this chapter, we demonstrated the conventional technique of watermarking. The experimental results provide an indication of the potential of the approach

- Patient information is hidden for innocuous eyes, and stays with the related image.
- The image can be unambiguously authenticated.
- Image can be recovered in its integrality for a reliable diagnosis.

Chapter 4

Result and Analysis

4.1 Introduction

In this section, we used visible and watermarking as an unsupervised algorithm to analysis our data for accumulating the requirements. In addition, we can find out similar effectiveness/productiveness methods included in watermark. More importantly, we can find out the easiest but time consuming process. We have used MATLAB programming for analyzing and visualizing our data.

4.2 Visible watermarking

Visible watermark starts with defining some sort of images that is based on diagnosis or MRI. In this entire procedure we asserted adult brain image in normal and critical condition. Initially each content carries medical information but afterwards we implement a label of box to ensure characteristics of data transfer without any harm.

Embedding:

```
folder = fullfile(desktop, '\thesis resized imgae');
baseFileName = '*.jpg';

fullFileName = fullfile(folder, baseFileName);

if ~exist(fullFileName, 'file')

    fullFileName = baseFileName;
    if ~exist(fullFileName, 'file')

        errorMessage = sprintf('Error: %s does not exist in the search path folders.', fullFileName);
```

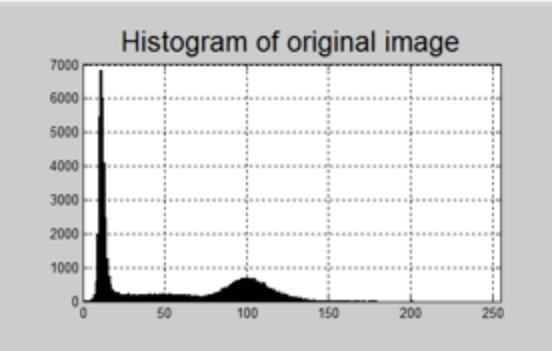
```
        uiwait(warndlg(errorMessage));
        return;
    end
end
grayImage = imread(fullFileName);

[rows, columns, numberOfColorBands] = size(grayImage)
```

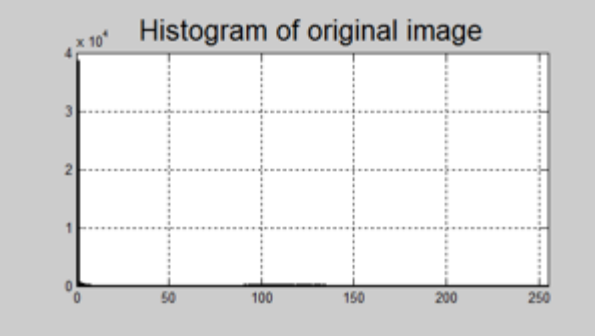
Firstly, an MRI image is taken which is made using MATLAB through the brain MRI images are collected. The input image is adjusted and enhanced then as below:

(a) (b)

Figure 4.1: (a), (b) Input MRI image

```
set(gcf, 'units','normalized','outerposition',[0 0 1 1]);

set(gcf,'name','Demo by ImageAnalyst','numbertitle','off')

 [pixelCount, grayLevels] = imhist(grayImage);
subplot(2, 2, 2);
bar(pixelCount);
grid on;
title('Histogram of original image', 'FontSize', fontSize);xlim([0 grayLevels(end)])
```





The histogram generates graphical representation and demonstrates the feasibility of using values as a simple and rapid technique of image decoding. We generated histogram against an original MRI image that is sized as 256*256 which provides the global description for visual purpose.

```
subplot(2, 2, 1);
promptMessage = sprintf('Drag out a box that you want to copy,\nor click Cancel to quit.');
titleBarCaption = 'Continue?';
button = questdlg(promptMessage, titleBarCaption, 'Continue', 'Cancel', 'Continue');
if strcmpi(button, 'Cancel')
    return;
end

k = waitforbuttonpress;
point1 = get(gca,'CurrentPoint');
finalRect = rbbox;
point2 = get(gca,'CurrentPoint');
point1 = point1(1,1:2);
point2 = point2(1,1:2);
p1 = min(point1,point2);
offset = abs(point1-point2);
xCoords = [p1(1) p1(1)+offset(1) p1(1)+offset(1) p1(1) p1(1)];
yCoords = [p1(2) p1(2) p1(2)+offset(2) p1(2)+offset(2) p1(2)];
```

x1 = round(xCoords(1));

x2 = round(xCoords(2));

y1 = round(yCoords(5));

y2 = round(yCoords(3))

