THRESHOLD DEPENDENT DATA EMBEDDING AND EXTRACTING SCHEME BASED ON PIXEL PAIR EXPANSION METHOD

Mandeep Singh[1], Neetu Sharma[2]

[1]*ECE, B.G.I.E.T, Sangrur, PTU, (India)*

[2]*Assistant Professor B.G.I.E.T Sangrur, PTU, (India)*

ABSTRACT

Digital watermark is a type of technology that embeds copyright information into digital image. Digital Watermarking works by hiding information inside digital data, such that it cannot be noticed without any software help with the purpose of building sure the covered data is present in all copies of the information that are completed whether legally or if not, in spite of efforts to scratch or eradicate it. Generally it is known that each watermark system consists of an embedding algorithm and an extracting algorithm. The embedding algorithm includes the watermark details in the data and the extracting algorithm decodes the watermark details. We have proposed a reversible embedding and extraction mechanism to embed data in an image which modify the embedded location in least significant bits. The algorithm has good embedding capacity along with preserving the original content of the image up to an acceptance level. This has been measured in terms of PSNR and MSE values which tell the degradation in watermarked image with respect to original image. The algorithm works in fully reversible domain in which there is no need of secret key as well as the original image as it uses only the watermarked image to extract the embedded bits in same sequence.

Keywords: Digital Watermarking, LSB, Spatial Domain, PSNR, MSE, Reversible, Blind.

I INTRODUCTION

With the rapid development of information technology and the wide application of network, the protection of copyright ownership becomes more and more necessary. The conventional information encryption is not safe enough because the document can be copied and distributed easily. As a new method against the failure of encryption, digital watermarking has been proposed as an effective way to protect the ownership of digital documents, especially the ownership of digital images. Digital watermarking techniques for image have been wildly researched in recent years. There are two different watermarking techniques for image, spatial domain techniques and frequency domain techniques. The watermarking is embedded straightly into an image in the spatial domain. The simplest method is the LSB (least significant bit) algorithm, in which the watermarking information is embedded into the LSB or multiple bit layers of image. Watermarking techniques can complement encryption by embedding a secret imperceptible signal into the host signal in such a way that the embedded signal always remains present. Figure 1 represents the embedding and extracting process of digital watermarking in reversible and non-reversible domain. When an watermark is inserted in a host signal with a known key followed by an algorithm, then this is known as embedding process of digital watermarking.

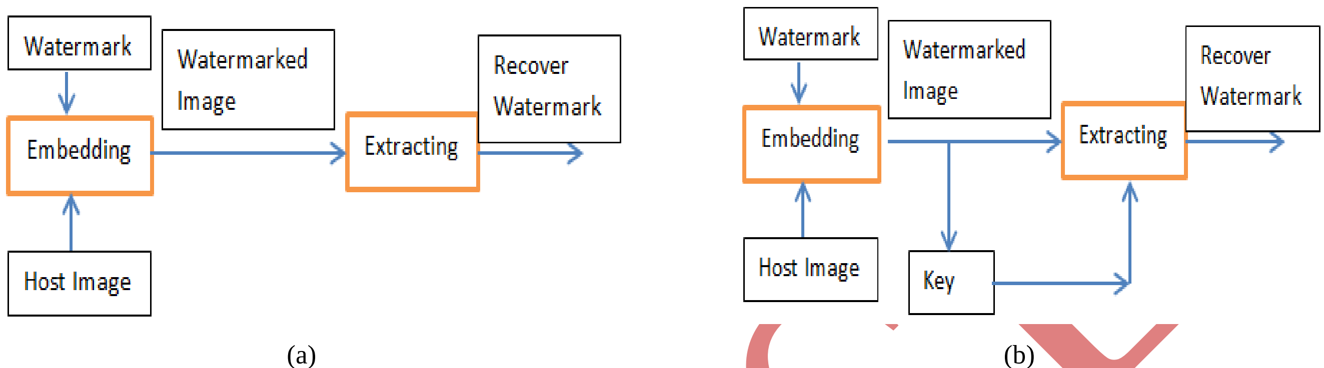

Fig. 1: Embedding and extracting process of (a) reversible (b) non-reversible digital watermarking

