Reversible Fragile Medical Image Watermarking with Zero Distortion

Nagaraj V. Dharwadkar & B. B. Amberker
Computer Science & Engineering
National Institute of Technology, Warangal
Andhra Pradesh, India
nvd@nitw.ac.in, bba@nitw.ac.in

Supriya & Prateeksha B. Panchannavar
Information Science & Engineering
B. L. D. A's College of Engg. & Tech.
Bijapur, Karnatak, India
supriya046@gmail.com,prateeksha026@gmail.com

Abstract- The modern telemedicine often lacks in the infrastructure to deploy image security standards. The fragile watermarking scheme provides good security solution to medical images in telemedicine. In this paper, we present a reversible (distortion free), fragile, spatial domain watermarking scheme for medical images. The medical image authenticity and security can be achieved by two modes of watermarking operations. In the first mode, the watermark (fingerprint) is embedded into host image and later, for copy-right justification the watermark (fingerprint) is extracted from host image. In the second mode of the operation the watermark (fingerprint) is extracted from unaltered components of the image ie. stored as the key. Later, this key information is used for recovering the watermark. The proposed scheme uses the second mode of operation which extracts the watermark from the unaltered pixel components of image. The extracted watermark is used for copy-right justification. As medical images have zero tolerance for noise our scheme produces noise free watermarked medical images. The scheme is robust to different types of attacks. The fragility and robustness of the scheme is analyzed considering different types of image processing attacks.

Keywords- LSB, EPR, MSB, Reversible, Medical image watermarking.

I. INTRODUCTION

Internet has many applications like telemedicine, online-banking, teleshopping etc. One crucial application of the Internet is telemedicine, where healthcare professionals use the Internet for transmitting or receiving Electronic Patient Records (*EPR*) via e-mail. An *EPR* typically contains the health history of a patient, including X-ray images, CT-Scan images, physical examinations report, laboratory tests, treatment procedures, prescriptions, radiology examinations etc.[1]. An *EPR* can be represented in various forms such as diagnostic reports, images, vital signals, etc. An *EPR* transmitted through the Internet is very important since it contains the medical information of a person in digital format. The tampering of an *EPR* would embarrass the individuals. Thus, due to the rapid development of telemedicine the security of the medical images became important [2, 3]. In telemedicine, for the security and authenticity of medical images, encryption and watermarking approaches are used. In comparison with encryption, watermarking scheme supports multiple level of medical image integrity [4]. In image watermarking, the authentication information is embedded in to the image, later it is extracted to define the copy-rights of the author [7]. Most of the watermarking techniques modify or distort the host image inorder to embed the authentication information. Except telemedicine, all other image applications can tolerate the loss of image fidelity as long as the original and modified images are perceptually similar. In medical imaging applications, there are stringent constraints on image fidelity that strictly prohibit any permanent image distortion by the watermarking [4]. For instance, artifacts in a patient's diagnostic image due to image watermarking may cause errors in diagnosis and treatment, which may lead to possible life-threatening consequences.

Thus, to overcome the problem of occurrence of artifacts and to produce zero distorted or noise free watermarked medical images, we propose a new fragile medical image watermarking scheme based on the identification marks (fingerprints) of the image [5, 6]. This scheme uses pixel component of an image as the watermark (fingerprint). In this scheme, the watermark bits are matched by using the bit values of a pixel of the cover image. The information of these matched locations will be stored into two arrays. Later, these arrays are used to extract the watermark. Without these two arrays, it is tough to extract the watermark. Since the Least Significant Bits (*LSB*) of a pixel are sensitive to filtration and bit-flipping operations, this scheme uses the matching Most Significant Bits (*MSB*) of the pixel with watermark bits.

The rest of the paper is organized as follows. In Section II the related work in medical image watermarking is explained. The proposed watermarking scheme is explained in Section III. Section IV gives details of the experimental results. The comparison of the proposed scheme with Wang's fragile scheme is explained in Section V. Section VI concludes the paper.

II. RELATED WORK

For general image watermarking more schemes have been proposed but, a very few schemes are proposed for medical image watermarking. In 2001, Zhou et. al.[8] proposed a watermarking scheme for verifying authenticity and integrity of mammography image. This scheme uses digital envelope as watermark. In this scheme, the *LSB* of randomly selected pixel of the mammogram image is replaced by one bit of the digital envelope. The *MSB* of pixels are used for verifying integrity of the image. To reduce the storage and transmission overhead Acharya et. al.

