REVERSIBLE WATERMARKING TECHNIQUE USING TEXT IN MEDICAL IMAGES

By

T.PRABHU

Reg. No. 0920107014

of

KUMARAGURU COLLEGE OF TECHNOLOGY

(An Autonomous Institution affiliated to Anna University of Technology, Coimbatore)

COIMBATORE – 641 049

A PROJECT REPORT

Submitted to the

FACULTY OF ELECTRONICS AND COMMUNICATION ENGINEERING

In partial fulfilment of the requirements

for the award of the degree

of

MASTER OF ENGINEERING

IN

COMMUNICATION SYSTEMS

APRIL 2011

BONAFIDE CERTIFICATE

Certified that this project report titled **"REVERSIBLE WATERMARKING TECHNIQUE USING TEXT IN MEDICAL IMAGES"** is the bonafide work of **Mr.T.PRABHU** [Reg.No:0920107014] who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Sasikala 7/4/11

Project Guide
Ms.S.Sasikala

Head of the Department
Dr. Rajeswari Mariappan

The candidate with University Register No. 0920107014 was examined by us in Project Viva-Voce examination held on 21-4-2011

D. Mo 21/4/11

Internal Examiner

21/4/11

External Examiner

ACKNOWLEDGEMENT

First I would like to express my praise and gratitude to the Lord, who has showered his grace and blessing enabling me to complete this project in an excellent manner.

I express my sincere thanks to our beloved Director **Dr.J.Shanmugam**, Kumaraguru College of Technology, for his kind support and for providing necessary facilities to carry out the work.

I express my sincere thanks to our beloved Principal **Dr.S.Ramachandran**, Kumaraguru College of Technology, who encouraged me in each and every steps of the project work.

I would like to express my deep sense of gratitude to our HOD, the ever active **Dr.Rajeswari Mariappan**, Department of Electronics and Communication Engineering, for the valuable suggestions and encouragement which paved way for the successful completion of the project work.

In particular, I wish to thank with everlasting gratitude to the project coordinator **Ms.D.Mohanageetha(Ph.D)., Associate Professor**, Department of Electronics and Communication Engineering, for the expert counselling and guidance to make this project to a great deal of success.

I am greatly privileged to extend my heartfelt thanks to my project guide **Ms.S.Sasikala, M.Tech., Assistant Professor-SRG,** Department of ECE, Kumaraguru College of Technology, throughout the course of this project work and I wish to convey my deep sense of gratitude to all the teaching and non-teaching staffs of ECE Department for their help and cooperation.

Finally, I thank my parents and my family members for giving me the moral support and abundant blessings in all of my activities and my dear friends who helped me to endure my difficult times with their unfailing support and warm wishes.

ABSTRACT

The transmission of digitized medical information has become very convenient due to the generality of Internet. Internet has created the biggest benefit to achieve the transmission of patient information efficiently. However, it is easier that the hackers can grab or duplicates the digitized information on the Internet. This will cause the problems of medical security and copyright protection. In order to fulfil the security and convenience issues of the patients following goals like the prevention of medical fault, the real-time detection of abnormal event, the support of clinical decision and developing of medical service based on patient has to be achieved.

The medical images are differed from ordinary images. Because, they are captured through different devices(for example X ray, Computed Tomography, Magnetic Resonance Imaging and Positron Emission Tomography). The reversible data hiding is an emerging field for authentication of the information content embedded in an image. The most important requirement of reversible data hiding is that the distortions to the original signal should be minimum, such that artifacts are not visible

For this purpose this paper proposes the technique called Reversible Watermarking Technique Using Text in Medical Images. In this method the (ROI) Region of Interest is selected from the medical image such that it contains all the diagnostic information, then the patient information and ROI are encoded separately in the medical image with a key. At the decoding side the patient information and ROI are retrieved separately from the watermarked medical image with the same key.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

BMP	Bit Map
CE	Consumer Electronics
CCI	Copy Control Information
DVD	Digital Versatile Disc
DCT	Discrete Cosine Transform
ED	Euclidean Distance
TIFF	Tagged Image File Format
JPEG	Joint Pictures Experts Group
ROI	Region of Interest
LSB	Least Significant Bit
SMVQ	Side Match Vector Quantization
VQ	Vector Quantization

CHAPTER 1

INTRODUCTION

Data hiding is a covert communication method that uses an image as the cover to hide the truth from potential attackers that some secret message hidden in the image is being transported. Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures can be used for hiding the data. Different methods such as steganography, cryptography and watermarking has been developed in order to protect the digital data and also for the secure transmission of the digital information.

1.1. Steganography

Steganography is the technique which hides the existent of data in the cover medium. There many types of Steganography techniques like physical Steganography, digital Steganography which are being used in the past and also in the present. The former one is the technique where the data is hidden in the body of the medium like writing on the wooden table or tattooing on the shaved head of a trusted slave, the latter one is the technique where the data is being inserted in the least significant points of an image or an audio file.

Generally, we first encrypt the data to be sent and replace it with the insignificant points in the cover image. The cover image is usually a camera image which has the richest texture activity, so as to hide large amount of data. The points are chosen in such a way that it does not alter the image. The image obtained after embedding is the stego image which contain the hidden data in it. It resembles same as that of the original image for the human eye. Then the stego image is sent to the recipient without the suspicion of the intruders

At the recipient side the reverse process is done to get the data hidden in the stegoimage, also the original cover image. If the existence of the data in the cover medium is visible to the intruder then the Steganography fails to hide the data.

1.2. Cryptography

Cryptography is technique where the data is transformed into another form. It is one of the techniques used to send data securely. In this the data to be sent is encrypted using a different methodology which is being accepted by the two parties. Then with the help of a secret key the data are converted into another form which is known as cipher text. The cipher text is the transformed form of the original data and it is sent to the recipient. The intruders can easily suspect the presence of data in the cipher text. They go for the common methodology, with many number of iterations they are able to break the code or they will encrypt the cipher text again and the hidden information will be lost.

1.3. Watermarking

Watermarking is also a data hiding technique. The primary goal of watermarking is Robustness that is it should be impossible to remove the watermark that is being embedded within the image without degrading the image quality. It is used to have intellectual information, protect the copy rights of the data or file.Digital watermarking techniques are information hiding techniques similar to steganographic approaches with the overall goal to embed information into the original signal. A digital watermark is a perceptually transparent pattern inserted in digital data using an embedding algorithm and an embedding key. A detection algorithm using the appropriate detection method can retrieve the watermark information.

1.4. Attributes of watermarking

The main attributes of an watermarking algorithm is

1.4.1. Imperceptibility

A watermark can be embedded into an image as either visible or invisible. The visible watermark is perceptible and is just like a noise. It mostly can be removed by noise removing process. In order to decrease the risk of cracking, most of the proposed watermarking methods are invisible. On the other hand, the quality of the image is also important. If the watermark embedding process seriously affects the quality of the watermarked image, the watermarked image will draw the attention of attackers or even lose its value. Therefore, the quality between the original image and the watermarked image should not be highly degraded. This property is called imperceptibility.

1.4.2. Robustness

A watermarking scheme should resist destruction from standard image processing and malicious attacks. The watermarked image may be incurred in several intentional or the unintentional attacks to try to remove the embedded watermark. A robust watermarking scheme has to ensure the retrieved watermark is recognized, when the image quality does not get harmed. Robustness is more important property and requirement of watermarking. The watermark should be able to survive any reasonable processing inflicted on the original image.

1.4.3. Security

The watermarked image should not reveal any clues of the presence of the watermark, with respect to un-authorized detection, or (statistical) undetectability or unsuspicious (not the same as imperceptibility).

1.4.4. Capacity

The capable size of embedding information is defined as the embedding capacity. Due to the reversible watermarking schemes having to embed the recovery information and the watermark information into the original image, the required embedding capacity of the reversible watermarking schemes is much more than the conventional watermarking schemes. The embedding capacity should be high, but it should not affect the accuracy of the recovered image.

1.5. Types of watermarking

The different types of watremarking techniques are

- Reversible and irreversible watermarking
- Visible and invisible watermarking
- Blind and non-blind watermarking
- Semi-fragile and roboust watermarking

1.5.1. Reversible and irreversible watermarking

In reversible watermarking, the original information can be completely recovered at the receiver side. But, in the irreversible techniques the original information cannot be completely reconstructed.

1.5.2. Visible and invisible watermarking

The watermarking techniques, in which the watermark is visible in the original signal, are known as visible watermarking. In some techniques the watermarks are invisible in the original signal. Such techniques are known as invisible watermarking.

1.5.3. Blind and non-blind watermarking

The schemes in which the cover signal (the original signal) is not needed during the detection process to detect the watermark. The key, which is typically used to generate some random sequence used during the embedding process, is required for the detection. Such methods are known as blind watermarking or public watermarking. The techniques in which the original cover signal is required during the detection process are known as the non-blind watermarking or private watermarking.

1.5.4. Semi-fragile and robust watermarking

A semi-fragile watermark is a technique which is highly sensitive to a modification of the stego-medium. This watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification. It serves at proving the authenticity of a document.

On the opposite, a robust watermark should be stuck to the document it has been embedded in, in such a way that any signal transform of reasonable strength cannot remove the watermark.

1.6. Applications of digital watermarking

1.6.1. Digital watermarking technology for rights management

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from the content owners to the receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user. Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment. The major technical requirements for this application are as follows

- The watermark does not incur visible (or audible) artifacts to the ordinary users.
- The watermark is independent of the data format.
- The information carried by the watermark is robust to content manipulations, compression, and so on.
- The watermark can be detected without the unmarked original content.
- The watermark can be identified by some kind of "keys" that are used to identify large number of individual contents uniquely.

The contents may be changed to the other formats, edited or trimmed by the users or compressed for the storage and transmission, and it is desirable to be able to detect the watermark from those processed contents. Usually, the watermark signal embedded into the content does not disappear after the editing of the content, but becomes more and more difficult to detect while the content is distorted. In general, higher robustness can be achieved by increasing the strength of the watermark signal, thus improving the detection capability. In other words, the robustness of the watermark is a trade-off between the amount of watermark signal that applies to the content and the overhead to the detection. Currently, several commercial products and services using watermarking technology are available. They include applications for watermark embedding/detection and services to search the Internet for the contents with certain designated watermarks. These applications are mainly taking place between the large content owners (e.g. electronic publishers/distributors), and their customers (e.g. the content creators).Because the usage is limited within relatively smaller groups, each group tends to use their own proprietary watermark rather than a common one. Among these groups, the standardization is not an urgent issue until their markets shift to public domain consumers.

1.6.2. Digital watermarking technology for authentication and tamper proofing

Another application of digital watermark is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/Printing/Exposing (DPE) compared to the traditional chemical photos. However, there are some critical issues for applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos. The way to realize this feature is to embed a layer of the authentication into the subject digital image using a digital watermark. This additional layer of watermark is used as a "sensor" to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. The technical requirements for this application are as follows

- Invisible to the ordinary users.
- Applicable to compressed image format (most digital cameras use JPEG compatible format)
- Sensitive to content manipulations, compression, and so on.

1.6.3. Watermarking technology for DVD playback and record control

In most of the cases, those applications are targeting at a closed environment or exist between limited numbers of member, e.g., between image libraries and content creators, insurance companies and repair shops, and so on. In this section, I would like to focus on the watermark application that has much more public impact, namely DVD Copy Control.

Watermarking technology can be viewed as a way to provide a secure data channel along with the contents without modifying the installed-base Consumer Electronics (CE) devices. The embedded watermark is transparently passing through the conventional data path, and will only be detected at the digital recorders. When the watermark detection is mandated in these recorders, this watermark can be used to trigger the copy protection mechanism implemented in it. The watermarking data embedded into the video is difficult to remove without damaging the quality of the content because it is carefully "woven" into the visible part of the video data. In this application, the data called Copy Control Information (CCI) is embedded into the video data to indicate that the status of the contents is "Never Copy", "One Copy Allowed" or "Copy Freely". Recording devices will be mandated to facilitate a "watermark detector" to detect the embedded CCI from the incoming and outgoing video data, and responding properly to the recording/playback rules that are defined. The major advantage of the watermark technology is that CCI can be transmitted over the analog video channels. Even advanced digital encryption schemes cannot extend its protection over the analog video channel, but digital watermark could. The embedded CCI will survive even if the video content is transmitted through the analog video channel, recorded to video cassette, and re-digitization. As far as the digital recorders are facilitated to detect the watermark from the video, the copy protection mechanism can be extended over all the devices. From the implementation viewpoint, because the watermark is completely transparent to the existing system or devices, it does not require that any of the install-base devices to be modified or be made obsolete. The video contents with watermarks looks and works just the same as the contents without watermarks for the devices and channels that have nothing to do with the embedded CCI, thus can be treated transparently by current and future video transmission infrastructures and devices. Although the primary focus of this system is DVD video, the same watermark can also be applied to other forms of video contents, such as videocassettes, laser discs or broadcasted contents. The major functional requirements for this application are

- High robustness
- High image quality
- Low false positive ratio
- Low detection cost
- Real-time embedding/detection capability.

The embedded data needs to survive various kinds of video processing, and be detected on the fly with low-cost detection logic to be implemented in consumer electronics devices.

CHAPTER 2

REVERSIBLE DATA HIDING

In recent years, a special kind of digital watermarking is discussed widely, called reversible watermarking. Reversible watermarking, which is also called lossless watermarking, embeds invisible data (payload) into a digital image. As a basic requirement, the quality degradation on the image after data embedding should be low. A special feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image.

From the information hiding point of view, reversible watermarking hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. The motivation of reversible watermarking is distortion-free data embedding. Though imperceptible, embedding some data will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required.

From the application point of view, original image can be used as an information carrier. Since the difference between the embedded image and original image is almost imperceptible from human eyes, reversible data embedding could be thought as a covert communication channel. Similar to conventional watermarking schemes, reversible watermarking schemes have to be robust against the intentional or the unintentional attacks, and should be imperceptible to avoid the attraction of attacks and value lost. Therefore, the reversible watermarking also has to satisfy all requirements of the conventional watermarking such as robustness, imperceptibility, and readily embedding and retrieving. Except for these requirements, reversible watermarking has to satisfy the following two additional requirements.

