

Biomedical Image Watermarking in Wavelet Domain for Data Integrity Using Bit Majority Algorithm and Multiple Copies of Hidden Information

Koushik Pal¹, G.Ghosh^{1,*}, M. Bhattacharya²

¹Institute of Radio Physics and Electronics, University of Calcutta, Kolkata, 700014, India

²Indian Institute of Information Technology and Management, Gwalior, India

Abstract The current paper presents a novel and unique scheme for biomedical image watermarking in wavelet domain by hiding multiple copies of the same data in the cover image using bit replacement in the horizontal (HL) and vertical (LH) resolution approximation image components. The proposed scheme uses an approach for recovering the hidden information from the damaged copies due to unauthorized alteration of the data by applying an algorithm to find the closest twin of the embedded information by bit majority algorithm. Experimental results of the proposed watermarking technique show much enhancement in the visual and statistical invisibility of hidden information after data recovery that supports the improvement in performance.

Keywords Discrete Wavelet Transform, Watermarking; Noise Attack, Salt and Pepper Noise, Compression, Bit Majority

1. Introduction

The advancement in technology has helped in gradually replacing conventional analog images by digital images providing low cost of reproduction, ease of storage and distribution but on the other hand has added an additional dimension to the complexity in securing the image in digital format. This is quite understandable because digital format is easy to edit, modify, and exploit. It can be readily shared via computer networks and conveniently processed for queries in databases. Also, digital storage does not age or degrade with usage. The higher capacity of storage devices and data communication channels offers an added advantage of using digital formatting. In modern health care, systems such as HIS (Hospital Information System) and PACS (Picture Archiving and Communications System) form the information technology infrastructure for a hospital based on the DICOM (Digital Imaging and Communication in Medicine) standard[33]. Medical images are increasingly captured, transmitted and stored in digital format nowadays as EPR (Electronic Patient Record) for future reference [3,36]. Advancement of medical information system has changed the way patient records are stored, accessed and distributed[24,25]. The integrity of the records such as

medical images needs to be protected from unauthorized-modification or destruction or quality degradation of information of the medical images[10,11,37]. While working with images, there comes another problem of dealing with copyright protection. Due to the widespread accessibility over Internet, multimedia data, such as images, can be modified easily with existing image processing tools available. For that matter it becomes essential to provide copyright protection for proprietorship of medical images[4]. One of the methods to provide image copyright protection is to embed a watermark in the parent image. Such a method is termed “watermarking”. Digital watermarking is a technique of embedding a digital code into a cover image without changing the image size or format and also keeping the visible quality and information of the biomedical image intact[30,32].

The usual constraints of watermarking are invisibility of the mark, secrecy to unauthorized persons, and robustness against attempts to attack. These demands also exist in the medical domain but additional constraints are added as the information content is critical. Four main objectives are foreseen in the medical domain[9].

Data hiding: Required for embedding information so as to make the image useful or easier to use.

Integrity control: Required for verifying that the image is intact and has not been modified in an unauthorized manner [15, 18].

Authenticity: Required for verifying that the image is originating from an authentic source. More often an at-

* Corresponding author:

goggle.rpe@gmail.com (G.Ghosh)

Published online at <http://journal.sapub.org/ajbe>

Copyright © 2012 Scientific & Academic Publishing. All Rights Reserved

tached key, file or a header, which carries all the needed information, identifies an image[2]. An alternative would be to embed all such information into the image data itself.

Imperceptible / Reversible Watermarking: For recovery of the original pixel values the watermarking method must be reversible as medical tradition requires very strict preservation of quality of biomedical images[27,28,35]. This limits significantly the capacity and the number of possible methods. An alternative way is to define ROI (regions of interest), to be left intact, and leave us with regions of insertion where the watermark could be inserted and does not interfere or disturb the radiologist.

Medical images are often not allowed to be modified in any way. Watermarking in medical images provides a promising alternative to current security tools used to protect the integrity of medical images[12,13]. The watermarking scheme being used needs to be reversible and the exact pixel value also needs to be recovered. Therefore, the methods should minimize the possibility of the image degradation and increase the security to a large extent[15].

1.1. Types of Watermarking

Digital watermarking can be visible or invisible. The efficiency of the watermarking technique is found out with the capacity, robustness and perceptibility of the method.

