

# EMBEDDING OF MEDICAL DATA IN DIGITAL MRI IMAGE

Mrs.SamataR. Bhosale  
SRIEIT, Shiroda - Goa

**Abstract-**In today's world man is addicted to internet. With the help of internet one can easily transmit data, files, important documents etc from one place to another. Along with these advantages there are some drawbacks that is lack of security that is the data transmitted over the internet can be hacked by unwanted user and can change and manipulate the information resulting in wrong data reaching the destination. Therefore some sort of security is necessary, steganography is one of the method to secure the data by hiding the data in the host image such that only the sender and the receiver knows that there exist some data in the image. At the receiving end the data is extracted securely without causing any distortion to the host image. In this paper I am hiding patients data in his MRI image using histogram based reversible data hiding based on pixel differences with prediction and sorting. In this paper I am hiding the patients data in lung MRI image and making analysis by comparing the host image with the image after extracting the message by finding the Peak signal to noise ratio, the mean square error and the entropy difference. I am tabulating the PSNR, MSE and entropy difference by hiding the data in seventeen different lung images. Here I am also introducing a secret key for embedding data and the same secret key is to be entered before extracting the data. is done by finding the PSNR.

**Keywords-** Histogram, Lossless, Reversible, Steganography.

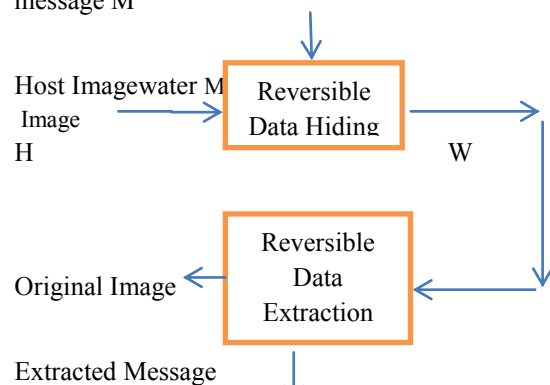
## OBJECTIVES

The main objective of this project is to provide security in medical field by hiding the patient's information in his MRI image and extracting the data and image without any losses. Hiding data

inevitably destroys the host image even though the distortion introduced by hiding is imperceptible to the human visual system. However, there are some sensitive images where any embedding distortion made to the image is intolerable, such as military images, medical images or artwork preservation. For example, even slight changes are not accepted in medical images due to a potential risk of a physician giving a wrong explanation of the image. Hence, reversible data hiding techniques give a solution to the problem of how to embed a large message in digital images in a lossless manner so that the image can be completely restored to its original state before the embedding occurred.

## I. INTRODUCTION

message M



**Fig. 1 Block Diagram Of Reversible Data Hiding.**

Fig shows the block diagram of Reversible Data Hiding procedure. The message is embedded in the host image resulting in the watermarked image and the original image and message is been extracted without distortion of the host image

## II. PROPOSED WORK

The method implemented in the proposed work is hiding message in digital image using an improved histogram based lossless data hiding scheme based on prediction and sorting. This project presents the pixel prediction sorting to

enhance the correlation of the neighboring pixels [2]. Here a rhombus prediction is used where a pixel in white set is predicted by considering four neighboring pixels of the gray set, if the data is embedded in white set or a pixel in gray set is predicted by considering four neighboring pixels in the white set, if the data is to be embedded in gray set. In order to hide more data with less visual degradation, the order to hide data into the pixel difference needs to be changed. Thus the cover pixels can be rearranged by sorting according to the prediction of neighboring pixels. To ensure the reversibility, we use a stable sorting algorithm to sort the prediction values. Sorting cover pixels according to the prediction values enables hiding data in pixel difference with high embedding capacity. In this method the histogram of the given host image is generated and the peak point and the zero point is calculated. The peak point is a point which indicates the maximum occurrence particular pixel in the given image and the zero point indicates the occurrence of no pixel in the given image. Let M be the peak point and N be the zero point. The range of the histogram between the peak point and the zero point that is (M+1, N-1) is shifted by 1 to the right hand side so that the zero point will be at M+1. If a pixel with value 'M' is found and if the message bit is '1', increase the value of the pixel by '1' [6]. If the pixel with value other than 'M' is found then no change is required. The number of message bits that can be hidden in the host image is equal to the number of pixels at the peak point. The data extraction is the reverse process of data hiding

