Survey on Various LSB (Least Significant Bit) Methods

Mayuri Bomewar
Student, Information Technology
Maharashtra Institute of Technology
Pune, India
bomewar.mayuri@gmail.com

Trupti Baraskar
Assistant Professor, Information Technology
Maharashtra Institute of Technology
Pune, India
trupi.baraskar@mitpune.edu.in

Abstract –X-ray, Magnetic Imaging Resonance (MRI), Ultrasound, Computed Tomography (CT) these are digital medical images which are used for diagnosis. These medical images are transferred through internet connection and stored in Picture Archiving and Communication System (PACS) for various purposes. Compression technique is applied on medical images as these medical images are large in size and it requires more bandwidth. For telediagnosis purpose and insurance claim purpose we need to provide security and integrity so no try to make malicious attempts on image. Here we defined some compression and security techniques which are based upon Least Significant Bit (LSB) method they are LSB Modification, MNEB (Maximum Number of Embedded Bits), ISB (Intermediate significant bits) and n-LSB Planes. PSNR, MSE, NCC values are used to compare these methods.

Keywords: *Embedding, ISB (Intermediate Significant Bit), LSB (Least Significant Bit), DICOM, Watermarking*

*****

I. INTRODUCTION

The multimedia data such as images, digital images and medical images, audio and video becomes widespread on the internet. These multimedia data are exchanged over the insecure open networks. Here, we are concentrating on medical images such as DICOM images which are sends from client to server for diagnosis purpose. Medical images are produced from radiological modalities such as MRI, CT etc [7]. So while transferring these images any third person can access these medical images and can make modification to images, hence there is need to provide security to the images. These images should be protecting from any malicious attempts and threats, so there should not be any loss of data and modification of an image.

These DICOM images are stored for different purpose such as diagnosis, research and study purpose for medical students. These medical images will be in large size and it is stored in Picture Archiving and Communication System (PACS)[14]. As these image are in large size so it occupies more space in database and it requires more bandwidth over the internet. Because of these problems, compression of medical image is required.

Digital Watermarking technique is used for the security purpose of medical image. Digital watermarking is a technique for inserting information (the watermark) into an image, which can be later extracted or detected for variety of purposes including identification and authentication purposes [1]. A watermark can be a logo, a picture, identity number or signature. There are two different types of watermarking such as spatial domain and frequency domain. In spatial domain the watermark is embedded by directly modifying the pixel values and in frequency domain watermark embedded in transform space by modifying coefficients.

Mainly perceptibility provides the digital image watermarking. If the watermarked image is degraded or distracted easily then performing watermark technique on image is useless. The two essential requirements of ideal watermarking technique is Integrity and Security. Digital image Watermarking is one of the prominent method which defines the difference between the copyright issues and digital distribution of data and it is very good medium for copyright issues. This technique is very useful in the copyright protection, copy control, content authentication , finger printing, metadata binding and covert communication[9].

LSB (Least Significant Bit) method comes under spatial domain watermarking. LSB Modification, MNEB (Maximum Number of Embedded Bits), ISB (Intermediate significant bits), n-LSB Planes and PVD (Pixel Value Differencing) this are the method which are the extension of simple LSB method. PSNR (Peak Signal to noise Ratio), MSE (Mean Square Error) and NCC (Normalized Cross Co-relation) are the parameters which are used to measure image quality. Above mention methods are get compare by using these parameters.

In section 2, there is description of DICOM format image. Section 3, literature survey for various LSB methods we define various parameters which are used for compare the LSB methods. Section 4 we define various parameters which are used for compare the LSB methods. and Section 5 concludes the discussion.

II. DICOM

As we here we are describing about medical images, the images which are in DICOM format. DICOM is abbreviated as Digital Imaging and Communication in Medicine. This standard is developed by ACR (American College of Radiology) and NEMA (National Electrical Manufacturer Association). For the communication purpose it defines the ISO reference model of network and it incorporates the object oriented design concept. DICOM standard defines the some set of protocols for communication over a network. This standard has their own s yntax and commands and by using these protocols the information can be exchanged. Media storage services, file format and the way of accessing medical image and some related information are stored on media through which information can be shared. So in health care this type of connectivity must be present for cost effectiveness.