Digital watermarking can also be characterized by its robustness and fragility. Robust watermarking is resistant to possible attacks such as image processing. Fragile watermarking can be easily destroyed or undetectable after modification is done on the image. Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes[9]. A fragile watermarking scheme detects any manipulation made to a digital image to guarantee the content integrity while a robust scheme prevents the watermark removal unless the quality of the image is greatly reduced.

There are various types of watermarking schemes that use different types of domains to ensure protection of medical images and perform recovery of a tampered image[32]. Watermarking techniques can be classified according to where the watermark is embedded namely spatial domain and transform domain.

Spatial domain: One of the most straight forward and simple techniques is to embed the watermarking into the least significant bits of the image. Since the last binary bits are the least significant bits, its modification will not be perceived by the human eye. This technique is not as robust as the transform domain technique and rarely survives various attacks.

Transform domain: Most of the transform domain techniques embed the information into the transform coefficients of the cover image. DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) are the three popular methods in this category. The methods used need a certain amount of computation but can be reduced by compression and are more robust against geometric transformations such as rotation, scaling, transla-

tion and cropping.

In a watermarking application based on the DCT and DWT methods, it would be appropriate for a user to make a choice between DCT and DWT depending on the requirements of the watermarking system. If greater robustness is desired, DWT is more appropriate; however, if more fragility is required, DCT is more appropriate.

DWT separates an image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The whole process then can be repeated to compute multiple scale wavelet decomposition.

1.2. Attacks and Distortions

Watermarked image may be altered either on purpose or accidentally. The watermarking system should be robust enough to detect and extract the watermark similar to the original one[29]. Different types of alteration (distortions) which are known as attacks can be performed to degrade the image quality. The distortions are limited to those factors which do not produce excessive degradations in the image otherwise the transformed object would be unusable. These distortions also introduce degradation on the performance of the watermark extraction algorithm. To test for the robustness of the methods or a combination of the methods, an attack is performed intentionally on a watermarked document in order to destroy or degrade the quality of the hidden watermark. Compression is a common attack, as data transferred via a network is often compressed using JPEG, as high quality images like BMP images are often converted to JPEG images to reduce their size. Another method is deletion or shuffling of blocks. In images, rows or columns of pixels may be deleted or shuffled without a noticeable degradation in image quality. These may render an existing watermark undetectable. Salt and pepper noise is another type of attack that replaces the intensity levels of some of the pixels of an image resulting in loss of information from those pixels. Some of the popular attacks mentioned here may be intentional or unintentional, depending on the application. In this paper we have taken (a) *Salt and Pepper noise* and (b) *JPEG compression* as intentional attacks.

2. Proposed Methodology for Biomedical Image Watermarking

We have developed a new medical image watermarking scheme that uses multiple copies of information logo hidden in several bits of the cover image starting from lower order to higher order to hide the information logo in wavelet domain. Discrete wavelet transform (DWT) separates the image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The whole process is repeated to compute multiple scale wavelet decomposition. Here we generally hide several sets of the same information logo into the cover image. So even if some of the information is lost due to an attack, we

can still collect the remaining information from the cover image using the bit majority algorithm, described later, so as to reconstruct the hidden information resembling the original one very closely.

The embedding and recovery of information logo is analysed in detail as follows:

2.1. Embedding the Digital Watermark

Step 1: First, a gray scale medical image of size 256 X 256 or 512 X 512 is taken where we can hide the information logo. Then a binary image, basically a sequence of 0's and 1's, is taken as information or logo of size 16 X 16 or 32 X 32 as another input.

Step 2: Next, to make the program compatible to run for any size of the cover image and information logo, keeping in mind the data carrying capacity of the cover image, the dimensions of the respective images are extracted and stored in two variables.

Step 3: After normalizing the information logo, it is reshaped into one dimension.

Step 4: The cover image is then transformed to wavelet domain using Discrete Wavelet Transform (DWT) by application of the 'Haar' transform. Here, the 1st level DWT was used to obtain more capacity for hiding the information. The cover image is decomposed into 4 sub-domains as HH, HL, LH and LL according to different frequencies of the cover image.

Step 5: The length of the transformed cover image and information logo in one dimension is then calculated.

Step 6: The size of each decomposed sub-domain cover image is calculated and reshaped into one dimension.