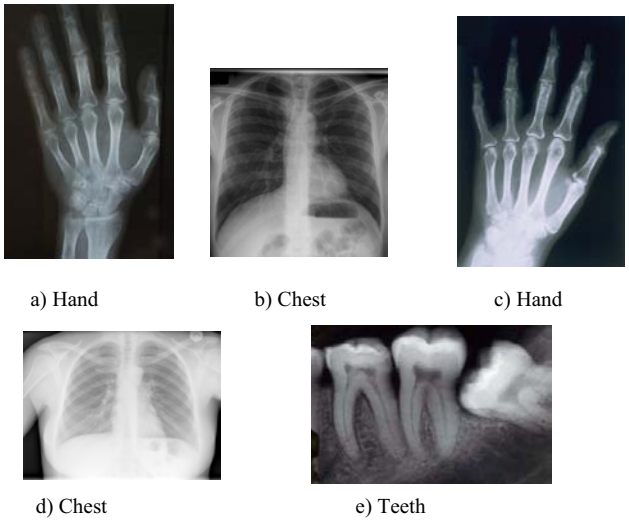
978-1-4244-9034-/10/$26.00©2010 IEEE

[9] proposed a scheme which uses the *LSB* based digital watermarking scheme for adding patient information to medical images. In 2002, Chao et. al. [10] proposes a Discrete Cosine Transform (*DCT*) based watermarking scheme which is capable of hiding *EPR* related data into a marked image. Another medical image watermarking scheme was proposed by Jagadish, N. et. al. [11] which embeds watermark in bit planes of the cover image. This scheme produces watermarked image with very low Normalized Root Mean Square Errors (*NRMSE*). The medical image watermarking schemes can be classified into different types based on various focus points. With the focus on the robustness of watermarked image the schemes are categorized as fragile, robust or semi-fragile. With the focus on perceptual degradation of cover image they are categorized as reversible and semi-reversible.

The fragile watermarking schemes are designed such that the watermark is destroyed if the watermarked image is tampered in the slightest manner. These schemes generally produce the imperceptible images with low degradation. These schemes are mainly used for medical image authentication. In 2001, Johnson et. al. [12] proposed fragile scheme which embed pseudo random sequences in the Least Significant Bit (*LSB*) plane. In this scheme the integrity and security of the image purely depends on pseudo random seed key. This scheme is more sensitive to bit stuffing attack. For assuring the high integrity of image, a public key self-embedding fragile image authentication scheme was proposed [13]. This scheme detects the localize alteration of image content. In 2009, Hideaki, et. al. [14] proposed asymmetric fragile watermarking which uses a number theoretic transform. In this scheme the signature data is extracted from watermarked image by determining the correlation functions which are computed using number theoretic transform. The security of this scheme decreases when the public key is altered. The robust medical image watermarking schemes are designed to resist the attempts to remove or destroy the watermark [15]. These schemes are widely used for copy-right protection and content tracking. More robust scheme [16] is proposed which uses the Fourier domain embedding technique for securing medical image. In this scheme the distortion occurs due to round-off errors and the robustness of this scheme depends on the size of the bit plane used. The semi-fragile schemes are less sensitive to change and are compatible to common operations like compression, scaling, filtering and rotation [17].

The medical tradition is strict with the quality of images; in this case it is not allowed to often modify the bit field values of the image. Thus the watermarking scheme must be reversible, where the original pixel values of the cover image must be recovered [18]. The distortions that occurred due to the watermarking should not interfere with the use of the watermarked object. Among the different approaches proposed for watermarking the medical images, the reversibility property allows the removal of the watermark from the image and the complete retrieval of the original image [19]. In 2009, P. Vishwanathan et. al. [20] proposed a semi-reversible watermarking scheme. This scheme embeds the watermark into medical image using text fusion method. In this scheme properties of semi-reversible watermarking are used to recover the original cover image.

