ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

Information Embedding and Authentication in Medical Images Using Least Difference Method

Sulakshna[1], Sonia[2]

Department of Electronics and Communication Engineering, BBSBEC, Fatehgarh Sahib, Punjab, India[1,2]

ABSTRACT: Digital image watermarking is proposed to overcome the problems of security, integrity in health care departments and that of defense personnel's as well as employees of national security agencies. Medical images, unlike most of images, require extreme care when embedding informatory information while embedding process because the additional information must not affect the image quality and readability of the required portions need to be diagnosed. In order to overcome any misdiagnose caused by embedding data into medical images, lossless data hiding techniques have been developed. This paper presents a lossless semi-reversible watermarking technique for DICOM images which works in semi reversible domain. This technique can embed high capacity of textual data in an image in noisy pixels of the image. It uses the technique of minimum value difference in characters integral value and the pixels of the image and finds the matching on least difference basis. There is no overlapping in the embedded data, hence full recovering of information at receivers end. It can be used to hide patient's data hiding and protecting the region of interest (ROI) with tamper detection and recovery capability. The experimental results show that the original image can be exactly extracted from the watermarked one in case of no tampering. In case of alterations, made in the transmitted medium by an unauthorized person, it is able to detect and locate them in the images.

Keywords: Watermarking, PSNR, ROI, Authentication

I.INTRODUCTION

The Internet has become the most important information provider, and offers many mediums to deliver and to interchange information. Digital images can be easily shared via the Internet and conveniently processed for queries in databases. However, these also imply that images can be modified easily and imperceptibly with malicious intentions. With some powerful image processing tools, one can modify some features in a picture easily without any detectable trace. These kinds of operations are regarded as tamper. But in some cases, the images are not allowed to be done such operations, such as images for military, medical, and judicative use. The validity of the image is of most importance in these conditions [12]. The production of ownership and prevention of unauthorized manipulation of digital images are becoming an important issue [13]. So some effective ways are needed to guarantee integrity of the image.

To get familiarize with the system of watermarking one have to be clear about some basic terms associated with watermarking systems:

Perceptibility: It is the perceptual similarity between the original and the stego images. It decides the visibility or non-visibility of watermarking system;

Reversibility: It is the ability to extract both the original image and the watermark. However sometimes it's difficult to obtain the original image from encrypted image, but ROI must be able to reconstruct fully or should not go through any alterations in medical images. Therefore most of the systems come in the domain of semi-reversibility.

Robustness: It is the ability to detect the watermark after the common signal processing operations.

Payload: It is the total number of encoded bytes of the watermark in the host image without including the redundant information;

Literature review-

The authentication and keeping integrity of region of are the main features need to be solved by the watermarking system. Few techniques which are good at these features are discussed below:

Pan J. et al. [3] Proposed Digital watermarking is used in the hiding of a secret message or information within an ordinary message and its extraction atits destination. The secret message embedded as water mark can be almost anything, for example: a serial number, plaintext, image, etc.

Zain *et al*. [8, 9] proposed a LSB-based scheme for ultrasound images, where theoriginal image can be recovered completely. Inembedding process, an SHA-256 hash code iscalculated for the ROI selected. After that, the hashcode is embedded into the LSBs of RONI. Thedrawback of these two schemes is that the reversibilityof the scheme is based on the fact that the originalvalues of RONI pixels were zeros before embedding, but for nonzero values, the scheme is not reversible. Zain *et al*.[10, 11] 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.
Chiang et al. **[7]** proposed two reversible schemes based on difference expansion technique (DE) for tamper detection and recovery [2]. In the two schemes, the image is divided into blocks of 4×4 each, and each block is transformed using two-level DE technique. Only smooth blocks, with equal pixel values, are used for embedding watermark. The drawback of this technique is the limited capacity because only smooth blocks are used for embedding; thus, it cannot be used for all image modalities.
Wu *et al*. [6] 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.
Umamageswari et al. [10] 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.
Prbhakaran et al. [4] proposes a video watermarking with text data (verification message) by using the Quick Response (QR) Code technique. A quick response (QR) code is a two dimensionalbarcode invented by the Japanese corporation Denso Wave. The QR Code is watermarked via a robustvideo watermarking scheme based on the (singular valuedecomposition) SVD and (Discrete Wavelet Transform) DWT**.** This method is convenient, feasible and practically used for providing copyright protection.SVD is an algebraic transform for watermarking applications. SVD is applied to the cover I-frame. The extracted diagonal value is fused with logo (or) watermark. DWT is applied on SVD cover image and QR code image. This method has achieved the improvedimperceptibility and security watermarking.
Chakraborty et al. [1] proposes a digital watermarking technique which is a class of fragilereversible 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.