The main purpose of this is to have communication between medical imaging devices. The DICOM file contains both alphanumeric operation such as name of the patient, date of birth, age, diagnosis and the multiple images. A DICOM file has the following structure:

- A preamble of 128 bytes
- Prefix (4 bytes) where are stored the letters ‘D’, ‘I’, ‘C’, ‘M’ which represent the signature of the DICOM file
- Data Set, which stores a set of information such as: patient name, type of image, size of the image, etc.
- Pixels that compose the image (s) included into the DICOM file.

Data Set is composed of a number of Data Elements. The Data Set represents a single SOP Instance related to a single SOP Class (and corresponding IOD).An IOD (Information Object Definition) is a model of abstract and object-oriented data, which allow specifying information about objects from the real world. This DICOM format is useful as particular patient image and patient data is together in particular file. The size of images becomes large because its header for that we need to compress image.

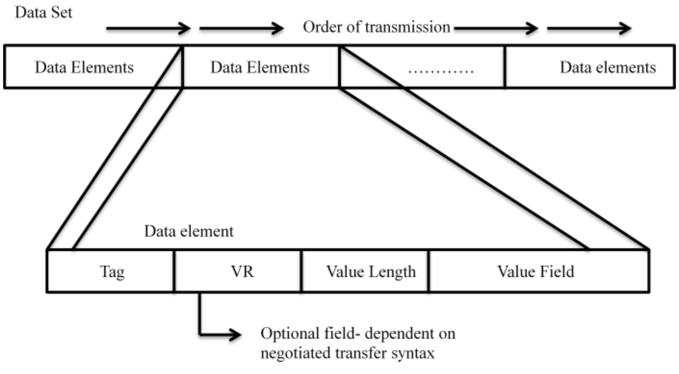

Fig 1. Data Element of DICOM structure.

DICOM Standard number has form of "PS 3.X- YYYY". Here, X is a part number and YYYY is publication year. For example, DICOM Part 2 is "Conformance" and document number "PS 3.2 - 2003".[7]The above diagram is the Data element of DICOM file structure. One attribute represents one data element and several data element represents whole IOD instance. In Data element first field Tag contains two integers and it specifies patients ID. VR means Value Representation describes characteristics information. In the value length consist of length of the data. Value field actually it represents the data and in if value field contains name(data) , so it is represented as PN(DA) where PN means Patient Name and DA means Date. From the above description of DICOM it is understood that DICOM image file format contains important information which should not be modified by anyone. So DICOM image should be secured..

III. RELATED WORK

Least Significant Bit is one of the earliest techniques and it is best known Spatial Domain Watermarking technique. In this embedding of watermark is done by choosing a subset of image pixels and substituting the LSB of each of the chosen pixel with watermark bits. The advantage of this algorithm are embeds more information and it is less computational algorithm. The various techniques are defined below:

A. LSB Modification

Least Significant Bit algorithm is strong and less perceptible. Watermark is embedded into an image by replacing least significant bit to hide the information [8]. Though it simple methods it suffers from many drawbacks such as highly sensitive to noise and easily destroyed.

LSB methods generate pseudo random number which determines pixels of the embedded watermark based on given secret key presented in paper by Puneet Sharma and Rajni [3]. In this method, large watermark is embedded into original image means it uses some logo as watermark and spreads it out full image size.

Consider the binary value of an image pixel:

00100111 11101001 11001000 00100111
11001000 11101001 11001000 00100111

Now, 10100100 this binary value will get hide into an above image pixel by changing only the least significant bit. The result will be following:

00100111 11101000 11001001 00100110
11001000 11101001 11001000 00100110

So in this way by changing only LSB of the data embedding of the watermark has been done. It is simple and basic way of Least Significant Bit method.

B. MNEB (Maximum Number Embedded Bits)

Xuanwen and Qiang proposed lossless compression method; it has relative large data embedding capacity [12]. This method can increase embedding capacity by compressing each bit plane of the image The main motto of this method to compress image and to insert the data in saved space.LSB bit planes which are formed by least significant bit of an image are compressed losslessly and later data is embed into saved space. Each bit plane of an image is compressed to increase the capacity of embedding data. In reverse direction, embedded data is extracted and compressed image is decompressed. When the second least significant bit which is denoted as LSB1 is used to embed data then Maximum Number of embedded Bits (MNEB) increases. As least significant bit plane get increases then MNEB also increases. But for some image the value of MNEB for higher bit plane is less as compare to lower bit plane. Finally it is trend to increase the bit plane level as MNEB increased.