When watermark is recover from the watermarked signal using host signal and the key is known as extracting process of digital watermarking. There are various algorithms for digital watermarking. The success of the watermarking scheme largely depends upon the choice of the watermark structure and insertion strategy [1]. The quality of digital watermarking can measure with two distinct parameters: imperceptibility and robustness. Imperceptibility is measured by PSNR of host image and embedded image in DB. Higher PSNR is desired as it means to hide the marked image efficiently. And robustness is measured by correlation of the original mark image and recovered mark image [1]–[5]. Depending on the need of the original image, watermarking is classified to non-blind and blind watermarking. The requirement of original image for detecting the watermark is known as non-blind watermarking, while the blind technique does not require the original image. Another way to classify watermarking that is transform domain watermarking and spatial domain watermarking. Early watermarking schemes were in the spatial domain, where the watermark is added by modifying pixel values of the host image [4], [5]. Some of the spatial domains watermarking approaches are based on the modification of the least significant bit (LSB) of both: host and marked images [7] -[9], [6]. of an image based on the assumption that the LSB data are insignificant generally. The spatial domain watermarking is easy to implement from a computational point of view but too fragile to resist numerous attacks [1], [3], [5]. In order to have more promising techniques, researches were directed towards watermarking in the transform domain, where the watermark is not added to the image intensities, but to the values of its transform coefficients. Then to get the watermarked image one should perform the transform inversely. In our work we proposed fully reversible blind watermarking technique in which bits are embedded in spatial frequency in least significant bits.

II REQUIREMENTS AND FEATURES OF WATERMARKING SYSTEM

1. The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation [10], and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement [11]. In addition, not all watermarking algorithms have the same level of robustness, Some techniques are robust against some manipulation operations, however, they fail against other stronger attacks [12]. Moreover, it's not always desirable for watermark to be robust, in some cases; it's desired for the watermark to be fragile [10]. Therefore, the robustness can be classified as following:

- Fragile: The watermark in this type is designed to be destroyed at any kind of modification, to detect any illegal manipulation, even slight changes, involving incidental and intentional attacks. Fragile watermarks are mainly used in content authentication and integrity verification. They use blind detection type [14], as it will be discussed in Detection Types. In addition, the implementation of fragile techniques is easier than the implementation of robust ones [15].
- Semi-fragile: The watermark in this type is robust against incidental modifications, but fragile against malicious attacks [16]. And it is used for image authentication [17].

2. Imperceptibility (also known as Invisibility and Fidelity) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image [10]. In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness.
3. Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for [10]. Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness [12].
4. Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection [10]. According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks.
5. The cost is the reason behind studying the complexity, so it should be at a reasonable cost [13]. It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used. The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors [10]. So these are some factors which need to understand in watermarking systems. Below is a literature survey for the existed work in the watermarking systems.

III RELATED WORK

As digital image watermarking systems can be characterize and differentiate by many factors, we give a brief review of some of the literature here, which are from both spatial as well as transform domain. Below is a brief from some papers we read while developing our method.

Huang et al. [20] Proposed Digital watermarking is used in the hiding of a secret messageor information within an ordinary message and its extraction at its destination. The secret message embedded as watermark can be almost anything, for example: a serial number, plain text, image, etc.