II.PROPOSED TECHNIQUE

We proposed a scheme which is based both on the fragility of embedding mechanism and also keeping ROI integrated in order to make it safe from any alterations. We present our approach in the context of gray scale medical DICOM images. Watermarks are made from collaboration of diagnosis report data as well as authentication code used to authenticate the sender and images. Each character has been inserted in non-region of interest by separating the effected organ of the patient called ROI and the unwanted noise present in the image i.e. non-region of interest.This scheme operates in semi-reversible domain where we recovered only the region of interest of the original image

Watermark: Watermark we used isconsisting of two types of data in which first one is the radiologist's diagnosis report about the patient's problem. As there can be large amount of data to be embedded depending upon the report we used spatial domain for encryption instead of frequency domain as we can't embed much data in frequency domains. And Second portion of the watermark signal is the message authentication code which has been generated from the secret message developed by the embedded in order to authenticate the images. A hash code has been evaluated from this secret message and concatenated together in order to make the message authentication code and embedded along with other data. The same secret message will be sent to the receivers end separately from encrypted image or can be provided by other means like on telephones. The receiver will calculate the MAC by his own means and compare it with MAC decrypted from the image. Decisions can be made regarding tampering of image by the means discussed above.

A. Encryption process

1. Read Image into MATLAB environment and separate REGION OF INTEREST and NON REGION OF INTEREST using cropping tool.

3. Evaluate Message authentication code from secret message and concatenate it with Diagnosis report called informatory data

4. Generate an array in order to put the integer form of Concatenated string data.

5. Scan the host image for a value which has been chosen one at a time in a sequence from array and match for minimum difference match in non-region of interest.

6. Scan secret key array, if the co-ordinates of that pixel present look for another location. Otherwise put the values of co-ordinates in the secret key array.

7. Update the encrypted image array according to the value used by that pixel. And update the secret key.

8. When algorithm run for all the data, watermarked signal image will be produced, if it fails in the middle, try fewer payloads.

B. Decryption process

1. Load the Watermarked image and secret key send by the embedder.

2. Extract the coordinates of the pixel by using the secret key sequence.

3. Extract the informatory data and MAC by converting back to characters in string form.

4. Compute the MAC code separately from the secret message delivered separately and compare the extracted hash to the computed hash. If both are same, received image is authentic, otherwise declare it as unauthentic.

5. Save the decoded data string in a text. File.

III. EXPERIMENTAL RESULTS

We received many images of X-ray, CT and MRI scan from city radiologists. But only few patients have diagnosed for a problem. We discarded all the images and keep only five images about which we received the exact information about the disease or any irregularities. We applied embedded algorithms to all but here we will provide the results about spinal cord X-ray image.

***Fidelity measure**:*

The PSNR (PEAK SIGNAL TO NOISE RATIO) of an image is a typical measure used for evaluating image quality by considering that the few noticeable distortions are uniform in all coefficients in a specific domain, such as spectral domain, frequency domain, or some transform domain. Since PSNR is more computable and can be used to provide a generic bound for the watermarking capacity. So, we use the PSNR to analyze the watermark embedding distortions on images. We need to calculate MEAN SQUARE ERROR (MSE) in order to calculate PSNR.

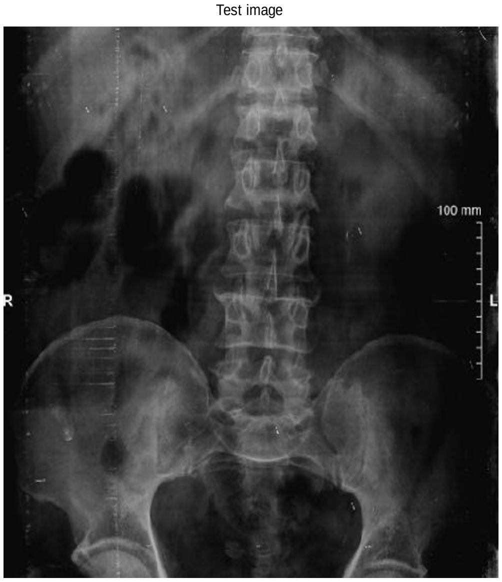


Figure1: Host image used for experimental results

Equations used for evaluating PSNR and MSE are

PSNR = 10log10 *(255^2/MSE)

MSE = I, J [host image (i, j) – encrypted image (i, j)] 2/ j

Where255 is the maximum fluctuation of intensity in the input image data type.