1)Embedding Method: Patient data is embedded in the particular patients image in this way:

- The size of typical JPEG image is 256 X 256 pixels. Consider an image of size p x q, where p denotes rows and q denotes column, first losslessly compress bit plane r (r=1,2…8) for image.
- The compressed bit-plane stream is placed in the up portion of an image. The stream begins at image

coordinate (1, 1) and ends at (Pp, Qp) with row major.

The saved space begins from (Ps, Qs) to (p, q) in the bit-plane.

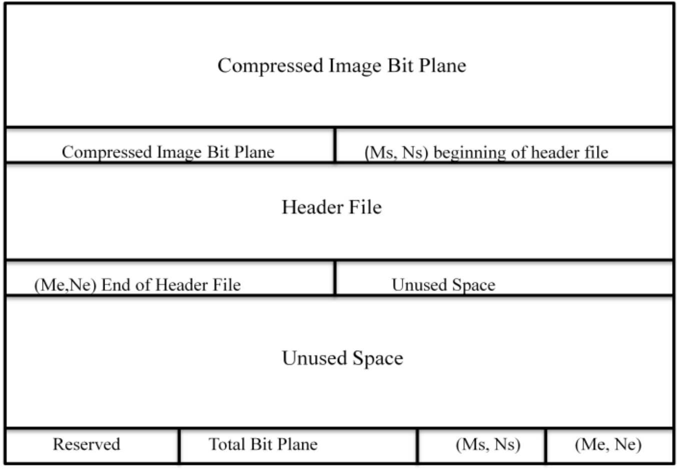
Compressed Image Bit Plane
Compressed Image Bit Plane
(Ms, Ns) beginning of header file
Header File
(Me,Ne) End of Header File
Unused Space
Unused Space
Reserved
Total Bit Plane
(Ms, Ns)
(Me, Ne)

Fig. 2 Structure of watermarked image

- Qp<q, then Ps=Pp and Qs=Qp +1;
  Qp=q, then Ps=Pp + 1 and Qs = 1.
- The header file is placed in the saved space from (Ps, Qs) to (Pe, Qe) but Pe< p. The (Ps, Qs) and (Pe, Qe) are stored in row p to indicate the header file location..

After compressing and embedding the data into image, the image is stored in the way which is given in the above figure. (Ps, Qs) and (Pe, Qe) are the beginning and ending of the header file respectively. Header file is embedded data and unused space is the space which is remains after embedding data. This method provides compression but does not provide much security as it does not provide more robustness. So this method is not that much useful.

C. *ISB (Intermediate Significant Bits)*

To increase the robustness of the watermarked image Shabir Parah and G.M.Bhatt developed Intermediate Significant Bit algorithm [11]. In Intermediate Significant Bit the data is embedded in middle range bit planes, so the image will be more secured from any attacks. This method also belongs to spatial domain watermarking[2]For embedding data into an image, first data is divided into number of blocks equal to number of bit planes such as L1, L2, L3 and L4 if four bit planes are there. Then L1 data is embedded into first bit plane, L2 in second bit plane and so on. The figure 4 represents watermarking procedure in the ISB method. In this method, first cleared all the location of an original image where data need to be embedded. Secret image is used for communicating with receiver which is in the form logo or text and it is convert into binary vector. Binary vector is divided in parts which are equal to bit plane. Later secret key function generated a pseudo random vector which is capable of addressing all bit locations and the in selected bit planes data embedded to get stego image. At the receiver side data extracted from the stego image. For the extraction same key is used which was used at the transmitter side. After the extraction output will be the secret image.

In this method, first cleared all the location of an original image where data need to be embedded. Secret image is used for communicating with receiver which is in the form logo or text and it is convert into binary vector. Binary vector is divided in parts which are equal to bit plane. Later secret key function generated a pseudo random vector which is capable of addressing all bit locations and the in selected bit planes data embedded to get stego image .At the receiver side data extracted from the stego image. For the extraction same key is used which was used at the transmitter side. After the extraction output will be the secret image. This technique has been implemented in MATLAB 7. But this technique it may not be useful sometime for medical image. As it destroys the information which are present in Intermediate significant bit