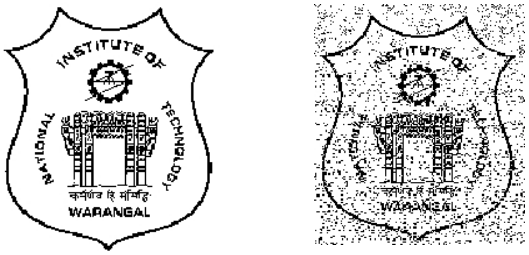
To overcome the problem of addition of artifacts and to provide a secured fragile watermarking for medical image. Our scheme uses the pixel component of the image content for image authenticity and security. In the following section the proposed model of the scheme is explained.



a) Hand b) Chest c) Hand

d) Chest e) Teeth

Figure 1. X-Ray medical cover images



a) Original Watermark b) Extracted watermark with NC=0.78

Figure 2. Watermark used

III. PROPOSED SCHEME

For the gray-level image, the intensity value of pixel is represented using 8 bits. The proposed scheme relies on binary stream of intensity of pixel to define space for embedding the watermark bits. We used the redundancy in binary stream of a pixel to achieve high embedding capacity. The bit values of pixel are used to match with the watermark bits. The matched locations of pixel are stored into two arrays. Later, these arrays are used to extract the watermark bits. Thus, our scheme produces zero distorted watermarked images.

Let's explain the scheme with a simple example. Assume we have cover image *I* and watermark image *W* of size 3×3

$$I = \begin{pmatrix} 35 & 20 & 10 \\ 15 & 25 & 30 \\ 50 & 40 & 60 \end{pmatrix} \qquad W = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Parameters	Cover image	Original watermark	Extracted watermark	Cover image	Original watermark	Extracted watermark	Cover image	Original watermark	Extracted watermark	Cover image	Original watermark	Extracted watermark	Cover image	Original watermark	Extracted watermark
															
MSE	0.0947			0.1153			0			0			0.1705		
PSNR	10.2261			9.3807			INF			INF			7.6825		
NC	0.9009			0.8830			1			1			0.8212		
SC	1.09			1.11			1			1			1.19		
NAE	0.0898			0.1023			0			0			0.1628		
AD	0.0786			0.0895			0			0			0.1425		
MD	1			1			0			0			1		

Figure 3: Sample cover images and extracted watermark

Blurring Factor	10	20	30	40	50	60	70	80	90	100
Original Cover image										
Blurred Image										
Extracted watermark										
NC	0.8045	0.7377	0.7071	0.6777	0.6434	0.5984	0.5540	0.5155	0.5823	0.5581
Original Cover image										
Blurred Image										
Extracted watermark										
NC	0.7453	0.6747	0.5971	0.5853	0.5946	0.6155	0.5749	0.5819	0.5959	0.6033
Original Cover image										
Blurred Image										
Extracted watermark										
NC	0.8487	0.8223	0.7180	0.6092	0.5712	0.6117	0.7424	0.5787	0.6560	0.6355
Original Cover image										
Blurred Image										
Extracted watermark										
NC	0.7114	0.7064	0.7052	0.7262	0.7414	0.7262	0.7048	0.6849	0.6697	0.6626