➢ Blind

Some of the conventional watermarking schemes require the help of an original image to retrieve the embedded watermark. However, the reversible watermarking can recover the original image from the watermarked image directly. Therefore, the reversible watermarking is blind, which means the retrieval process does not need the original image.

➢ Higher embedding capacity

The capable size of embedding information is defined as the embedding capacity. Due to the reversible watermarking schemes having to embed the recovery information and watermark information into the original image, the required embedding capacity of the reversible watermarking schemes is much more than the conventional watermarking schemes. The embedding capacity should not be extremely low to affect the accuracy of the retrieved watermark and the recovered image. The procedure of conventional and reversible watermarking schemes can be illustrated in Figure 2.1. The steps of conventional watermarking and reversible watermarking are similar except there is an additional function to recover the original image from the suspected image. Therefore, the reversible watermarking is especially suitable for the applications that require high quality images such as medical and military images.

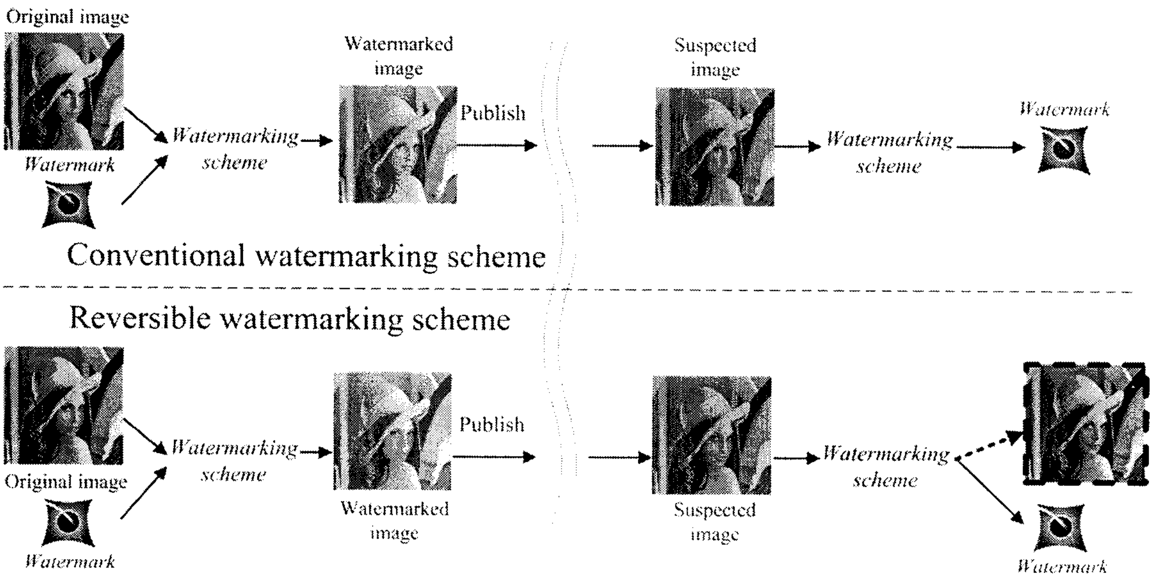


Figure.2.1 Representation of difference between conventional watermarking and reversible watermarking

2.1. Reversible watermarking techniques

Some of the reversible watermarking techniques are

- Lossless data embedding
- Circular Interpretation using bijective transformation
- Difference expansion technique
- Data hiding based on side match vector quantization
- Histogram shifting technique

2.2. Lossless data embedding

In this method, Jessica Fridrich introduce a new method for data embedding in images (lossless data embedding) that has the property that the distortion due to embedding can be completely removed from the watermarked image after the embedded data has been extracted. This method is a lossless embedding method for the uncompressed formats (bit map (BMP), TIFF) and for the joint pictures experts group (JPEG) format. The concept of lossless data embedding can be used as a powerful tool to achieve a variety of nontrivial tasks, including lossless authentication using fragile watermarks, steganalysis of least significant bit (LSB) embedding, and distortion-free robust watermarking. This is an attempt to develop a general lossless data embedding technique that would be extendable to all formats while providing large capacity and small distortion.

Assume that, there exists a subset B in the original image I, such that B can be lossless compressed (using some lossless data compression method), and at the same time, B can be randomized without causing perceptible changes to the original image I. If such a subset can be found, then we can embed data lossless by replacing the set B with its compressed form C (B) and a message M. The capacity of this method is $|B|-|C'\ (B)|$, where $|x|$ denotes the cardinality of x.

The general methodology described above is equally applicable to lossy formats. Actually, it is easier to identify a suitable subset B for the JPEG format than for uncompressed formats, such as the BMP or TIFF formats. Here, they also use bit planes as the set B. However, in this method higher payloads forced us to use higher bit-planes, thus quickly increasing the distortion in the image beyond an acceptable level.

Two lossless data embedding techniques have been introduced for JPEG images. The data is embedded in the quantized DCT coefficients in an invertible way, so that it is possible to reconstruct from the watermarked image the exact copy of the original image.

2.3. Circular Interpretation using bijective transformation

Circular interpretation using bijective transformations is proposed by De Vleeschouwer to implement a method that fulfils all quality and functionality requirements of lossless watermarking. The embedding process hides a binary message, i.e., the watermark payload, into a picture. Each bit of the message is associated with a group of pixels (a block in the image). Each group is equally divided into two pseudo-random sets of pixels, zone A and zone B. In this method, the average luminance value of each zone is not the discriminating factor. The histogram of the gray scale or luminance values of each zone is mapped to a circle and the position of the histogram on the circle replaces the concept of average value. In concrete terms, a weight proportional to the occurrence of each luminance value is placed on the corresponding position on the circle as shown in Fig. 2.2. The position of the centre of mass resulting distribution of weights replaces the concept of mean value. The histogram of each zone is mapped to a circle.

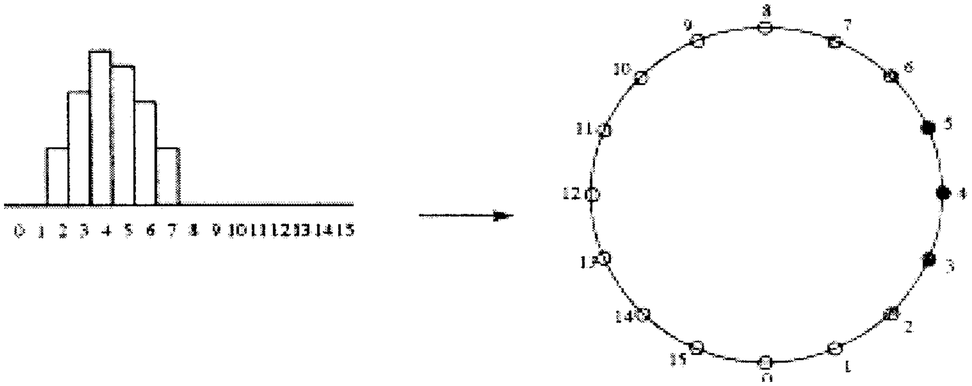


Figure.2.2 Histogram mapping around a circle

Let the vectors V_a and V_b points the center mass, C_a and C_b of the zones A and B, respectively as shown Fig.2.3. These vectors define the position of each histogram. The vectors Va and V_b will be very close to each other. Slight rotation of these vectors in opposite directions allows the information embedding. The rotation pushes V_a in clockwise direction to embed the bit '1'and for embedding the bit '0' the rotation of V_a will be in anti-clockwise direction. At the receiver, the bit is inferred from the sign of the smallest angle between the vectors V_a and V_b.

The extraction process is first partitioning the image into zones A and B, similarly to the embedding process. Histograms of each zone are mapped to the circle. For both zones, the center of mass is computed.

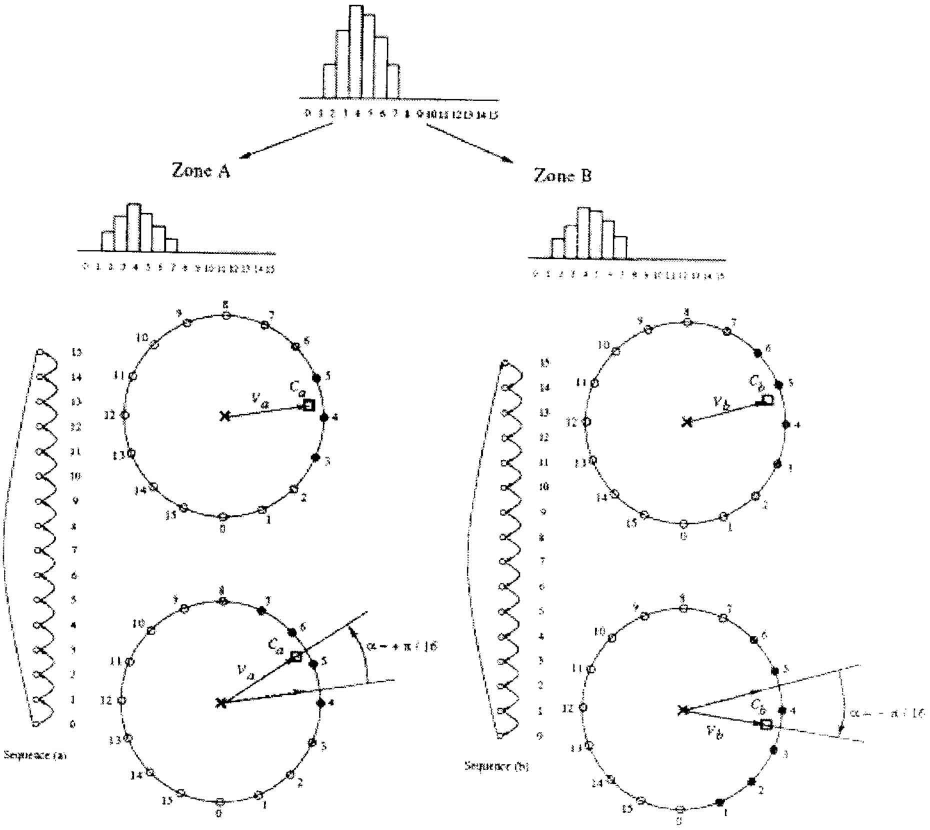


Figure.2.3 Illustration of embedding process

Let γ be the angle between the vectors V_a and V_b, pointing from the circle center to each center of mass. The magnitude of differentiates message embedded blocks from others. The sign of γ provides the direction of rotation during the embedding process and enables bit retrieval and reversibility. Once the embedded bit has been retrieved, the original block can be recovered. This is called the inversion process; it consists in following the embedding process depicted in Fig.2.3 in the reverse order.

In Fig.2.3, the shifts of luminance caused by sequence (a) and (b) are equivalent to modulo additions or subtraction. A major advantage of this approach is that, it avoids unreliable retrieval caused by the impact of wrapped around pixels on average values. Nevertheless, our method is not free from salt-and pepper artifact. In order to prevent it, an alternative mapping of the histogram to the circle is proposed in Fig.2.4.

At the circle level, the embedding transform is still the same. However, at the pixel level no value is shifted by an outstanding large step anymore. The transform is now free from disturbing visual artefact such as the "salt-and-pepper" effect. The change in the transform somewhat impacts the retrieval process. In Fig.2.4, odd and even luminance values are spread symmetrically around the circle. As a result, the histogram is also spread symmetrically around the circle and the center of mass is close to the vertical axis of symmetry. For intermediate luminance value the center of mass is close to the circle center.

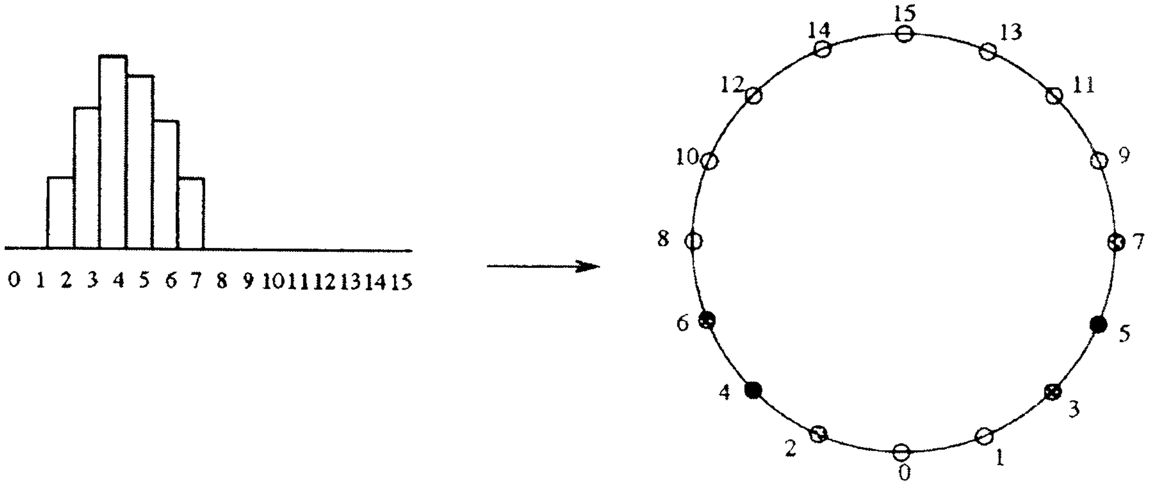


Figure 2.4 Alternative mapping of the histogram to the circle

2.4. Difference expansion technique

This method was proposed by Jun Tain. Here, in the embedding process, in the first step the original image is grouped into pairs of pixels. A pair consists of two neighbouring pixel values. Next, integer transform is applied to each pair. If the grayscale pixel pair is (x,y),then the integer average 'l' and the difference 'h' is given by

$$l = \left\lfloor \frac{x+y}{2} \right\rfloor \text{ and } h = x - y \qquad (2.1)$$

The inverse transform is

$$x = l + \left\lfloor \frac{h+1}{2} \right\rfloor \text{ and } y = l - \left\lfloor \frac{h}{2} \right\rfloor \qquad (2.2)$$

The reversible integer transforms in equation (2.1) and (2.2) are also called as integer Haar wavelet transform or the S transform. The reversible integer transforms set up a one-to-one correspondence between (*x*,*y*) and (*l*,*h*).To prevent the overflow and underflow problems, i.e., to restrict (*x* ,*y*) in the range of [0, 255], it is equivalent to have

$$0 \le l + \left\lfloor \frac{h+1}{2} \right\rfloor \le 255 \text{ and } 0 \le l - \left\lfloor \frac{h}{2} \right\rfloor \le 255 \qquad (2.3)$$

Since both '*l*' and '*h*' are integers, one can derive that the above inequalities are equivalent to

$$h \le 2(255-l) \text{ and } |h| \le 2l+1 \qquad (2.4)$$

We say the difference value '*h*' is expandable under the integer average value '*l*' if

$$(2\times h+b) \le \min(2(255-l), 2l+1) \qquad (2.5)$$

where '*b*' is the message bit to be embedded. We say a difference value '*h*' is changeable under the integer average value '*l*' if

$$2\times \left\lfloor \frac{h}{2} \right\rfloor + b \le \min(2(255-l), 2l+1) \qquad (2.6)$$

We calculate the difference values '*h*' and order them as a vector.

