A Reversible Data Hiding Method with Contrast Enhancement for Medical Images by Preserving Authenticity

Riny Joy
PG Student
Department of Computer Science and Engineering
Federal Institute of Science and Technology

Jyothish K John
Assistant Professor
Department of Computer Science and Engineering
Federal Institute of Science and Technology

Abstract

This paper presents a reversible data hiding method with contrast enhancement for medical images by preserving authenticity. Here the objective of reversible data hiding is to embed some secret information such as diagnosis report, patient ID etc., into the medical image in an invisible manner. In addition with the embedding of information into the image the proposed method achieves contrast enhancement without any visual distortions as in the previous methods. In addition with the contrast enhancement, the proposed method also provide security by introducing a visually meaningful image encryption so that instead of producing a noise like or texture like encrypted image this method will produce a visually meaningful encrypted image. Thereby it reduces the chance of security attacks. Also the embedding of digital watermark with this encryption will helps to ensure the authenticity of the medical images.

Keywords- Authentication, Background Segmentation, Encryption, Region of Interest, Reversible Data Hiding

I. INTRODUCTION

The advances in information technology have drawn lots of attention especially in medical field. These advances in medical field help to provide fast exchange of information for telediagnosis, teleconsulting, telesurgery, cooperative working session etc. At the same time, ensuring the security of these exchanged medical information becomes a challenging concern.

In recent years, Reversible data hiding or reversible data embedding has been extensively studied to embed some secret information into a digital object in a reversible manner so that the original object can be exactly recovered. This method can be effectively employed in the medical field to hide information such as patient ID, diagnosis report etc., in the medical image.

Fig. 1 illustrates the process of reversible data hiding(RDH).I denotes the digital image for the secret transmission of the data and S denotes the secret information that is to be reversibly embedded. After accomplishing the reversible data hiding the image containing the secret information I ' and the additional information A should be transmitted to the decoder. And at the decoder side by using the received image I ' and additional information A the original image I and secret information S can be recovered accordingly.

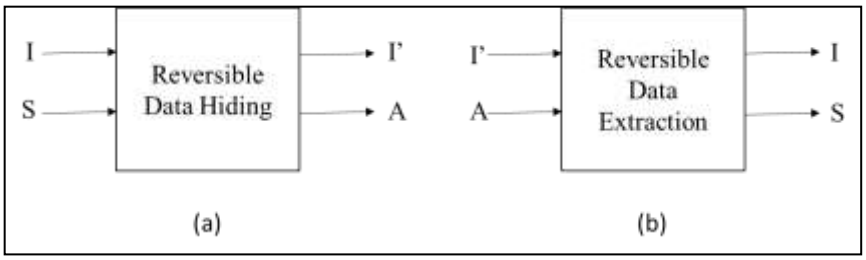

Fig. 1: (a) Block diagram for Reversible Data Hiding (b) Block diagram for Reversible Data Extraction

For evaluating the goodness of the algorithm parameters including reversibility, output image quality, capacity and overhead of the side information need to be considered. There are a lot of applications for reversible data hiding in medical field including telediagnosis, teleconsulting, cooperative- working session and telesurgery.

In addition with the reversible data hiding this work also adapt an encryption method to protect image content .Many of the encryption algorithms protect the image content by changing their pixel value thereby producing a texture like or noise like images. However in this case it is easy to distinguish between an original image and an encrypted one. As a results these encrypted images definitely brings the people attentions and thus leads to a large number of attacks and analysis. The attack may include cryptanalysis, illegal edition, modification or even deletion of image contents. In order to avoid this type of security attacks this work adopts an encryption system which will produce a visually meaningful encrypted image instead of a texture or

noise like one. Also this encryption system adopted a simple mechanism of digital watermark to detect the presence of tampering.

The rest of this paper is organized as follows. In section II, literature survey is briefly described. Section III describes the methodology. In section VI presents the experimental results and analysis and finally section V summarizes the system.

II. RELATED WORKS

In the literature, many RDH algorithms (e.g. [3]-[14]) have been proposed. Among them, most of them are for the digital images in the plain text domain (e.g. [3]-[6], [11]-[12]), and also in the encrypted domain (e.g. [7]-[8]). The basic requirement for RDH is the quality degradation on the image after RDH should be low and also the ability of reversibility, that is, one can extract the embedded data to restore the original digital image.

In [3] Jun Tian proposed Reversible Data Embedding Using a Difference Expansion. This work used a technique called difference expansion in which it discovers the extra space needed for the payload embedding by exploring the redundancy in the image content. However this work has the lack of a method which improves the perceptual quality of images.

In [4] Zhicheng Ni et al. proposed another Reversible Data Hiding technique which can embed a greater amount of data (580 kb for a 512*512*8 grayscale image) while keeping a very high visual quality for the output images. It utilizes the zero point and peak point of the histogram and slightly modifies the grayscale pixel values to reversibly embed the data thereby produces a histogram equalization effect. The method is quite simple and need only low computational cost since no transforms are needed. But it does not work in an image having an exactly horizontal histogram.

Hsiang-Cheh Huang et al. presents Authenticity Preservation with Histogram-Based Reversible Data Hiding and Quadtree Concepts in [5].The quadtree decomposition will decompose the original cover image into large and small blocks based on the smoothness of the region. After that a two round histogram based reversible data hiding method is performed to reversibly embed secret information and additional informations needed for decoding. With this method, the increase of the size of side information can be reduced, while keeping reversible data hiding possible. The need of high computational cost and time are the main drawbacks of this work.

In [6] Hao - tian et al. proposed a Reversible Image Watermarking on Prediction Errors by Efficient Histogram Modification. Multiple pairs of histogram bins are considered sequentially for embedding. Instead of selecting highest histogram bin pair for embedding this work adopted an efficiency criterion based histogram bin pair selection for embedding. This method provide higher embedding rate than the previous ones. The main advantage of this method is that the image content is better preserved, especially for high pay- load data hiding. However the more processing time and the size of each block is to be recorded for the decoding makes it difficult.

