Adaptive Medical Image Watermarking Technique based on Wavelet Transform

Mohammed Abduljaleel
Baghdad College of Economic Sciences University

الملخص:

في هذا البحث، تم اقتراح تقنية تكيفية لإضافة العلامة المائية للصور الطبية استناداً على التحويل المويجي و خصائص نظام الرؤيا البشري لغرض المحافظة على وثوقية الصور الطبية. عملية تضمين العلامة المائية نفذت من خلال تحويل الصور الطبية الى المجال المويجي ومن ثم احتساب قيمة العتبة التكيفية من اجل اختيار مواقع الإخفاء في معاملات الصورة. بيانات العلامة المائية تم تضمينها في المعاملات التي هي اقل إدراكا من قبل نظام الرؤيا البشري لغرض المحافظة على دقة الصور الطبية. النتائج العملية وضحت ان مقدار التشوه الناتج عن طريق تضمين العلامة المائية هو صغير جدا ولا يمكن إدراكه بالاضافه الى ذلك فان التقنية المقترحة تحافظ على دقة الصور الطبية ثم تقيم مستوى الدقة للتقنية المقترحة تم تقيمه باستخدام ثلاثة من مقاييس جودة الصور. نتائج التقييم بينت نتائج جيدة جدا بما يتعلق بدقة الصور الطبية.

Abstract

in this paper, we propose adaptive medical image watermarking technique based on wavelet transform and properties of human visual system in order to maintain the authentication of medical images. Watermark embedding process is carried out by transforming the medical image into wavelet domain and then adaptive thresholding is computed to determine the suitable locations to hide the watermark in the image coefficients. The watermark data is embedded in the coefficients that are less sensitive to the human visual system in order to achieve the fidelity of medical image. Experimental results show that the degradation by embedding the watermark is too small to be visualized. Also, the proposed adaptive watermarking technique can preserve the fidelity of medical image. The fidelity performance of the proposed technique was evaluated by three image quality metrics which are PSNR, UQI and SSIM. The evaluation results exhibit a very good results of the proposed technique with respect to fidelity of medical image.

Keywords: Digital watermarking; wavelet transformation; Medical Image.

1. Introduction

Rapid growth in the use of Internet in every field leads to availability of digital data to the public. Internet has been spread in many applications like telemedicine, online-banking, teleshopping etc. One of this application telemedicine is crucial one, where Internet is used to transfer or receive medical data by healthcare professional. Due to advancement in information and communication technologies, a new context of easier access, manipulation, and distribution of this digital data have been established [1].

Medical image sharing through internet becomes very popular nowadays to make telediagnosis, telesurgeries and teleconsultation [2]. Most hospitals and health care systems involve a large amount of data storage and transmission, such as medical images, patient information, and administrative documents. Among these data, the patient information and medical images need to be protected against any malicious attempts. To prevent patient's information from any attack, three things are required present the intrgrity, Privacy and Authenticity of medical images [3].

To maintain the privacy, patient data can be embedded into the medical images. After data embedding, the output image should be as similar as its original image so that doctors can perform proper treatment by using the images with hidden data when necessary. The integrity of the medical image is another important issue. This is necessary to ensure that the data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion or replay). Also, the authentication of medical image is required to ensure that the communicating entity is the one that it claims to be. A proof that the information belongs indeed to the correct patient [4].

Recently, medical image applications play an important role in our lives [4]. In practical applications, lot of people could now easily make unauthorized modifications and manipulation on medical images in such a way that may lead to big financial or human lives losses. A possible false diagnosis can jeopardize the patient life, if the stored image underwent malevolent manipulations, storage errors or compression, such that the resulted distortions cannot be detected by the doctor. This is an example where modifications are not tolerated [5].