Step 7: The maximum coefficient value of each of the 4 sub-domains is then determined.

Step 8: The position where the information logo can be hidden into the transformed cover image should be such that the position for hiding the binary logo in each sub domain must be between zero and the maximum coefficient value of that sub-domain.

Step 9: More than one set of the same information (8 sets in our case) is hidden in HL and LH bands or domains for easier and good quality recovery. The hiding process in each of these domains follows a specific formula. The black pixels in each set of the one dimension information logo are hidden in a position of the information logo from where a constant value is subtracted.

Step 10: Three secret keys are also hidden in the cover image which is used to recover the information. Here we use the row and column size of the information logo as two secret keys and the total number of black dots (0's) in the one dimension logo, which is actually the information to be hidden separately in the transformed cover image, as the third key.

Step 11: At the end, the decomposed image is reshaped back to its normal dimension and the watermarked image is written to a file for future use.

2.2. Recovery of the Embedded Watermark

We assume that the cover image hiding the watermark is available at the receiving end. So again, in the process of recovery we first take the original image that has been used to hide the information. Along with that we also send the receiver of the message, 3 keys which essentially act as private keys. These keys are required to decrypt and to extract the encrypted, embedded messages.

The steps in the recovery process are as follows:

Step 1: The watermarked and original image is taken at first as input.

Step 2: The first level decomposition of both the two inputs using DWT is to be found as we are using first level discrete wavelet transform (DWT).

Step 3: The size of each sub domain of both the decomposed cover and original image is to be found for further calculations.

Step 4: Decomposition of both the watermarked and original cover image is reshaped into one dimension.

Step 5: The two input keys are taken from the user equal to the dimension of the logo to find the size of the 4 decompositions of logo.

Step 6: The remaining input key from the user is taken which is the number of black dots that was hidden in the watermarked image.

Step 7: After that we have to determine the maximum coefficient values of the original cover image.

Step 8: Those positions are then found that were used to hide the logo for each of the 4 decompositions.

Step 9: Positional sets for different sets of the logo from each decomposition are extracted.

Step 10: Finally, different sets of logo are recovered from each of the sub bands using bit majority algorithm and the final logo is constructed from the different recovered sets.

Bit Majority Algorithm is a technique to find the closest twin by several comparisons between different sets of data. After recovering 8 different sets from the attacked watermarked image the best sets of pixel which are much closer to the original information logo are taken. The rest of the portions of black dots are replaced by white dots. For this every set of the recovered logo is checked with one another to find the similarity. From the obtained results it can be easily understood that the 8 recovered sets are practically not recognizable but the final derived logo is quite recognizable and the quality metrics also reflect the strength of this new algorithm.

3. Image Quality Metrics for Testing image Degradation

To measure the amount of visual quality degradation between the original and watermarked medical images different types of image quality metrics are used. In the present work we have used *peak signal-to-noise ratio* (PSNR) and *structural similarity index measure* (SSIM) for determining the quality measure[7,34].

3.1. Peak Signal-to-Noise Ratio (PSNR)

It is the ratio between the maximum possible power of a signal and the power of corrupting noise affecting the fidelity of image representation. PSNR is usually expressed in terms of dB for a wide range signals. The PSNR is most commonly used as a measure of quality of reconstruction of signal information undergoing lossy compression. The cover image in this case is the original data, and the information logo is the error introduced by watermarking. When comparing the deformed image with the original one an approximation to the quality of human perception of reconstruction is made. Therefore, in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR. A higher PSNR would normally indicate that the reconstruction is of higher quality.

PSNR is described in terms of the mean square error (MSE), which for two $m \times n$ monochrome images I and K is

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

where one of the images is considered a noisy approximation of the other.

The PSNR is then defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$

MAX_I is the maximum possible pixel value of the image.

When the pixels are represented using 8 bits per sample, MAX_I is 255.

3.2. Structural Similarity Index Measure (SSIM)

It is a method for measuring the similarity between two images. The SSIM index is a full reference metric. In other words, the measure of image quality is based on an initial distortion-free image as reference. SSIM is designed to improve on traditional methods like PSNR and MSE, which have proved to be inconsistent with human eye perception. The resultant SSIM index is a decimal value between -1 and 1, and where the value 1 is only reachable in the case of two identical sets of data. The SSIM metric is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

where μ_x is the average of x ; μ_y is the average of y ;

σ_x^2 is the variance of x ; σ_y^2 is the variance of y ;

σ_{xy} is the covariance of x and y ;

$c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ are two variables to stabilize the division with weak denominator;

L is the dynamic range of the pixel-values (typically this is $2^{\#bits \text{ per pixel}} - 1$); $k_1 = 0.01$ and $k_2 = 0.03$ by default.