In [7] Hsiang et al. proposed Hierarchy-based reversible data hiding. The modification of difference values between pixels by using histogram based method with extensions to hierarchical structure by utilizing inherent characteristics of original images is utilized. Decrease in the embedding capacity with the increase of the layer number is one of the drawback of this system.

In [8] Bo Ou et al. proposed a Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding. In addition to the previous Prediction Error Expansion methods, the work utilizes every two adjacent prediction-errors as a unit to generate a sequence consisting of prediction-error pairs and a histogram based reversible data hiding is performed on the two-dimensional prediction-error histogram. The pairwise Prediction Error Expansion is only designed for simple cases that the modification to a pixel value is at most 2, so that the capacity and reduction of distortion is limited to a particular level.

In [9] Xinpeng Zhang proposed Separable Reversible Data Hiding in Encrypted Image. We have discussed so many works regarding the plain text domain. Now this work is actually based on the encrypted domain. Compared to plain text domain this method provide more security. However, to keep a low computation complexity, the algorithm need to control many parameters, therefore the performance of content recovery is limited.

In [10] Xiaotian Wu et al. proposed High-capacity Reversible Data Hiding in Encrypted Images by Prediction Error. Two methods for reversible data hiding in encrypted images, namely a joint method and a separable method, are used by adopting prediction error. High PSNR and number of incorrect extracted bits is significantly reduced in separable method improved reversibility and high PSNR in join method. But, Visual quality is not satisfactory in all cases.

In [11] a Reversible Data Hiding in Encrypted Images based on Absolute Mean Difference of Multiple Neighboring Pixels is proposed by Xin Liao et al.This work used a function that calculate the complexity of image blocks by employing two, three or four adjacent pixels according to coordinate of each pixel. Side match technique is also used to increase the correct rate. However, due to the small embedding ratio and incorrect extraction of bits we cannot consider it as an efficient method.

In [12] Hao-Tian et al. proposed a Reversible Image Data Hiding with Contrast Enhancement. This is the first algorithm that achieves contrast enhancement with reversible data hiding. Histogram based reversible data hiding by selecting highest histogram bins is used for payload embedding.Evenif it achieves a good visual quality for images through contrast enhancement , applying this method on medical images will not give a good result because it is not specifically designed for medical images. Also the preprocessing strategy adopted in this work to prevent the underflow and overflow of pixel values will create artificial distortions in the medical image.

In [13] Hao et al. proposed a reversible data hiding method with contrast enhancement for medical images. It uses a preprocessing strategy that is specially developed for medical images. Thus the visual distortions that appeared in [11] is completely eliminated in this work.

This paper is a combined version of two works to enhance the security using encryption techniques. The combined works are Reversible Data Hiding Method with Contrast enhancement for Medical Images proposed by Hao-Tian Wu, Jiwu Huang and Yun-Qing Shi and Generating visually meaningful encrypted images proposed by Long Bao and Yicong Zhou.

III. PROPOSED METHODOLOGY

The proposed reversible data hiding method with authenticity preservation consists of three processes:

- Data hiding process
- Meaningful Encryption and Watermark Embedding
- Extraction and Recovery process

The process of data hiding will produce a contrast enhanced medical image after embedding of the secret information. By the end of Meaningful encryption and watermarking process a visually meaningful encrypted image with embedded watermark is generated. In the third process, the contrast enhanced image is firstly recovered from the encrypted image containing watermark and after that the hidden data are extracted from the contrast enhanced image and the original image is recovered accordingly. In the following section, every step in the two processes will be introduced.

A. Data Hiding Process

As shown in Fig. 2, there are three major steps in the data hiding process, i.e., background segmentation, pre-processing, and data embedding.

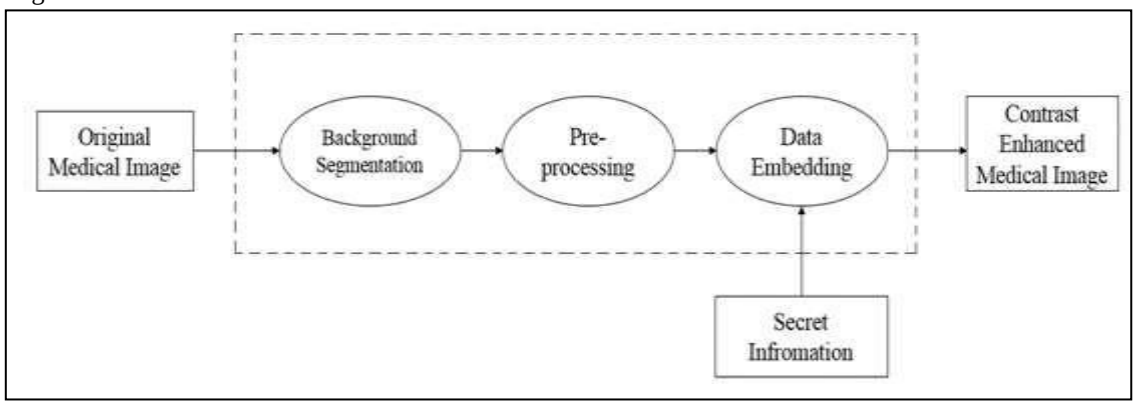

Fig. 2: Process of data hiding

1) Background Segmentation

A medical image contains region of interest (ROI) and non-region of interest (non-ROI) such as the 3 computed tomography images (CT) which consists of ROI and non-ROI shown in Fig 3. Since there is no need for enhancing the contrast of non-ROI the proposed method first performs background segmentation. For that Otsu's method [14] is adopted to automatically select the optimal threshold separating two classes of foreground and background pixels.