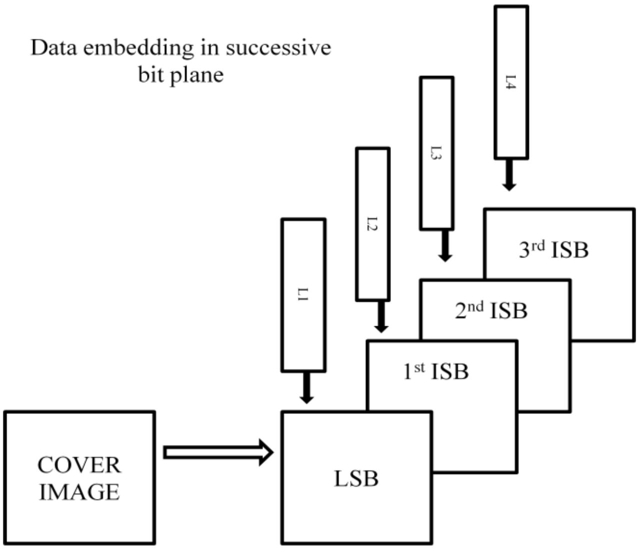

Fig.3 Data embedding Strategy

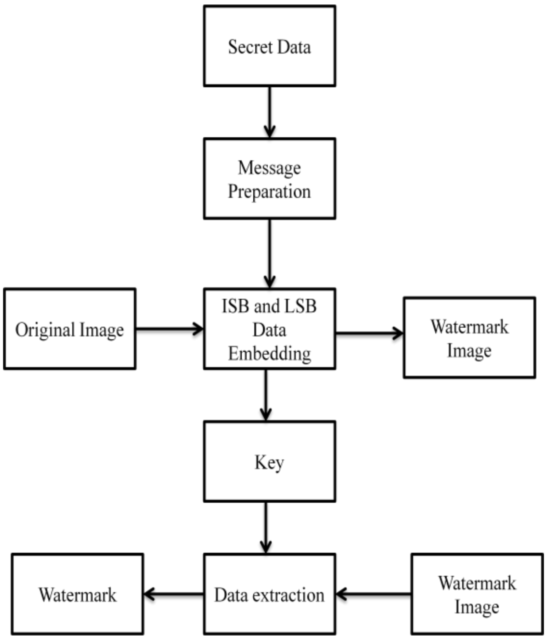

Fig. 4 High Capacity Data Embedding and Extracting Method Using ISB

D. n-LSB Planes

R.Velumani and V.Seenivasagam proposed the algorithm in which the patient's facial image is embedded into medical image in an invisible manner [9]. This algorithm also focuses on characteristics of reversibility and blind extraction. The embedding and extraction of the algorithm based on triangular number generator which is generated by encoding a pair of integers (a, b) into triangular number.

To create watermark image n number of LSB planes of medical image are combined with same number same number of MSB plane of facial image by applying triangular number generator functions. The visible degradation of watermarked image depends upon the higher value of n. The Triangular Number function is applied on is applied on the LSB plane of the medical image and MSB plane of the facial image is given in following way:

$$T_{ij} = f\left(C_{ij},F_{ij}\right) = \left[\left(C_{ij} + F_{ij}\right)^2 + 3C_{ij} + F_{ij}\right]/2$$

1) Embedding Method: Here, 4 MSBs and 4 LSBs are extracted from the medical image to form matrices MSB_M and LSB_M . Patient image is 4 MSBs extracted to form matrix MSB_P and shifted it right 4 times. To form matrix T LSB_M and shifted MSB_P are combined by using triangular number generator function. To generate remainder and quotient matrices Rem_T and Quo_T respectively modulo16 operation is performed on T. MSB_M and Rem_T are joined to form watermarked image WMI, Quo_T is preserved.

2) Extraction Method: From the watermarked image, 4 MSBs and 4 LSBs were extracted to form matrices MSB_{WMI} and LSB_{WMI} respectively, LSB_{WMI} is Rem_T. Quo_T key/quotient matrix is multiplied by 16, and it is added to resultant matrix with Rem_T to recover T. From T, LSB_M and shifted MSB_P are extracted then MSB_P 4 times shifted to left to extract the watermark. LSB_M and LSB_{WMI} are combined to recover the cover image. In this way, facial image is secured to particular patient image.