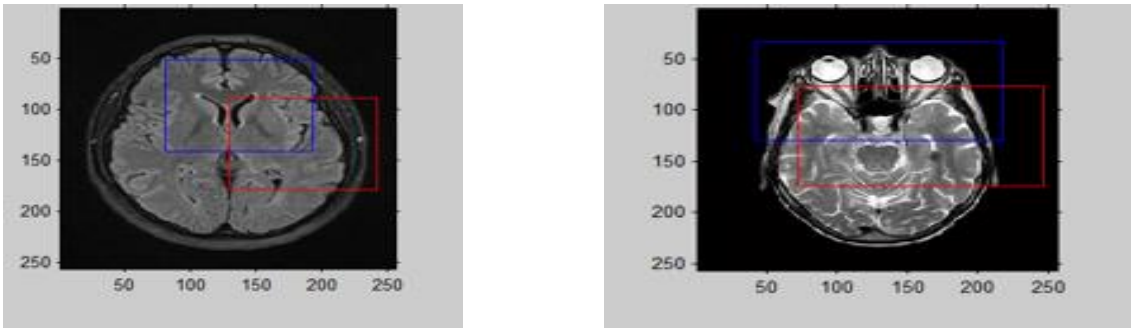
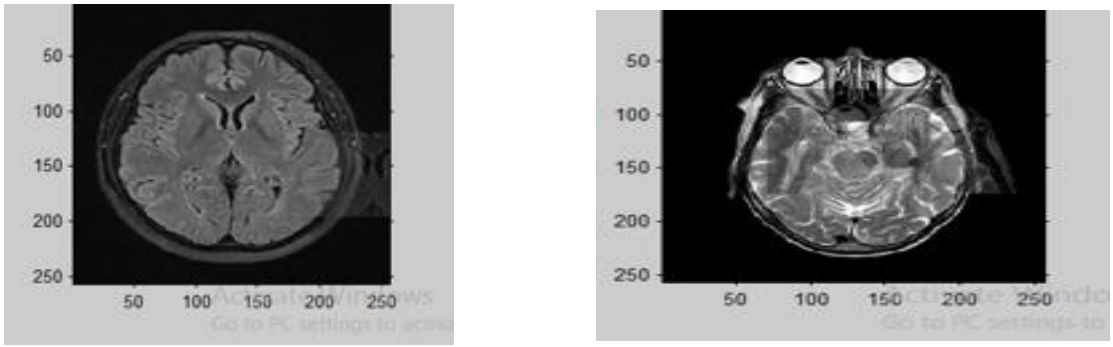


Figure 4.2: Examples of ROI based segmentations

Segmentation of image has been done by drawing a box over there. The picture indicates measured dimensions of the image information that we want to watermark as a logo and pasted the specific information. ROI approved watermark by considering region.



(a) (b)

Figure 4.3: Visible watermarked images

Watermark generated and the comparison of enhanced and morphological image comprehends the feature of these images.