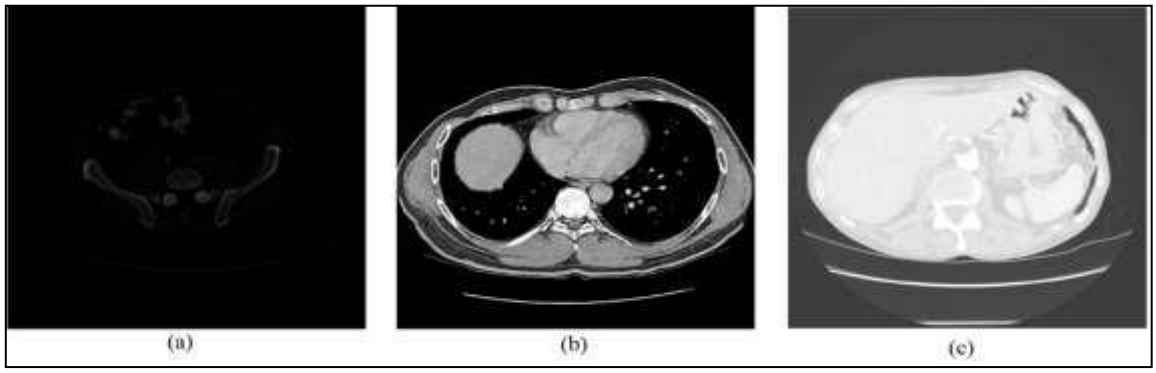

Fig. 3: Three Computed Tomography Images (size 512*512)

To exclude the background from contrast enhancement we need to identify the principle gray-scale values in the segmented background whose percentages above a pre-defined threshold (e.g. 2%) and exclude the corresponding histogram bins from being expanded.

2) Pre-Processing

In the case of reversible data hiding by histogram modification a pre-processing is to be performed on the bounding pixel values to prevent the underflow and overflow. Usually pre-processing is performed in the following way: Suppose S pairs of histogram bins are to be expanded in total, then the pixel values from 0 to S-1 are added by S, while the pixels from 256-S to 255 are subtracted by S.

Performing this type of normal pre-processing in natural images will not produce any problems. But if we perform it on medical images will produce visual distortions(Fig. 4) because a pixel with value S-1 will be brighter than a pixel with value S and a pixel with value 256-S will be darker than the pixel with value 255-S.This is called disordering of pixels. This is due to the fact that the number of bounding pixels (0 to S-1 and 256-S to 255) in natural images is relatively small so that few visual distortions are introduced while the pixels in medical images are often concentrative distributed.

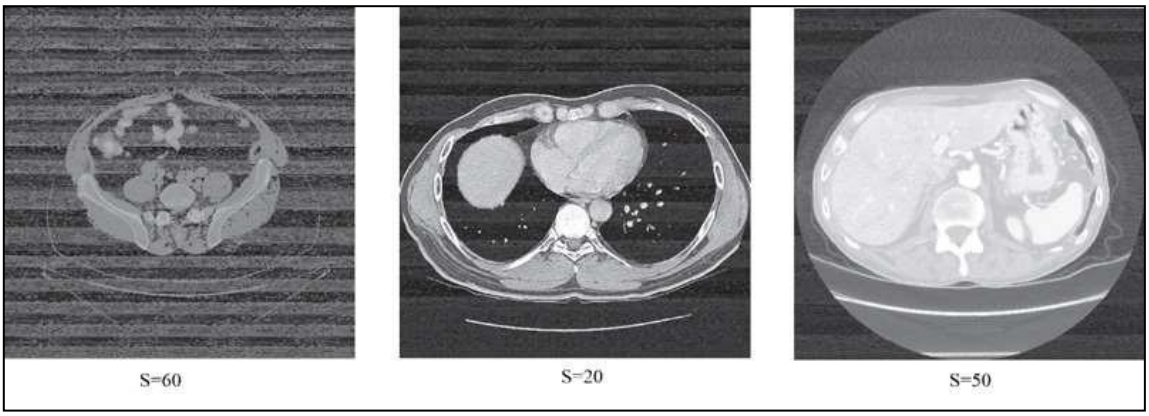

Fig. 4: Three medical images with data, generated by the method in [12]

There are quite a few empty bins in the histogram of medical images because the pixels in the medical images are often concentrative distributed as shown in Fig. 5.Fig 6 shows the histogram of natural images. It is clear that disordering of pixels in natural images will be negligible because the number of bounding pixels is very small.

In order to avoid this disordering due to the normal pre-processing in medical images this work adopted another pre-processing strategy suitable for medical images. Suppose we have to expand S number of histogram bin pairs where S [1, 64]. The pixels in the intervals of [a,a+S-1] and [a+s,a+2S-1] are counted with the integer a S [0 , 128 - 2S] while the pixels in the intervals of [256-b-S , 255-b] and [256-b-2S , 255-b-S] are checked with another integer b [0, 128 - 2S]. The two intervals containing the minimum pixels within [0,127] and [128,255] are illustrated in the Fig. 7.The interval [a, a+S-1] is checked for a [0, S-1] and [a+S, a+2S-1] is checked for a [0, 128-2S] to find out the interval with the minimum number of pixels in the interval [0,127].Similarly, the interval [256-b-S, 255-b] is checked for b [0, S-1] while [256-b-2S, 255-b-S] is checked for b [0, 128 - 2S] to find out the interval with the minimum number of pixels in [128,255].