The degradation in terms of PSNR and MSE in the test image and watermarked image for X-ray spinal cord image has-been shown in Table 1 and 2

Tables 1 show the degradation in visual quality of the watermarked image with respect to the original image by embedding watermarks of varying strengths in terms of PSNR and MSE. The perceptual appearance is far better by using this approach as we can't see changes by naked eye. Therefore difference image and a portion of modified histogram have been provided below.

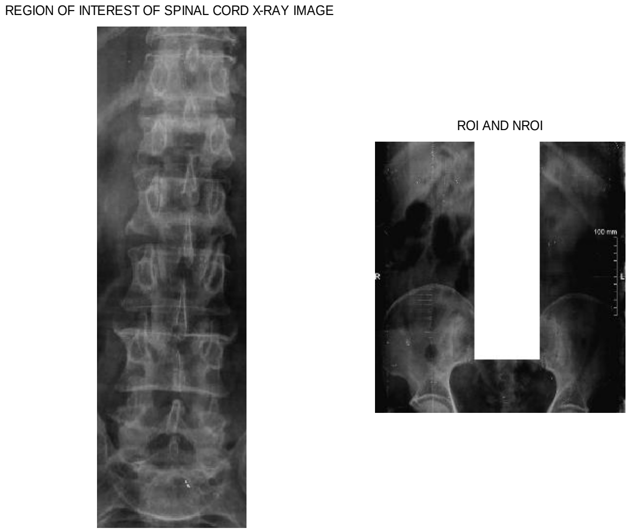


Figure 2: Showing separation of region of interest and non-region of interest.

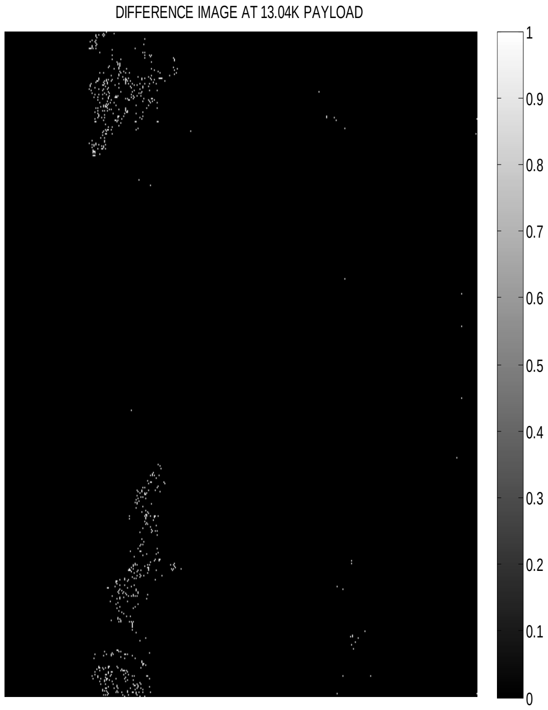


Figure 3: difference image showing pixels where data modified the pixels.