4.3 Least Significant Bit (LSB)

```
[hiddenFileName, pathname]=uigetfile('*.jpg', 'Enter the picture');
hiddenImage = imread([pathname hiddenFileName]);
hiddenImage=imresize(hiddenImage, [256 256]);
 [hiddenRows hiddenColumns numberOfColorChannels] = size(hiddenImage);
if numberOfColorChannels > 1

   hiddenImage = hiddenImage(:,:,1);
end
subplot(3, 3, 1);
imshow(hiddenImage, []);
title('Image to be Hidden', 'FontSize', fontSize);
 [pixelCount grayLevels] = imhist(hiddenImage);
subplot(3, 3, 2);
bar(pixelCount);
title('Histogram of image to be hidden', 'FontSize', fontSize);
xlim([0 grayLevels(end)]);
grid on;

thresholdValue = 50;
binaryImage = hiddenImage < thresholdValue;
 subplot(3, 3, 3);
imshow(binaryImage, []);
caption = sprintf('Hidden Image Thresholded at %d', thresholdValue);
title(caption, 'FontSize', fontSize);
```

Basically, we are hiding information of a MRI image with another MRI image by using LSB method. In this section a 256*256 MRI image is taken upon another MRI image which is denoted as original image and analysis our data. Analyzing number of rows and columns for original image. Histogram of the image is generated to observe information that is going to be hide.

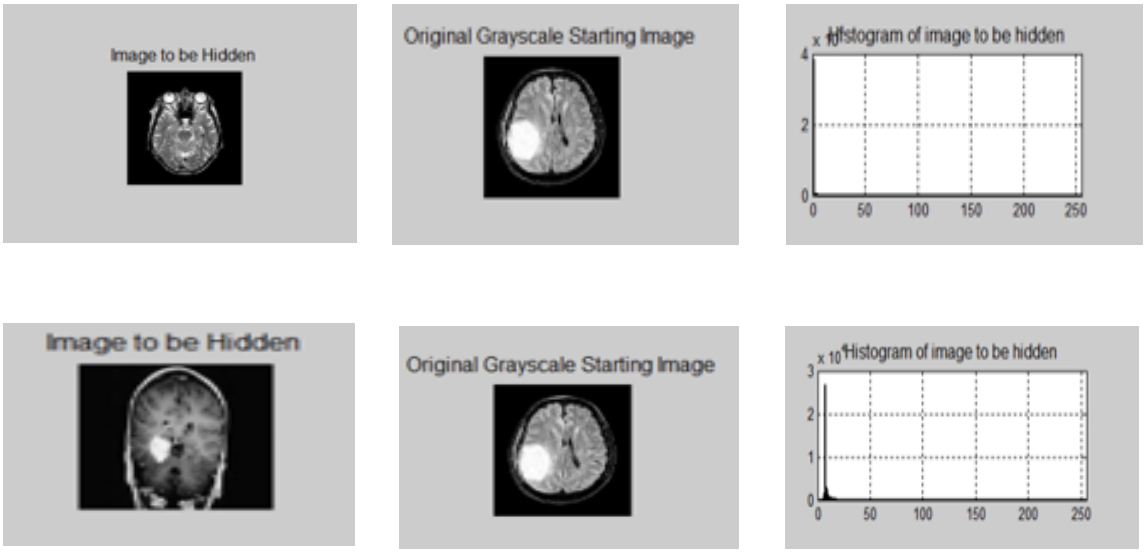


Figure 4.4 (a): MRI image of brain blood Circulation

Figure 4.4 (b): Original grayscale brain tumors image

Figure 4.4 (c): Histogram of the Image to be hidden

Next, Threshold voltage is applied to segregate the pixel intensity of the image take whose information is about to hide. In general MRI images has good spatial resolution. Thresholding techniques identify a region based on the pixels with similar intensity values. This technique provides boundaries in images that contain solid objects on a contrast background. Thresholding technique gives a binary output image from a gray scale image. At different threshold voltage outcome varies. So, application of right threshold value is necessary. Binary image is same as hidden image but that hidden image must have pixel intensity less than threshold value.