In next step we create four disjoint sets [EZ, EN, CN, and NC] from *h* values.

*EZ: contains all expandable *h*=0 and expandable *h*= -1.

*EN: contains all expandable *h* ≠ EZ.

*CN: contains all change able *h* ≠ (EZ U EN).

*NC: contains nonchangeable *h*.

Third, a location map of the selected expandable difference values is created. For every difference value '*h*' in EZ, it will be selected for difference expansion (DE). For EN, depending upon the payload size, some difference value will be selected for the DE. The subsets of the selected and not selected difference values in EN are denoted as EN1 and EN2, respectively. Each bit map is created as the location map, with its size equals to the number of pairs of pixels formed in first step. For an h in EZ U EN1, assign a value‘1’ in the location map; for an ‘*h*’ in EN2 U CN U NC, assign a value ‘0’. The location map is losslessly compressed by run length encoding and the compressed bit stream is denoted as £.

In next step, we collect original LSBs of the difference values in EN2 and CN. For each ‘*h*’ in EN2 U CN, LSB (*h*) will be collected into a bit stream *C* .In the fifth step, the location map £, the original LSB’s *C* and the payload *P* is embedded. The values of £, *C*, and *P* together into a binary bitstream *B*. After embedding al the bits inverse integer transform is applied to obtain the original image, which is given by equation (2.2). From the embedded bit stream *B*, by collecting the LSBs of all changeable difference values are retrieved. From *B*, we can decode the location map £ and the original LSBs *C*.

The decoding process contains five steps. First, the difference values are calculated. For the embedded image pairing is done by using the same method as in embedding and integer transform is applied to each pair. The difference values are calculated as vector. Next, two disjoint sets of the difference values are created, CH and NC.

*CH: contains all changeable *h*.

*NC: contains all nonchangeable *h*.

Then, LSBs of all difference values are collected in CH, and from a binary bitstream *B*. Next, the location map is decoded from *B* by using run length decoder. The decoder knows exactly the location in *B*, where it is the last bit from the location map bit stream £.

2.5. Data hiding based on Side Match Vector Quantization (SMVQ)

If a sender tries to hide secret data in the compression domain, the compression codes must be modified to hide the secret data, and the modifications may distort the compressed image. In addition, the original compression codes cannot be reconstructed or stored for later use as long as the secret data are hidden in the compression codes. That means the receiver could not use the received compression code as a carrier after extracting the hidden data. That condition is ineffective for communicating parties. To ensure that the original compression codes can be recovered directly during the extracting phase and stored for later use, we wanted to modify the codeword selection strategy of SMVQ and develop a novel data hiding scheme with the property of reversibility. To achieve this goal, we broke our proposed scheme into three phases: the preprocessing phase, the hiding phase, and the extracting and reversing phase. Those phases are described in greater detail in the following paragraphs.

2.5.1. Preprocessing phase

Secret data must be preprocessed for security reasons. Encrypting the hidden data prevents them from being illegally accessed or unscrambled. Some existing encryption techniques, such as DES, RSA, and others can be used to encrypt hidden data. Secret data also can be compressed in advance using lossless compression techniques to reduce the amount of hidden data and increase the visual quality of stego-image, and thus deceive potential grabbers. After preprocessing in our proposed scheme, the cover image is encoded using SMVQ and the SMVQ compressed image is created. The preprocessed secret data are then hidden in the SMVQ compressed image using our proposed hiding scheme. The stego-image is thus generated, ready for transmission to a receiver. Receivers can extract the secret data from the stego-image using our proposed extracting and reversing scheme. In addition, receivers can restore the original SMVQ compressed codes completely. The reconstructed SMVQ compressed codes can be stored directly to save storage space. The hiding, extracting, and reversing phases are described in detail in the following subsections.

2.5.2. Hiding phase

To explain this phase, we define the symbols to be used in hiding phase as follows: the main codebook Y=(y_0, y_1,..........., y_{n-1}), the SMVQ compressed cover image C , the subindices D=(d_0, d_1,...........,d_T) , and the secret data B=(b_0,b_1,...........,b_T), where b_i={0,1) and $0 \leq i \leq r$. The hiding phase consists of the following steps.

1) The SMVQ-compressed cover image C is divided into nonoverlapping blocks. Because the blocks in the first row and first column are encoded by VQ, the secret data B are hidden in the residual blocks.

2) For each residual block, the upper and left encoded blocks in C are used to generate the subcodebook K= (k_0,k_1,............k_{N-1}), where, k_i is i th the codeword and i=0,1,.....N-1 . The subindex d_i is used to find the corresponding codeword k_a from the subcodebook K.

3) If the secret bit b_i is equal to '0', then the codeword k_a becomes the content of the stego-image.

4) If the secret bit b_i is equal to '1', then we search the codeword k_b from the subcodebook K so that the codeword is k_b the closest to the codeword k_a. The approximate codeword becomes the content of the stego-image and is defined as

$$\text{Approximate codeword} = \left\lfloor \frac{2\times(k_a+1)\times k_a}{3} \right\rfloor \qquad (2.7)$$

5) Steps 2–4 are repeated until the whole stego-image is generated.

In this reversible data hiding scheme, the modified SMVQ compression codes are converted into a stego-image. The stego-image must be transmitted without extra messages being required to achieve reversibility.

2.5.3. Extracting and reversing phase

Once the stego-image is received, the receiver can extract the secret data without having to refer to the original cover image. The steps for extracting and reversing are as follows.

1) The stego-image is divided into nonoverlapping blocks. The first row and first column blocks are encoded using VQ and the indexes are generated.

2) For each residual block, the previously reconstructed upper and left blocks are used to generate a subcodebook $K=(k_0,k_1,\ldots\ldots,k_{N-1})$, where, k_i is the i th codeword and i=0,1,.....N-1. The codeword k_a is selected from the subcodebook K such that the Euclidean distance between the current block X$_i$ and the codeword k_a is the shortest.

If the Euclidean distance ED (X$_i$, k_a) is equal to '0', then the secret bit b_i=0. The index 'a' of the codeword k_a is outputted to restore the original state. If the Euclidean distance ED (X$_i$, k_a) does not equal '0', then the secret bit b_i =1,where, Euclidean distance,

$$ED(X_j,Y_k)=\sqrt{\sum_{i=1}^{n\times n}\left(X_{ij}-Y_{ik}\right)^2} \text{ for } 0\le k\le n-1 \qquad (2.8)$$

where,mxn is the dimension of the code book. The index 'a' of the codeword k_a is outputted to restore the original state.

Steps 2–4 are repeated until all the secret data are extracted and all the original indexes are generated. After all five steps in the extracting and reversing phase have been performed, the secret data $B= (b_0, b_1,..........., b_T)$ can be accurately extracted and the output indexes should equal the original SMVQ-compressed codes. The reconstructed compressed codes can now be stored directly to save storage space and can be reused repeatedly for a variety of applications.

2.6. Histogram shifting technique

This reversible data hiding technique based on histogram shifting was proposed by Zhicheng Ni. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image.

2.6.1. Embedding algorithm

Note that zero point defined above may not exist for some image histograms. The concept of minimum point is hence more general. By minimum point, we mean such a grayscale value b, that a minimum number of pixels assume this value, i.e., $h(b)$ is minimum. Accordingly, the peak point discussed above is referred to as maximum point. Therefore, in the following discussion, we use terms maximum and minimum points.

2.6.1.1. Embedding Algorithm with one pair of maximum and minimum points

For an M x N image, each pixel grayscale value $x \in [0,255]$.

1) Generate its histogram.

2) In the histogram $H(x)$, find the maximum point $h(a)$, $a \in [0,255]$ and the minimum point zero $h(b), b \in [0,255]$.

3) If the minimum point h (b) > 0, recode the coordinate (i,j) of those pixels and the pixel grayscale value 'b' as overhead bookkeeping information (referred to as overhead information for short). Then set h (b) =0.

4) Without loss of generality, assume $a < b$. Move the whole part of the histogram $H(x)$ with $x \in [0,255]$ to the right by one unit. This means that all the pixel grayscale values (satisfying $x \in$ (a,b)) are added by one.

5) Scan the image, once meet the pixel (whose grayscale value is 'a'), check the to-be-embedded bit. If the to-be embedded bit is '1', the pixel grayscale value is changed to (a+1). If the bit is '0', the pixel value remains 'a'.

The actual data embedding capacity, C is calculated as follows:

$$C = h(a) - O \qquad (2.9)$$

where, O denotes the amount of data used to represent the overhead information. It is also referred to as pure payload.

2.6.1.2. Example of embedding algorithm with one pair of maximum and minimum points

Consider a grayscale image of size MxN. The steps for embedding process will be as follows.

1) First generate the histogram of the grayscale image. In the histogram, find a zero point Z. and then a peak point P. A zero point corresponds to the grayscale value in which there is no pixel in the given image. A peak point corresponds to the grayscale value which the maximum number of pixels in the given image. Assume, only one zero point and one peak point in the histogram. The objective of finding the peak point is to calculate the embedding capacity of the image, since the number of bits that can be embedded into an image is equal to the number of pixels which are associated with the peak point.

2) The whole image is scanned in any sequential order. For example . consider the peak point P in the image is 121. The grayscale value of pixels between 122 and 254 is incremented

by '1'. This step is equivalent to shifting the range of the histogram, to the right-hand side by 1unit, leaving the grayscale value *122* empty.

3) The whole image is scanned once again in the same sequential order. Once a pixel with grayscale value of *121* is encountered, if the corresponding embedding bit in the message sequence is '1', then the pixel value is incremented by '1'. Otherwise, the pixel value remains unchanged.

2.6.1.3. Embedding algorithm with multiple pairs of maximum and minimum points

Without loss of generality, only a pseudo embedding algorithm for the case of three pairs of maximum and minimum points is resented below. It is straightforward to generate this code to handle the cases where any other number of multiple pairs of maximum and minimum points is used. Clearly, if the required payload is greater than the actual capacity, more pairs of maximum point and minimum point need to be used.

The embedding algorithm with multiple pairs of maximum point and minimum point is presented below. For an MxN image with pixel grayscale values.

1) Generate its histogram $H(x)$.

2) In the histogram $H(x)$, find three minimum point h(b_1), h(b_2), h(b_3).Without loss of generality, assume three minimum points satisfy the following condition:0 $< b_1 < b_2 < b_3$ < 255.

3) In the intervals of (0, b_1) and (b_3, 255), find the maximum point, h(a_1), h(a_3) , respectively, and assume $a_1 \in$ (0, b_1), $a_3 \in$ (b_3, 255).

4) In the intervals (b_1, b_2) and (b_2, b_3) find the maximum points in each interval. Assume they are h(a_{12}), h(a_{21}),$b_1 < a_{12} < a_{21} < b_2$ and h(a_{23}), h(a_{32}) , $b_2 < a_{23} < a_{32} < b_3$.

5) Find a point having a larger histogram value in each of the following three maximum point pairs , (h(a_1), h(a_{12})), (h(a_{21}), h(a_{23})) and (h(a_{32}), h(a_3)) , respectively. Without loss of generality, assume h(a_1), h(a_{23}),h(a_3) ,are the three selected maximum points.

6) Then, are the three pairs of maximum and minimum points. For each of these three pairs, apply Steps 3-5 described in Section 2.5.1. That is, each of these three pairs are treated as a case of one pair of maximum and minimum points.

2.6.2. Extraction algorithm

For the sake of brevity, only the simple case of one pair of minimum point and maximum point is described here because, as shown above, the general cases of multiple pairs of maximum and minimum points can be decomposed as a few one pair cases. That is, the multiple pair case can be treated as the multiple repetition of the data extraction for one pair case. Assume the grayscale value of the maximum point and the minimum points are '*a*' and '*b*', respectively. Without loss of generality, assume $a< b$. The marked image is of size MxN, each pixel grayscale value $x \in [0,255]$.

1) Scan the marked image in the same sequential order as that used in the embedding procedure. If a pixel with its grayscale value (a+1) is encountered, '*a*' bit '1' is extracted. If a pixel with its value '*a*' is encountered, '*a*' bit '0' is extracted.

2) Scan the image again, for any pixel whose grayscale value $x \in [0,255]$, the pixel value '*x*' is subtracted by '1'.

3) If there is overhead bookkeeping information found in the extracted data, set the pixel grayscale value as '*b*'.

In this way, the original image can be recovered without any distortion.

CHAPTER 3

EXISTING METHOD

The text fusion watermarking technique is used for better authentication of the medical image. In this existing method, the detector uses a threshold value as the number of characters for the key provided to extract the data from the medical image. It also proposes the concept of semi reversible properties in the image for data-hiding and to get back the medical image without any distortion during watermarking. The proposed method demonstrates how to reduce the probability of false negative detection without increasing the false positive detection rate. The coefficient variance of original medical image, watermarked image and reconstructed image is compared.