Table 1. Watermark embedding and resulting quality metrics

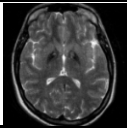

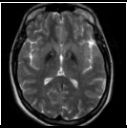
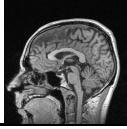

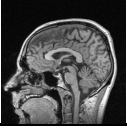
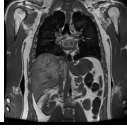

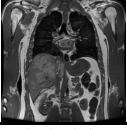
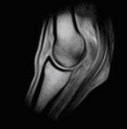

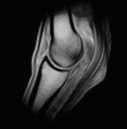



Cover image (256X256)	Message image (16X16)	Watermarked image	PSNR in dB	SSIM
			42.34	0.988
Brain CT	M Logo	Watermarked Brain CT		
			41.81	0.978
Side Face	R Logo	Watermarked Side Face		
			41.51	0.985
Abdomen MRI	JS Logo	Watermarked Abdomen MRI		
			42.16	0.981
Ankle Joint X-Ray		Watermarked Ankle Joint X-Ray		
			41.19	0.969
Knee Joint MRI		Watermarked Knee Joint MRI		

Table 2. Recovery of watermark from watermarked image without attack

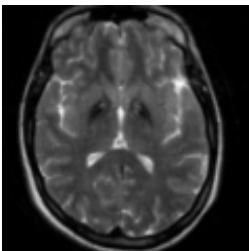









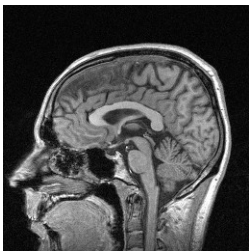









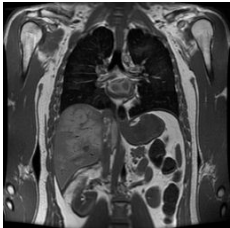









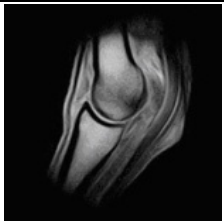



















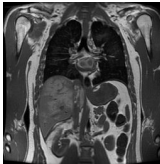
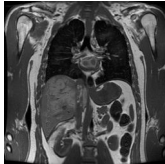








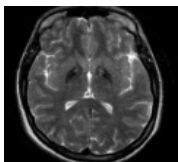
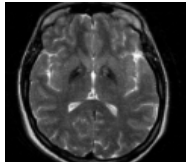









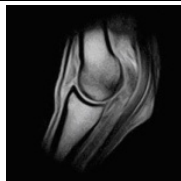








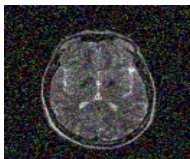
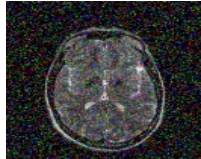


















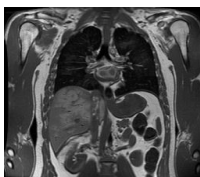
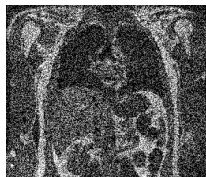


















Watermarked Image	8 different recovered sets and derived final logo using bit majority algorithm			
				
				
Watermarked Brain CT			SSIM	
			1	
				
				
Watermarked Side Face			SSIM	
			1	
				
				
Watermarked Abdomen MRI			SSIM	
			1	
				
				
Watermarked Ankle Joint X-Ray			SSIM	
			1	
				
				
Watermarked Knee Joint MRI			SSIM	
			1	

Table 3. Recovery of information from watermarked image under several attacks

Watermarked image (256X256)	Altered or Attacked Watermarked image	8 different recovered sets and derived final logo using bit majority algorithm			
					
Watermarked Abdomen MRI	2% JPEG compression				
					
Watermarked Brain CT	5%JPEG compression				
					
Watermarked Ankle Joint X-Ray	5%JPEG compression				
					
Watermarked Brain CT	20% salt & pepper noise				
					
Watermarked Side Face	30% salt & pepper noise				
					
Watermarked Abdomen MRI	40% Salt & Pepper noise				
					
Watermarked Knee Joint MRI	20% Salt & Pepper noise				

4. Results and Discussions

In this section several experimental results are given to demonstrate the outcomes of the proposed biomedical image watermarking technique.