(d) (e)

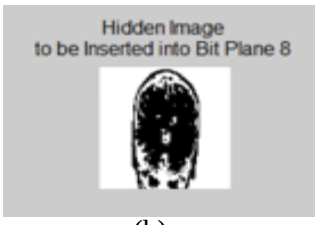
Figure 4.5: Examples of Thresholding MRI images at 70 and 50 respectively

```
      [hiddenRows hiddenColumns] = size(binaryImage);
end
    watermark = watermark(1:visibleRows, 1:visibleColumns);
else
   watermark = binaryImage;
end
subplot(3, 3, 5);
imshow(watermark, []);
caption = sprintf('Hidden Image\nto be Inserted into Bit Plane %d', bitToSet);
title(caption, 'FontSize', fontSize);
watermarkedImage = originalImage;
for column = 1 : visibleColumns
   for row = 1 : visibleRows
      watermarkedImage(row, column) = bitset(originalImage(row, column), bitToSet,
watermark(row, column));
   end
end
```

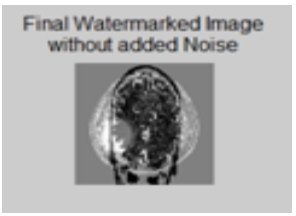
Now in this section bit plane is inserted into the threshold voltage applied image. This bit plane insertion can be any among (1-40). And then if the image is bigger than the original image size then it scales both images at an equal size. Attempts to update the columns and rows of the image and generated binary image as well. If the hidden images smaller, so that it will cover the original image. Crop it to the same size as the original image. Watermark the same size as the original image. Display the difference of threshold binary image and watermark image.

(f)

(g)



(h)

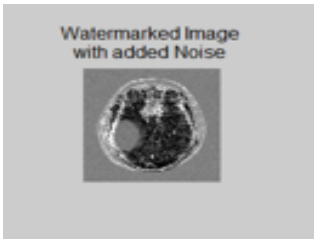


(i)

Figure 4.6: (f), (h) Image with bit insertion and (g), (i) watermarked image without added noise

```
noisyWatermarkedImage = imnoise(watermarkedImage,'gaussian', 0, 0.0005);

subplot(3, 3, 7);
imshow(noisyWatermarkedImage, []);
caption = sprintf('Watermarked Image\nwith added Noise');
title(caption, 'FontSize', fontSize);
```

Noise is added to the watermarked image. It provides difference between the noise added image and without added noise image. We add Gaussian noise to the watermark image and caption it as watermarked image with noise added.



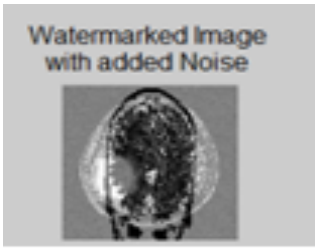
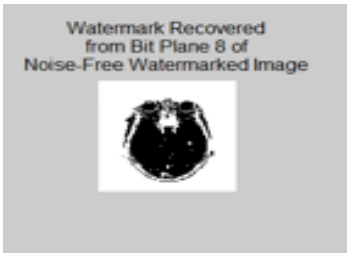


Figure 4.7: Watermarked image with noise

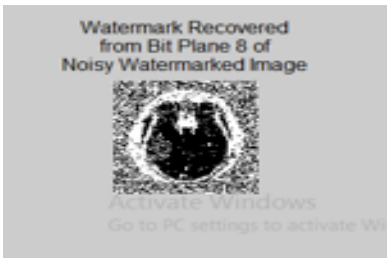
```
recoveredWatermark = zeros(size(noisyWatermarkedImage));
recoveredNoisyWatermark = zeros(size(noisyWatermarkedImage));
for column = 1:visibleColumns
   for row = 1:visibleRows
      recoveredWatermark(row, column) = bitget(watermarkedImage(row, column), bitToSet);
      recoveredNoisyWatermark(row, column) = bitget(noisyWatermarkedImage(row, column),
bitToSet);
```

```
    end
end

recoveredWatermark = uint8(255 * recoveredWatermark);
recoveredNoisyWatermark = uint8(255 * recoveredNoisyWatermark);

subplot(3, 3, 8);
imshow(recoveredWatermark, []);
caption = sprintf('Watermark Recovered\nfrom Bit Plane %d of\nNoise-Free Watermarked Image', bitToSet);
title(caption, 'FontSize', fontSize);
```

To extract the watermark from the image we are starting with the watermarked noisy corrupted image. We use the known bit plane of watermarked image to recover the watermark. Scale the recovered watermark to 0=255. Display the watermarked recovered from bit plane images which is noise free and noisy afterwards.