Figure 4: Effect of Blurring on watermarked images

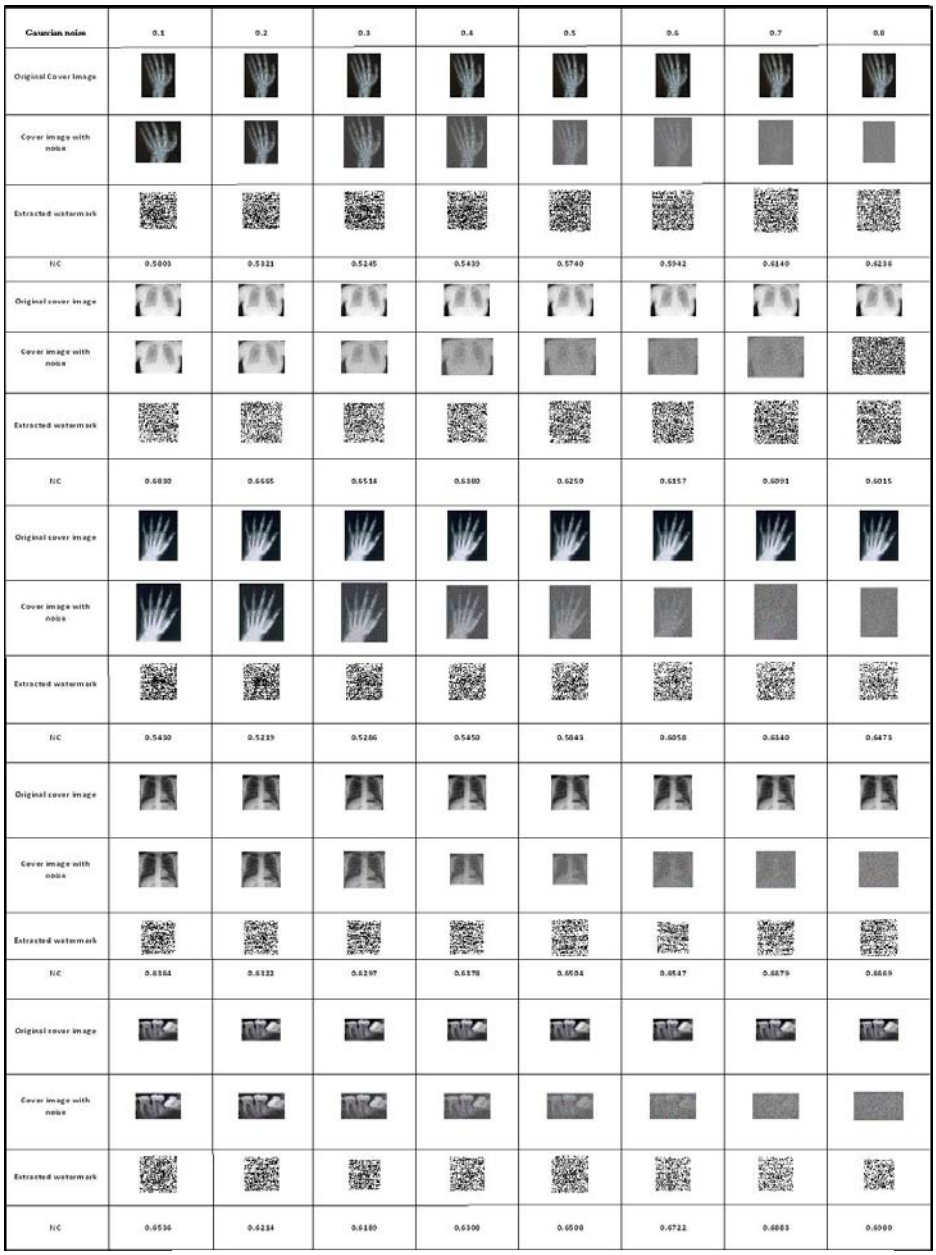


Figure 5: Effect of Gaussian noise on watermarked images

The output of embedding algorithm are the *LOCN* array that stores the locations of *MSB* bits from where the watermark bit occurs in binary stream of a pixel and the *ALTR* array that stores the decimal value of watermark bits if watermark bits doesn't occur in bit stream of a pixel or if single bit remains in the watermark. The output of embedding steps for cover image *I* and watermark *W* are as follows:

$$I = \begin{pmatrix} 35 & 20 & 10 \\ 15 & 25 & 30 \\ 50 & 40 & 60 \end{pmatrix} \qquad W = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$I(1,1)=35=(00100011)_2$,(a,b)=(W(1,1),W(1,2))=(1,0).Thus (a,b)=(1,0) will occur at 6th location of binary stream $(00100011)_2$ hence the *LOCN*(1)= 6. $I(1,2)=20=(00010100)_2$, $a=W(1,3)=1$ and $b=W(2,1)=1$ thus $(a,b)=(1,1)$ and this pattern doesn't occur in binary stream hence *LOCN*(2)=*0* then $ALTR(1)=(a, b)=(11)_2=3$. For $I(1,3)=10=(00001010)$, $(a, b)=(W(2,2), W(2,3)) = (0,0)$ hence *LOCN*(3) = 8. For $I(2,1)=15=(00001111)$ and $(a, b)=(W(3,1),W(3,2)) =(0, 1)$ hence *LOCN*(4) = 5. Finally for $I(2,2) =25 =(00011001)$ and

$W(3, 3)= a = 1$ only one bit then *LOCN*(5) = 99 and $ALTR(2) = W(3,3)=1$. Thus for entire 3×3 watermark image we have two arrays as *LOCN*= {6, 0, 8, 5, 99 } and *ALTR*= {3, 1}.