In Table 1, five sets of biomedical cover images along with information logos and the obtained watermarked images are shown as the outcome of our proposed embedding technique. The calculated value of the quality metrics such as PSNR and SSIM are also given to find the image quality. It is impossible to distinguish between the watermarked image and the cover image by the Human Visual System as they look very similar. From the table 1 we can find the value of SSIM in all the cases is closer to 1 which is the proof of similarity or original and watermarked cover image. The values of the quality metrics also indicate that the watermarked images are quite similar to the original cover images without any distortions or visual deformities.

In Table 2, the successful recovery of hidden information from the unaltered watermarked image is shown under no attack. The recovered logos are visually similar to the original one. Moreover the SSIM value of Recovered logo is 1 which describe that it is identical with the embedded one.

But when the watermarked image is subjected to unauthorized attacks the results can lead to fuzziness of the information logo which is described in the next sets of image under some attack in Table 3.

In Table 3, results using the same recovery technique are shown on some more biomedical images like X-Ray, MRI, CT scan etc. under presence of attacks known as salt and pepper noise and JPEG compression. From this table it is clear that the proposed algorithm can withstand 40% salt and pepper attack and 5% JPEG compression attack with ease and the information logo that is recovered from the 8 different hidden sets using bit majority algorithm closely resembles the original information logo.

Table 4. SSIM Value for different sets of recovered information logo

Used Logo	Types of Attack	Amount of distortion	SSIM
M Logo	JPEG Compression	1%	0.9872
		2%	0.8731
		5%	0.7842
S Logo	JPEG Compression	1%	0.8975
		2%	0.8512
		5%	0.7689
K Logo	Salt and pepper Noise	20%	0.9432
		30%	0.9378
		40%	0.7664
R Logo	Salt and pepper Noise	20%	0.9532
		30%	0.9351
		40%	0.7762
JS Logo	Salt and pepper Noise	20%	0.9614
		30%	0.9182
		40%	0.7987

In Table 4, the quality metrics of different sets of recovered

logo are compared under different types of noise attacks. The SSIM index indicates that the proposed algorithm is quite efficient for salt and pepper noise up to 40% and JPEG compression up to 5% as the SSIM is close to 1.

5. Conclusions

Watermarking in medical images has a lot of potential. From the large capacity available for embedding, a lot more information can be added to the image to make it more secure. The relevance of watermarking for bio-medical image analysis has been analysed in Healthcare and Telemedicine. Access to or sharing of an isolated medical document requires that the document can be identified. It can be easily understandable that, as a compliment to all other modern security tools, watermarking can raise up the security level by detecting system failure, unauthorized manipulations and malicious actions. It provides an ultimate guarantee of data authentication or content protection that no other techniques ensure. Careful selection of the watermarking techniques should be made to guarantee the acceptability of this new technique in bio-medical field. Practically, there is a need for a robust and distortion-less method adapted for various medical imaging processes such as X-Ray, CT, USG, MR, etc. The most important aspect regarding watermarking for biomedical images is that the image is still conforms to the DICOM image format even after watermarking is carried out. Moreover, the capability to embed maximum amount of data without image quality degradation satisfies the criteria of frequent applications in bio-medical data protection, safety and management.

Our proposed biomedical image watermarking scheme includes procedures for data embedding, extraction and verification for image quality.

Experimental results show that such a scheme could embed a large payload while keeping the distortion level low. Besides, the original information (image) can be recovered at the receiver end whose integrity can be strictly verified. The obtained PSNR and SSIM values support the quality and satisfy the statistics of performance of the proposed algorithm.

ACKNOWLEDGEMENTS

It is my pleasure to express my heartiest thanks to all the faculty members of the Institute of Radio Physics and Electronics, University of Calcutta, Kolkata for their cooperation.