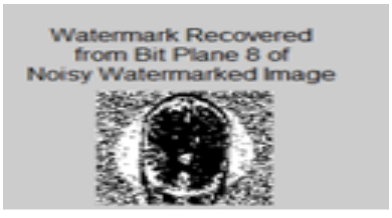


(i)



(j)

(k)



(l)

Figure 4.8: (i), (k) watermarked removed noise-free image and (j), (l) watermark removed noisy image

The entire procedure demonstrated into the following demo analysis below that indicates the embedding and extraction watermark of patient's a grayscale image (adult brain MRI) with a brain tumor MRI:

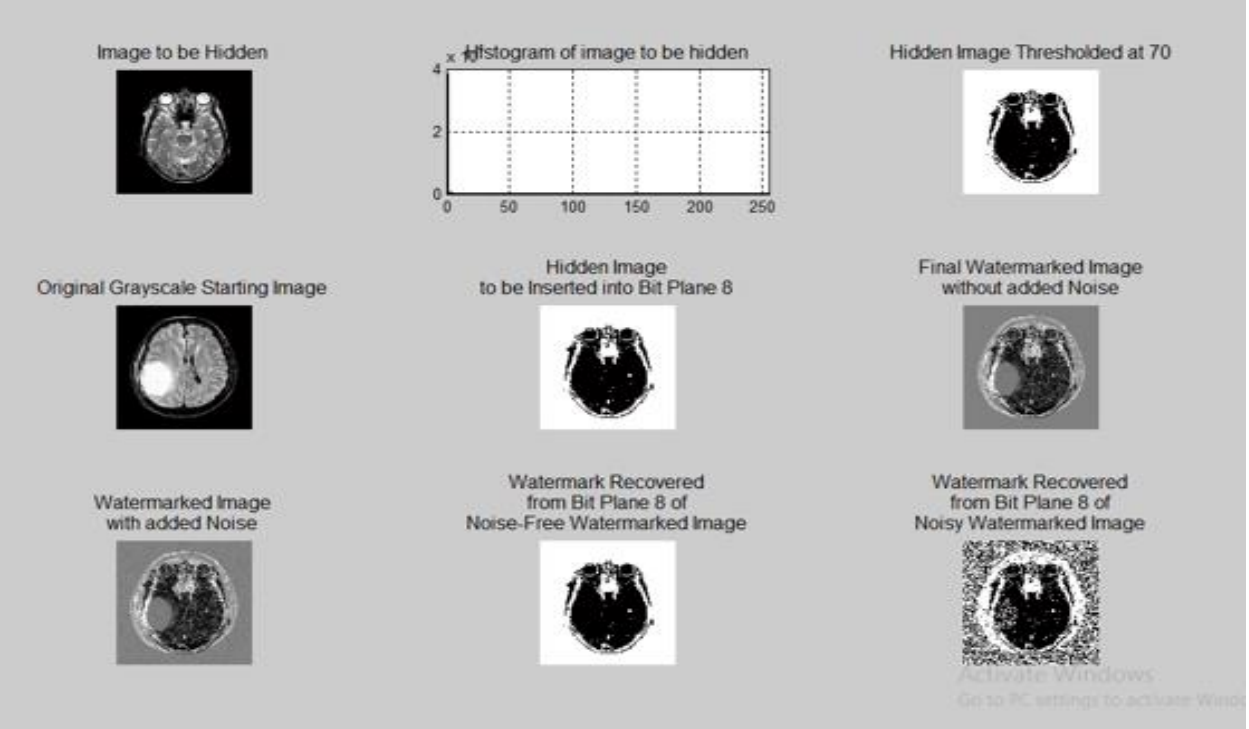


Figure 4.9: LSB watermark at application process

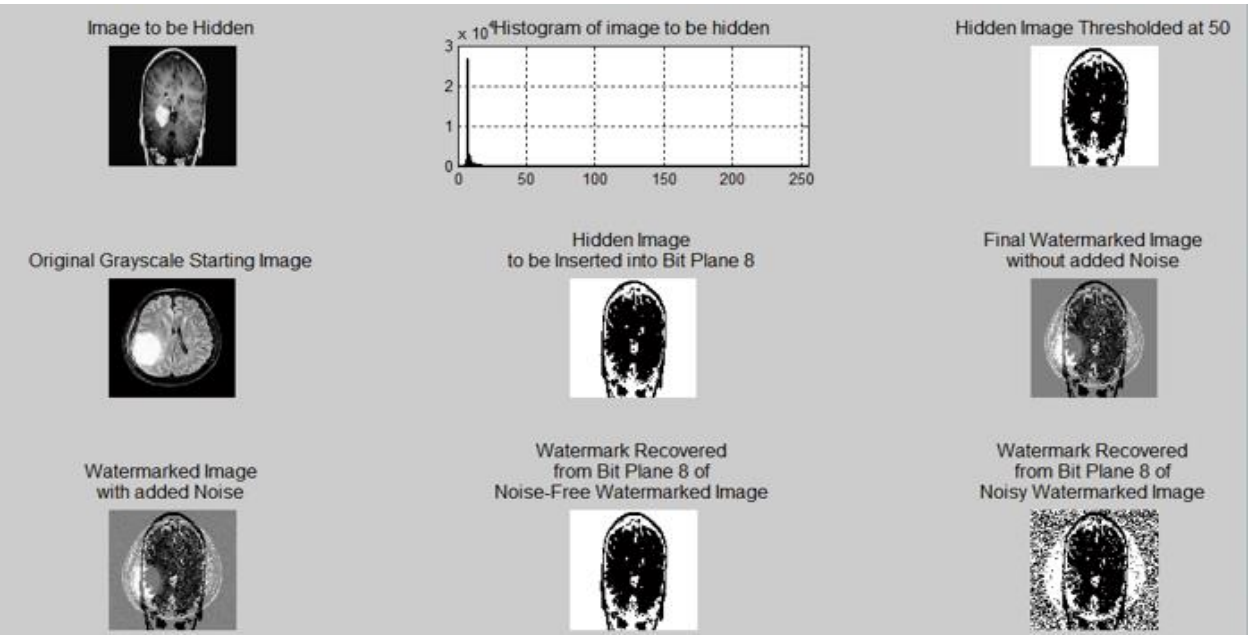


Figure 4.10: LSB watermark at application process

4.4 Summary

In this chapter we analyzed different medical image (MRI) and illustrate two different kind of procedure that hides data. This section reviews process of embedding and extraction that appears the result simulation of gray images to provide medical imagery field authentication. Thereafter the concept of watermarking extended in this scheme. We performed conventional technique and perceptible technique that was previously applied to multimedia components. The measured value of the characteristics parameters is obtained and observe the changes that arises.

Chapter 5

Transmission Medium (Cloud)

The internet is changing with the rise of social media networks after the invention of blogging, sharing content online became a common action performed by millions of people every day. From pandas being cute to sharing financial reports, there's almost nothing that you can't share, that's why cloud storage is the best for sharing. Our intension is to transmit watermarked medical data using cloud storage so that authentication of medical data and personal information remain secured. Here're some best cloud storages for sharing files:

5.1 Sync.com

About: Sync.com was founded in 2011. It has steadily built its reputation for capable security and user privacy, which makes it one of the best cloud storage from the top placing cloud storages.

Working Principle: From the Sync.com, users can share folders and files by using the "share" button that corresponds to the content they want to share. For a folder, user can invite specific users or user can generate a link which will be available to all. For a file, user will need to generate a link, where user can manually copy or send to others via email, even if they don't use Sync.com. Users can easily share upload links that will enable people to share their content directly into their cloud storage space instead of download links [13].