Algorithm 1: Embedding Algorithm

input : A Gray-level medical Image I of size $m \times n$ and Monochrome watermark W of size $p \times q$

output: A watermarked medical image of size $m \times n$, $LOCN$ array of size $\frac{1}{2}m \times n$ and $ALTR$ array of size v

$s = 1,\ t = 1,\ u = 1,\ v = 1$;
for $i \leftarrow 1$ **to** m **do**
  for $j \leftarrow 1$ **to** n **do**
    1) $X = I(i,j);\ a = W(s,t); b = W(s,t+1)$;
    2) $C = CONTAIN(X,a,b)$;
    3) **if** $C \neq 0$ **then** $LOCN(u) = C;\ u = u+1$;
    4) **if** $C == 0$ **then** $LOCN(u) = 0;\ u = u+1$;
       if $a == 0$ & $b == 0$ **then** $x = 0$;
       if $a == 0$ & $b == 1$ **then** $x = 1$;
       if $a == 1$ & $b == 0$ **then** $x = 2$;
       else $x = 3$;
       $ALTR(V) = x;\ v = v+1$;
    5) **if** $t \geq q$ **then** $s = s+1;\ t = 1;$ *continue* ;
       if $s > p$ **then** *exit* ;

The output of extraction steps from cover image I are explained as follows:

$I = \begin{pmatrix} 35 & 20 & 10 \\ 15 & 25 & 30 \\ 50 & 40 & 60 \end{pmatrix}$, two arrays as $LOCN$= {6, 0, 8, 5, 99} and $ALTR$= {3, 1}.

$I(1,1)$= 35 = $(00100011)_2$, $LOCN(1)$=6 and from binary stream (00100011) from *MSB* 6th position onwards the two bits of watermark are extracted ie. $W(1,1)$=1 and $W(1,2)$=0. For next pixel $I(1,2)$ =20 = (00010100), as $LOCN(2)$=0 the binary equivalent of $ALTR(2)$ = 3 represent the watermark bits hence $W(1,3)$=1 and $W(2,1)$=1. For $I(1,3$=10=(00001010), $LOCN(3)$=8 hence from *MSB* 8th position onwards the two bits of watermark are extracted ie. $W(2,2)$=0 and $W(2,3)$=0. For $I(2,1)$=15=(00001111), $LOCN(4)$=5 hence from 5th position of *MSB* bits the watermark bits extracted as $W(3,1)$=0 and $W(3,2)$=1. Finally for pixel $I(2,2)$=25=(00011001) and $LOCN(5)$=99 thus $W(3,3)$=$ALTR(2)$=1. The complete recovered watermark is

$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$

Algorithm 2: $CONTAIN(X,a,b)$

Result: Returns the location of occurrence of watermark bits into X else returns 0 if does not occurs

X=BINARY(X); i=StrLength(X); Locn=0;
while *not at beginning of X* **do**
  read X(i);
  if *X(i)* == *a* & *X(i-1)*== *b* **then** *Locn=i; exit* ;
end
return Locn

IV. RESULTS

Series of experiments have been conducted to evaluate the effectiveness of the proposed watermarking scheme. The evaluation of algorithm is performed based on two different points of view: invisibility and fragility. In these experiments the monochrome watermark of size 192×168 is embedded into medical cover images of varying size.