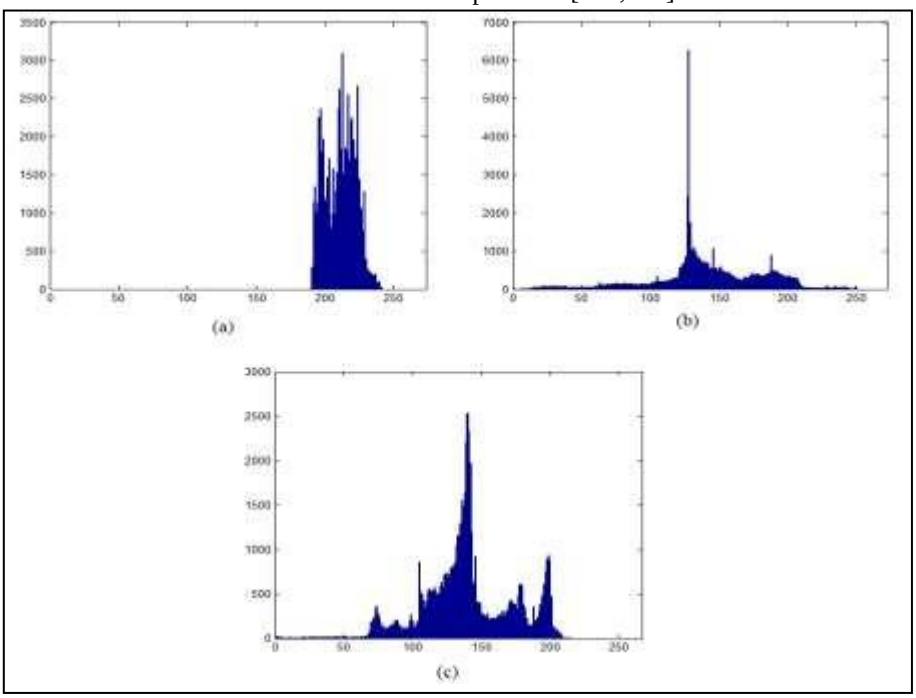

Fig. 5: Histogram of three Natural Images

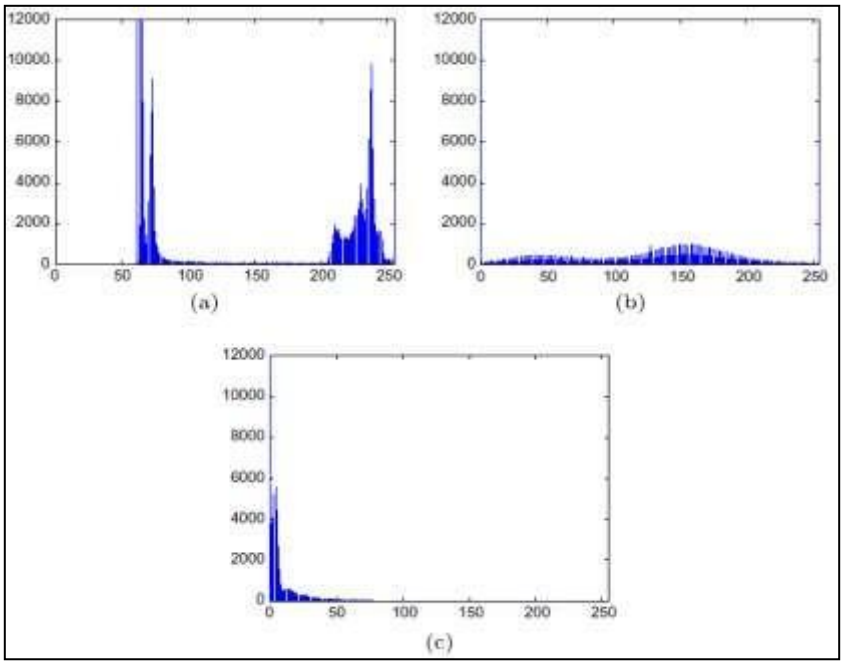

Fig. 6: Histograms of three medical images shown in Fig. 3

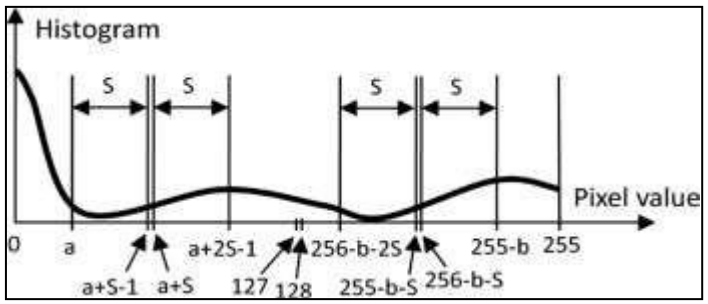

Fig. 7: Pre-processing strategy in [13].

If the interval [, +S-1] or [+S, +2S-1] contains the minimum pixels in [0,127], the pixel values in [0, +S-1] are added by S therefore [, +S-1] overlaps with [+S, +2S-1].Similarly, if [256- -S, 255-] or [256 2S, 255- -S] contains the minimum pixels in [128,255] the pixel values in [256 S, 255] are subtracted by S. In this way, the amount of disordered pixels is reduced because the number of pixels lies in one of the overlapped intervals is minimum. For the exact recovery of the original image these modifications is to be restored. Therefore to identify the modified pixels in the pre-processing a location map is generated with the same size of the original image and also the values of and need to be saved as well. In the location map assign 1's to the locations of those pixels contained in the two intervals containing the minimum pixels, and assign 0's to the other positions. In this way, the pixels contained in the overlapped intervals can be identified for the post-processing while the location map can be compressed to the minimum size.

