TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 15, No. 3, September 2015, pp. 544 ~ 553
DOI: 10.11591/telkomnika.v15i3.8432

Analysis of Secure Medical Image Communication with Digital Signature and Reversible Watermarking

A. Umamageswari[1], G.R. Suresh[2]
[1]Department of Computer Science and Engineering, Sathyabama University, Chennai
[2]Department of Electronica and Communication Engineering, Easwari Engineering College, Chennai

Abstract

Protection of Medical image contents becomes the important issue in computer network security. Lossless Watermarking has becomes a promising technique for medical content authentication, it allows to embed relevant information with the image, which provides confidentiality, integrity and authentication by embedding Digital Signature (DS) with the Medical image. In this paper we focus on need for reversible watermarking, Medical Image Compression and security related problems in medical images, it comparing the performances of various lossless watermarking techniques for various medical image modalities like MRI (Magnetic Resonance Imaging), US (Ultrasonic), CT (Computed Tomography), Endoscopic and Angiographic images. Region of Interest (ROI) supporting lossless watermarking systems only considered for discussions. Performance of all lossless watermarking with Digital Signature is analyzed by means of four parameters Capacity Rate, PSNR (Peak Signal to Noise ratio), NPCR (Number of Pixel Change Rate) and Compression Ratio (CR). This Paper also introduces new mechanism for open network security for medical images. This lossless watermarking is responsible for recovering the altered medical image content of the system.

1. Introduction

Medical image sharing through internet becomes very popular nowadays to make telediagnosis, telesurgeries and teleconsultation. Digital image watermarking is a relatively new approach in HIS (Hospital information System), which is highly suitable for medical, military, and archival based applications. Secret embedding of the watermark signal, no matter how much invisible it may be, can cause degradation to the resultant image quality. Therefore, reversible watermarking is applied which is able to overcome this drawback by applying a mechanism that can provide the exact original image after the watermark has been successfully extracted. Traditional approaches such as cryptography can also perform this reversibility operation but the basic shortcoming is the loss of semantic information of the host image, i.e., after encryption the image may not be visible/understandable, which is not the case in watermarking. Enforcing content protection using classical approaches are not suitable nowadays, so it is necessary to develop the new techniques to improve the security of medical images. The security of the medical images is purely based on the following things. (i) Confidentiality (ii) Integrity (iii) Authentication [1-3].

Confidentiality*:* The protection of data from unauthorized disclosure. It means that only the entitled users have access to the information.

Integrity*:* The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion or replay).

Authentication*:* The assurance that the communicating entity is the one that it claims to be. A proof that the information belongs indeed to correct patient.

To provide the above security to the contents embedded into the image and also to the image, ancient days we have used watermarking, digital fingerprint, encryption and digital signature algorithm. But all the above methods having some disadvantages [2]. Reversible or lossless watermarking has been proposed to overcome the disadvantages of the previous methods. In conventional watermarking we can get the watermarkback but we cannot get the original cover image. In reversible watermarking the assigned watermark is embedded into the original and also can recover the original image from the suspected image. The retrieved watermark can be used to determine the ownership by comparing the retrieved watermark with the assigned one [4].

Received May 12, 2015; Revised July 6, 2015; Accepted July 30, 2015

Since 1999s several Reversible watermarking techniques has been proposed with Digital Signature concepts. In those papers they have introduces lot of reversible watermarking methods with allowable distortion in medical images, which is expressed in terms of Capacity Rate (bpp) PSNR in dB for various medical image modalities like MRI (Magnetic Resonance Imaging), US (Ultrasonic), CT (Computed Tomography), Endoscopic and Angiographic images.