By this method cover image is recovered completely without any distortion. When the noise is injected into an image intensity of pixels gets altered. This method is novel as it is inserting an facial image into medical image but it is also increasing the size of an image

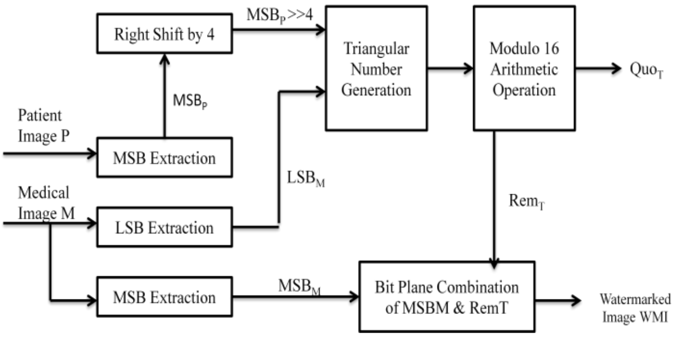

Fig. 5 Patient Facial Embedding Method

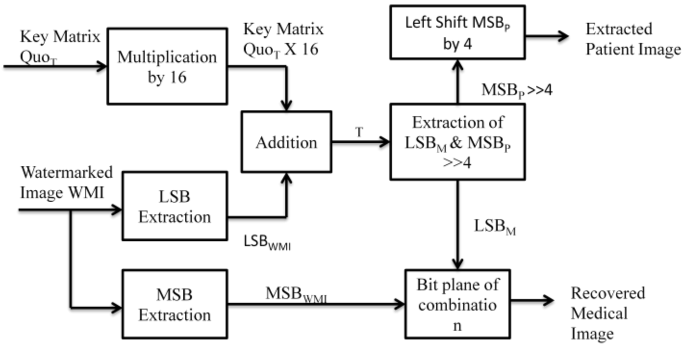

Fig. 6 Patient facial extraction method

E. PVD (Pixel Value Differencing):

Ki-Jong Kim, Ki-Hyun Jung proposed method for embedding the patient data in smooth area by using LSB substitution method and in edge area by using PVD (Pixel Value differencing).[4] This method provides higher capacity for embedding data. The embedding and extraction of algorithm is given:

Consider the two pixels which hides the 6 bit secret data

Step1:Say p_i and p_{i+1} are two pixels and difference d_i is computed as $d_i = |g_{i+1} - g_i|$ where g_i is pixel value of p_i

Step 2: Calculate value of R_i of the $d_{i,}$ $R_i = \min(u_{i,} k)$, where $u_i \geq k$, $k = d_i$ and R_i Є [$l_{i,}$ u_i]

Step 3: Rem_i , Rem_{i+1} and T_i calculate all this values for g_i and g_{i+1} by:

$Rem_i = g_i \bmod b$

$Rem_{i+1} = g_{i+1} \bmod b$

$T_i = (g_{i+1} + g_i) \bmod b$

Step 4: Now into g_{i+1} and g_i , embed the n bit secret data in two cases

Case i: R_i belongs to edge area

Case ii: R_i belongs to smooth area

Step 5: Compute g'_{i+1} and g'_i value which is out of boundary.

Extraction Scheme:

Step1: According the two consecutive pixel divide watermark image into two parts

Step 2: Calculate the value of d"i for two consecutive pixel g'_{i+1} and g'_i , $d''_i = g'_{i+1} - g'_i$

Step 3: Compute value R_i of d''_i according to range table

Step 4: By using LSB substitution extract secret data

This is the procedure for embedding and extracting data for Pixel Value Differencing Method. This method describes that the more data can be embedded in the pixels which belongs to edge area than the pixels belongs to smooth area. The hiding capacity of this method is more as compare to simple LSB and even hiding capacity of this method can be increased without distorting the human visual system.

IV. COMPARATIVE RESULTS

We studied all this algorithms and find out disadvantage and advantage of all this methods. In this paper we compare all this methods by using various parameters such as PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and NCC (Normalized Cross Correlation). MSE and PSNR are the two parameters which are used to measure image quality. PSNR is the ratio between the original image and watermarked image where as MSE calculates the distortion of an image.