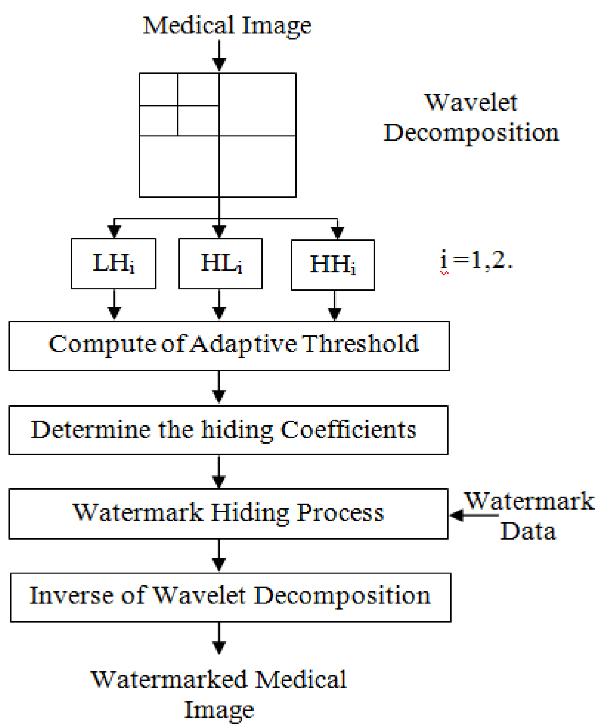
In addition to the mentioned above, in number of medical applications, special safety and confidentiality is required for medical images, because critical judgment is done on medical images, which leads to the proper treatment. Therefore, it must not be changed in an illegitimate way; otherwise, an undesirable outcome may results due to loss of decisive information. Therefore, there is a need to provide a strict protection in medical images to ensure only occurrence of legitimate changes. Now-a-days exchange of medical images between hospitals located in different geographical location is very common. Moreover, as this exchange of "medical reference data" done via unsecured open networks leads to the condition of changes to occur in medical images and creates a threat which results in undesirable outcome. Considering this fact, demand of privacy is getting higher due to easy reproduction of digitally created medical images [6].

So there is a need to embed watermark in the medical images. To fulfill the need of privacy, integrity and authenticity we can use the digital watermarking scheme for receiving correct information and providing proper treatment to the patients [4]. In previous literature there are many watermark techniques designed for medical images. *El-Sheimy N. et al.* [7], presented a new method for protecting the patient information in which the information is embedded as a watermark in the discrete wavelet packet transform (DWPT) of the medical image. *Mohamed A. et al.* in [8], introduced a new approach for watermarking of medical image that they are trying to adapt to telemedicine. This approach is intended to insert a set of data in a medical image. These data should be imperceptible and robust to various attacks. In [9] *Rupinder K.*, proposed semi-fragile watermarking technique to embedded binary watermark into medical image based on the Discrete Cosine Transform (DCT) domain. The binary watermark is achieve low degradation level of the host image and thus gives high quality level.

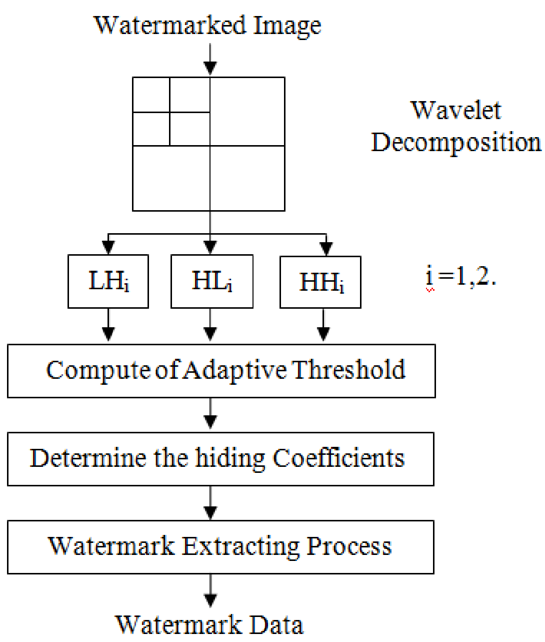
In this paper, we propose a new adaptive watermarking technique based on wavelet transform for medical image. The adaptive thresholding approach is employed to determine appropriate coefficients to hiding watermark. This paper is organized in the following manner. The proposed watermark inserting and extracting method is presented in Section 2. Experimental results are shown in Section 3. Section 4 present the conclusions of this paper.