Figure 1 shows the cover images used in the experiments. As we are not changing the cover content, after embedding the watermarked image is perceptually similar to the original image. Figure 2 shows the original watermark and the extracted watermark from the image. Figure 3 shows the table containing the set of cover images and the respective embedded watermark and the extracted watermark from the images. As shown in the Figure 3 the difference between the original watermark and extracted watermark is computed using (Peak Signal to Noise Ratio) *PSNR*, (Mean Square error) *MSE*, (Normalized Cross-correlation) *NC*, (Standard Correlation) *SC*, (Normalized Absolute Error) *NAE*, (Average Difference) *AD* and (Maximum Difference) *MD*. The extracted watermarks from all cover images are having *NC* equal to 1. The fragility of algorithm can be assessed by using similarity measurement *NC* between original watermark and extracted watermark. This *NC* defines the normalized cross-correlation between original watermark and extracted watermark. For the detection of tampering, if *NC* is not equal to 1 we can conclude that the cover image was tampered during transmission. For any two images whose pixel values differ by a small scale factor will produce the *NC* value equal to 1, if the images are completely different the *NC* has a value lower than 1. For any two non-zero binary patterns which are different in all bits *NC* is -1. Thus the value of *NC* represents the Cosine of angle between two images. The angle between image varies from $0°$ to $180°$ and the corresponding *NC* varies between 1 and -1. Figure 4 shows the table containing the tampered cover images using the image blurring operation. Due to the effect of blurring, the correlation between the extracted watermark and original watermark is less than 1. Figure 5 shows the effect of Gaussian noise on watermarked images. Here also

Algorithm 3: Extraction Algorithm

input : A Gray-level medical Image I' of size $m \times n$, $LOCN$ array of size $\frac{1}{2}m \times n$ and $ALTR$ array of size v

output: Monochrome watermark W' of size $p \times q$.

$s = 1,\ t = 1,\ u = 1,\ z = 1$;
for $i \leftarrow 1$ **to** m **do**
  for $j \leftarrow 1$ **to** n **do**
    1) *X=I(i,j)* ;
    2) **if** $LOCN(u) \neq 0$ **then**
       $W'(s,t) = MSB(X, LOCN(u))$ *and*
       $W'(s,t+1) = MSB(X, LOCN(u)-1)$;
       u=u+1;
    3) **if** $LOCN(u) == 0$ **then**
       tmp=$ALTR(z)_2$; $W'(s,t) = MSB(tmp)$ *and*
       $W'(s,t+1) = LSB(tmp)$;
       z=z+1;
    4) **if** $t \geq q$ **then** $s = s+1;\ t = 1;$ *continue* ;
       if $s > p$ **then** *exit* ;

due to the addition of Gaussian noise the *NC* between the original watermark and extracted watermark is always less

than 1. From experiments and analysis, we conclude that the algorithm is highly fragile such that applying any image processing operation on the cover image will change *NC* value.

V. COMPARISONS

Table I shows the comparison of proposed scheme with Wang's [21] reversible fragile scheme. The Wang's scheme embed the watermark into cover image and this adds the noise to cover image which is computed by *PSNR*=60.76 between original image and watermarked image. But in our scheme the watermark is marked into separate array which does not add any noise to cover image. Thus the *PSNR* in our scheme will be infinity. The number of bits that can be embedded in our scheme is 2 bits/pixel. The security of proposed scheme is based on the security of Location and Altered array. The tampering of medical image is decided by calculating the *NC* between original watermark and extracted watermark.

TABLE I. COMPARISON OF PROPOSED SCHEME WITH WANG'S FRAGILE SCHEME

Properties	Wang's scheme	Proposed Scheme
Type of Scheme	**Reversible and Fragile**	**Reversible and Fragile**
PSNR between original and watermarked cover image	**60.76 dB**	**Infinity**
Embedding capacity	**---**	**2 bits/pixel**
Embedding method	**LSB**	**First MSB then LSB bits of pixels**
Security	**Hash function and DWT**	**Location and Alter array**

VI. CONCLUSION

We have proposed a new fragile medical image watermarking scheme. The watermark bits of image are matched adaptively with gray-level medical image bits. The embedding algorithm produces zero distorted or noise free medical image. The security to the watermarking scheme is improved by Location and Altered arrays. Without complete knowledge of these two arrays the watermark will not be extracted. In this scheme, we achieve maximum embedding capacity of 2 bits/pixel. As the watermark is marked considering only *MSB* bits of pixel, hence the scheme is rigid to frequent image processing attacks like *LSB* bit flipping. As the proposed scheme is fragile, it detects image tampering that may occur during medical image transmission. The security of the proposed scheme can be further increased by mapping the watermark to the pseudo random array using the secret key.

REFERENCES

[1] Shigekoto Kaihara, Realization of the computerised patient record: Relevance and unsolved problems, Elseviers, International Journal of Medical Informatics, vol. 49, issue 1, pp.1-8, 1998.