3.1. The Existing method is divided into five modules

- Encoding
- Decoding
- Authentication
- Reconstruction
- Image Variance

3.1.1. Encoding

The watermark data is the text data having the patient information stored in the text file which is to be fused in the medical image.

Grey scale image

Our existing method uses an X-ray image which is an intensity (grey scale) image where it takes an 8-bit value i.e. (0,255).

Watermark Embedding

The embedding process is to mix the text data in the medical image. Firstly the text file having the patient information is read and then it was converted to binary data using the equation (1)

$$B\ (t) = ((\text{text}\ (i)\ \&2^{\wedge}7) <<1)/\ (2^{\wedge}7) \qquad (1)$$

Where, $1<= i <=$ count,

$1<=t<=8$ and B is the binary data, count is the no of characters and text () is the text data in the file. In order to have the reversible property that is higher order function is performed using the equation (2)

$$I(x,y)=I(x,y)\ \&\ (2^{\wedge}8\text{-}2) \qquad (2)$$

Where, $t<=i<=\text{count}*8$ and

$I(x,y)$ is the source image

Finally the binary content of the text data is embedded in the medical image using the equation (3)

$$W(x, y) = I(x, y) + B\ (t) \qquad (3)$$

Where, W(x, y) represent the watermarked image. Now the text data which has the patient information is hidden in the medical image with reversible property by bit by bit encoding of higher order sequence

3.1.2. Decoding

During the decoding process the data encapsulated in the watermarked medical image is extracted for the authentication process.

Watermarked Image

Our method uses an X-ray image which is intensity (Grey scale) image where it takes an 8-bit value i.e. (0,255) embedded with the text data.

Watermark Extraction

In our method the binary data of the text information Embedded in the medical image is extracted. During extraction, the number of characters embedded is given as the key to decode the binary data and the medical watermarked image is performed using the equation (4).

$$B(t) = W(x, y) \& 1 \qquad (4)$$

After the extraction the binary data is converted to the text data using the equation (5) for the authentication.

$$Text=B(t) * 2^{\wedge}(8-t) \qquad (5)$$

Where, 8<=t>=I, 1<=i<=count

3.1.3. Authentication

It is the process to determine the ownership of the information or image provided. Here the multiple authentication is performed, once the user didn't give the correct key the extraction will not be performed and if the key is given correct, the extraction is performed and the text data is stored in the text file to compare with the information of the patient, if the data is correlated with the patient information then the image is authenticated else the image is not authenticated. Thus the authentication is performed

3.1.4. Reconstruction

Once the image is the medical image it must not be affected due to watermarking and if even though it is affected we ought to recover the affected area, to obtain the original medical image from the watermarked image so the image must be reconstructed. This process follows only when the image is authenticated. After the image is authenticated then the watermarked image is reconstructed to recover the originality of medical image by using the semi reversible property followed using the equation (6)

$$I(x, y) = W(x, y) + B(t) \qquad (6)$$

The reconstruction process is same as encoding process but the parameter is watermarked image and the binary data of the text obtained from the extracted resultant text data, finally the original image is obtained.

3.1.5. Image Variance

Finally our attention is to the check the variance of the image before watermarking, after watermarking and after the reconstruction of image. Here we used the coefficient variation to detect the variation or changes in the image after the various modules like encoding, decoding and reconstruction. The variation is plotted in the graph relation in decibels (dB) using the Mean, Standard deviation (SD) and Variance

$$Mean = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (7)$$

$$SD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \mu)^2}{N}} \qquad (8)$$

$$Variance = \frac{Mean}{SD} \qquad (9)$$

CHAPTER 4

PROPOSED ALGORITHM

The proposed algorithm describes an efficient method of Reversible watermarking technique. A lossless data hiding scheme is based on spatial domain technique. This works by using the ASCII number representation of the characters in the key is used to create the coordinate pairs that represent the places in the matrix where the unit alterations of the picture matrix will be made and it creates the matrix used to find the points to hide the patient details. The ROI (Region of Interest) will be Embedded after checking whether the size of the original medical image is greater than size of the cropped medical image.

4.1. Embedding and extracting the patient details in medical images

For example consider the message as "Lipohemarthroses of the hip are rare" and key as "prabhu". This works by using the ASCII number representation of the chars in key to create coordinate pairs that represent the places in matrix where the unit alterations of the picture matrix will be made.

a. For e.g. key = 'prabhu'

b. Double the key value as double(key) and store that in A

   A= 112 114 97 98 104 117

c. Cumsum (A) returns the cumulative sum along different dimensions of an array and store that in B

   B=112 226 323 421 525 642

d. Reverse the key as 'uhbarp' and store that in keyb

   Keyb = 'uhbarp'

e. Double the keyb value as double (keyb) and store that in C

C=117 104 98 97 114 112

f. Cumsum(C) returns the cumulative sum along different dimensions of an array and store that in D

D=117 221 319 416 530 642

g. Consider row values as B and column values as D

h. Consider the dim1 and dim2 as picture matrix

i. First check whether the row values are less than the dim1 then by using the remainder after division method i.e. rem (dim1, row) remaining value will added with one and store that in rows and then check whether the column values are less than dim2 then by using the remainder after division method i.e. rem (dim2, col) remaining value will be added with one and store that in cols and finally setting the rows and cols as one

j. Extracting works same as embedding, by entering the decoding key it double the values by using double(key) and reverses the key and store that in keyb and it doubles the value by using double(keyb) and by checking the row and col value is less than the dim1, dim2 and set the row and col value as 1 and by using the remainder after division it checks rem(idx,2)==1 and if the condition satisfies it sets the value as one finally we get the patient details by reading the char(bin2dec).

k. Embedding the Region of Interest in the original medical image by checking the size of the cropped image is smaller than the original medical image.

l. Patient fault is cropped from the original medical image and crop needs a four- element position vector, [xmin ymin width height] and the position is find out by using imtool

m. For each image the fault position varies and the position is find out by using imtool

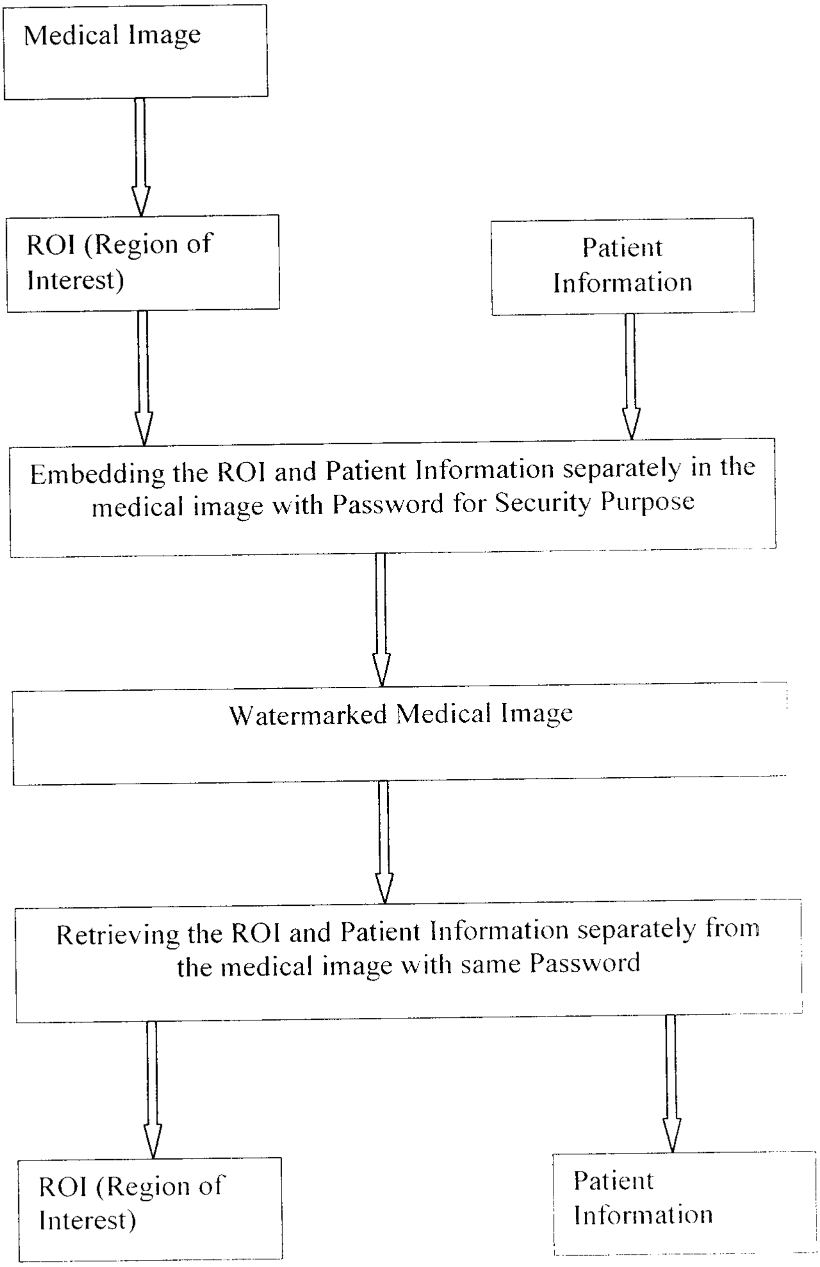

Medical Image
ROI (Region of Interest)
Patient Information
Embedding the ROI and Patient Information separately in the medical image with Password for Security Purpose
Watermarked Medical Image
Retrieving the ROI and Patient Information separately from the medical image with same Password
ROI (Region of Interest)
Patient Information

Figure.4.1 Architecture of Reversible Watermarking

4.2. The Proposed Reversible Watermarking Algorithm

Step1: Select the medical image from that the ROI is cropped

Step2: Enter the Patient information to be hidden in the Medical image

Step3: The patient information size should not exceed 1000 characters

Step4: In the encoding section, the ROI and Patient information are separately embedded in the Medical Image using the key.

Step5: In the decoding section, the ROI and patient information are separately retrieved from the medical image with the same key.

The embedding process done by using the key values was explained in section 4.1. The embedding capacity of message in the medical image was 1000 characters and size of the ROI (Region of Interest) to be embedded will be selected according to the size of the original medical image.

CHAPTER 5

SIMULATION RESULTS

The simulations are done by using MatlabR2008b. The performance of the proposed data hiding scheme is evaluated for different medical images.

5.1. Embedding and extracting the message in different medical images

Embedding and extracting the data (patient details) by using a key. Consider the message as "Lipohemarthroses of the hip are rare" and key as "prabhu". This works by using the ASCII number representation of the chars in key to create coordinate pairs that represent the places in matrix where the unit alterations of the picture matrix will be made. Embedding the ROI (Region of Interest) by checking whether the size of the original image is greater than the size of the ROI then ROI will be embed in the original medical image.

For example key='prabhu'

By doubling the value of 'prabhu' will get as

A=112 114 97 98 104 117

Cumsum (A) returns the cumulative sum along different dimensions of an array.

B=112 226 323 421 525 642

Considering the B value as rows

Reversing the key as keyb='uhbarp'

By doubling the value of 'uhbarp' will get as

C=117 104 98 97 114 112

Cumsum(C) returns the cumulative sum along different dimensions of an array.

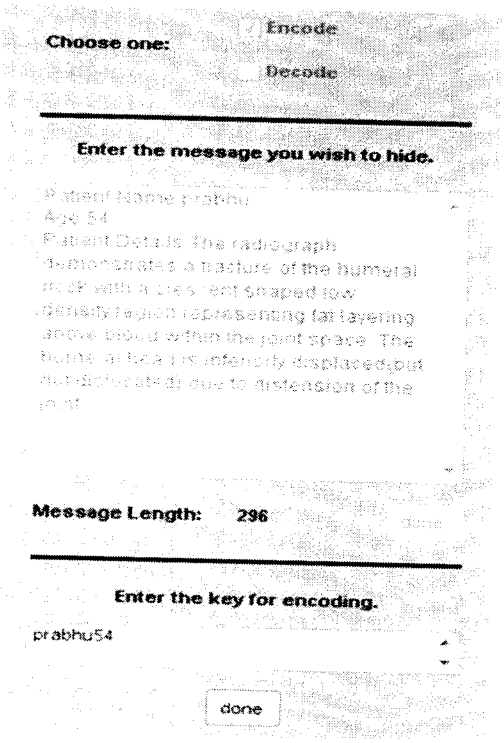
D=117 221 319 416 530 642

Considering the D value as columns

First it checks whether the row value is less than the dimension1 and if the condition is true then by using remainder after division rem (dim1, row) the remaining value will be added with one and then it checks whether the column value is less than the dimension2 and if the condition is satisfied then by using remainder after division rem (dim2, col) the remaining value will be added with one and finally setting the row and column value as one.

5.1.1. Embedding and extracting the patient information in shoulder image

Consider the patient information as "The radiograph demonstrates a fracture of the humeral neck with a crescent shaped low density region representing fat layering above blood within the joint space. The humeral head is inferiorly displaced (but not dislocated) due to distension of the joint". The watermarked medical image is shown in **Fig.5.1** and region of interest shows that the patient problem and it is shown in **Fig.5.1.1 (c)**



Choose one: ○ Encode ○ Decode

Enter the message you wish to hide.