2. Proposed Watermarking Technique

In this section, new image watermarking technique is proposed based on DWT to embed the watermark into the medical image in such a way that it is imperceptible by the HVS. The adaptive thresholding method is employed to determine appropriate coefficients to hiding watermark by decomposing the medical image into different regions and select the regions which are less sensitive to the HVS. The HVS is sensitive to changes in the lower frequencies as they are associated to the more significant characteristics of the image. The higher frequencies give the details of the image and changes in the higher frequencies are not easy notes by HVS. In this technique, we exclude low frequencies when inserting watermark data to medical image in order to preserve the fidelity of medical image. The block diagram of the proposed watermarking method is shown in Fig.1.



(a)



(b)

Fig.1: Block diagram of the adaptive watermarking technique based on DWT : a) Hiding Function; b) Extracting Function.

2.1 Hiding Function

The aim of this function is to insert the watermark data into medical image. This function consists of five steps. The first step involves applying two level discrete wavelet decomposition to the medical image. In second step, the adaptive threshold is computed for each level. The third step determines hiding coefficients which are store the watermark bits. In fourth step, we inserts the watermark in the selected coefficients. At the last step, we performs the inverse wavelet transform to construct the watermarked medical image.

A. Wavelet Decomposition

The medical image watermarking technique achieves the watermark hiding based on the DWT domain. The first level of wavelet decomposition produces four sub-bands, termed LL, LH, HL and HH. The LL is a low resolution version of the medical image and LH, HL and HH are the detailed sub-images in horizontal, vertical and diagonal directions respectively. The LL band is iteratively decomposed to obtain second level wavelet transform as shown in Fig.2.

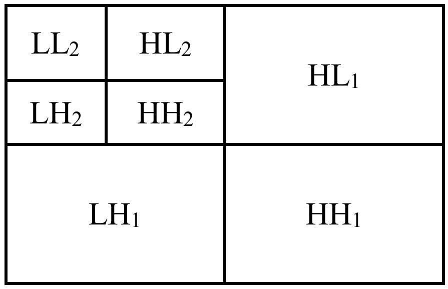


Fig.2: DWT Decomposition with Two Levels.

As clear in Figure (3.3) the seven sub-bands are obtained. In this step, the Haar wavelet basis is chosen due to its simplicity.

B. Compute of Adaptive Threshold

After transforming medical image into wavelet domain through two-level DWT, then the adaptive thresholds are computed for each level. Here, we describes the method for computing threshold value (*T*), which is adaptive to different level characteristics.

The threshold value is calculated according to the decomposition level. In the 2-level decomposition, the largest coefficients C_1 for 1- level subbands (LH1, HL1, HH1) is selected and the threshold T_1 is calculated by equation (1), T_2 for the subsequent level is calculated by using the same equation.

$$T_I = 2^{(\log_2 \max(C_I))-I} \qquad \dots (1)$$

where C_i represents the largest coefficient in i-level. The watermark is embedded only to the selected coefficients. Since, we performs two level of wavelet decomposition the adaptive threshold computed for first and second levels. The (LL_2) band can further be decomposed to obtain another level of decomposition. The Fig.3 represents the adaptive threshold.

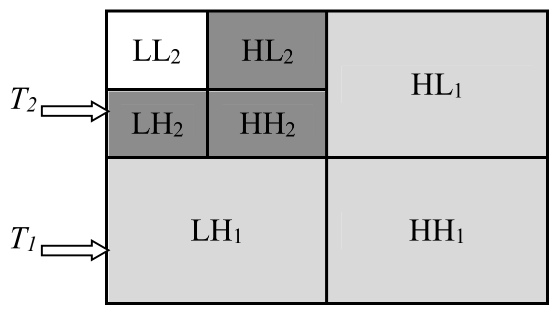


Fig.3: Adaptive Threshold.

The algorithm which computes threshold values in wavelet domain it very simple to implement and computationally is more efficient. It has the following steps:

Thresholding Algorithm

Begin

Step1: Load the resulted image of L-levels decomposition wavelet transform.

Step2: For i= 1To number of levels (L)

Begin

- Find the large coefficient in i-level (LHi, HLi, and HHi).
- Compute the threshold value (T_i) using equation (3.1).

End.

Step3: Save the threshold values results.

End.