Plans: For free plan, Sync.com offers 5GB. For personal users there are two plans: Pro Personal 500GB ($49 for a year) and Pro Personal 2TB ($96 for a year). For single business users there is Business Solo plan ($96 for a year). Business Pro plans require a minimum of two users which cost from $60 to $180 per year, depending on the number of users and storage space.Sync.com offers 5GB

Pros:

- Secure link sharing
- Zero-knowledge security
- Great support

Cons:

- No block-level file copying
- No monthly plans

5.2 pCloud

About: pCloud can store files from multiple devices to a one beautiful and intuitive cloud storage space. pCloud was started in 2013. Now pCloud service has eight million users.

Working Principle: To share contents, just need to add the invitee's name or an email (if they're not on pCloud). By using upload links, Others can share their files too with the uploader (pCloud user). To protect links, users need to set up the expiry dates and passwords, but these features are only available with premium plans. Also, by using pCloud's zero-knowledge encryption add-on, user will be able to share only files that aren't encrypted with it [14].

Plans: For free users, the free plan gives 10GB of storage and 1GB for every referral (10GB limit). For personal uses, you can choose between Premium (500GB for $4.99 per month) and Premium Plus (2TB for $9.99 per month). Both plans will keep files history for 30 days and will allowed to make unlimited remote uploads.

Pros:

- Affordable plans
- Zero-knowledge encryption
- Good customer service

Cons:

- File encryption is a paid add-on service

5.3 Tresorit

About: Tresorit is one of the most secure cloud storage services. Its headquarters are in Switzerland. The word "tresor" comes from German's word which means vault. Tresorit keeps data on servers in the Netherlands and Ireland.

Working Principle: For folder sharing, Tresorit has more options. For files sharing, it can only be shared via link, while users can share folders with a specific individual by inputting their email address. Only those registered on Tresorit will be able to access the content whose using emails. Folders allows to set up permissions for others, which include view only, edit and manager access [15].

Plans: Users find to be objectionable about Tresorit is the price because Tresorit plan's prices are higher than the other cloud's plans. The cheapest individual plan called Premium which costs $12.50 a month for 200GB, more than most services charge for 1TB. For personal plan named Solo, will give you 2TB of data, along with password protected links which will gives the ability to sync up to ten devices instead of five and unlimited instead of 90-day versioning. All those benefits add to $30 a month. There is a discount if you pay for the year.

Pros:

- Secure file sharing
- Zero-knowledge encryption
- Good platform support

Cons:

- Expensive
- Unimpressive sync speeds

5.4 Box

About: Box service was founded in 2005. Box allows content to be stored online, so it can be accessed, managed, and shared from anywhere.

Working Principle: By using Box, users can easily share their links with other licensed users with no restriction. If users have proper permissions, then they can share their files with the outside users as well.

By clicking the "share" button user can send an email invite, or user can generate a link and then send it. Box allows users to set up their expiry dates, also allows to use a password to protect links and even restrict downloads on shared links. There's also an audit page where users can check what they've shared [16].

Plans: Box offers plan for the starters plans which is called Starter Plan and it costs only $5 per month per user (minimum of three) but offers only 100GB. For Business plans, Box offers Business which cost $15 per user a month and Business Plus which cost $25 per user a month. Both plans offer unlimited storage.

Pros:

- Strong security & content control
- Unlimited storage plan

Cons:

- No block-level sync
- No annual discount)

5.5 Dropbox

About: One of the oldest services in the industry is Dropbox which was founded in 2007 by a couple of MIT students. Since then Dropbox, has become one of the most recognized names in technology. There are 500 million users and its second only to Google Drive.

Working Principle: Dropbox users can share their any folder and file that they stored with Dropbox, regardless of whether they use a desktop computer, a smartphone or browser. When user want to share a file or folder, a link will be generated for that user when he/she will click on "share." User can easily email this link or just copy-paste it. Free and Dropbox Plus users don't have options to further secure shared links, but if they're willing to pay for Dropbox Professional, they can add password protection and expiry dates to their links [16].

Plans: Dropbox Plan offer free users called Basic where they will get 2GB of storage. Users can add to their free space with 500MB per referral. If users want more storage, then there are two personal plans that users can choose from: Plus, and Professional. Dropbox Plus gives a fair price of $10 for 1TB of storage space. By using Professional, users will get more features but not more storage.