[2] Kong Xuan, Feng Rui, Watermarking Medical Signals for Telemedicine, IEEE Transactions on Information Technology in Biomedicine, vol .5, issue 3, pp.195-201, 2001.

[3] F.Cao, H.K.Huang, X.Q.Zhou, Medical image security in a HIPAA mandated PACS environment, Computerized Medical Imaging and Graphics, vol. 27, issue 2, pp.185-196, 2003.

[4] Jasni M Zain, Abdul R M Fauzi, Azian A Aziz, Clinical Evaluation of Watermarked Medical Images, Proceedings of the 28th IEEE EMBS, Annual International Conference, pp.5459-5462, 2006.

[5] Jin S. Seo, Jaap Haitsma, Ton Kalker, Chang D. Yoo, A robust image fingerprinting system using the Radon transform, Elsevier, Signal Processing: Image Communication, vol. 19, pp.325-339, 2004.

[6] Houtan H. L., Gholamali R. R., A New Spatial Domain Algorithm for Gray Scale Images Watermarking, IEEE International Conference on Computer and Communication Engineering, pp.157-161, 2008.

[7] I.J. Cox, M.L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Second edition, Morgan Kaufmann Publishers, 2008.

[8] Zhou X.Q., Huang H.K. and Lou S.L., Authenticity and integrity of digital mammography images, IEEE Transactions on Medical Imaging, vol. 20, issue 8, pp.784-791, 2001.

[9] Rajendra Acharya, U. Acharya, D. Subbanna Bhat, P. Niranjan, U.C., Compact storage of medical images with patient information, IEEE Transactions on Information Technology in Biomedicine, vol. 5, issue 4, pp.320-323, 2001.

[10] H.M. Chao, C.M. Hsu and S.G. Miaou, A data-hiding technique with authentication, integration, and confidentiality for electronic patients records, IEEE Transactions Information Technology in Biomedicine, vol. 6, issue 1, pp.46-53, 2002.

[11] Jagadish, N., Subbanna Bhat, P., Acharya, R., Niranjan, U. C. , Simultaneous storage of medical images in the spatial and frequency domain: a comparative study. Biomedical Engineering, BioMedical Engineering OnLine, vol. 3, issue 1, pp.1-10, 2004.

[12] Johnson, N. F., Duric Z., and Jajodia S. Information Hiding: Steganography and Watermarking Attacks and Countermeasure, Journal of Electronic Imaging, vol.10, issue 3, pp.825-826, 2001.

[13] Ammar M. H., Yassin M. Y. H., Ayoub Al-H, Mohamed A. A., Bernd M.,A novel public key self-embedding fragile watermarking technique for image authentication, 16th IEEE International Conference on Image Processing, (ICIP 2009), pp.1261-1264, 2009.

[14] Hideaki T., Tsuyoshi Y., Asymmetric Fragile Watermarking Using a Number Theoretic Transform, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E92-A, issue 3, pp. 836-838, 2009.

[15] Lin, T., Podilchuk, C. I., and Delp, E. J., Detection of image alterations using semi-fragile watermarks. In Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II, vol. 3971, pp.152-163, 2000.

[16] Jasni M. Zain, Abdul R.M. Fauzi, Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR), Proceedings of the 29th Annual International Conference of the IEEE EMBS, pp.5661-5664, 2007.

[17] HU yu-ping, Wavelet Domain Semi-fragile Watermarking Algorithm for Image Authentication, Acta Electronica Sinica, vol. 34, no.4, pp.653-657, 2006.

[18] B. Macq and F. Deweyand, Trusted Headers for Medical Images, DFG VIII-DII Watermarking Workshop, Erlangen, Germany, Oct. 1999.

[19] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, A review of image watermarking applications in healthcare, IEEE International Conference, EMBS-EMBC, pp.4691-4694, 2006.

[20] P.Viswanathan, P.Venkata Krishna, Text fusion watermarking in Medical image with Semi-reversible for Secure transfer and Authentication, International Conference on Advances in Recent Technologies in Communication and Computing, pp.585-589, 2009.

[21] Wang Gang, Rao Ni-ni, A Fragile Watermarking Scheme for Medical Image, Proceedings of the 2005, 27th IEEE Engineering in Medicine and Biology, pp.3406-3409, 2005.