C. Determine the hiding Coefficients

After computing the adaptive threshold for each level, then we need to decide what the sub-bands are to use for hiding the watermark. Inserting watermark data in the middle and high resolution levels (LH, HL and HH) gives a higher fidelity for medical image but lowers the robustness to common image processing operations. On the contrary, embedding in the low resolution level (LL) will improve the watermark robustness while it is highly perceptible by human eye. Therefore, we exclude LL_2 sub-band to preserve the ROI and used the remaining sub-bands to embed the watermark in medical image. In this case, two of coefficients types are used to store watermark. First, coefficients in high level (HH_1 and HH_2) Second, coefficients in middle levels (HL_2, LH_2, HL_2 and LH_2).

D. Watermark Hiding Process

The goal of this work is to embed a watermark data into the DWT coefficients of medical image. Before the hiding process, we convert the watermark data to string of binary numbers (0 and 1). These bits are embedded into the selected DWT coefficients using adaptive threshold. To the selected coefficients, the watermark is inserted in an additive way using the following algorithm:

Hiding process algorithm
Input :watermark data
Output: watermarked medical image

Step 1: each level, all coefficients of the LH_i, HL_i and HH_i sub-bands are firstly concatenated into a single sequence *S*. Three coefficients with the same coordinate of the three subbands, which correspond to the same spatial location, are continuously adjacent in the new sequence. Let $f_{LHi}(n,m)$, $f_{HLi}(n, m)$ *and* $f_{HHi}(n, m)$ denote the coefficients of the different sub-bands, where *(n,m)* represents the position of the coefficient in the corresponding sub-band. The coefficients are rearranged in the following way:

$\{ f_{LHi}(0,0), f_{HLi}(0,0), f_{HHi}(0,0), f_{LHi}(0,1), f_{HLi}(0,1), f_{HHi}(0,1), \ldots\ldots, f_{LHi}(N-1,M-1), f_{HL2}(N-1,M-1), f_{HH2}(N-1,M-1)\}$.

where *N* and *M* are the horizontal and vertical size of the sub-band, respectively.

Step 2: Then, the binary watermark is inserted into the coefficients which are satisfying the condition as follows:

$$|\ Coefficient\ Magnitude\ | > Threshold\ of\ Level \qquad \ldots(2)$$

Step 3: Inserting the watermark in these selected coefficients is done by change the specific bit of the coefficients.

E. Inverse of Wavelet Decomposition

Finally, the watermarked medical image is obtained by performing the inverse wavelet transformation. The algorithm of this technique is as shown below:

Input: Medical Image, and Watermark Data.
Output: Watermarked Medical Image.

Begin
Step 1: Perform 2-level decomposition for the input image by using (DWT).
Step 2: For each level do the following:
- i. Extract coefficients of three sub-bands LH_i, HL_i, and HH_i.
- ii. Concatenate the coefficients of the LH_i, HL_i, and HH_i subbands into a single sequence *S*.
- iii. Determine hiding coefficients:
  1) Sorting the coefficients sub-bands LH_i, HL_i, and HH_i.
  2) For coefficients in middle and high levels (LH_i, HL_i, and HH_i), the hiding coefficients are determine by using adaptive thresholding.

Step 3: Convert the watermark data into the binary form.
Step 4: Insert the watermark bits into the selected coefficients which are satisfying the condition:
$$|\ Coefficient\ Magnitude\ | > Threshold\ of\ level.$$
Step 5: Reconstruct the watermarked medical image by using inverse the DWT
Step 6: Save and display the watermarked medical image.
End.

2.2 Extracting Function

The first step of the extraction function consists also of decomposition of the watermarked medical image with the same wavelet levels used in the hiding function. The watermark bits are extracted from DWT coefficients which are selected according to the same method with embedding watermark for LH_i, HL_i, and HH_i sub-bands.

For each level the adaptive thresholding is calculated to corresponding level. Another necessary procedure is to acquire watermark from extracted binary watermark.

The algorithm described below is used to extract watermark from the watermarked medical image which embedded based on DWT and adaptive thresholding.

Input: Medical Image.
Output: Watermark data, decision if the image authentic or unauthentic.

Begin
Step 1: Load the medical image.
Step 2: Perform 2-level decomposition for the input image by using (DWT).
Step3: For each level, compute the threshold (except LL_2).
Step4: Extract the watermark bits from the coefficient which is greater than threshold value (T_i).
Step5: If watermark bits are found in medical image then

- Collect the extracted bits and convert them to values.
- Display the extracted watermark data on screen; this means the loaded medical image is authentic.