Clarke et al. [24] [25] proposed a LSB-based scheme for ultrasound images, where the original image can be recovered completely. In embedding process, an SHA-256 hash code is calculated for the ROI selected. After that, the hashcode is embedded into the LSBs of RONI. The drawback of these two schemes is that the reversibility of the scheme is based on the fact that the original values of RONI pixels were zeros before embedding, but for nonzero values, the scheme is not reversible. He also proposed two schemes to integrate the ability of detecting tampering and subsequently recovering the image. In embedding process, the image is divided into blocks of 8×8 pixels each. Each block B is further divided into four sub-blocks of 4×4 pixels. The watermark, which is embedded using LSBs, in each sub-block, is a 3-tuple (v, p,r). The drawbacks of these two schemes are the lack of reversibility and using of averages as recovery information.

Wang et al. [22] proposed two schemes based on modulo 256 and discrete cosine transform (DCT). At first, the image is divided into several blocks, and for each block, an adaptive robust digital watermarking method combined with modulo operation is used to hide the watermark. The drawback of this scheme is limited hiding capacity, where only authentication and recovery data are embedded. Besides, the scheme is not reversible exactly due to preprocessing used to avoid pixel flipping.

Fauzi et al. [27] proposed a reversible watermarking technique to embed information into medical images. In this paper Region of interest (ROI) and Region of non interest (RONI) is defined. ROI is protected and effort is made to embed data in RONI. When medical image shared through network, for the compression purpose the JPEG2000 algorithm is proposed and to improve the information security to maintain the secrecy, reliability and accessibility of the embedded data Arnold's cat map method (Arnold Transform) is proposed. Patient information and disease information is embedded into DICOM images. Increase in authentication can be achieved using Kerberos technique.

Naskar et al. [18] proposes a digital watermarking technique which is a class of fragile reversible watermarking that constitutes and find application in authentication of medical and military imagery. Reversible watermarking techniques ensures that after watermark extraction, the original cover image can be recovered from the watermarked image pixel-by-pixel. This paper also proposes a novel reversible watermarking technique as an improved modification of the existing histogram bin shifting technique. It develop an optimal selection scheme for the "embedding point" (gray scale value of the pixels hosting the watermark), and take advantage of multiple zero frequency pixel values in the given image to embed the watermark. Experimental results for a set of images shows that the adoption of these techniques improves the peak signal-to-noise ratio (PSNR) of the watermarked image compared to previously proposed histogram bin shifting techniques.

IV PROPOSED METHOD

There are many algorithms available for blind digital watermarking. Blind watermarking scheme is also known as public watermarking scheme. This is the most challenging type of watermarking system as it requires neither the cover (original data), nor the embedded watermark. These systems extract n bits of the watermark data from the watermarked data (i.e. the watermarked image). The algorithm proposed in this paper uses Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. Given the extraordinarily high channel capacity of using the entire image, a fully reversible algorithm has been proposed for embedding and extraction process. The main point in this algorithm is that it considers the noise level threshold value for varying the embedded bits. Below are the steps in proposed algorithms for embedding and extraction process.

Steps for embedding process:

1) Convert RGB image to gray scale image.
2) Make double precision for image.
3) Put two rows and columns of minimum intensity value surrounding the input image
4) Make non-overlapping pairs of pixels taking two at a time from the rows sweeping left to right
5) For each pair generate a surrounding window with two pixels right hand side and two pixels downwards. By using this window calculate horizontal and vertical gradients and calculate Gap element and noise threshold
6) Generate two variables by subtracting First pixel in the pair from second pixel for first variable and by differencing gap element produced in step 5 from second pixel value in the pair for second variable.
7) Apply expansion embedding and shifting modifications to the pair pixels according to the table shown below for embedding process.
8) For each pixel pair, put the modified pixels in two dimensional array and name it watermarked array.
9) When algorithm run for all pixel pairs, save the two dimensional array as an image in the folder and term it as watermarked image.
10) Calculate PSNR and MSE values for the watermarked image

Below is the table which has been modified by us from [26] for two bit embedding as generated it for one bit embedding. We have also shown the results for [26] in comparison to our work

	j	J+1	J+2	J+3
i	X	Y	V1	V2
I+1	V3	V4	V5	V6
I+2	V7	V8	V9	V10

Fig 2: Window for Evaluating Gap Element

In window above, v1 to v10 are neighboring pixels and x and y is the pixel-pair.