After embedding the watermark inside into an image, image quality can be calculated by Peak Signal to Noise Ratio (PSNR) using ROOT Mean Square Error (RMSE) and compression Ratio. Compression Ratio and PSNR should be maximum for better quality image [5, 6]. Compression Ratio can be calculated by the ratio between the size of the image before compression and size of the image after compression [7, 8].

$$CompressionRatio = \frac{SizeoftheOriginalImage}{SizeoftheCompressedimage} \quad (1)$$

The quality of the watermarked image is measured by PSNR. Bigger in PSNR better in quality of watermarked image. PSNR for image with size M×N is:

$$PSNR(I,Iw) = 10log_{10}(((2^p - 1)^2|MSE)) \quad (2)$$

$$MSE = \frac{1}{MN}[\sum_{i=0}^{M}\sum_{j=0}^{N}[\tilde{f}(m,n) - f(m,n)]^2] \quad (3)$$

Where f (m, n) is pixel gray values of the original image.f[1] (m, n) is pixel gray values of watermarked image. NPCR (number of Pixel Change Rate) becomes a widely used security analyses in the image encryption community for differential attacks [24].

Number of Pixel Change Rate (NPCR):

$$NPCR = \frac{\sum_{i,j} D(i,j) \times 100\%}{T} \quad (4)$$

Where, Suppose ciphertext images before and after one pixel change in a plaintext image are C1 and C2, respectively; the pixel value at grid(i,j) in C1 and C2 are denoted as C1(i,j) and C2(i,j); and a bipolar array D is defined in Equation (5).

$$D(i,j) = \begin{cases} 0, if C^1(i,j) = C^2(i.j) \\ 1, if C^1(i,j) = C^2(i,j) \end{cases} \quad (5)$$

T represents the total number of pixels in the image.

The rest of this paper is organized as follows. Section 2 discusses the Integrity verification by various Reversible watermarking methods using Digital Signatures, Various Compression algorithms; Section 3 discusses the Performance analysis. The paper concludes in section 4.

2. Existing Methodologies

2.1. Integrity Verification by Various Digital Signatures in Reversible Watermarking

Strict authentication can be achieved by using cryptographic hash functions [9]. Hash functions accepts a variable size message m as input and produces the fixed size output referred to as hash code H(m). A hash code does not use a key but it is a function only of the input message. These hash codes also referred as a message digest or hash value. Such a cryptographic hash functions can be used to produce the digital signature, to this algorithm we are giving input as a medical image we want to communicate, for the entire image the hash code can be chosen by using any of the hash algorithm like MD5, SHA 1, SHA-256, SHA-512 and RIPEMD-160. The strength of the hash function against brute force attack depends only on the length of the hash code produced by the algorithm (if the length of MD is long then strength is also very high). The generated Digital Signature is encrypted using any of the encryption algorithm to create the Digital Signature (DS). For encryption purpose definitely we should use public key cryptographic techniques than Symmetric key cryptography to increase achieve the higher level of authentication.

The RSA (Rivest-Shamir-Adelman) algorithm [10] has since that time reigned supreme as the most widely accepted and implemented general purpose approach to public-key encryption. This is a block cipher in which a plain text and cipher text are integers between 0 and n-1 for some n. To this algorithm we can give hash value of an image as an input. This uses two different keys for encryption and decryption. One of these two keys is acts as a public-key, known to other user also, and second key is a private key used for reverse process. If private key is used for encryption with the confidentiality we can increase the authentication also [11, 12], then the public key of the sender key can be used for decryption because these two keys are related together. If the public-key of the sender is used for encryption then anyone can able to read the message happily, so only the sender is using its private-key for encryption. The hash value generated by using MD5, SHA 1 or RIPEMD- 160, which is given as a input to RSA public-key cryptographic algorithm to produce the digital signature[13].

Figure 1. Creation of Digital Signature

A digital signature is usually stored in the header of the DICOM (Digital Imaging and communication in Medicine) image file. When we share the image, the image file will be lost after converting it into another format for representation like JPEG. For the avoidance of loss of information only they have introduced Reversible or lossless watermarking in Region of Non-Interest (RONI). This DS is computed over the input medical image. We use this signature to verify the reliability of the information. The difference between the signature and the reconstructed will indicate the information has been corrupted during transmission. The combination of Patient information, Disease information EMR (Electronic Medical Record) and DS is called as Watermark. This watermark is embedded inside the image using reversible watermarking in the sender side. In the receiver side the signature and patient and disease information is extracted from the suspected image and hash value of the original image is also computed in the receiver side because we used reversible watermarking, the hash value is encrypted to find the digital signature then this DS is compared with the Signature extracted from the suspected image, If these two signatures are same we can say that no alteration in the suspected image during transmission. So we can maintain integrity, authenticity and Reliability over medical images during communication with high robustness.