Else

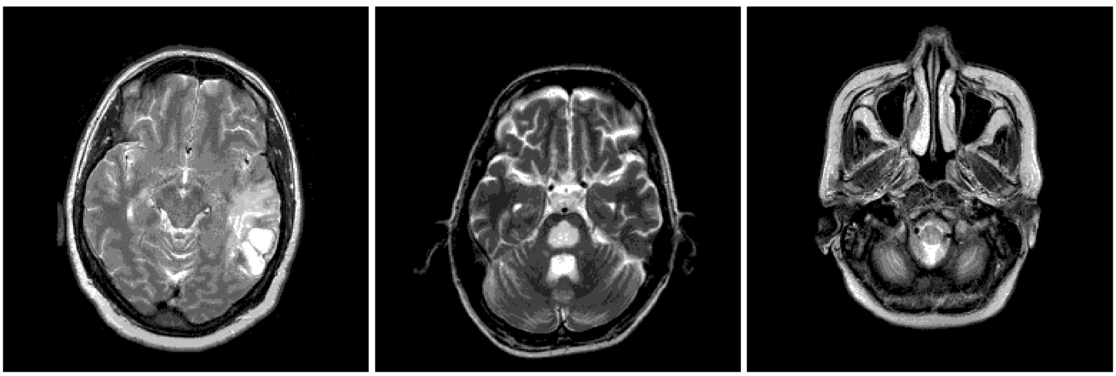
- Display message" the loaded medical image is unauthentic "; this means the medical image is either replaced or modified".

End.

---

3. Experimental Results

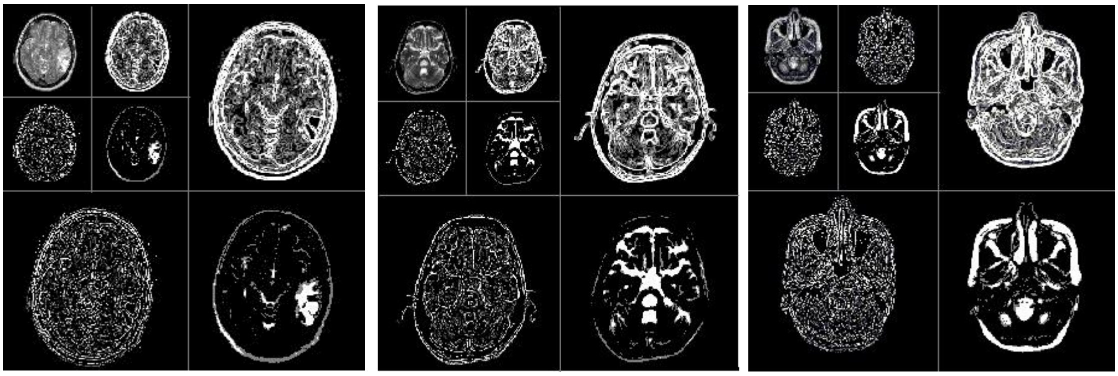
In order to evaluate the proposed medical image watermarking technique, several medical images from are used. This technique embeds the watermark data based on DWT. As shown previously, the watermark bits are embedded in the coefficients of the

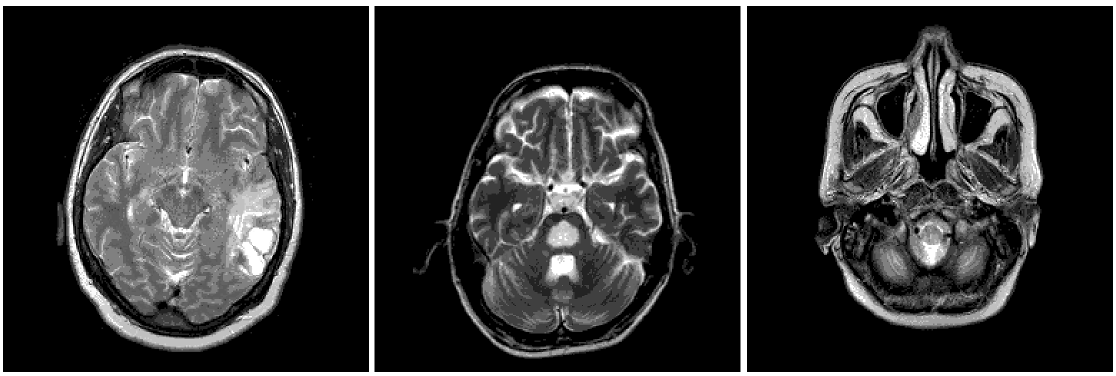


LH_i, HL_i and HH_i sub-bands depended on the adaptive thresholding. This experiment has been implemented using three medical images of size 512×512. Fig.4. shows the medical images with their corresponding two level