I am also thankful to all the faculty members of the Electronics and Communication Engineering Department of Guru Nanak Institute of Technology, Sodepore, Kolkata for their ungrudging support.

I am also very grateful to my family members for their continuous encouragement.

REFERENCES

- [1] F. A. Allaert and L. Dusserre, "Security of Health Sys-tem in France. What we do will no longer be different From what we tell," International Journal of Biomedical Computing, vol.35, no.Suppl.1, pp. 201-204,1994.
- [2] P.W. Wong, "A public key watermark for image verification and authentication", in Proceedings of the IEEE International Conference on Image Processing, Chicago, IL, October 1998, pp. 455-459.
- [3] D. Anand and U.C. Niranjana, "Watermarking Med-ical Images with Patient Information," in proc. IEEE/EMBS Conference, Hong Kong, China, Oct. 1998,pp.703-706.
- [4] A. Maeder and M. Eckert. Medical image compression: Quality and performance issues. SPIE: New Approaches in Medical Image Analysis, 3747:93-101, 1999.
- [5] M.L.Miller, I.J.Cox, J.M.G.Linnartz and T.Kalker, "A Re-view of Watermarking Principles and Practices," in Digital Signal Processing for Multimedia Syatems, K.K. parhi and T. Nishitani Eds.New York,1999,pp. 461-485.
- [6] F. Hartung and M. Kutter, "Multimedia watermarking tech-niques, "Proceedings of the IEEE, vol. 87, no. 7,pp. 1079-1107, July 1999.
- [7] M. Kutter and F. A. P. Petitcolas. A fair benchmark for image watermarking systems. In Proc. SPIE Security and Water-marking of Multimedia Contents, vol 3657, pp 226-239, San Jose, USA, Jan.1999.
- [8] B. Macq, F. Dewey, "Trusted Headers for Medical Images," in DFG VIII-DII Watermarking Workshop, Erlangen, Ger-many, 1999.
- [9] E.T.Lin, E.J.Delp, "A Review of Fragile Image Watermarks," in Proceedings of the Multimedia and Security Workshop ACM, Ed., Orlando, Florida, USA, Oct. 1999, pp.35-39.
- [10] P.Wong,"A watermark for image integrity and ownership verification, " Final Program and Proceedings of the IS&T PICS 99, pp. 374-379.
- [11] S.G. Miaou, C.H. Hsu, Y.S. Tsai, and H.M. Chao, "A Secure Data Hiding Technique with Heteroge-neous Data-Combining Capability for Electronic Pa-tient Records," in Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Health care Records, IEEE-EMB, Ed., Chicago, USA, July2000.
- [12] G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging," in Proc. IEEE Int. Conf. ITAB, USA,2000, pp. 250-255.
- [13] Kong, X. and Feng, R., 2001, "Watermarking Medical Sig-nals for Telemedicine," IEEE Trans on.Information Tech-nology in Biomedicine, vol. 5, no. 3, pp. 195-201.
- [14] X. Q. Zhou, H. K. Huang, S. L. Lou, "Authenticity and integrity of digital mammography images," IEEE Trans. on Medical Imaging, vol. 20, no.8, pp.784-791, 2001.
- [15] G. Coatrieux, B. Sankur, H. Maître, "Strict Integrity Control of Biomedical Images," in Proc. Electronic Imaging, Security and Watermarking of Multimedia Contents, SPIE, USA, 2001, pp.229- 240.
- [16] Johnson.N.F., Duric.Z., Jajodia.S., 2001, Information Hiding: Steganography & Watermarking-Attacks & Countermeasures' Kluwer Academic Press.
- [17] G. Coatrieux, B. Sankur, H. Maître, "Strict Integrity Control of Biomedical Images," in Proc. Electronic Imaging, Security and Watermarking of Multimedia Contents, SPIE, USA, 2001, pp.229- 240.
- [18] Rafael C Gonzalez and Richard E. Woods, Digital Image Processing, Prentice Hall, 2002, ISBN-81-7808-629-8.
- [19] J. Fridrich,M. Goljan and R.Du, Lossless Data Embedding for All Image Formats, Proc. SPIE Photonics West, Electronic Imaging,Security and Watermarking of Multimedia Contents, vol.4675, San Jose, Ca., USA, pp. 572-583,Jan. 2002.
- [20] Ling Na Hu,Ling Ge Jiang 'Blind Detection of LSB Water-marking, at Low Embedding Rate in Grayscale Images'. M. Celik, G. Sharma, E.Saber and A.Tekalp. Hierarchical wa-termarking for secure image authentication with localiza-tion.IEEE Trans.Image Process,pp.585-595, June2002.
- [21] Cox I. J., Miller M., Bloom J., 2002, "Digital Watermarking," Morgan Kaufmann Publishers.
- [22] Chao,H.M., Hsu, C.M. & Miaou,S.G, 2002, "A data-hiding technique with authentication, integration, and confidentiality for electronic patients records,"IEEE Transactions Informa-tionTechnology in Biomedicine, vol.6, no.1, pp. 46-53.
- [23] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "A medical image watermarking scheme based on wavelet transform," in Proc. of the 25th Annual Int. Conf. of the IEEE EMBS, vol. 1, 2003, pp. 856-859.
- [24] R. Acharya, U.C. Niranjana, S.S. Iyengar, N. Kannathal, L.C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," Computer Meth-ods and Programs in Biomedicine, vol. 76, pp.13-19, 2004.
- [25] G.T. Oh, Y-B. Lee, S.J. Yeom, "Security mechanism for medical image information on PACS using invisible water-mark," in Proc. Of Int. Conf. High Performance Computing for Computational Science, VECPAR, 2005, pp.315-324.
- [26] D. Osborne, D. Abbott, M. Sorell, and D. Rogers. Multiple embedding using robust watermarks for wireless medical images. In IEEE Symposium on Electronics and Telecom-munications, page section 13(34), Timisoara, Romania, Oct. 2004.
- [27] Shi Y. Q., "Reversible Data Hiding," IWDW 2004, Korea, Lecture Notes in Computer Science (LNCS) 3304, pp. 1-12.
- [28] F. Bao, R. H. Deng, B.C. Ooi, Y. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. on Information Technology in Bio-medicine, vol. 9, no.4, pp.554-563, 2005.
- [29] C.G. Boncelet, "The NTMAC for authentication of noisy messages," IEEE Trans. on Information Forensics and Secu-rity, vol.1, no.1, pp.320-323, 2006.
- [30] Zain, J.M.; Fauzi, A.R.M., "Medical Image Watermarking with Tamper Detection and Recovery", 28th Annual Interna-tional Conference of the IEEE Engineering in Medicine and Biology Society, 2006. EMBS, pp. 3270 -3273.
- [31] Giakoumaki, A.; Pavlopoulos, S.; Koutsouris, D., "Multiple Image Watermarking Applied to Health Information Man-agement", IEEE Transactions on Information Technology in