Horizontal and vertical gradients in step 5 have been calculated using formula as under:

dv=|v3-v7|+|v4-v8|+|v5-v9|+|v1-v5|+v2-v6|+v6-v10|……………………..A

dh=|v3-v4|+|v1-v2|+v5-v6|+v7-v8|+v9-v10|…………………………….B

u=(v1+v4)/2+(v3-v5)/4…………………………………………..……C

Table 1: For Embedding Process:

Conditions	Operations	Direction change	Changes
(variable1==-1 & variable2<=-2) or variable1==-1 & variable2==-1	Modify	left	(x-b, y)
(variable1>=1 & variable2<=-2) or variable1>=2 & variable2==-1	shifting	down	(x, y-mbit)
(variable1<=-2 & variable2<=-2) or variable1<=-2 & variable2==-1	shifting	left	(x-mbit,y)
(variable1==0 & variable2==0)	Modify	up	(x,y+b)
variable1>=2 & variable2>=1	shifting	right	(x+mbit, y)
variable1<=-1 &variable2>=0	shifting	up	(x,y+mbit)

Steps for extraction process:

1) Read the watermarked image in software workspace
2) Make double precision for image.
3) Put two rows and columns of minimum intensity value surrounding the input image
4) Make non-overlapping pairs of pixels taking two at a time from the rows sweeping left to right

5) For each pair generate a surrounding window with two pixels right hand side and two pixels downwards. By using this window calculate horizontal and vertical gradients and calculate Gap element and noise threshold
6) Generate two variables by subtracting First pixel in the pair from second pixel for first variable and by differencing gap element produced in step 5 from second pixel value in the pair for second variable.
7) Apply expansion extraction and shifting modifications to the pair pixels according to the table shown below for extraction process.
8) For each pixel pair, put the modified pixels in two dimensional array and name it extracted image array.
9) When algorithm run for all pixel pairs, save the two dimensional array as an image in the folder and term it as extracted image.
10) Compare this extracted image with original image and check for reversible process

Below is the table for the extraction process

Table 2: Table for Extraction Process

Conditions	Extracted bit	Changes
(variable1==3 or variable1==2) & variable2==-2	variable1-1	(x,y+b)
(variable1==-4 or variable1==-3 or variable1==-2 or variable1==-1) & variable2<=-2	1- variable1	(x+b,y)
(variable1==1 & variable2==-1) or (variable1==2 & variable2==-2)	variable1-1	(x,y+b)
(variable1==-4 or variable1==-3 or variable1==-2 or variable1==-1) & variable2==-1	-1- variable1	(x+b,y)
(variable1==7 & variable2==-2) or (variable1==8 & variable2==-3)or (variable1>=1) & (variable2==0 or variable2==-1 or variable2==-2 or variable2==-3)	- variable2	(x,y+b)
variable1>=5 & variable2>=1	No change	(x-mbit,y)
(variable1==1 or variable1==2 or variable1==3 or variable1==4) & variable2>=1	variable1-1	(x-b,y)
variable1<=-4 & variable2>=3	No change	(x, y-mbit)

Below we have shown results for test image for proposed technique

Fig 3: Test Image

Fig 4: Yellow portion showing embedding at T1=0, T2=15, T3=25 and T4=104 respectively for Test Image

V BPP FOR EMBEDDING CAPACITY

The number of distinct colors that can be represented by a pixel depends on the number of bits per pixel (bpp). A 1 bpp image uses 1-bit for each pixel, so each pixel can be either on or off. Each additional bit doubles the number of colors available, so a 2 bpp image can have 4 colors, and a 3 bpp image can have 8 colors and so on. We used this parameter for checking the total embedding capacity. BPP (bits per pixel) has been calculated for both techniques. From result, it is found that proposed technique embed approx. double bits than the old method.