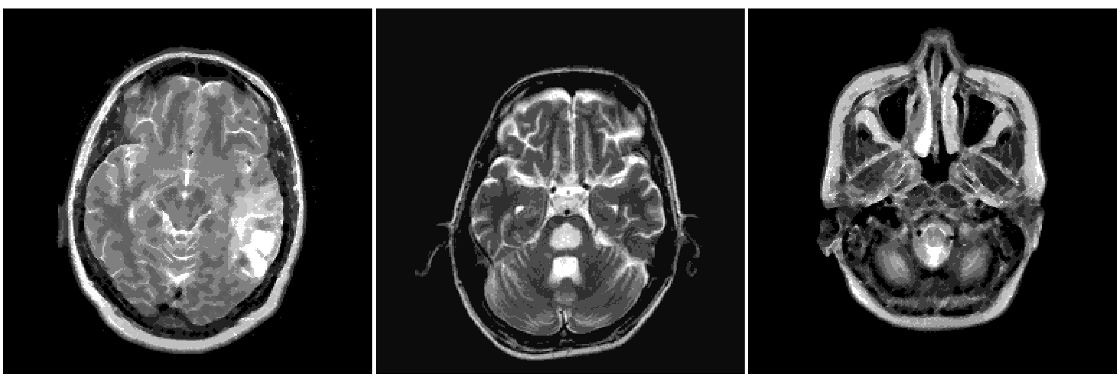
Fig.4: Medical images with their corresponding 2-level decompositions.

In order to testing the performance and effectiveness of the proposed technique we will embed a watermark data to medical images with various amounts of the capacity of the watermark. At start, we embed the watermark data with 400 bytes into medical images these watermark data distributed into six bands LH_i, HL_i, and HH_i. Also, we repeat this operation using 800 bytes. In this way, we can study the relationship between the capacity of the watermark and the amount of the resulting distortion due to embed a watermark into medical images. Fig.5 shows the original medical images and their watermarked versions with different capacity amounts of watermark data.

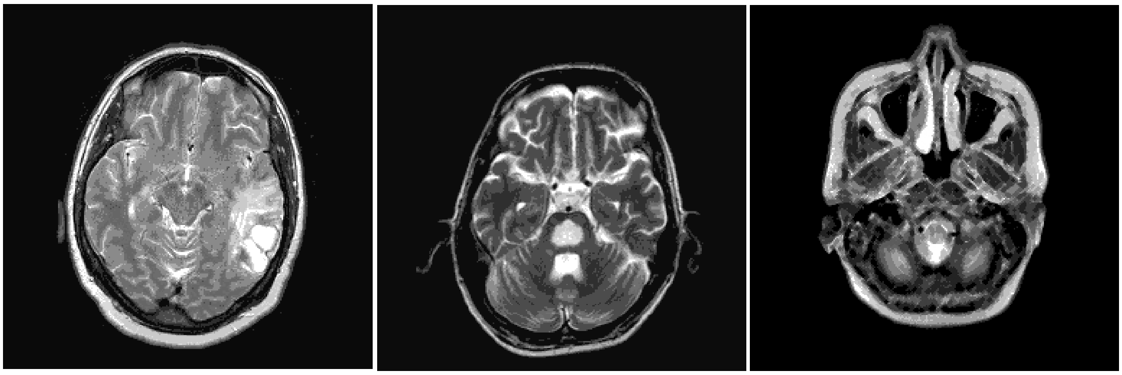




(a) (b) (c)



(a1) (b1) (c1)



(a2) (b2) (c2)

Fig.5: Results of watermarking technique based on DWT and adaptive thresholding, a-c) original medical images, a1-c1) watermarked images with 400 bytes, a2-c2) watermarked images with 800 bytes.