2.2. Reversible Watermarking

Lossless watermarking has a special feature that the original digital watermark can be completely restored [14]. This feature is suitable for some important media such as medical and military images, because these kinds of media do not allow any losses. It will satisfy all the requirements of conventional watermarking such as robust imperceptibility and using embedding and retrieval, it also provides blind and higher embedding capacity. The goals of lossless watermarking are to protect the copyrights and can recover the original image. We are mainly having two schemes in reversible or lossless watermarking, spatial domain techniques and Transform domain techniques. Spatial domain only suitable for medical image watermarking, it supports two schemes (i) Additive insertion (ii) Substitutive Insertion (LSB Method) [15, 16].

In additive scheme the watermark w to be embedded is embedded in to the original image (host). $I_w = I + w$ (It is fully based on signals). The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or some times floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of di□erent keys will be very low. The noise should not correlate with the content of the image either. Assuming that we want to embed binary stream W □ {0,1} into original signal I.

Where,

I w=Watermark image
I = Original Image
W = Watermark
In Substitutive insertion the basic LSB scheme removes the pixels least significant bits by bits of the message to be embedded.

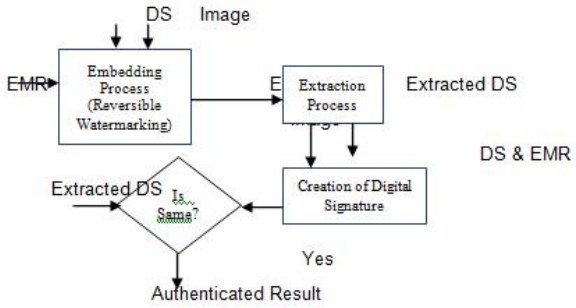

Figure 2. Embedding and Extraction Procedure

The method relies on the manipulation of LSBs of images, in a manner which is undetectable and imperceptible to human eyes. In some applications instead of discarding LSBs of original image, the LSBs are compressed with some lossy compression such as Run length algorithm (RLE) or Arithmetic Encoding to save the space for embedding the watermark. The LSB substitution method is very simple to implement and does not produce any significant distortion in the watermarking image.

2.3. Medical Image Compression

Compressing the medical image is more important before embedding digital signature and watermark into it, because through the internet we are trying to transfer our image with data, since our internet is very busy network we should use the bandwidth effectively, so only we are introducing compression. If we compress the image after embedding then there is a major collapse between the original image, watermark and digital signature to avoid this we should introduce the compression before embedding [17]. There are two compression techniques (i) Lossy Compression (ii) Lossless Compression. In Lossy compression, In this compression there is loss of information and the original image is not recovered exactly. In Lossless Compression, The goal of lossless image compression is to represent an image signed with the smallest possible number of bits without loss of any information; it reproduces the original image without any quality loss. Medical Images are captured in large amount and stored. There are several lossless image compression algorithms for the applications of compressing medical images. In this lossless JPEG, JPEG-LS, JPEG 2000, PNG and CALIC are tested as an image data set. Comparing all, JPEG-LS are the algorithm with best performance with compression ratio and compression speed [18]. Here an image set of 382 medical images which are organized to 20 groups according to [19] is taken. In this study we have characterized the various compression algorithm and implementation.

2.3.1. Lossless JPEG

This describes the predictive image compression algorithm with Huffman or arithmetic entropy coder [20].

2.3.2. JPEG-LS

This describes low complexity image compression algorithm with entropy coding and the algorithm used is LOCO-I. This is developed with the aim of providing low complexity lossless and near lossless image compressions.

2.3.3. JPEG-2000

This describes the algorithm based on wavelet transform image decomposition and arithmetic coding. This supports both lossy and lossless compression, this produce higher quality final image.

2.3.4. PNG

This describes a predictive image compression algorithm using LZ77 and Huffman coding.

2.3.5. CALIC

This describes Arithmetic Entropy codes which has high compression ratio. When tested with all these algorithms JPEG2000 and JPEG-LS has best Compression Speed (CS) and Compression Ratio (CR).