	$V_{i-1,j}$		
$V_{i,j-1}$	$U_{i,j}$	$V_{i,j+1}$	
	$V_{i+1,j}$		

when a pixel with value (M+1) is found message

bit '1' is extracted and the pixel value is reduced to 'M' and when a pixel with value 'M' is found message bit '0' is extracted. After the entire message is been extracted, the range of the histogram (M+2, N) is shifted to the left hand side by 1. The analysis of the host image and the extracted image after embedding the message is made by comparing the host image and the extracted image by finding the peak signal to noise ratio (PSNR), mean square error (MSE) and the Entropy difference. This method has a good influence on increasing the number of message bits that can be hidden. Characteristics of the pixel difference are used to achieve large hiding capacity while keeping low distortion.

### III. METHODOLOGY

The method implemented is an improved histogram based lossless data hiding scheme based on prediction and sorting. A comparative study of the host image and the extracted image is done by finding the PSNR, Mean square error and Entropy difference. This method has a good influence on increasing the embedding capacity. Characteristics of the pixel difference are used to achieve large hiding capacity while keeping low distortion.

**IV. Implementation:** The method used in the project is summarized below. All pixels of the image are divided into two sets the white set and the gray set. The pixel value U of the white set can be predicted by using the four neighboring pixels of the gray set to hide the data. The center white pixel  $U_{i,j}$  can be predicted from the four neighboring pixels  $V_{i,j-1}$ ,  $V_{i-1,j}$ ,  $V_{i,j+1}$ ,  $V_{i+1,j}$  using the formula below[2]

$$U_{i,j} = [ V_{i,j-1} + V_{i-1,j} + V_{i,j+1} + V_{i+1,j} ] / 4 \text{ -----1}$$

In order to increase the embedding capacity the cover pixels can be rearranged by sorting according to the prediction of neighboring pixels this enables hiding data in pixel difference with high embedding capacity [2].

- If  $d_i = P$ , modify  $x_i$  according to the message bit

$$x_i + b, \text{ if } d_i = P \text{ and } x_i \geq x_{i-1}$$

$$y_i =$$

$$x_i - b, \text{ if } d_i = P \text{ and } x_i < x_{i-1}$$

where  $y_i$  is the water marked value of pixel  $i$ .

**Fig.2 Rhombus Prediction**

The reversible data hiding scheme for white set is designed as follows

- Predict the pixel value  $U_{i,j}$  in white set using equation 1
- Sort the host pixel  $U_{i,j}$  according to the prediction value  $U_{i,j}$  and produce the sorted pixels  $\{x_0, x_1, x_2, x_3, \dots, x_i\}$  for  $0 \leq i \leq N-1$

- Construct the watermarked white set according to the sorted pixels  $\{y_0, y_1, y_2, \dots, y_i\}$  for  $0 \leq i \leq N-1$  where  $N$  is the pixel number of white set.

Where  $N$  is the pixel number of white set.

- Calculate the pixel difference  $d_i$  between pixels  $x_{i-1}$  and  $x_i$  by using the formula

157	156	157	158	$d_i =$  $ x_{i-1} - x_i $ otherwise
159	157	159	157	
155	156	156	156	
153	155	154	155	

Host Image

- Determine the peak point  $P$  from the pixel differences.

The above figure shows the gray scale image with 4x4 pixels with the specified pixel values.

If  $d_i > P$ , shift  $x_i$  by 1 unit

$x_i$  if  $i=0$  or  $d_i < P$

$y_i = x_{i+1}$  if  $d_i > P$  and  $x_i \geq x_{i-1}$

$x_{i-1}$  if  $d_i > P$  and  $x_i < x_{i-1}$

where  $y_i$  is the water marked value of pixel  $i$ .