Biomedicine, Volume: 10 , no.4, Publication Year: 2006 , pp. 722 – 732.

- [32] Zain, J.M.; Fauzi, A.R.M., “Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)”, 29th Annual International Conference of the IEEE on Engineering in Medicine and Biology Society, 2007. EMBS 2007. pp. 5661 – 5664.
- [33] Kobayashi, L.O.M.; Furuie, S.S.; Barreto, P.S.L.M., “Providing Integrity and Authenticity in DICOM Images: A Novel Approach, IEEE Transactions on Information Technology in Biomedicine”, vol.13 , no. 4, Digital, Publication Year: 2009 , pp. 582 – 589.
- [34] Fallahpour, M.; Megias, D.; Ghanbari, M., “High capacity, reversible data hiding in medical images”, 16th IEEE International Conference on Image Processing (ICIP), 2009, pp. 4241 – 4244.
- [35] Siau-Chuin Liew; Zain, J.M., “Reversible medical image watermarking for tamper detection and recovery”, 3rd IEEE International Conference on Computer Science and Information Technology, 2010, vol. 5, pp. 417 – 420.
- [36] Velumani, R.; Seenivasagam, V., “A reversible blind medical image watermarking scheme for patient identification, improved telediagnosis and tamper detection with a facial image watermark”, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2010, pp.1 – 8.
- [37] Huang, H.; Coatrieux, G.; Shu, H.Z.; Luo, L.M.; Roux, C.; “Medical image integrity control and forensics based on watermarking — Approximating local modifications and identifying global image alterations”, Annual International Conference of the IEEE , Engineering in Medicine and Biology Society, 2011, pp. 8062 – 8065.