3) Data Embedding

After performing the pre-processing the obtained histogram is used in this stage. The bins excluding the labelled ones in the background segmentation are used for data embedding. From the unlabeled histogram bins the highest two bins are taken and expanded using the (1) .The highest two bins can be further chosen for expansion thereby achieving the contrast of ROI while the contrast of background is maintained.

$$p' = \begin{cases} p-1 & \text{if} \quad \mathrm{p} < p_{\mathrm{L}} \\ p-b & \text{if} \quad \mathrm{p} = p_L \\ p & \text{if} \quad \mathrm{p}_{\mathrm{L}} < p < p_R \\ p+b & \text{if} \quad \mathrm{p} = \mathrm{p}_{\mathrm{R}} \\ p+1 & \text{if} \quad \mathrm{p} > \mathrm{p}_{\mathrm{R}} \end{cases} \qquad (1)$$

Where p' is the modified pixel value of p, b is a binary value (0 or 1) to be embedded. The peak two bins in the new histogram can further be chosen to be expanded, and so on until satisfactory contrast enhancement effect is achieved. In this way,

the contrast of ROI can be enhanced by expanding the chosen unlabeled histogram bins while the contrast of background is unchanged.

By taking the medical image Fig.3 (a) as the test image, the experimental results of the proposed method in different stages is shown in the Fig. 11. Firstly, at the sender side, the background segmentation of the input image is performed. For that Otsu's method is adopted to automatically select the optimal threshold separating two classes of foreground pixels and background pixels and by setting R=5% the principle values in the segmented background are identified. The result of background segmentation on the image Fig.8 (a) is shown in Fig.8 (b).In the second step, to prevent the underflow and overflow a special preprocessing with minimum disordering of pixels for medical images is adopted. The result of preprocessing is shown in the Fig.8(c).After that, the reversible data embedding is performed thereby achieving contrast enhancement.

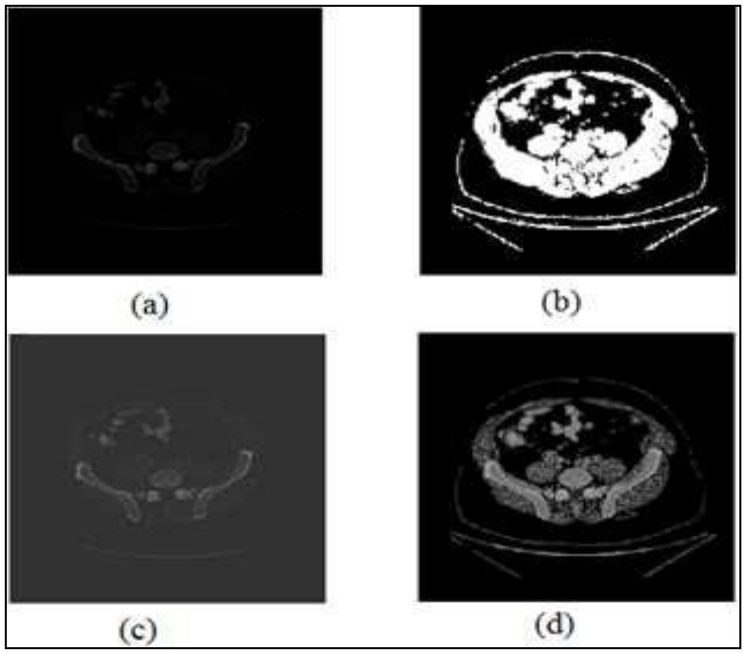

Fig. 8: Results of reversible data hiding with contrast enhancement with R=5% and S=50
(a)Input Image (b) after background Segmentation (c) After pre-processing (d) after data embedding

B. Meaningful Encryption and Watermark Embedding

The phase of the meaningful encryption process is shown in Fig.9. The idea of this encryption is that it uses a normal image as the reference image and gives a visually meaningful encrypted image that has an appearance similar to the reference image.

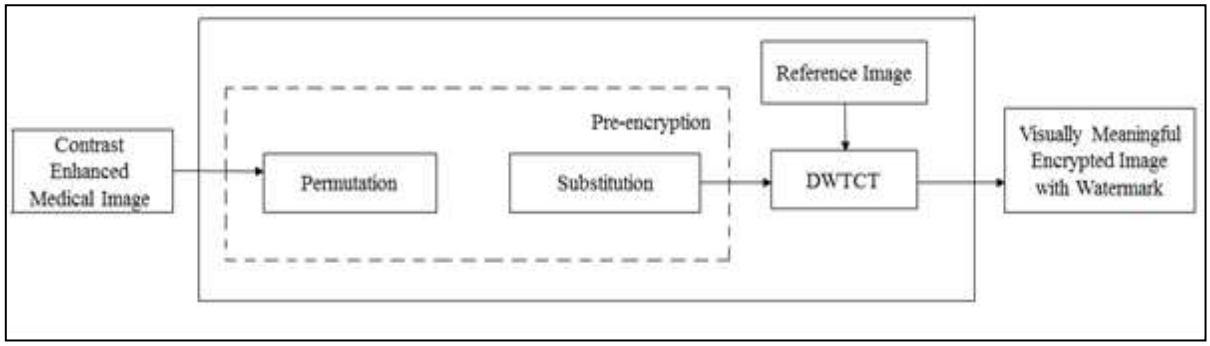

Fig. 9: The block diagram of the image encryption system

The process of encryption consists of two parts. The pre-encryption process uses permutation and substitution to change image pixel locations and values. The output of this phase is a noise-like image. In the second phase this noise-like image is transformed by DWTCT and produces a visually meaningful encrypted image that has an appearance similar to the reference image. The goal of DWTCT is to divide each pixel value of the pre-encrypted image into two portions and put them into CV and CD (where CA, CH, CV and CD denote the LL, HL, LH, and HH sub-bands (L = Low-frequency, H = High-frequency). Also in the meaningful encryption of the contrast enhanced image the proposed method stores a digital watermark into the CH, where CH is the HL sub-band of the DWTCT of the pre-encrypted image. This watermark is then extracted at the receiver side and compared with the original watermark to detect the presence of tampering. The results of meaningful encryption and embedding of digital watermarking is shown in the Fig.10.