Patient Name prabhu
Age 54
Patient Details The radiograph demonstrates a fracture of the humeral neck with a crescent shaped low density region representing fat layering above blood within the joint space. The humeral head is inferiorly displaced(but not dislocated) due to distension of the joint

Message Length: 296

Enter the key for encoding.

prabhu54

Figure 5.1 (a) Patient Details and Encoding Key

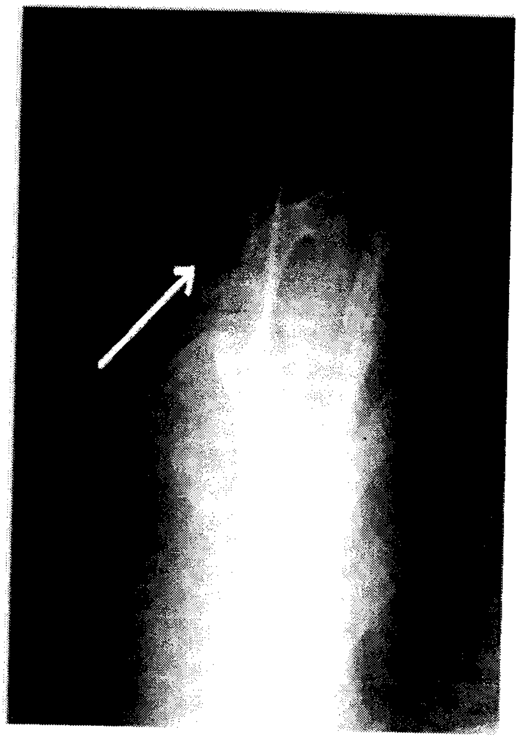


Figure 5.1 (b) Original Medical Image

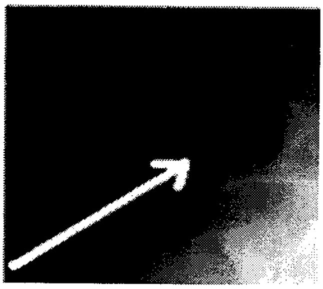
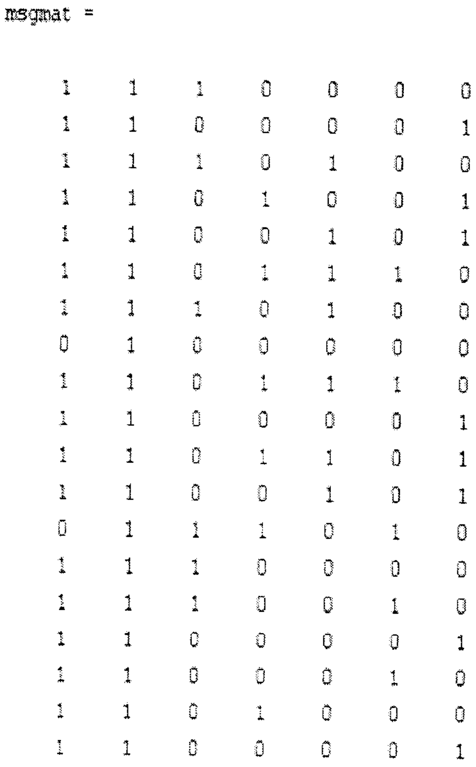
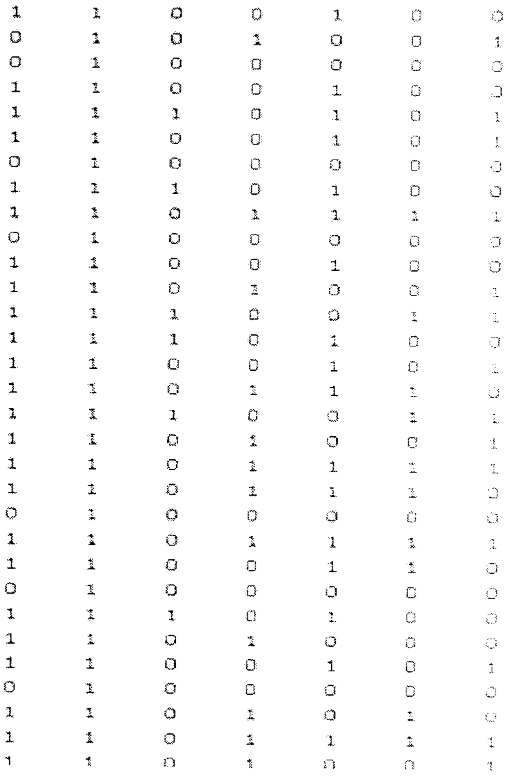


Figure 5.1 (c) ROI of Original Medical Image

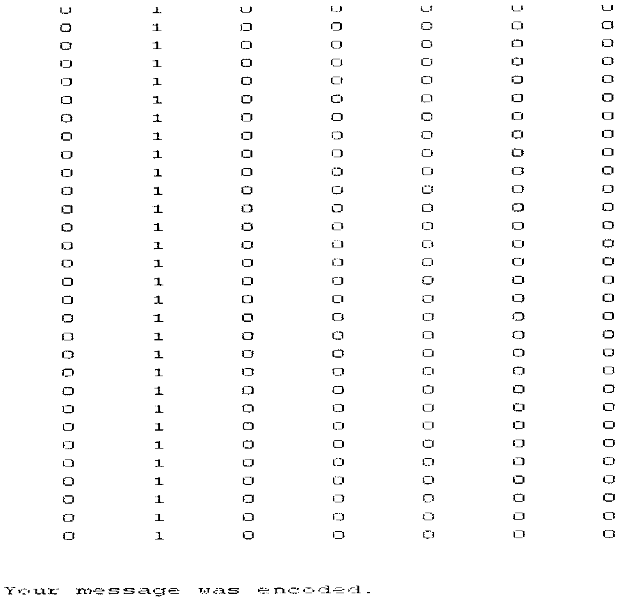


```
msgmat =


     1     1     1     0     0     0     0
     1     1     0     0     0     0     1
     1     1     1     0     1     0     0
     1     1     0     1     0     0     1
     1     1     0     0     1     0     1
     1     1     0     1     1     1     0
     1     1     1     0     1     0     0
     0     1     0     0     0     0     0
     1     1     0     1     1     1     0
     1     1     0     0     0     0     1
     1     1     0     1     1     0     1
     1     1     0     0     1     0     1
     0     1     1     1     0     1     0
     1     1     1     0     0     0     0
     1     1     1     0     0     1     0
     1     1     0     0     0     0     1
     1     1     0     0     0     1     0
     1     1     0     1     0     0     0
     1     1     0     0     0     0     1
```



```
     1     1     0     0     1     0     0
     0     1     0     1     0     0     1
     0     1     0     0     0     0     0
     1     1     0     0     1     0     0
     1     1     1     0     1     0     1
     1     1     0     0     1     0     1
     0     1     0     0     0     0     0
     1     1     1     0     1     0     0
     1     1     0     1     1     1     1
     0     1     0     0     0     0     0
     1     1     0     0     1     0     0
     1     1     0     1     0     0     1
     1     1     1     0     0     1     1
     1     1     1     0     1     0     0
     1     1     0     0     1     0     1
     1     1     0     1     1     1     0
     1     1     1     0     0     1     1
     1     1     0     1     0     0     1
     1     1     0     1     1     1     1
     1     1     0     1     1     1     0
     0     1     0     0     0     0     0
     1     1     0     1     1     1     1
     1     1     0     0     1     1     0
     0     1     0     0     0     0     0
     1     1     1     0     1     0     0
     1     1     0     1     0     0     0
     1     1     0     0     1     0     1
     0     1     0     0     0     0     0
     1     1     0     1     0     1     0
     1     1     0     1     1     1     1
     1     1     0     1     0     0     1
```



```
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0
0    1    0    0    0    0    0

Your message was encoded.
```

Figure 5.1 (d) Binary representation of the message

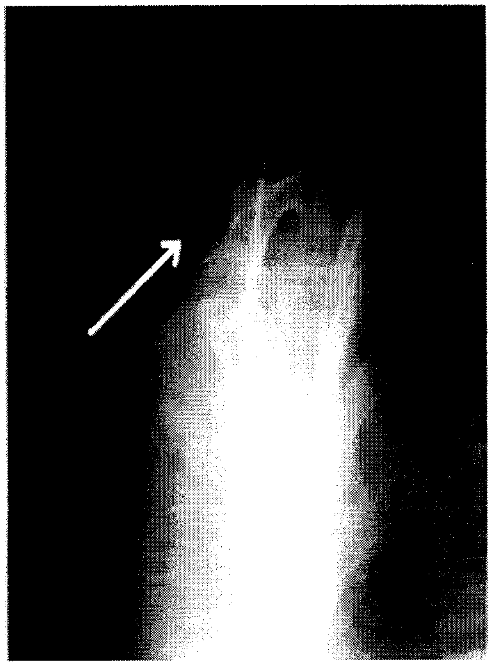
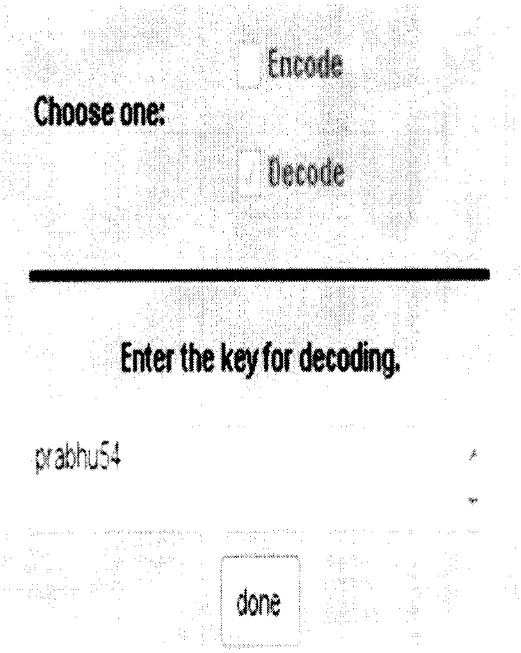


Figure 5.1 (e) Watermarked medical image

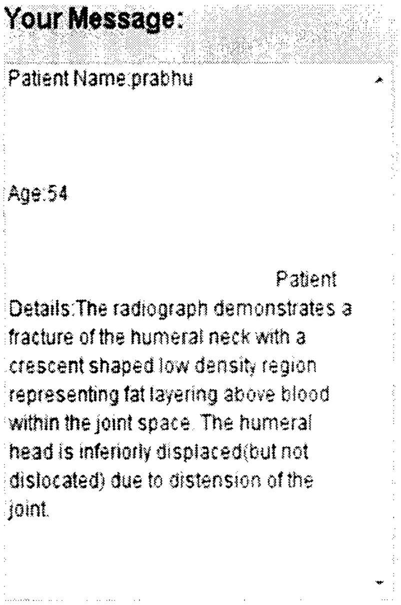


Choose one: □ Encode ☑ Decode

Enter the key for decoding.

prabhu54

Figure 5.1 (f) Decoding key



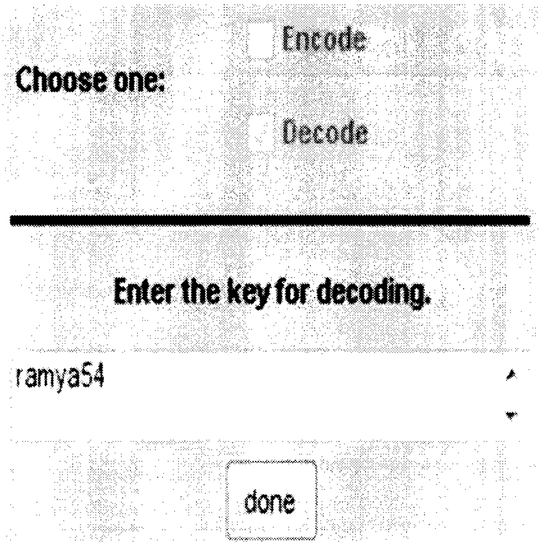
Your Message:

Patient Name:prabhu

Age:54

Patient Details:The radiograph demonstrates a fracture of the humeral neck with a crescent shaped low density region representing fat layering above blood within the joint space. The humeral head is inferiorly displaced(but not dislocated) due to distension of the joint.

Figure 5.1 (g) Decoded Messages



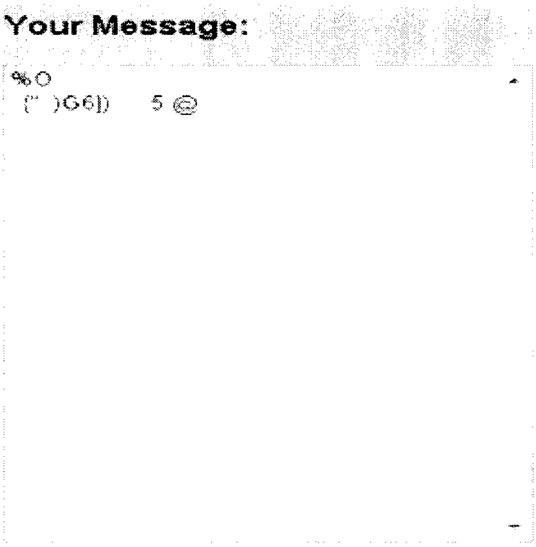
Choose one:

□ Encode

□ Decode

Enter the key for decoding.

ramya54



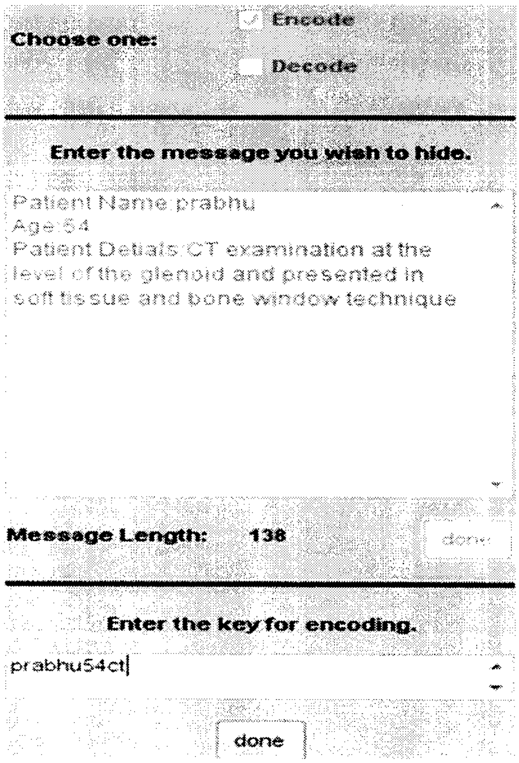
Your Message:

%○
{")G6]) 5 ©

Figure 5.1 (h) Illustrates entering unauthorized key **Figure 5.1 (i) Shows false message**

5.1.2. Embedding and extracting the patient information in shoulder ct1

Consider the patient information details as "CT examination at the level of the glenoid and presented in soft tissue and bone window technique" and giving the encoding key as "prabhu54ct "



Choose one: ☑ Encode □ Decode

Enter the message you wish to hide.