VI PERFORMANCE EVALUATION FOR CHECKING DIFFERENCE IN QUALITY

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE parameter, the lower is the error. To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. computes the PSNR using the following equation:

$$PSNR = 10 log_{10}\left(\frac{R^2}{MSE}\right)$$

It has been found that proposed method has an acceptable PSNR values but it has been decreased due to more embedding than the old method.

PROPOSED TECHNIQUE			
IMAGE	BPP	PSNR	MSE
T1	0.213989	42.205	3.913635
T2	0.198975	42.30836	3.821594
T3	0.16272	42.68535	3.503845
T4	0.034302	46.96397	1.308228

Fig 5: BPP, PSNR, MSE values for proposed method

REFRANCE TECHNIQUE			
IMAGE	BPP	PSNR	MSE
T1	0.128296	51.72951	0.436646
T2	0.119324	51.8172	0.427917
T3	0.098206	52.24385	0.387878
T4	0.021179	56.49284	0.145813

Fig 6: BPP, PSNR, MSE values for reference method

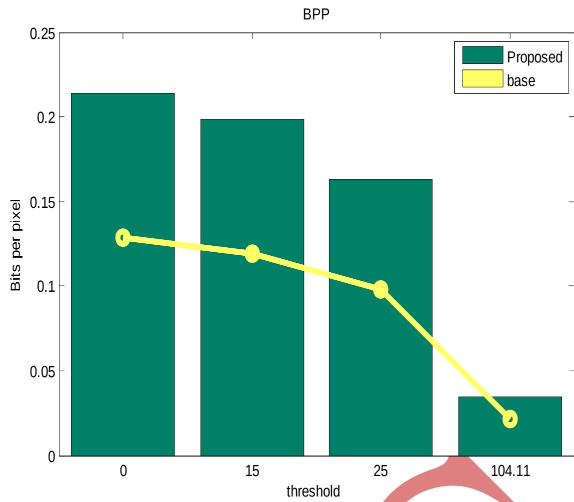

Fig 7: BPP vs. threshold plots for proposed method and reference technique

VII CONCLUSION

This paper covers the study of reversible watermarking system, which is mostly adopted in application such as authentication. This method is used to transfer useful information along with the original image. So in the proposed method also our aim is to transfer this useful information in the form of bits with increase in the embedding capacity along with high visual quality and less loss. Our technique has higher embedding capacity along with good value of PSNR values. We have generated the embedded bits randomly, but technique can be used for embedding any information by converting it into binary form.

REFERENCES

[1] YosephAbatte, "Digital Image Watermarking", Addis Ababa University, 2005.

[2] Ingemar J. Cox, , ISBN 978-953-307-656-0.

[3] Shital Gupta and Sanjeev Jain, "A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", Department of Computer Science & Engineering, LNCT, Bhopal.

[4] Koushik Pal, G. Ghosh, and M. Bhattacharya, "A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique", Institute of Radio Physics and Electronics, University of Calcutta, Kolkata Indian Institute of Information Technology and Management, Gwalior India.

[5] Ibrahim Nasir, Ying Weng, and Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain", School of Informatics, University of Bradford, UK.

[6] R.G. Van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A Digital Watermark", Scientific Technology, 21 Walstab St, E. Brighton, 3187, Australia.

[7] S. Rohith and K.N. haribhat, “A Simple Robust Digital Image Joe Kilian, Tom Leighton, and Talal G. Shamoon, “Secure spread spectrum watermarking for multimedia”, IEEE International Conference on Image Processing, ICIP 97, volume 6, pages 1673 1687, Santa Barbara, California, USA, October 1997.

[8] Abrar Ahmed Syed, “Digital Watermarking”, the University of Texas at Arlington.