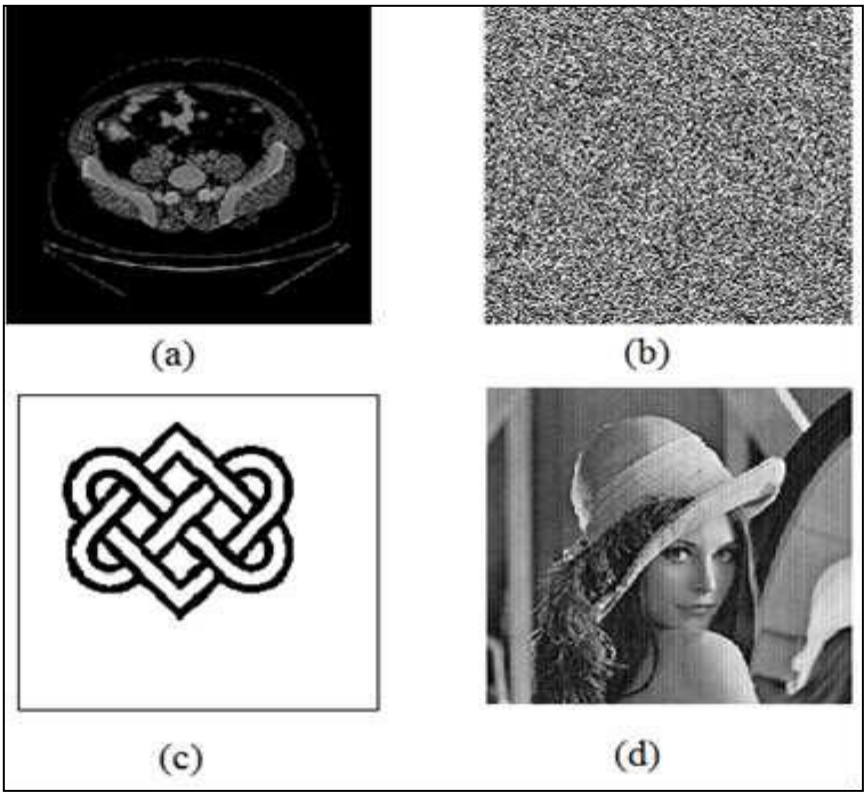

Fig. 10: Results of encryption of image and embedding of watermark (a) Contrast enhanced Image
(b) Pre-encrypted Image (c) Watermark to be embedded (d) After meaningful encryption and embedding of the watermark

C. Extraction and Recovery process

There are three steps to recover the original medical image,

- Decryption of Image and Extraction of Watermark
- Data Extraction
- Post-processing

1) Decryption of Image and Extraction of Watermark

The process of decryption of image and extraction of watermark is shown below in the Fig. 11.

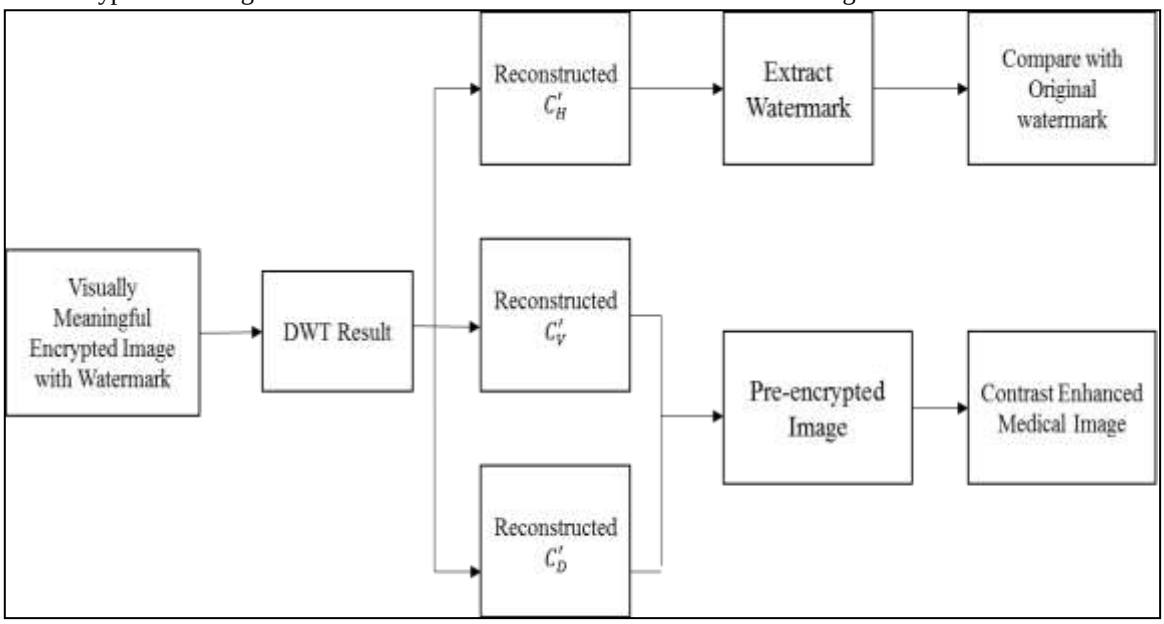

Fig. 11: The block diagram of the Decryption of Image and Extraction of Watermark

The results of decryption of image and extraction of watermark are shown in the Fig.12.