Patient Name:prabhu
Age:54
Patient Detials:CT examination at the level of the glenoid and presented in soft tissue and bone window technique

Message Length: 138

Enter the key for encoding.

prabhu54ct

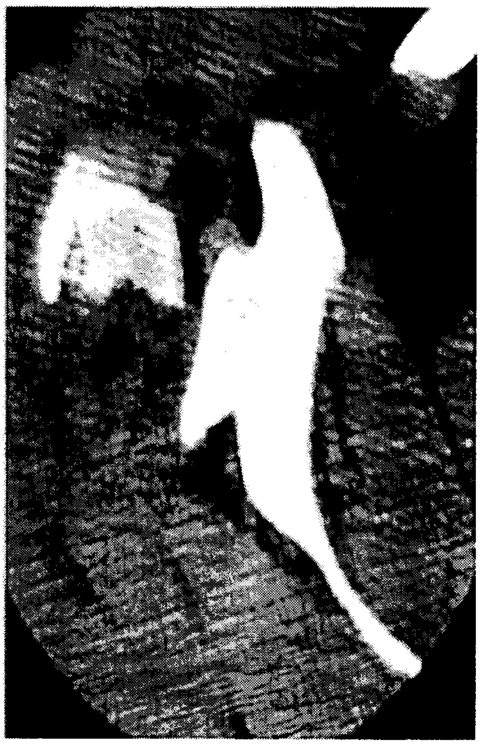


Figure 5.2 (a) Patient details and encoding key Figure 5.2 (b) Original Medical image

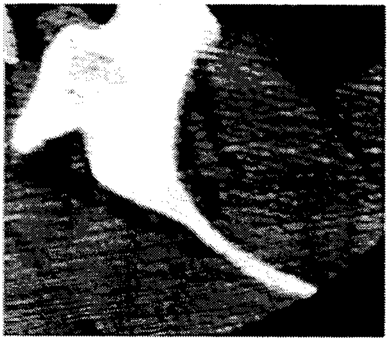


Figure 5.2 (c) ROI of Original Medical image

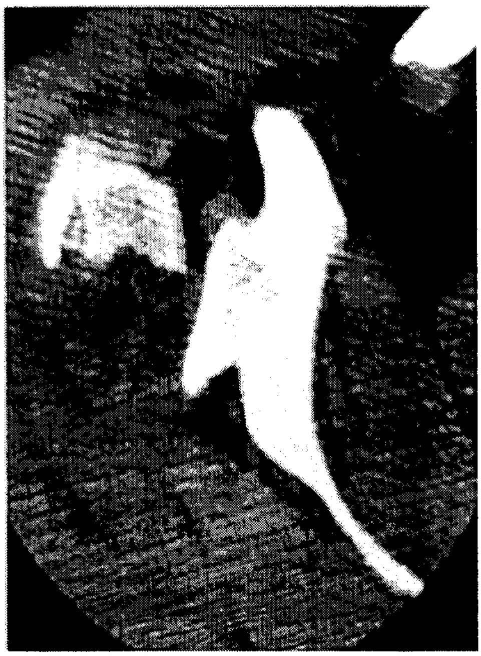
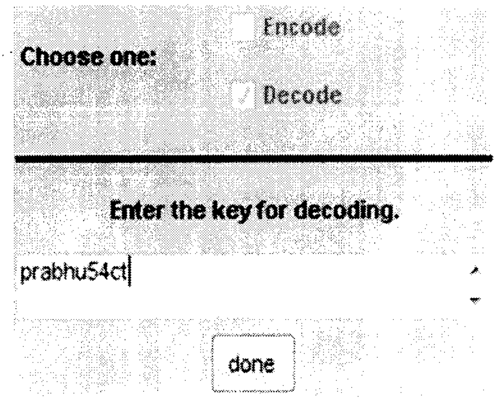


Figure 5.2 (d) Watermarked Medical image



Choose one:

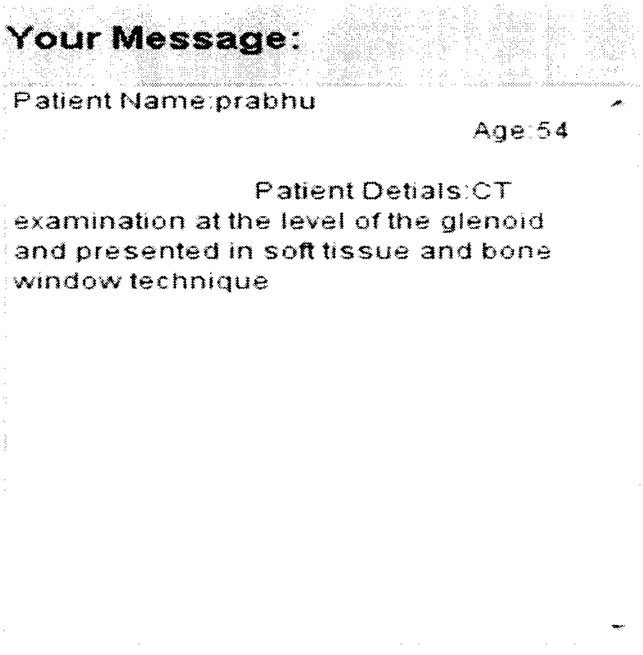
□ Encode

☑ Decode

Enter the key for decoding.

prabhu54ct

Figure 5.2 (e) Decoding key



Your Message:

Patient Name:prabhu

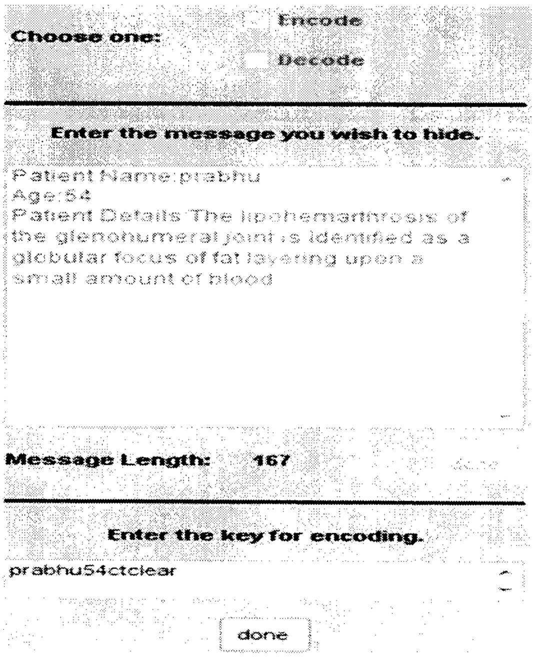
Age:54

Patient Detials:CT examination at the level of the glenoid and presented in soft tissue and bone window technique

Figure 5.2 (f) Decoded messages

5.1.3. Embedding and extracting the patient details in shoulder ct2

Consider the patient details as "The lipohemarthrosis of the glenohumeral joint is identified as a globular focus of fat layering upon a small amount of blood" and giving the encoding key as "prabhu54ctclear"



Choose one: Encode
□ Decode

Enter the message you wish to hide.

Patient Name:prabhu
Age:54
Patient Details The lipohemarthrosis of the glenohumeraljoint is identified as a globular focus of fat layering upon a small amount of blood

Message Length: 167

Enter the key for encoding.

prabhu54ctclear

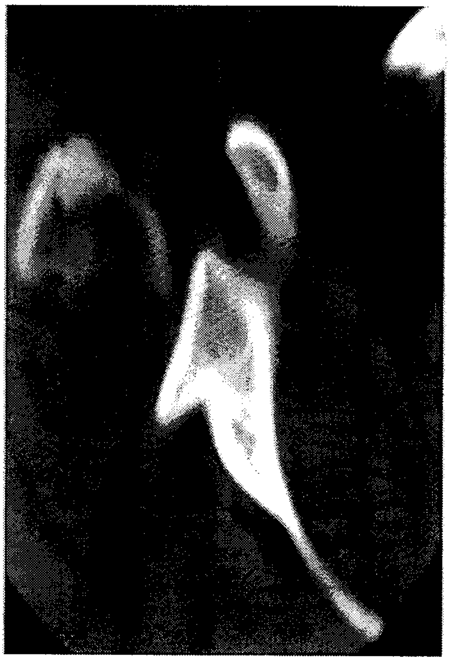


Figure 5.3 (a) Patient details and encoding key Figure 5.3 (b) Original Medical image

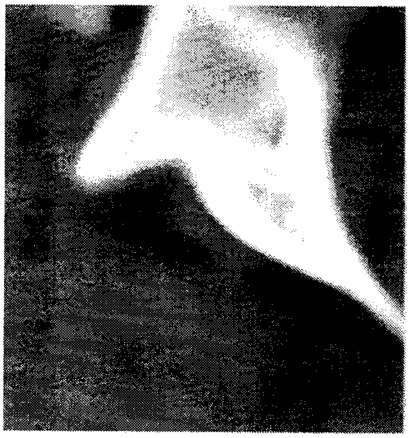


Figure 5.3 (c) ROI of Original Medical image

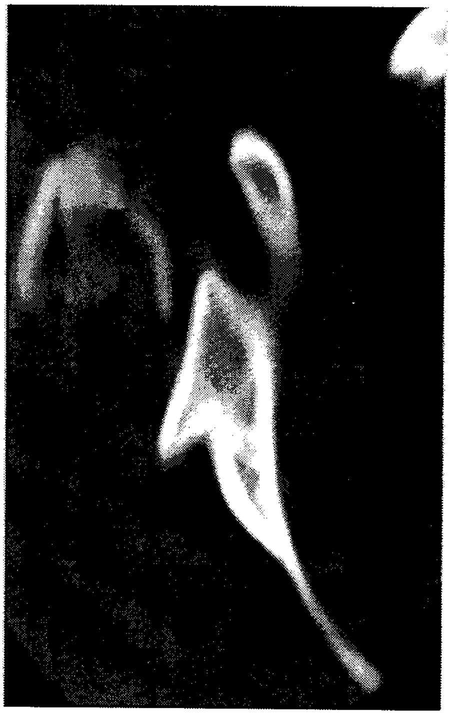
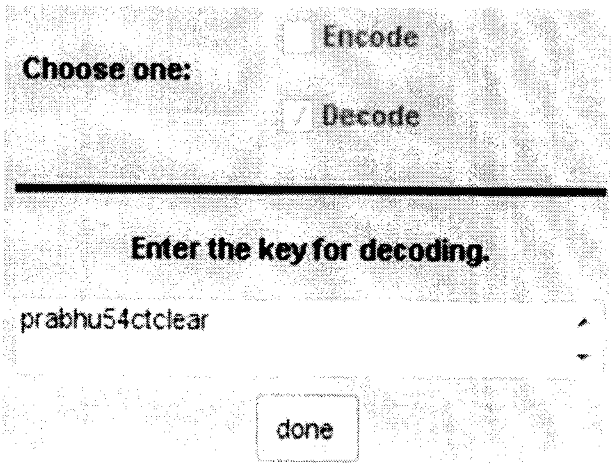


Figure 5.3 (d) Watermarked Medical image



Choose one:

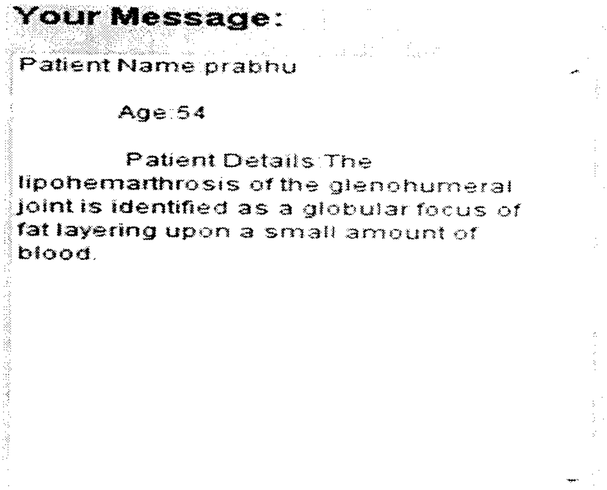
□ Encode

☑ Decode

Enter the key for decoding.

prabhu54ctclear

Figure 5.3 (e) Decoding key



Your Message:

Patient Name prabhu

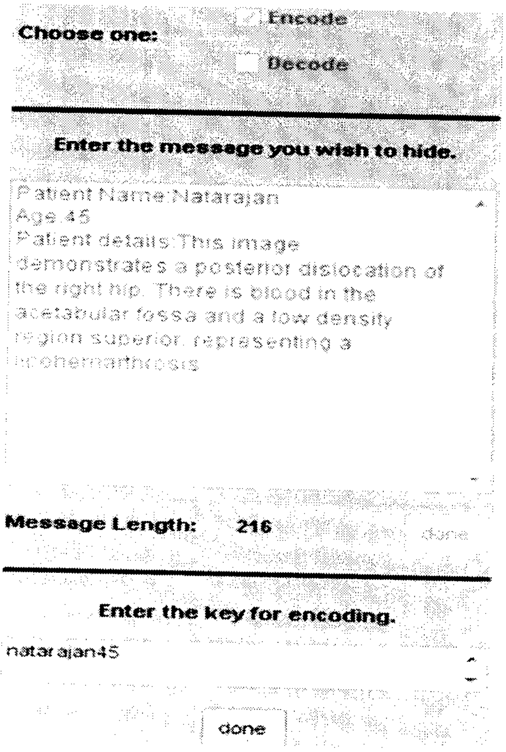
Age 54

Patient Details The lipohemarthrosis of the glenohumeral joint is identified as a globular focus of fat layering upon a small amount of blood.