3. Performance Analysis

Performances of the various algorithms in reversible watermarking can be compared with various modalities like MRI (Magnetic resonance imaging), US (Ultrasonic), CT (Computed Tomography), Endoscopic and angiographic images by using their capacity rate (C) and Peak to Signal Noise Ratio (PSNR) value. We tested 50 medical gray level images of various modalities like MRI, CT and US that had been saved in 512×512×8 JPEG format. The images had been acquired from the DICOM standard. Capacity Rate is number of bits in the image divided by the number of pixels in the image. C should be minimum Image and PSNR should be maximum for better quality image. In all these methods image distortion has beenpresent due to only compression not based on reversible watermarking techniques. Table 1 shows the PSNR value according to the capacity rate for various reversible watermarking with digital signature techniques.

Table 1. PSNR of Various Reversible watermarking Techniques

Sl.NO	Methods Used	Power (kW)
1	Reversible Watermarking	49.11
2	Lossless watermarking with DSA	48.51
3	Reversible watermarking with SHA-256	41.00
4	Reversible watermarking with RSA approach	51.52

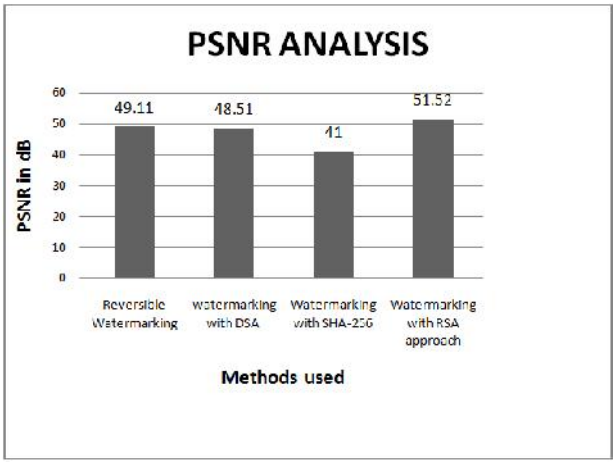

Figure 3. PSNR Analysis

Table 2 compares the PSNR value of various Capacity rate in different modalities. From the figure we can say that if Capacity rate increases there is a decrease in PSNR value in all the three modalities. Normally in CT images PSNR value is high when compared to other two

modalities if PSNR increases then also there is very low variation in PSNR with accepted compromise of distortion in an image. They achieved 97.27 dB PSNR for 0.13 bpp Capacity rate and 85.87dB as a PSNR for 0.21 bpp Capacity rate.

Table 2. Average PSNR and Capacity Rate of Various Reversible Watermarking Techniques over different modalities

Image Modalities	No of Images	Capacity Rate in bpp	PSNR in dB
US	79	0.05	52.60
	80	0.22	48.44
	99	0.49	40.58
MRI	79	0.02	72.4
	80	0.19	64.29
	99	0.26	59.02
CT	79	0.13	97.27
	80	0.20	87.87
	99	0.21	85.87

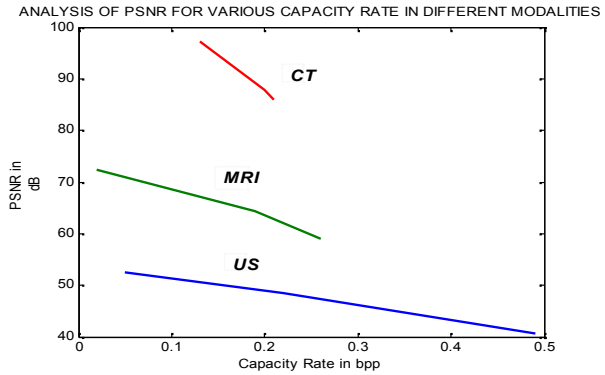

Figure 4. Analysis of PSNR for various Capacity Rate in different Modalities

If capacity rate is highly increased in all the three modalities then obviously image quality gets decreased because of very high distortion in reconstructed image. In MRI images they have achieved up to 72.4 dB as a PSNR value for 0.02 bpp capacity rate and 59.02 dB for 0.26 bppcapacity rate. In US images we can increase the capacity rate highly but there is a small variation in PSNR. They achieved 52.6 dB for 0.05 bpp capacity rate and 40.58 dB for 0.49 bpp capacity rate. Figure 3 shows the Graphical representation of PSNR Analysis and Figure 4 shows the graphical representation of Table 2.