As shown in Figure (5), it is difficult to note the resulting distortions due to hide watermark data into the watermarked medical images that are generated using the proposed adaptive watermarking technique. We evaluate the proposed watermarking technique in terms of fidelity of medical image. For that, we use three image quality metrics are peak signal-to-noise ratio (PSNR) [10], universal image quality (UIQ) index [11] and structural similarity (SSIM) index [12]. The results of fidelity evaluation are shown in Table 1.

Table (1): fidelity evaluation for the proposed adaptive watermarking technique.

Watermarked Image	PSNR	UIQ	SSIM
Image1_400	44.85	0.967	0.928
Image1_800	42.65	0.923	0.892
Image2_400	43.45	0.955	0.898
Image2_800	41.63	0.907	0.824
Image3_400	45.24	0.975	0.934
Image3_800	43.05	0.959	0.902

As is obvious in Table (1), the proposed adaptive watermarking technique achieve the ideal results with respect to fidelity of medical images. Also, the distortion amount in watermarked medical image is increased when the payload of watermark data increase.

4. Conclusions

In this paper, we have proposed adaptive watermarking technique for medical images based on wavelet transform and adaptive thresholding approach which can be used for authentication of medical image. Experimental results show that the degradation by embedding the watermark is too small to be visualized. Therefore, the proposed adaptive watermarking technique can preserve the fidelity of medical image. In addition, this technique is good enough to detect the distortions that can occur for medical images stored in the databases or transmitted over network. Future work will focus on making the watermarks robust against geometrical attacks and optimizing the technique to provide higher capacity and fidelity.

References:

[1]. Sonika C. R., "Medical Image Authentication through Watermarking Preserving ROI," MSc. Thesis in Computer Engineering, Department of Computer Engineering and Information Technology, College of Engineering, Pune, June 2012.

[2]. Umamageswari A., Ferni U., Suresh G.R. "A Survey on Security in Medical Image Communication," *International Journal of Computer Applications*, Vol. 30, no.3, pp 53-61,September 2011.

[3]. Joint NEMA/COCIR/JIRA Security and Privacy Committee, "Defending Medical Information Systems Against Malicious Software," National Electrical Manufacturers Association-USA, December 2003.

[4]. Mandeep K. AND RUPINDER K. "REVERSIBLE WATERMARKING OF MEDICAL IMAGES: AUTHENTICATION AND RECOVERY-A SURVEY," *Journal of Information and Operations Management*, vol.3, Issue 1, pp-241-244, 2012.

[5]. Archana T. and Manisha S. "*Semifragile Watermarking Schemes for Image Authentication- A Survey*," I. J. Computer Network and Information Security, vol. 2, pp. 43-49, 2012.

[6]. Sonika C. and Vandana S., "ANALYSIS OF WATERMARKING TECHNIQUES FOR MEDICAL IMAGES PRESERVING ROI," Computer Science & Information Technology (CS & IT), pp. 297–308, 2012.

[7]. El- sheimy N., Salwa A.K., Tolba A.S., Abdelkader F.M. and Hisham M. E., "Wavelet Packets-Based Blind Watermarking for Medical Image Management," *The Open Biomedical Engineering Journal*, vol.4, pp.93-98, 2010.

[8]. Mohamed A. H. , Abdellatif M.A., El-bey B., "A Watermarking of Medical Image: Method Based LSB," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 12,pp.123-127, December 2011.

[9]. Rupinder K., "A Medical Image Watermarking Technique for Embedding EPR and Its Quality Assessment Using No-Reference Metrics," I.J. Information Technology and Computer Science, vol. 2, pp. 73-79, 2013.

[10]. Wang Z. and Bovik C., "Universal Image Quality Index," IEEE SP letters, vol. 9, pp. 81-84, March 2002.

[11]. Wang Z., Bovik C., Sheikh H. , and Simoncelli E., "*Image quality assessment: From error visibility to structural similarity*," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, Apr. 2004.

[12]. Der-Chyuan Lou, Ming-Chiang Hu, and Jiang-Lung Liu, "*Healthcare Image Watermarking Scheme Based on Human Visual Model and Back-Propagation Network,*" Journal of C.C.I.T., Vol.37, No.1, November, 2008.