Figure 5.3 (f) Decoded messages

5.1.4. Embedding and extracting the patient details in Hip Lipohemarthrosis

Consider the patient details as "This image demonstrates a posterior dislocation of the right hip. There is blood in the ace tabular fossa and a low density region superior, representing a lipohemarthrosis" and giving the encoding key as "natarajan45"



Choose one: ☑ Encode ☐ Decode

Enter the message you wish to hide.

Patient Name:Natarajan
Age 45
Patient details:This image demonstrates a posterior dislocation of the right hip. There is blood in the acetabular fossa and a low density region superior, representing a lipohemarthrosis

Message Length: **216**

Enter the key for encoding.

natarajan45

Figure 5.4 (a) Patient Details and Encoding key

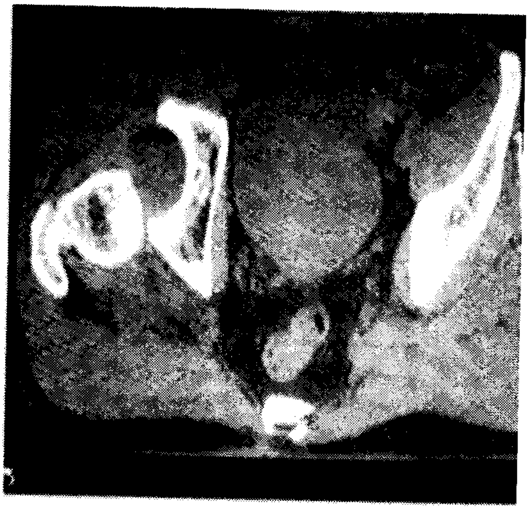


Figure 5.4 (b) Original Medical image

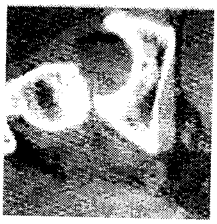


Figure 5.4 (c) ROI of Original Medical image

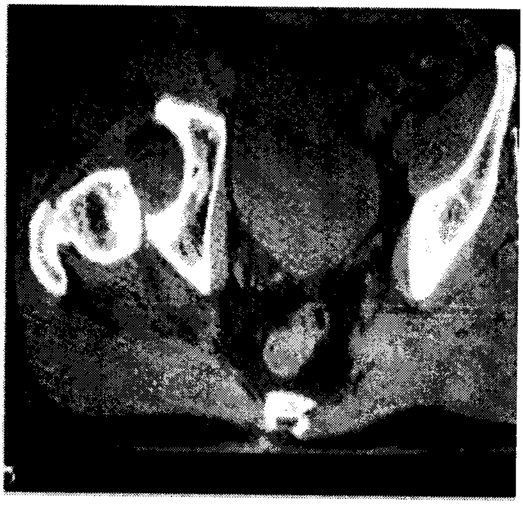
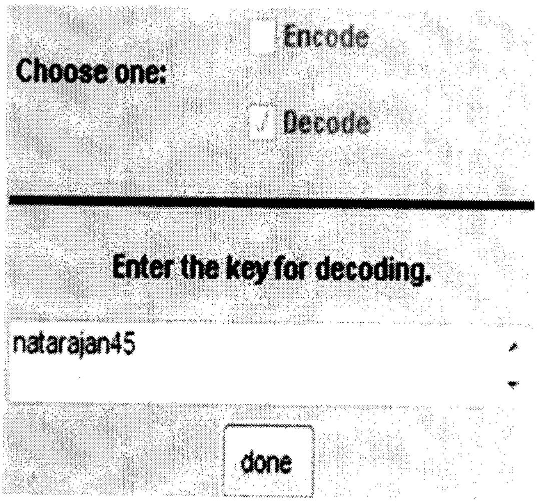


Figure 5.4 (d) Watermarked Medical image

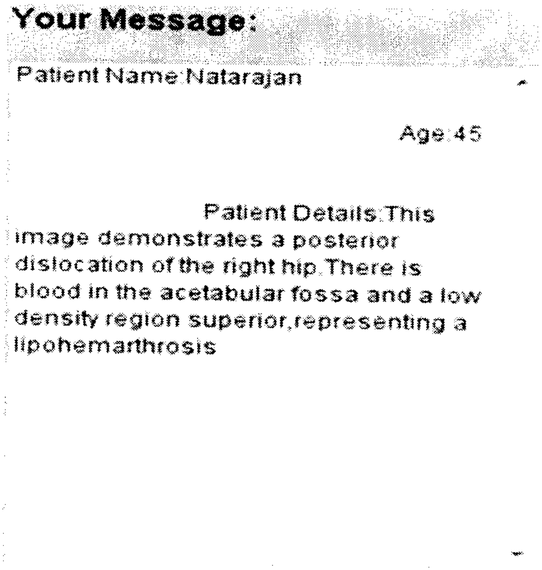


Choose one: ☐ Encode ☑ Decode

Enter the key for decoding.

natarajan45

Figure 5.4 (e) Decoding Key



Your Message:

Patient Name:Natarajan

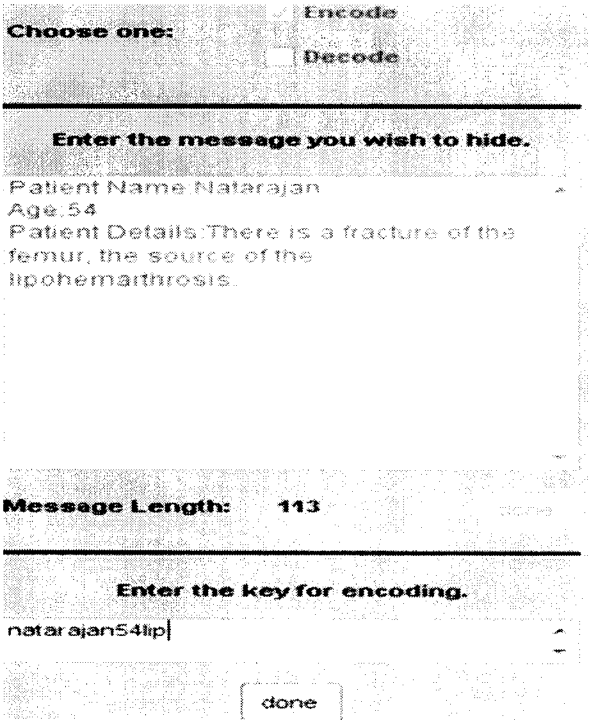
Age:45

Patient Details:This image demonstrates a posterior dislocation of the right hip.There is blood in the acetabular fossa and a low density region superior,representing a lipohemarthrosis

Figure 5.4 (f) Decoded Message

5.1.5. Embedding and extracting the patient details in hip joint image

Consider the patient information details as "There is a fracture of the femur, the source of the lipohemarthrosis" and giving the encoding key as "natarajan54lip"


Choose one: ☑ Encode □ Decode

Enter the message you wish to hide.

Patient Name:Natarajan
Age:54
Patient Details:There is a fracture of the femur, the source of the lipohemarthrosis.

Message Length: 113

Enter the key for encoding.

natarajan54lip

Figure 5.5 (a) Patient Details and encoding key

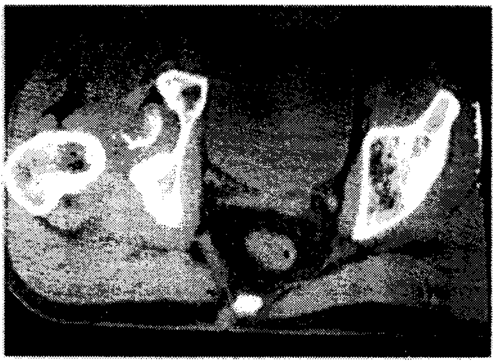


Figure 5.5 (b) Original Medical image

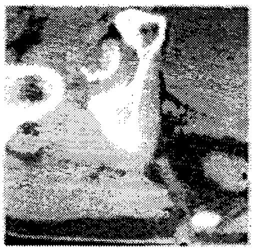


Figure 5.5 (c) ROI of Original Medical Image

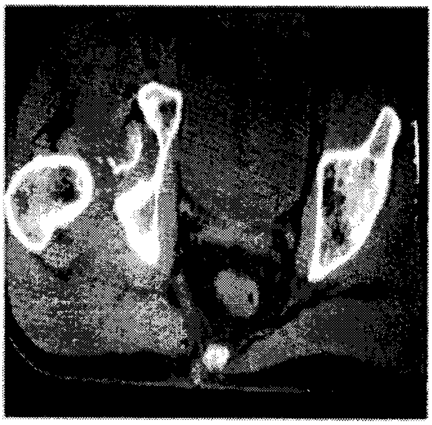
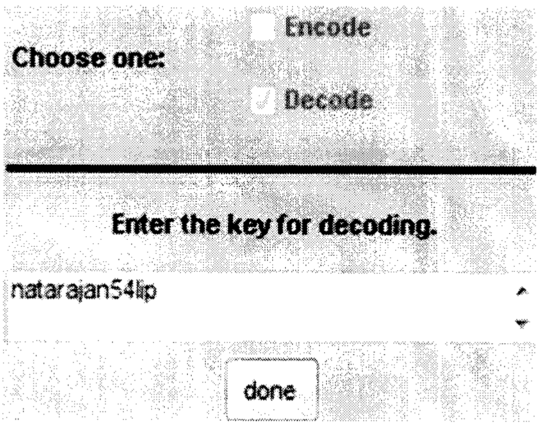


Figure 5.5 (d) Watermarked Medical image



Choose one:

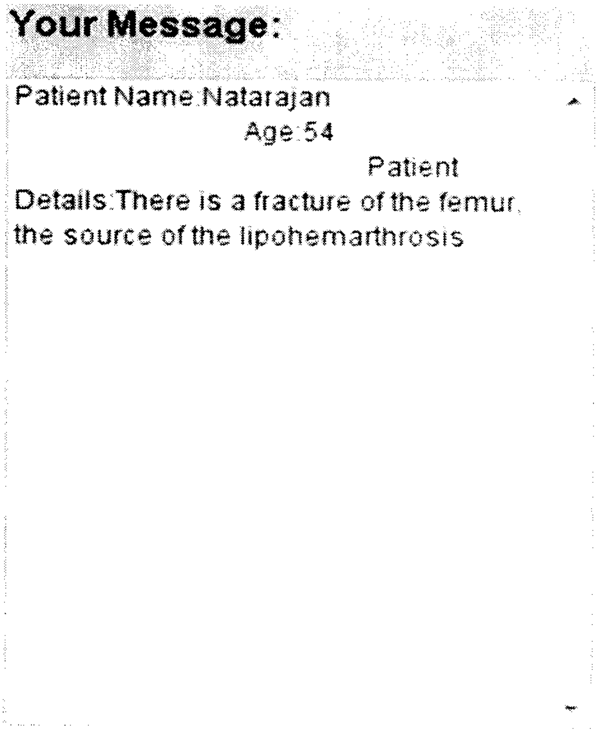
□ Encode

☑ Decode

Enter the key for decoding.

natarajan54lip

Figure 5.5 (e) Decoding Key



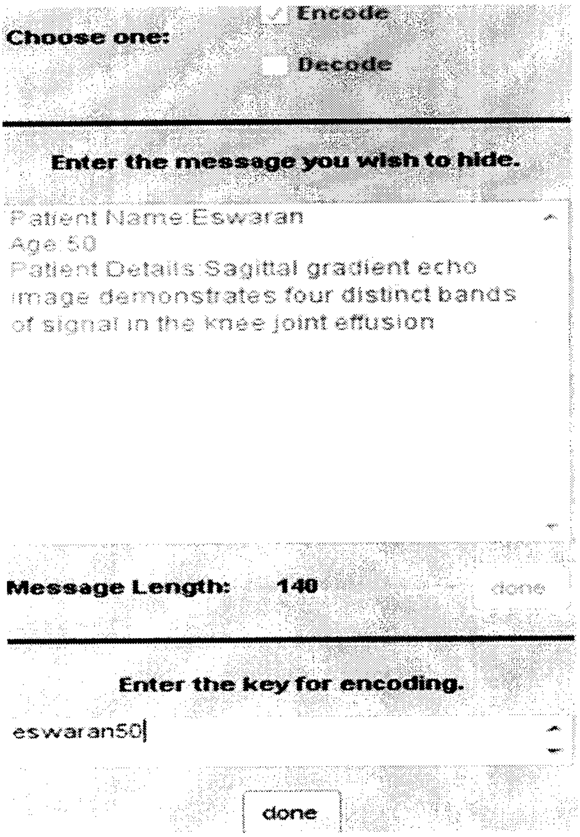
Your Message:

Patient Name:Natarajan
Age:54
Patient
Details:There is a fracture of the femur,
the source of the lipohemarthrosis

Figure 5.5 (f) Decoded Messages

5.1.6. Embedding and extracting the patient details in sagittal gradient echo image

Consider the patient information details as "Sagittal gradient echo image demonstrates four distinct bands of signal in the knee joint effusion" and giving the encoding key as "eswaran50"



Choose one: ☑ Encode □ Decode

Enter the message you wish to hide.