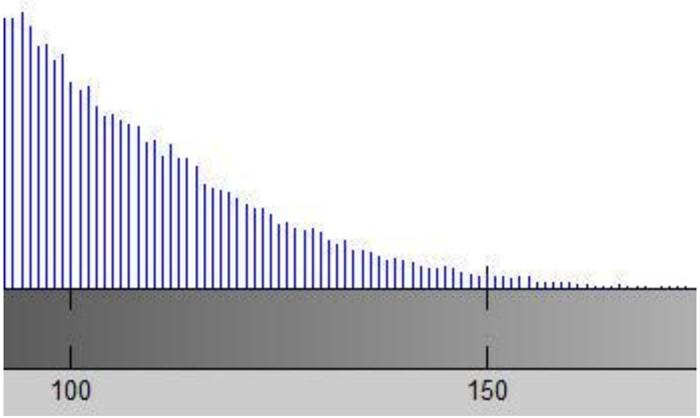


Figure 4: a portion of histogram Host image

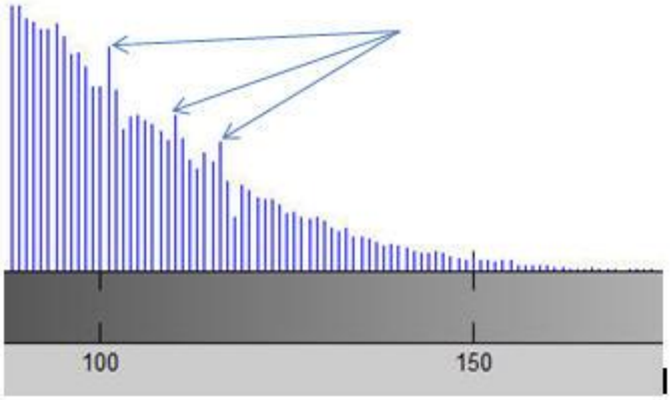
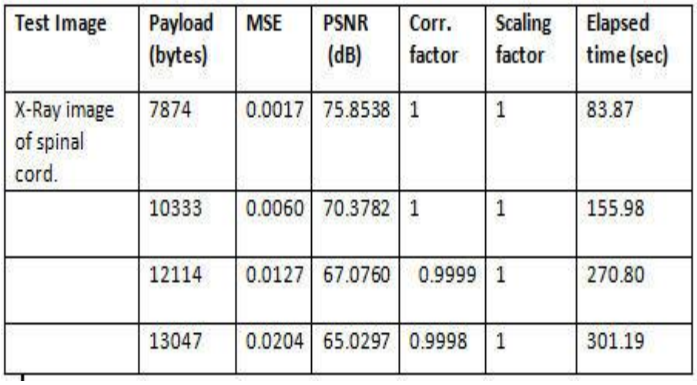


Figure 5: Same portion of encrypted image that has been modified showing encryption.

Table 1. Experiment Result



Test Image	Payload (bytes)	MSE	PSNR (dB)	Corr. factor	Scaling factor	Elapsed time (sec)
X-Ray image of spinal cord.	7874	0.0017	75.8538	1	1	83.87
	10333	0.0060	70.3782	1	1	155.98
	12114	0.0127	67.0760	0.9999	1	270.80
	13047	0.0204	65.0297	0.9998	1	301.19

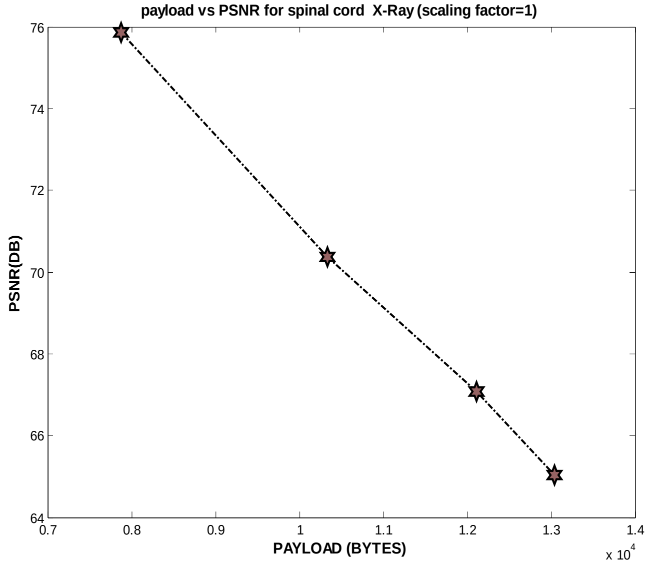
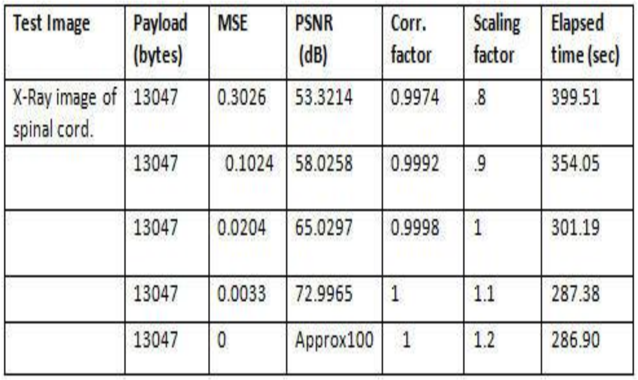


Figure 6: Showing Payload vs. psnr for spinal cord x-ray at constant scale factor

It is hard to locate the in two images with naked eye. But in the same chosen portion of the histograms of host and encrypted image, one can see the modified pixels.

Authentication: The integrity of images at the receiving end is checked by comparing the MAC from decoded string which comes as output in extraction process with that of evaluated MAC produced from the separately sent secret message. If it is unaltered i.e. it matched, then call it authenticated. Otherwise it has been altered. Gaussian noise, median filtering, compression are some of the attacks which can result in tampering of image and hence we can't authenticate the image if tampered. One can check tampering by comparing corresponding pixels in the images.

Table 2. Shows the data results for X-ray image of spinal cord at constant payload bytes.