Predicted Values

157	156	157	158
159	157	159	157
156	156	156	156
153	154	154	155

The above figure shows the predicted pixel values of the white set by considering the adjacent four pixels of the gray set.

$x_i =$

155	155	155	156	157	157	157	157
-----	-----	-----	-----	-----	-----	-----	-----

The above figure shows the sorted values of pixels  $x_i$  of the white set of the host image, next calculate the pixel difference  $d_i$  by using the formula mentioned in the above steps shown below

$d_i =$

155	0	0	1	1	0	0	0
-----	---	---	---	---	---	---	---

From the pixel difference table the peak value of the pixel is given by  $P=0$  and let us assume the

158	156	158	158
159	157	159	158
156	156	157	156
153	155	154	155

message bits to be embedded as 01101. The next

step is to calculate the watermarked value of pixel  $i$  that is  $y_i$  as shown below where in the message is been embedded.

$y_i =$

158	156	158	158
159	157	159	158
156	156	157	156
153	155	154	155

**Fig.3 An example of the reversible data hiding scheme for white set**

Thus the output of the embedding scheme for white set is the unchanged pixels from the gray set and the watermarked pixels from the white set. Similarly we can embed data in the gray set by considering the predicted values of white set.

Watermarked image

The white and gray embedding schemes are similar in nature. As a result the consecutive usage of the white embedding scheme and the

155	155	156	157	158	158	157	158
-----	-----	-----	-----	-----	-----	-----	-----

gray embedding scheme results in nearly double the embedding capacity.

The watermarked image thus obtained is as shown below this is the image after the message is been embedded.

Watermarked image

**A. Process of embedding the message in image:**

Let us assume that the bit stream to be embedded is 01101. We know that from the above example[2]

$X_i =$

155	155	155	156	157	157	157	157
-----	-----	-----	-----	-----	-----	-----	-----

Since  $|x_0 - x_1| = |155 - 155| = 0 = P$ , the first message bit 0 is embedded in  $x_1$  leaving the pixel value unmodified that is  $y_1 = x_1$ . The difference between  $|x_1 - x_2| = 0 = P$ , then the second message bit 1 is embedded in  $x_2$  and since the difference is equal to  $0 = P$  and the message bit 1 is encountered increase the pixel value by 1 that is  $y_2 = x_2 + 1 = 155 + 1 = 156$ . As  $|x_2 - x_3| = |155 - 156| = 1 > P$  the third message bit 1 is embedded in  $x_3$  and since  $x_3 > x_2$  so  $y_3 = x_3 + 1$  similarly  $|x_3 - x_4| = |156 - 157| = 1 > P$  and the fourth message bit 0 is embedded in  $x_4$  and since  $x_4 > x_3$ ,  $y_4 = x_4 + 1$ . Thus the embedding process continues until all of the message bits are embedded and then the resulting watermarked pixels are obtained and finally we construct the watermarked white set according to the sorted pixels  $\{y_0, y_1, y_3, \dots, y_i\}$ .

$Y_i =$

155	155	156	157	158	158	157	158
-----	-----	-----	-----	-----	-----	-----	-----

The above steps complete the data hiding process where only the white set is used to embed data. Note that large embedding capacities can be obtained by repeated data hiding process in white set and gray set.

**B. Process of extracting the hidden message and the original host image:**

At the receiving end, the recipient extracts message bits from the embedded image by scanning the image in the same order as during the embedding. The message bit 'b' can be extracted by using formula

$$0, \text{ if } |y_i - x_{i-1}| = P$$

$b =$

$$1, \text{ if } |y_i - x_{i-1}| = P + 1$$

Then the original pixel value of  $x_i$  can be restored by

$$y_i + 1, \text{ if } |y_i - x_{i-1}| > P \text{ and } y_i < x_{i-1}$$

$$x_i = y_i - 1, \text{ if } |y_i - x_{i-1}| > P \text{ and } y_i > x_{i-1}$$

$$y_i, \text{ otherwise}$$

Thus the exact copy of the original host image is obtained.