Consider f(x, y) and f'(x, y) are the functions for original image and watermark image. M, N is the size of an image. Then MSE are calculated in the following way [10]:

$$MSE = \frac{1}{M\,N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(f(x,y) - f(x,y))^2$$

PSNR is calculated by using value of MSE and it should be 30db. It is represented by:

$$PSNR = 10\log_{10}\frac{255^2}{mse}db$$

To verify the robustness of an image NCC parameter is used[2].NCC is important performance parameter while extraction of a watermark logo and it is calculated in given way:

$$NCC = \frac{\sum_x\sum_y f(x,y)f^{'}(x,y)}{\sum_x\sum_y[f(x,y)]^2}$$

Table 1. Experimental Result of All Parameters

	PSNR	MSE	NCC
LSB Modification	50.4310	0.6811	0.6258
MNEB	43.2594	3.0701	0.8547
ISB	35.7783	10.6593	0.7528
n-LSB Planes	34.8987	21.0479	0.9893
PVD	36.2040	4.5029	0.9910

From above table we figured out that n-LSB Planes method is best watermarking algorithm from all above algorithms and provides better image quality and more distortion tolerance because the value of MSE is high and PSNR value is nearby standard value.NCC value of n-LSB Plane is high so this method are secured from geometric attacks LSB Modification watermarking algorithm has low NCC and MSE value and it basic LSB method so it is not that much secured algorithm. The methods LSB modification, ISB, n-LSB planes provides more security but does not compression whereas MNEB method compresses the image but does not give more security. The experimental results make us easy to do comparative study for all this algorithms.

V CONCLUSION

The outcome obtained from by applying various watermarking algorithm is that they give different results when applied on different medical image. Our aim is to develop the technique which provides not only security but also compression for medical image and particular patient data. These techniques provide more security to algorithms but there are some drawbacks like except MNEB method other algorithm does not compress image, low distortion tolerance and less robustness. Hence research is going on to overcome these drawbacks and also to enhance security parameters with high compression rate for medical data.

REFERENCES

[1] Rafael C. Gonzalez and Richard E. Woods, "*Digital Image Processing*" Third Edition, Pearson.

[2] Akram M. Zeki, Azizah A. Manaf, 2009, "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit)", World Academy of Science, Engineering and Technology, 989-996.

[3] Deepshika Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, 2012, "LSB Based Digital Image Watermarking For Gray Scale Image" Vol.6, Issue-1, 36-41

[4] Ki-Jong Kim, Ki-Hyun Jung and Kee-Young Woo, 2008, "A High Capacity of Data Hiding Using PVD and LSB", International Conference on Computer Science and Software Engineering, 876-879.

[5] Koushik Paul, Gautam Ghosh and Mahua Bhattacharya, 2012, "Reversible Digital Image Watermarking Scheme Using Bit Replacement and Majority Algorithm Technique", Journal of Intelligent Learning System and Applications, 199-206.

[6] Luiz Octavio Massato Kobayashi, Seirgo Shiguemi Fururie and Paulo Seirgo Liccardi Messender Barreto, July 2009, "Providing Integrity and Authenticity in DICOM Images: A Novel Approach", IEEE Transaction on Information Technology in Biomedicine, Vol. 13, No. 4, 582-589.

[7] Piyamus Suapang, King Mongkuts, Kobchai Dejchan, Surapan Yimmun, Aug 2010, "A Web based DICOM format Image Archive, Medical Image Compression and DICOM Viewer system for Teleradiology Application", SICE Annual Conference. 3005-3011,

[8] Puneet Sharma and Rajni, July 2012, "Analysis of Image Watermarking Using Least Significant Bit Algorithm", International Journal of Information Sciences and Techniques, Vol.2, No.4, 95-101.

[9] R.Velumani and V. Seenivasagam, 2010, "A Reversible Blind Image Watermarking Scheme for Patient Identification, Improved Technologies and Tamper Detection with Facial Watermark Image", IEEE.

[10] [10] Rodriguez Colin Raul, Feregrino- Uribe Claudia, Trinidad- Blas Gershom de J, 2007, "Data Hiding Scheme for Medical Images", IEEE Trans, 17th International conference on Electronics, Communication and Computer

[11] Shabir A. Parah, Javaid A. Sheikh and G.M. Bhatt, 2012, " High Capacity Data Embedding Using Joint Intermediate Significant Bit (ISB) and Least Significant Bit (LSB) Technique", journal of information engineering and applications, Vol 2, No.11, 1-11.

[12] Xuanwen Luo and Qiang Cheng, 2004, "Health Information Integrating and Size Reducing", IEEE, 3014-3018