Test Image	Payload (bytes)	MSE	PSNR (dB)	Corr. factor	Scaling factor	Elapsed time (sec)
X-Ray image of spinal cord.	13047	0.3026	53.3214	0.9974	.8	399.51
	13047	0.1024	58.0258	0.9992	.9	354.05
	13047	0.0204	65.0297	0.9998	1	301.19
	13047	0.0033	72.9965	1	1.1	287.38
	13047	0	Approx100	1	1.2	286.90

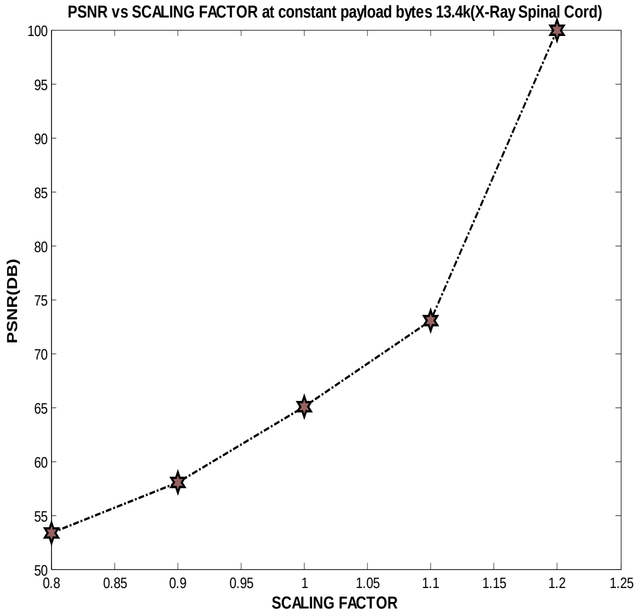


Figure 7: Showing Payload vs. PSNR for spinal cord x-ray at constant payload

Integration of ROI: We have integrated region of interest from any changes while embedding process. A technique has been developed in which the algorithm will not scan the effected organ pixels while encryption and embed data only in non-region of interest.

Computational efficiency has been increased by this method as the algorithm needs to scan only once per character to embed the data in the image.

Payload: Maximum Payload of 13k bytes has been used in the process which is far enough for any diagnosis report.

IV. CONCLUSION AND FUTURE SCOPE

It has been shown that the watermark embedding is invisible and has a good PSNR if the embedding factor is low. So the quality of the image will not be affected by the watermarking embedding. The watermark embedding is very sensible to any distortion. While embedding the data, ROI of medical image is avoided to ensure the integrity of ROI. However, the method developed is not fully reversible as it can't build non area of interest. Maximum Payload of 13k has been used but found low PSNR value at very large data payloads. So in future, work can be done on the algorithm in order to make it fully reversible and to increase PSNR at high payloads.

ACKNOWLEDGMENT

I wish to Acknowledge Mrs. Sonia for her contribution in developing and maintaining this paper. I wish Mrs. Sonia my deepest regard for her immense cooperation.

REFERENCES

[1] P.Nagarju, R.Naskar, R.Chakraborty, "Improved Histogram Bin Shifting based ReversibleWatermarking", International Conference of Intelligence systems & Signal processing (ISSP).IEEE 2013.

[2] 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.

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

[4] G Prbhakaran, R.Bhavani, 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.

[5] A.Umamageswari , G.R.Suresh," Security in Medical Image Communication with Arnold's Cat map method and Reversible Watermarking". International Conference on Circuits, Power and Computing Technologies, 2013.
[6] 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, vol. 21, pp. 59-76. 2008.
[7] 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, vol. 21, pp. 59-76. 2008.
[8] J. M. Zain, L. P. Baldwin, M. Clarke, "Reversible watermarking for authentication of Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society", pp. 3237 - 3240. 2004.
[9] J. M. Zain, "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.
[10] J. M. Zain, A. R. M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery", in Proceedings of the 28th IEEE EMBS Annual International Conference, pp. 3270-3273, 2006.
[11] J. M. Zain, A. R. M. Fauzi, "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW- TDR)," in The 29th Annual International Conference of the IEEE EMBS, pp. 5661-5664, 2007.
[12] Y. Liu, W. Gao, H.Yao, S. Liu, "A Texture-based Tamper Detection Scheme by Fragile Watermarking", Computer Science and Technology Department of Harbin Institute of Technology IEEE, 2004.
[13] M.E. Yalçin, J. Vanderwalle, "Fragile Watermarking and Unkeyed Hash Function Implementation for Image Authentication on CNN-UM", Katholicke Universite it Leuven,Department of Electrical Engineering (ESAT), April 2002.