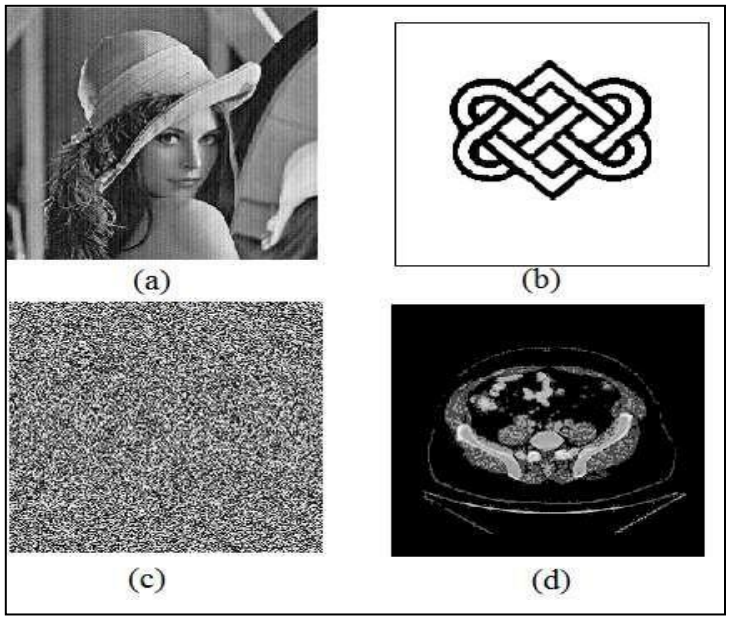

Fig. 12: Results of decryption of image and extraction of watermark (a) Retrieved image (b) Extracted Watermark (c) Retrieved pre-encrypted Image (d) Retrieved Contrast enhanced Image

2) Data Extraction

The different phases of data extraction process is shown in the Fig. 13.It consists of data extraction to extract the embedded data and post-processing to restore the pixel values in post-processing.

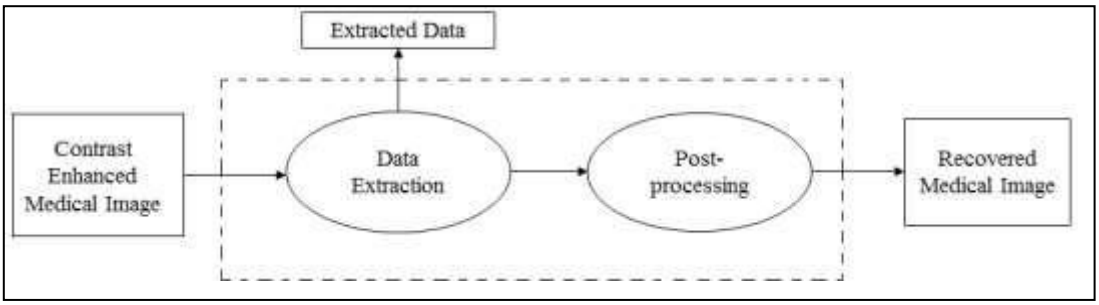

Fig. 13: Flowchart of the extraction and recovery process

Given the values of expanded bins and we can extract the embedded data from each pixel p' as follows:

$$b' = \begin{cases} 1, & \text{if } p' = p_L - 1 \text{ or } p' = p_R + 1 \\ 0, & \text{if } p' = p_L \text{ or } p' = p_R \\ null, & \text{otherwise} \end{cases} \quad (2)$$

Where is the extracted value. The following operation is performed to restore the histogram:

$$p = \begin{cases} p'+1 & \text{if } p' < p_L \\ p' & \text{if } p_L - 1 < p' < p_R + 1 \\ p'-1 & \text{if } p' > p_R \end{cases} \quad (3)$$

If all the expanded bin values are known (2) and (3) can be repeatedly used until all bins are expanded and the data are extracted.

3) Post-Processing

To recover the original medical image all the pixels which are modified in the pre-processing should be restored. For that we have to use the values, S and the compressed location map. The pixel values that are added by S should be subtracted by S in post-processing. Similarly the pixel values that are subtracted by S should be added by S to recover the original medical image.

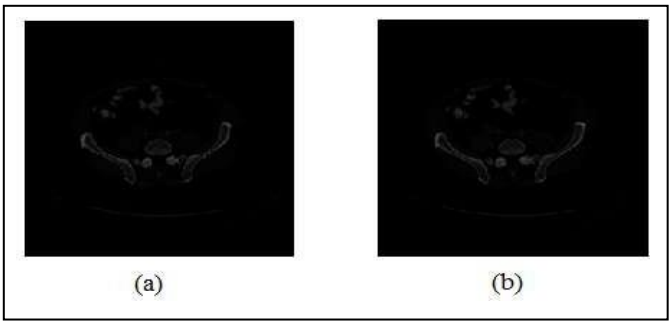

Fig. 14: (a) Retrieved Contrast enhanced image (b) Retrieved Original Image

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The method was implemented in a MATLAB 2014 prototype. In the experiments, 3 Computed Tomography (CT) medical images downloaded from [16] were used as test images. Since we use Otsu's method for background segmentation no parameters are need to be specified in that step. To find out the principal gray scale values in the segmented background the percentage of threshold needs to be specified, which denoted by R. Also the number of histogram pairs to be expanded, denoted by S is also needs to be specified.

The proposed method is performed on the medical images on a desktop PC with the following characteristics: Intel Core i5 CPU, 2.5 GHz, 6 GB RAM.

For analyzing the performance of the proposed method the values of Relative Contrast Error, Structural Similarity, Peak Signal to Noise Ratio and data embedding rate (defined in [17]) are calculated between the original image and the contrast enhanced image for the test images in the Fig. 3.

The numerical results obtained from 3 CT images as shown in Fig. 3 for the proposed method,[12] and [13] are shown in Table 1, where the proposed method is set with R =2.

Table 1: Evaluation results of the proposed and previous methods ([12], [13]) obtained from 3 CT images as shown in Fig. 3.