[9] Ali Assi, Engineering Education and Research Using MATLAB Watermarking against Salt and Pepper Noise using Repetition Codes”, Nagarjuna College of Engineering and Technology, Bengaluru, Karnataka, India.

[10] M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, Digital Watermarking and Steganography: Morgan Kaufmann Publishers, 2008.

[11] Z. Yanqun, "Digital Watermarking Technology: A Review," in Future Computer and Communication, 2009. FCC '09. International Conference on, 2009, pp. 250-252.

[12] R. F. Olanrewaju, "Development of Intelligent Digital Watermarking via Safe Region," PHD, Electrical and Computer Engineering, International Islamic University Malaysia, Kulliyyah of Engineering, 2011.

[13] J.-S. Pan, H.-C.Huang, and l. C. Jain, Eds., Intelligent Watermarking Techniques (Series on Innovative Intelligence. World Scientific, 2004, p.^pp. Pages.

[14] L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in Information and Communication Technologies, 2005.ICICT 2005. First International Conference on, 2005, pp. 337-341.

[15] N. Cvejic, "Algorithms for Audio Watermarking and Steganography," Department of Electrical and Information Engineering, University of Oulu, 2004.

[16] A. G. Charles Fung, Walter Godoy Junior, "A Review Study on Image Digital Watermarking," presented at the The Tenth International Conference on Networks, St. Maarten, The Netherlands Antilles, 2011.

[17] S. Jun and M. S. Alam, "Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking," Instrumentation and Measurement, IEEE Transactions on, vol. 57, pp. 595-606, 2008.

[18] PasunuriNagarju, RuchiraNaskar and RajatSubhraChakraborty, “Improved Histogram Bin Shifting based ReversibleWatermarking”, International Conference of Intelligence systems & Signal processing (ISSP).IEEE 2013.

[19] X. Guo and T.-g.Zhuang, "A Region-Based LosslessWatermarking Scheme for Enhancing Security of MedicalData," Journal of Digital Imaging, vol. 0, pp. 1-12, 2007.K.-H. Chiang, K.-C.Chang-Chien, R.-F.Chang, and H.-Y.Yen, "Tamper Detection and Restoring System for MedicalImages Using Wavelet-based Reversible Data Embedding,"Journal of Digital Imaging,

[20] J. Pan, H. C. Huang, and L. C. Jain. Intelligent Watermarking Techniques.World Scientific, 2004.

[21] G Prbhakaran, R.Bhavani, and M.Ramesh, “A Robust QR- Code Video Watermarking Scheme Based On SVD and DWT. Composite Domain” International Conference onPattern Recognition, Informatics and Mobile Engineering (PRIME) IEEE 2013.

[22] J. H. K. Wu, R.-F.Chang, C.-J.Chen, C.-L.Wang, T.-H.Kuo, W. K. Moon, and D.-R. Chen, "Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique " Journal of Digital Imaging, 2008, vol. 21, pp. 59-76.

[23] J. H. K. Wu, R.-F.Chang, C.-J.Chen, C.-L.Wang, T.-H.Kuo, W. K. Moon, and D.-R. Chen, "Tamper Detection and

Recovery for Medical Images Using Near-lossless Information Hiding Technique " Journal of Digital Imaging, 2008, vol. 21, pp. 59-76.

[24] J. M. Zain, L. P. Baldwin, and M. Clarke, "Reversiblewatermarking for authentication of Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2004, pp. 3237 - 3240.

[25] J. M. Zain and C. M., "Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images," International Journal of Computer Science and Network Security, vol. 7, pp. 19-28, 2007.

[26] X. Li, W. Zhang, X. Gui and B. Yang, "A novel reversible data hiding scheme based on two dimensional difference histogram modification" IEEE Trans. On Information Forensics and Security, vol. 8, no 7, pp. 1091-1100, July 2013.

[27] J. M. Zain and A. R. M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery " in Proceedings of the 28th IEEE EMBS Annual International Conference, 2006, pp. 3270-3273.