We can completely restore the image to its original state before the embedding occurred. The process of extracting the hidden message and thus the original host image is as follows. Whenever the pixel is P, message bit 0 is extracted and whenever the pixel is P+1 message bit 1 is extracted and the pixel value reduces to P. Since  $|y_1 - x_0| = |155 - 155| = 0 = P$ , a message bit 0 is extracted and  $x_1 = y_1 = 155$ . Since  $|y_2 - x_1| = |156 - 155| = 1 = P + 1$ , a message bit 1 is extracted and  $x_2$  is restored by setting  $x_2 = y_2 - 1 = 156 - 1 = 155$ . Since  $|y_3 - x_2| = |157 - 155| = 2 > P$  and  $y_3 > x_2$  so  $x_3 = y_3 - 1 = 157 - 1 = 156$ . Since  $|y_4 - x_3| = |158 - 156| = 2 > P$  and  $y_4 > x_3$ ,  $x_4 = y_4 - 1$  that is  $158 - 1 = 157$ . Since  $|y_5 - x_4| = |158 - 157| = 1 = P + 1$ , a message bit 1 is extracted and  $x_5$  is restored by setting  $x_5 = y_5 - 1 = 158 - 1 = 157$ . Since  $|y_6 - x_5| = |157 - 157| = 0 = P$ , a message bit 0 is extracted and  $x_6 = y_6 = 157$ . Since  $|y_7 - x_6| = |158 - 157| = 1 = P + 1$ , a message bit 1 is extracted and the original pixel is restored by setting  $x_7 = y_7 - 1 = 158 - 1 = 157$ .

l=157. The extracting process continues until all of the message bits are extracted. Thus the watermarked image is reverted to the exact copy of the original host image as shown below. The extracted pixels by the above method are given by as shown below.

$x_i =$

0    1    2    3    4    5    6    7

155	155	155	156	157	157	157	157
-----	-----	-----	-----	-----	-----	-----	-----

And the host image after extracting the message is given as shown below which is exactly same as the original host image before embedding occurred