Patient Name:Eswaran
Age:50
Patient Details:Sagittal gradient echo image demonstrates four distinct bands of signal in the knee joint effusion

Message Length: 140

Enter the key for encoding.

eswaran50

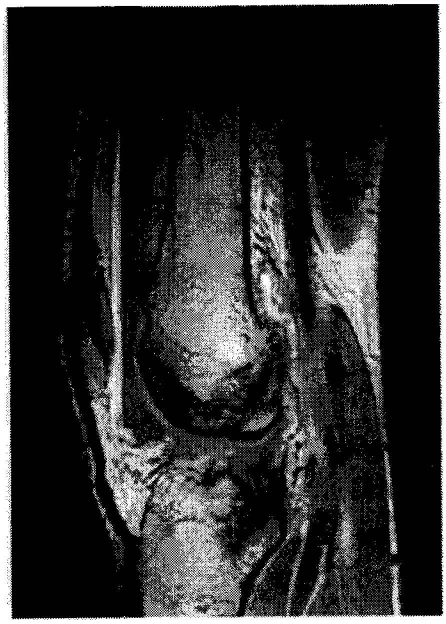


Figure 5.6 (a) Patient details and Encoding key Figure 5.6 (b) Original Medical image

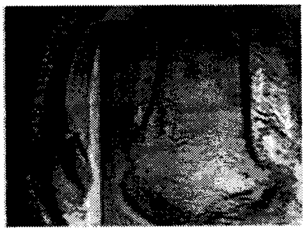


Figure 5.6 (c) ROI of Original Medical image

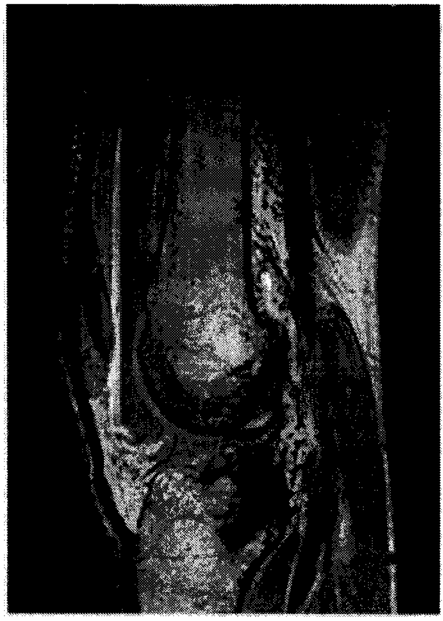
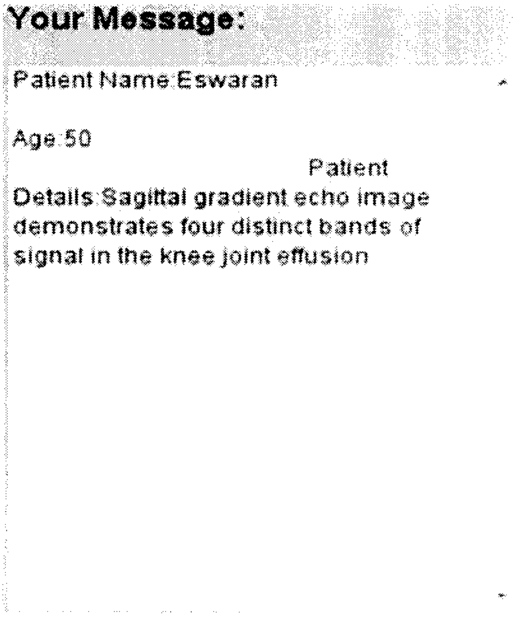


Figure 5.6 (d) Watermarked Medical image



Your Message:

Patient Name:Eswaran

Age:50

Patient Details:Sagittal gradient echo image demonstrates four distinct bands of signal in the knee joint effusion

Figure 5.6 (e) Decoded Message

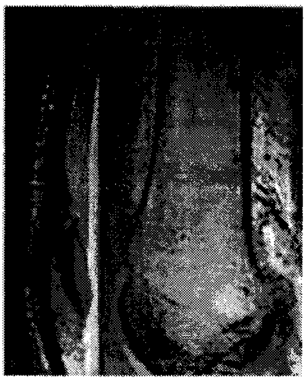
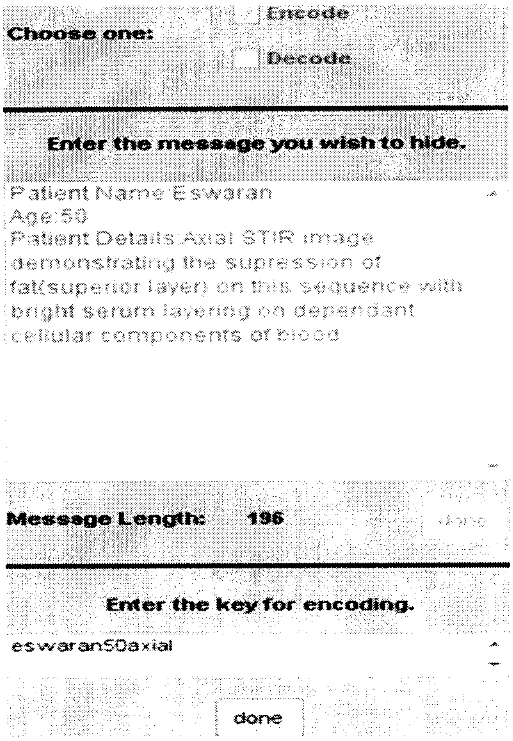


Figure 5.6 (f) Decoded ROI

5.1.7. Embedding and extracting the patient details in Axial STIR image

Consider the patient information details as "Axial STIR image demonstrating the suppression of fat (superior layer) on this sequence with bright serum layering on dependant cellular components of blood" and giving the encoding key as "eswaran50axial"



Choose one: ☑ Encode □ Decode

Enter the message you wish to hide.

Patient Name Eswaran
Age:50
Patient Details:Axial STIR image demonstrating the supression of fat(superior layer) on this sequence with bright serum layering on dependant cellular components of blood

Message Length: 196

Enter the key for encoding.

eswaran50axial

Figure 5.7 (a) Patient details and encoding key

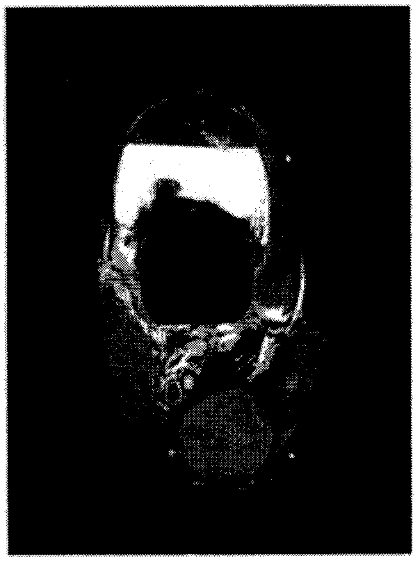


Figure 5.7 (b) Original Medical image

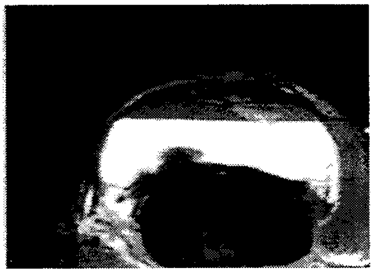
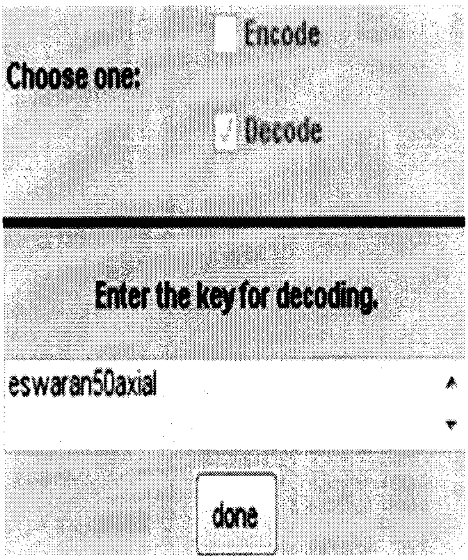


Figure 5.7 (c) ROI of Original Medical image



Choose one:

□ Encode

☑ Decode

Enter the key for decoding.

eswaran50axial

Figure 5.7 (d) Decoded key

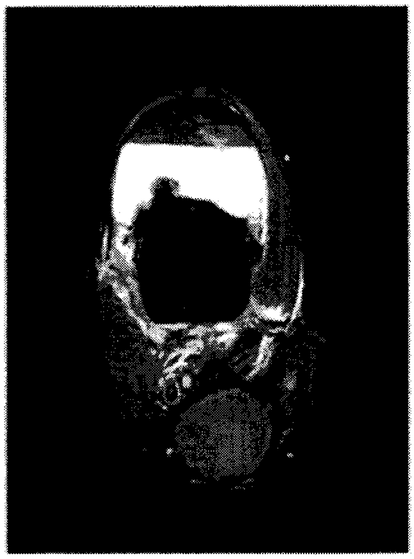


Figure 5.7 (e) Watermarked Medical image

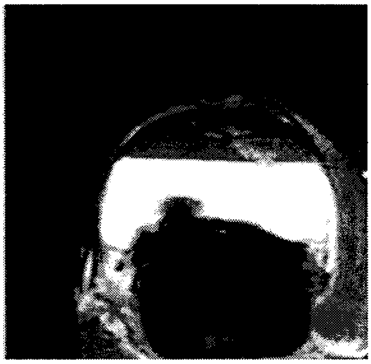
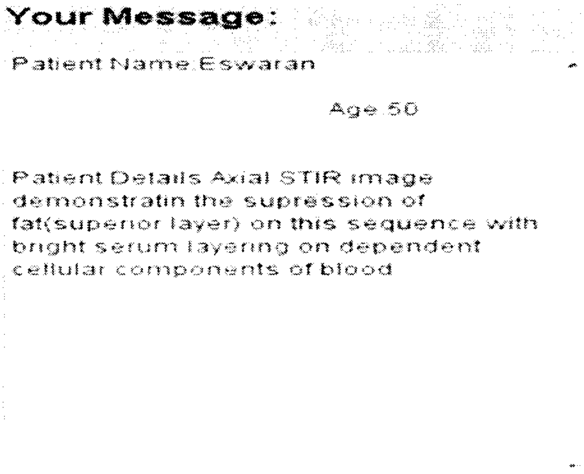


Figure 5.7 (f) Decoded ROI



Your Message:

Patient Name Eswaran

Age 50

Patient Details Axial STIR image demonstratin the supression of fat(superior layer) on this sequence with bright serum layering on dependent cellular components of blood

Figure 5.7 (g) Decoded Messages

Table 5.1. Size of the source image and the information embedded in that image

Medical Images	Xmin	Ymin	Width	Height	Used % of the source image
Shoulder X-ray	75	68	150	150	24.4557
Shoulder ct1	146	210	230	300	50.0218
Shoulder ct2	170	125	300	300	89.0133
Hiplipct4200	20	24	80	80	50.7068
Hiplipoct5200	20	24	100	100	78.3759
Knee MRI GE	20	24	150	150	70.5282
Knee MRI STIR	60	70	100	100	31.7708

CHAPTER 6

CONCLUSION

A new reversible watermarking scheme for medical images and to encode the patient information using a key is presented. This uses the ASCII number representation of the characters in KEY to create coordinate pairs that represent the places in matrix where the unit alterations to the picture matrix will be made and patient fault is cropped manually from the medical image. Both the patient information and ROI are encoded separately in the original medical image.

FUTURE WORK

In future, the proposed algorithm may be implemented

- For 3D images
- For higher capacity of patients information.

REFERENCES

[1] Poonkuntran Shanmugam, Rajesh .R.S, Eswaran Perumal "A Reversible Watermarking with Low Warping: An Application to Digital Fundus Image", International Conference on Computer and Communication Engineering 2008 May 13-15, 2008 Kuala Lumpur, Malaysia

[2] Viswanathan P., P.Venkata Krishna, "Text fusion watermarking in Medical image with Semi-reversible for Secure transfer and Authentication", 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[3] William Stallings. Cryptography and Network Security- Principles and Practices. Prentice-Hall, 2003.

[4] J. Tian, "High capacity reversible data embedding and content authentication", in proc. ICASSP '03, Acoustics, Speech, and Signal Processing, IEEE International Conference on, Vol. 3,pp. 6-10, April 2003.

[5] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", Image Processing, IEEE Transactions on, Vol. 13, Issue 8, pp. 1147_ 1156, Aug. 2004.

[6] N. Zhicheng, Y.Q. Shi, N. Ansari, S. Wei,"Reversible data hiding", in proc. ISCAS '03, Circuits and Systems,International Symposium on, May 2003, Vol. 2, pp. 25-28.

[7] Mingyan Li, Radha Poovendran, Sreeram Narayanan, Protecting patient privacy against unauthorized release of medical images in a group communication situation,Computerized Medical Imaging and Graphics 29 (2005) 367–383.

[8] Rajendra Acharya U., P. Subbanna Bhat, SathishKumar, Lim Choo Min, Transmission and storage of medical images with patient information, Computers in Biology and Medicine 33 (2003) 303–310.

TAMILNADU COLLEGE OF ENGINEERING
COIMBATORE-641659

New heights old traditions

bringing the world locally

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that Dr./Mrs./Mr..........PRABHU T , PG SCHOLAR.............. KUMARAGURU COLLEGE OF TECHNOLOGY , COIMBATORE.... **has presented a paper titled** HIDING PATIENT INFORMATION IN MEDICAL IMAGES USING INVISIBLE WATERMARKING TECHNI **authored by** ....PRABHU T ........AND.......MS. S SASIKALA...................................... **in the two day National Conference on Emerging Trends in Computer Communication and Informatics - ETCCI 2011, technically co-sponsered by CIIT International Journal held on 10th and 11th MARCH 2011.**

Mrs.S.Latha Shanmuga Vadivu
Asst. Prof. ECE
CO-ORDINATOR

V. K
Mr.V.Karthikeyan
Lect. ECE
CO-ORDINATOR

Dr.M.Karthikeyan
HOD

Dr.C.Kalaiarasan
PRINCIPAL

Department of Electronics and Media Technology

NATIONAL CONFERENCE

on

Signals, Systems & Technologies in Media

This is to certify that

.......................T. Prabhu.......................

presented a Paper titled ......Reversible......Watermarking..............

........Technique......Using......Text......in......Medical......Images..............

in the National conference held on 25th and 26th of Feb 2011.

G. Bala

Dr.(Mrs) G.Joesmin Bala
CONVENER & HOD, EMT

Dr. Anne Mary Fernandez
REGISTRAR

Paul P. Appasamy

Dr. Paul P. Appasamy
VICE CHANCELLOR