4. Proposed Methodology

Existing methods used already existing algorithms for the generation of DS and embedding process. Following are the issues in the existing systems. Digital signature (DS) is transmitted with the image as a separate file or the image header, and hence there is a risk of losing the DS during transmission. If watermark is embedded in the ROI, then sensitive information will get lost. DS will be lost, if the image file is converted to another format. If we use DES, Block Ciphers, RC4, LFSR, RC5 etc. for creation of digital signature, then we cannot avoid some attacks like brute force attack etc. Attack tests like adding noise, signal distortion and different geometric operations (scaling, rotation, shearing etc.) performances were not satisfactory in existing methods.

4.1. Additive Hash Function (AHF)

This hash algorithm accepts the first row of the pixel mapped table of the original image as input and some confusion and diffusion are introduced mathematically to produce fixed length of output as a message digest value. The output message digest size will be of only 128 bits. The following algorithm explains the entire step by step procedure of AHF.

Step 1: Convert 512×512 image to pixel mapped table. Take the first row as separate table. (512 elements=4096 bits).
Step 2: Divide the 512 elements into 4 divisions namely x1 x2 x3 x4 each of 128 elements (128 elements=1024 bits).
Step 3: Add alternate sets. y1=x1+x3; y2=x2+x4
Step 4: Subtract y1 and y2, H1024=y2-y1
Step 5: Divide H1024 into 8 parts (128 bits) namely z1 z2 z3 z4 z5 z6 z7 z8.
Step 6: Add alternate values, each value of H has 16 elements=128 bits
H1=z1+z5 H2=z2+z6 H3=z3+z7 H4=z4+z8
Step 7: Add and subtract the alternate values of H.
Hashfinal1 = H3-H1 Hashfinal2 = H4+H2
Step 8: Add Hashfinal1 and Hashfinal2 to obtain the Hash128 value AHF = Hashfinal1+Hashfinal2, AHF has 16 elements=128 bits. Where AHF= Additive Hash Value or Message Digest

4.2. Creation of Digital signature

Authentication is maintained through the DS. This DS is computed over the input medical image. We use this signature to verify the reliability of the information. The difference between the signature and the reconstruction will indicate the information, which has been corrupted during communication. We planned a new approach named ACC or RSA to generate the DS hash value computed by SHA I (only first 128 bits of message digest) and AHF will be encrypted using ACC. The combination of electronic medical record (EMR) and DS is called watermark. This watermark is embedded inside the image using lossless modified difference of expansion technique at the sender side. At the receiver side the watermark is extracted from the suspected image.

Step 1: Obtain random number from server.
Step 2: Obtain hash from the image by using AHF.
Step 3: Use the random number as vignere substitution value.
Step 4: Change the hash key with respect to the random number.
Step 6: Now use this hash key as a prime text for play fair algorithm.
Step 7: Encrypt the patient details with the play fair algorithm.
Step 8: Use the encrypted hash key as digital signature.
In the actual execution, all values are 128 bit, which are 16 characters.

Vignere Vector = {1 2 3} Hash Value = {a b c}
a->1=b; b->2=d; c->3=f First level of encryption = BDF

B	D	F	A	C
E	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

DATA = NSCHAR NS ->SX CH->FK AR->DT Second Level of Encryption (Digital Signature) = SXFKDT

Hash value of the original image is also computed at the receiver side and then this hash value is encrypted using ACC or RSA to find the digital signature. If the computed DS is same as the digital signature extracted from the suspected image's watermark, then there is no alteration during the communication.When JPEG2000 is used for compression, lossless watermarking with DS is created using AHF and RSA approach and Kerberos is used for authentication, reliability and integrity maintenance.