Pros:

- Very fast sync
- Good user experience

Cons:

- Expensive
- Not zero-knowledge)

Chapter 6

Conclusion

Our main concern is to provide an intense security layer to medical data and along with authentications and traceability abilities. Previously, with the pace of digital technologies many multimedia elements have been saved from misuse but in medical criterion the increasing amount of valuable data concerns its ownership environment.

We are now trying to incorporate here a successful hidden medical information which convey more specific and important of that data by cloud. We have mentioned earlier different types of cloud storage that we can use as our transmitting medium.

We applied one conventional but unique technique: 1) LSB (least significant bit) 2) Visible watermarking. By analyzing the outcome, it concludes data hiding properties and also considering digital transmission medium.

- The concept of watermark has been clarified
- Watermark optimization methods with embedding and extraction has been done.
- These two proposed scheme is designed for not only the optimum watermark of MRI but also the optimum utilization of storage data, access, authentications and traceability abilities in further imaging techniques.

Chapter 7

References

1. A Lossless Watermarking Based Authentication System For Medical Images Samia Boucherkha and Mohamed Benmohamed World Academy of Science, Engineering and Technology International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering Vol:1, No:1, 2007.
2. Chunlin Song Llewellyn-Jones, "Analysis of Digital Image Watermark Attacks", Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE.
3. A Survey of Digital Watermarking Techniques and its Applications Lalit Kumar Saini1, Vishal Shrivastava2 M.Tech1 Research Scholar, Professor2 Department of Computer Science and Engineering, Arya College of Engineering. & Information Technology, Jaipur, India.
4. C.-Y. Lin, D. Sow, and S.-F. Chang. Using Self-Authentication-and-Recovery for Error Concealment in Wireless Environments. *Proceedings of SPIE*, Vol. 4518, Aug. 2001.
5. M. Barni, F. Bartolini, "Data hiding for fighting piracy," IEEE Signal Processing Magazine, vol. 21, n°2, pp.28–39, 2004.
6. G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging," in Proc. IEEE Int.Conf. ITAB, USA,2000, pp. 250–255.
7. Xuanwen Luo, Qiang Cheng, Joseph Tan, *A Lossless Data Embedding Scheme For Medical in Application of e- Diagnosis*, Proceedings of the 25th Annual International Conference of the IEEE EMBS Cancun, Mexico. September 17-21, 2003.
8. LSB Based Digital Image Watermarking For Gray Scale Image Deepshikha Chopra1, Preeti Gupta2, Gaur Sanjay B.C.3, Anil Gupta4
9. Braudaway G. W., Magerlein K. A. and Mintzer F.,"Protecting Publicly Available Images with a Visible Image Watermark", *Proc. of International Conference on Image Processing*, 1997, Vol.1, pp. 524 -527.
10. A DCT Domain Visible Watermarking Technique for Images *Saraju P. Mohanty**Dept. of Comp. Science & Engg. University of South Florida, FL 33620, USA*K.R. Ramakrishnan*

Dept. of Electrical Engg. Indian Institute of Science School of Computing National University of Singapore Kent Ridge, Singapore 119260.

11. M. Li, R. Poovendran, S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," Computerized Medical Imaging and Graphics, vol. 29, n°5, pp. 367-383, 2005.
12. Y. Srinivasan, B. Nutter, S. Mitra, B. Phillips, D. Ferris, "Secure transmission of medical records using high capacity steganography," in Proc. 17th IEEE Symposium on Computer Based Medical Systems, 2004, p.122-127.
13. https://www.sync.com/?_m=taz&gclid=EAIaIQobChMIhJmim9DP3wIVVB0rCh2aMATZEAAYASAAEgLs1PD_BwE
14. https://www.cloudwards.net/review/pcloud/
15. *https://www.google.com/search?client=firefox-b-ab&q=tresotit+cloud+storage*
16. https://www.cnet.com/how-to/onedrive-dropbox-google-drive-and-box-which-cloud-storage-service-is-right-for-you/