Test image	*Algorithm*	*S*	*RCE*	*SSIM*	*PSNR(dB)*	*Rate(bpp)*
	PropR2	*30*	*0.5000*	*0.8955*	*25.1302*	*8.7921*
Image(a)	*[13]*	*30*	*0.5064*	*0.7975*	*17.98*	*0.629*
	[12]	*30*	*0.5155*	*0.7193*	*24.16*	*1.936*
	PropR5	*20*	*0.5000*	*0.9550*	*27.3064*	*0.1689*
Image(b)	*[13]*	*20*	*0.5064*	*0.9788*	*27.3064*	*0.1689*
	[12]	*20*	*0.4956*	*0.3954*	*20.84*	*3.439*
	PropR2	*60*	*0.5005*	*0.6358*	*13.6840*	*3.3494*
Image(c)	*[13]*	*60*	*0.5922*	*0.8382*	*20.18*	*0.305*
	[12]	*60*	*0.6376*	*0.0140*	*10.56*	*5.997*

From the results in Table 1, it can be seen that compared to [12] more contrast enhancement effects were achieved with PropR2 for test image (c) when S=30; while comparable contrast enhancement results are achieved by the PropR2 when compared to [13].Although much higher hiding rates were accomplished with [12], it could not achieve contrast enhancement effect for test image (b).The proposed method achieves low SSIM value compared to methods in [12] and [13] for test image(a) indicating that the image content is not greatly changed. PSNR results are also comparable with the method in [13].The proposed method gives good data hiding rates compared with other methods.

The structural similarity measure between the original image and retrieved original image shows that the original image can be exactly recovered from the retrieved encrypted image without any loss of information. The original medical image (a) and the retrieved original image is shown in the Fig.15.

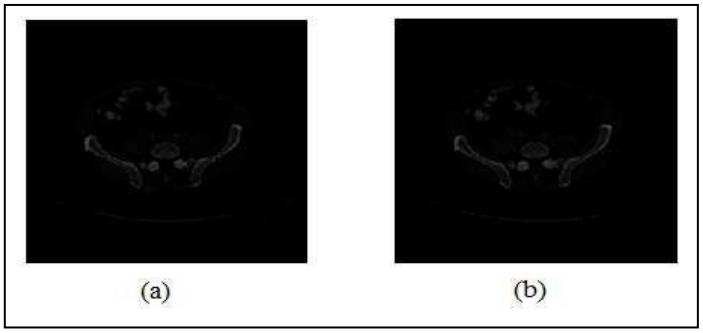

Fig. 15: (a) Original image (b) Retrieved Original Image with Structural SIMilarity =1

V. CONCLUSION

This work presented a reversible data hiding method with contrast enhancement for medical images by authenticity preservation. It adopted an improved preprocessing strategy used in [13].This work presents a method to hide useful information in medical images in a reversible manner so that the blind recovery of the original image is possible. In addition with the reversible data hiding it also achieves contrast enhancement of the medical image thereby improving visual quality. Therefore, it is very efficient in the applications where contrast enhancement of medical images and reversible data hiding are both needed. It also ensures the security and authenticity preservation using a meaningful encryption and a digital watermark schemes respectively. After reversible data hiding with enhancement and encryption of the original medical image it can be exactly recovered without any distortions.

REFERENCES

[1] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, “Relevance of watermarking in medical images ", in: IEEE EMBS Int. Conf. Information Technology Applications in Biomedicine, 2000, pp. 250255.
[2] W. Pan, G. Coatrieux, J. Montagner, N. Cuppens, F. Cuppens, C. Roux, “Comparison of some reversible watermarking methods in application to medical images", in: 31st Annual Int. IEEE Conf. Engineering in Medicine and Biology Society, 2009, pp. 21722175.
[3] J. Tian, “Reversible data embedding using a difference expansion", IEEE Trans. Circ.Syst. Video Technol. 13 (8) (2003) 890896.
[4] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, “Reversible data hiding", IEEE Trans. Circ. Syst.Video Technol. 16 (3) (2006) 354362.
[5] H.C. Huang, W.C. Fang, “Authenticity preservation with histogram-based reversible data hiding and quadtree concepts”, Sensors 11 (10) (2011) 97179731.
[6] H.T. Wu, J. Huang, “Reversible image watermarking on prediction error by efficient histogram modification", Signal Process. 92 (12) (2012) 30003009.
[7] H.C. Huang, F.C. Chang, “Hierarchy-based reversible data hiding", Expert Syst.Appl. 40 (1) (2013) 3443.
[8] B. Ou, X. Li, Y. Zhao, R. Ni, Y.-Q. Shi, “Pairwise prediction-error expansion for efficient reversible data hiding", IEEE Trans. Image Process. 22 (12) (2013) 50105021.
[9] X. Zhang, “Separable reversible data hiding in encrypted image", IEEE Trans. Inform. Forensics Secur. 7 (2) (2012) 826832.
[10] X. Wu, W. Sun, “High-capacity reversible data hiding in encrypted images by prediction error”, Signal Process. 104 (2014) 387400.35
[11] X. Liao, C. Shu, “Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels of multiple neighboring pixels", J. Vis. Commun. Image Represent. 28 (4) (2015) 2127.
[12] H.T. Wu, J.L. Dugelay, Y.Q. Shi, “Reversible image data hiding with contrast enhancement", IEEE Signal Process. Lett. 22 (1) (2015) 8185.
[13] Hao-Tian Wua, Jiwu Huang, Yun-Qing Shi, “A reversible data hiding method with contrast enhancement for medical images", J. Vis. Commun. Image R. 31 (2015) 146153
[14] Otsu’s Method. <http://en.wikipedia.org/wiki/Otsu’s method>
[15] Long Bao, Yicong Zhou “Image encryption: Generating visually meaningful encrypted images", Information Sciences(2015)
[16] National Biomedical Imaging Archive. <http://imaging.nci.nih.gov>
[17] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, “Image quality assessment: from error measurement to structural similarity”, IEEE Trans. Image Process. 13 (1) (2004) 600–612.