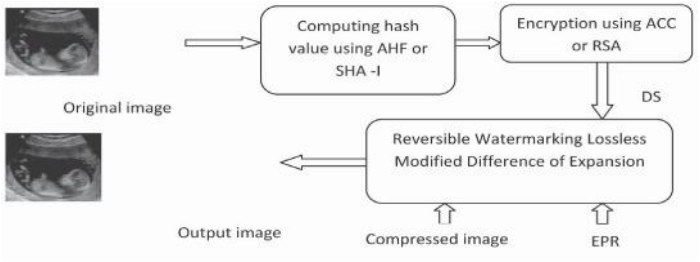

Figure 5. Embedding Process

Table 3. PSNR of existing and proposed work

Image	Payload(bpp)	Proposed Method	Existing Method	NPCR %
1	0.1	78.32	68.84	98.5
	0.25	76.17	67.72	99.2
	0.5	68.02	64.02	98.7
2	0.1	74.21	58.77	99.1
	0.25	72.02	55.46	98.6
	0.5	68.13	53.23	98.9
3	0.1	60.75	49.32	99.1
	0.25	65.23	52.17	98.7
	0.5	72.29	45.49	99.4

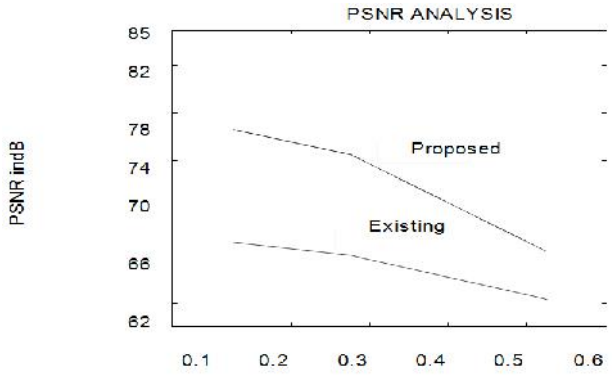

Figure 6. Comparative results of PSNR for existing

Table 3 shows the PSNR of existing and proposed methodologies of these 3 images, when capacity is 0.1 bpp, 0.25 bpp and 0.5 bpp. The parameter PSNR and NPCR are best in our proposed methodology, because in our 69.6 dB, almost in all of our 512×512 medical images with the embedding size of 64×64 images, we got 68.4 dB to 78.9 dB as the PSNR value and average NPCR is 98.9 %. From Table 3, we observe that the PSNR value of proposed method is better than existing, for increase in capacity rate. From figure 6 we can conclude that PSNR value is decreasing, when increasing the capacity rate. However, when compared to existing method, our method gives better quality reconstructed image with small amount of distortion in an extracted image. This distortion has occurred only because of the JPEG2000 compression. Compression ratio is also better in our JPEG 2000 compression algorithm, as it is up to 3.57.

4.3. Comparison of Algorithm

Figure 7 shows the performance analysis of various algorithms. Performance is recorded by using CPU-Z and the program was executed in matlab. So we have only proposed novel algorithms like ACC and AHF. It's execution time is less when compared to message digest 5 (MD5) and data encryption standard (DES).

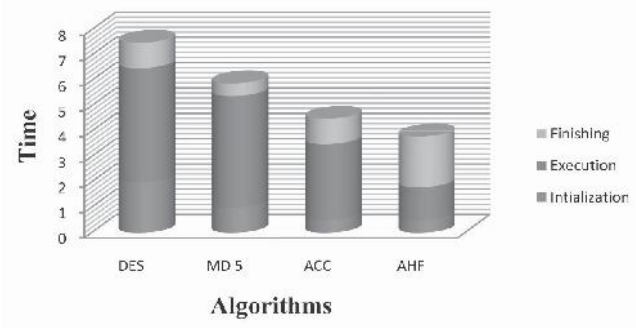

Figure 7. Performance analysis of various algorithms

5. Conclusion

Medical content authentication is very important to communicate medical images through internet. Medical image security system based on lossless watermarking to achieve authentication, reliability and integrity analyzed in this paper. How reversible watermarking working with compression techniques and compared image qualities for various modalities with their capacity rate and Peak noise to signal ratio. In future we can introduce new algorithm for Digital Signature creation to improve the Security. Still no paper has considered about the open network security, so we can propose new method to improve secure the medical content in open network during transmission.