Host Image

157	156	157	158
159	157	159	157
155	156	156	156
153	155	154	155

**V.RESU  
LT**

HOST IMAGE



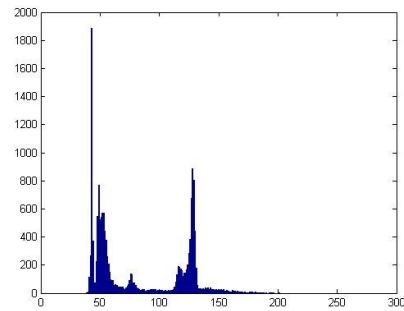
**Fig.4 Host Image**

PATIENT'S INFORMATION

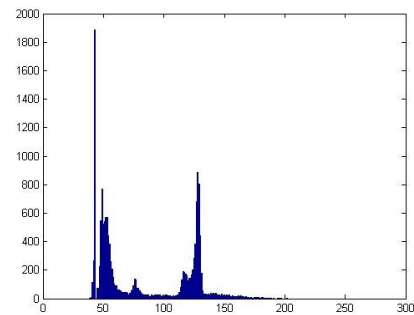
**Patient Name : xyz**

**Age : 40**

**Heart Rate : 98**  
**Blood Pressure : 170**  
**Suger : 160**



**Fig.5 Histogram of host image**



**Fig.6 Shifted Histogram Of Host Image**

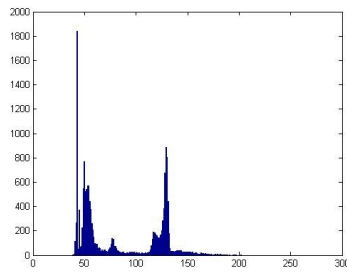
Invisible Watermarking done Image



**Fig.7 Embedded Image**



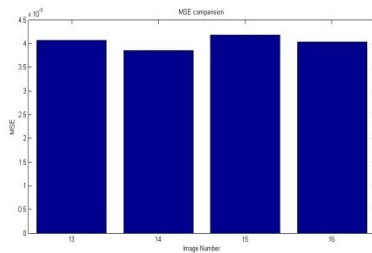
**Fig.8 Extracted Image**



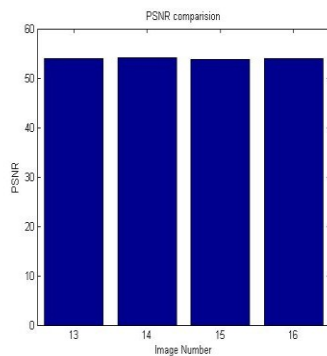
**Fig.9 Histogram Of Extracted Image**

**Extracted Patient Information**

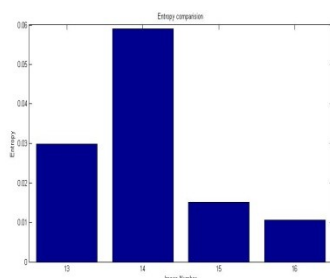
**Patient Name : xyz**  
**Age : 40**  
**Heart Rate : 98**  
**Blood Pressure : 170**  
**Suger : 160**



**Fig.10 Mean square error comparison**



**Fig.11 Peak signal to noise ratio**



**Fig.12 Entropy difference**

The above three bar charts shows the plot of MSE, PSNR and Entropy difference after comparing the host image with the extracted image for four different host images that is lung13.jpg, lung14.jpg, lung15.jpg and lung16.jpg.

**VI. Conclusion**

From the result analysis of the proposed project work we can conclude that the data hiding is lossless because after comparing the host image with the extracted image the values of MSE and Entropy difference are negligible which indicates that there is no error between the host image and the image after extracting the message. Also the values of PSNR obtained is high that is above 50 dB which indicates that the signal is high and the noise is low. The values of PSNR, MSE and Entropy difference are tabulated for seventeen different lung images. Since this method uses Rhombus prediction and sorting data can be embedded in either the white set or gray set of the image. As a result the consecutive usage of the white embedding scheme and the gray embedding scheme results in nearly double the embedding capacity. Large embedding capacities can be obtained by repeated data hiding process in white set and gray set.

**ACKNOWLEDGEMENT**

This research paper is made possible through the help and support from everyone including parents, teachers, family and friends. First and foremost I would like to thank Prof.S.S.Guravfor his support and encouragement. He kindly read my paper and offered invaluable advice on the theme of the paper.

I would also like to thank Prof. Kakadeto read my thesis and to provide valuable advice.

Finally I sincerely thank to my parents, family and friends who provide the advice and financial support.

## 8. REFERENCES

- [1] **Dr. EktaWalia a, PayalJainNavdeep***This paper presents analysis of Least Significant Bit (LSB) basedSteganography and Discrete Cosine Transform (DCT) based Steganography.*
- [2] **Ya-Fen Chang and Wei-Liang Tai.** *Histogram based Reversible Data Hiding Based on Pixel differences with prediction and sorting Vol 6 No 12, Dec. 2012.*
- [3]**Puneet Kr Sharma1 and Rajni2***This paper presents the general overview of image watermarking and different security issues*
- [4]**S. Yousefi1, H. R. Rabiee2, E. Yousefi3, M. Ghanbari4***presented a paper on a lossless data hiding method using integer wavelet transform.*
- [5]**D.MangaRatnam, L.Padmalatha***In this paper three different Reversible Data hiding techniques based on histogram was implemented*
- [6] **A Reversible Data Hiding Scheme Based on Side Match Vector Quantization.**
- [7] **S-F Chioua, Y-C Lub, I-E Liaoa and M-S Hwang.***In this paper an efficient reversible image data hiding scheme based on side match vector quantisation*
- [8] **Wei Huang, Yao Zhao, and Rong-RongNi***Recently, an edge adaptive image stegano- graphic method based on least significant bit (LSB) matching revisited (EA-LSBMR) has been proposed*
- [9] **Hedieh SAJEDI, Mansour JAMZAD***In this paper, a new adaptive steganography method based on contourlettransform*