References

[1] G coatrieux, H Maitre, B Sankur, Y Rolland, R Collorec. *Relevance of watermarking in medical imaging*. In proc, IEEE Int. Conf. ITAB. Arlington, VA. 2000: 250-255.
[2] G Coatrieux, L Lecornu, B Sankur, Roux. *A review of image watermarking applications in health care*. In proc, IEEE EMBS Annual international conf. New York City, USA. 2006: 4691-4694.
[3] Gouenou Coatrieux, Clara le Guillou, J Cauvin, Ch Roux. Reversible watermarking for knowledge digest embedding and reliability control in medical images. *IEEE transaction on information technology in biomedicine*. 2009; 13(2).
[4] G Coatrieux, M lamard, W Daccache, J Puentes, Ch Roux. *A low distortion and reversible watermarking application to angiographic images in the retina.* In proc. of the IEEE EMBC conf. Shangai, China. 2005: 2224- 2227.
[5] Baisa L Gunjal, Suresh N Mali. *ROI based embedded watermarking of medical images for secured communicationin Telemedicine*. In the International journal of Computer and Communication Engineering. 2012: 293-298.
[6] Imen Fourati Kallel, Mohamed Salim Barehlel, Jean-Christophe Lapayre. Improved Tian's Method for Meedical Image Reversible Watermarking. *GVIP.* 2007; 7(2): 1-7.
[7] Ma Li, Xiaoshi Zheng, Yanling Zhao, Huimin Wu, Shifeng Li. *Robust algorithm of Digital Image watermarking based on Discrete Wavelet Transform*. Electronic Commerce and Security, international Symposium. 2008: 942-945.
[8] Saied Q Amirgholipour kasmani, Ahmad Reza Naghsh-Nilchi. *A new Robust Digital Image Watermarking technique based on Joint DWT-DCT transformation*. Convergence and hybrid Information technology, 2008, ICCIT'08, Third International Conference. 2008; 2: 539-544.
[9] Jansi mahammad Zain. Strict authentication watermarking with JPEG compression for medical images. *European journal of scientific research.* 2010; 42: 233-241.
[10] R Rivest, A Shamir, l Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communication of ACM*. 1978; 21(2): 120-126.
[11] Shrikannde Rohini, Vinayak Bairagi. Lossless medical image security. *International journal of applied engineering research*. Dindigul. 2010; 1(3): 536- 541.
[12] William stallings. Cryptography and network security. 2010.
[13] Gouenou Coatrieux, Clara le Guillou, J Cauvin, L locarnu, Ch Roux. *Enhancing shared medical image functionalities with image knowledge digest and watermarking*. Presented in the IEEE EMBC conf. Int. Tech-nol. Appl. Biomed. Joannina, Greece, Oct. 2006.
[14] Jen-Bang Feng, Iuon-Chang Lin, Chewi-Shoyong Tsai, Yen-Ping Chu. Reversible watermarking: current status and key issues. *International Journal of network security.* 2006; 2(3): 161-171.
[15] X Wu, ZH Guan, Z Wu. A Chaos Based Robust Spatial Domain Watermarking Algorithm. Spring Verlog, LNCS. 2007; 4492: 113-119.

[16] F Sebe, T Domingo-Ferrer, J Herrera. Spatial Domain Image Wateramrking Robust Against Compression, Filtering, Cropping and Scaling. Springer Verlog, LNCS. 1975: 44-53.
[17] C Kim. Compression of Color Medical Images in Gastrointestinalendoscopy: A review. *Med.Informatics*. 1998; 9: 1046-1050.
[18] G Schaefer, R Starosolski, SY Zhu. *An evaluation of Lossless compression algorithms for medical infrared images.* In Proc. IEEE Eng. Med. Biol. Conf. 2005: 1673-1676.
[19] EFJ Ring, K Ammer, A Jung, P Murawski, B Wiecek, J Zuber, S Zwolenik, P Plassmann, C Jones, BF Jones. *Standardization of infrared imaging*. In I. 2004: 1183-1185.
[20] G Langdon, A Gulati, E Seiler. *On the JPEG model for Lossless image compression*. In 2nd Data Compression Conference. 1992: 172-180.