A New Cryptographic Digital Signature for Secure Medical Image Communication in Telemedicine

A.Umamageswari
Research Scholar
Department of CSE
Sathyabama University
Chennai

G.R.Suresh
Professor
Department of ECE
Easwari Engineering College
Chennai

ABSTRACT
Medical image security can be enhanced using the reversible watermarking technique, it allows us to embed the relevant information with the image, which provides confidentiality, integrity and authentication by embedding RSA encrypted digital signature with the image. Protection of Medical Image content is very much important for tele-diagnosis and tele-surgery. Our work proposes a novel algorithms AHF (Additive Hash Function) and RSA for the production of DS (Digital Signature) to achieve high confidentiality and Authentication. An image is compressed using JPEG2000 (DWT) algorithm and EPR (Electronic Patient Record) is embedded in RONI (Region of Non Interest) of compressed image using Lossless Watermarking Technique then shared through the open network. The PSNR (peak Signal to Noise ratio) value is up to 72dBs for 512×512 US(Ultrasonic) images. Increase in Authentication can be achieved when medical expert's access secured medical images from the web servers using Kerberos technique.

Keywords
Lossless Watermarking; Medical Image Security; medical Image Compression; Authentication and Confidentiality; JPEG2000 Compression; Kerberos; AHF; RSA

1. INTRODUCTION
Medical image communication is used in a variety of application like tele-surgery and tele-diagnosis[1][2],with the advances internet technology, Especially in healthcare, images can be cross-exchange in correct time allowing new medical practice[3].Image compression is useful to reduce the size of an image during communication, so the bandwidth can be effectively utilized. JPEG2000 offers numerous advantages over the JPEG standard. It also offers both lossy and lossless compression. When high quality is a concern, JPEG2000 process promises a higher quality final image, even when using lossy compression and also it offers higher compression ratios. The JPEG2000 image compression system has a rate distortion advantage over the original JPEG [4][5].Data encryption techniques and Digital Signature algorithms are important on protecting confidential information [6]. To generate the Digital Signature, hash value of the medical image (Covering image) is calculated using a novel algorithm called AHF (Additive Hash Function Algorithm. The algorithm is an iterative, one way hash function that can process image to produce a condensed representation called a message Digest. The algorithm enables the integrity of a message to be determined and any change to the message will, with a very high probability, result in a different message Digest [7][8]. The Rivest-Shamir-Adleman(RSA) scheme has since the time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption. RSA makes use of an expression with exponential. Four possible approaches to attacking the RSA Algorithm are Brute force attack, Mathematical attack, timing and chosen cipher text attack [9][10][11].

Medical image knowledge digest consists of Electronic Patient Record (EPR) which consists of patient information like patient name, patient-ID, disease description, procedures with doctor's information [12].Combination of medical image knowledge digest and digital signature of the medical image will be the watermark. This watermark is embedded into the image which has to be shared by using lossless watermarking technique. The data hiding scheme should have a large embedding capacity to carry more general information. The goals of the reversible watermarking are to protect the copyrights and can recover the original image. Reversible watermarking provides robustness, imperceptibility, high embedding capacity and readily retrieving capacity [13]. To share medical images with some extra header information, unfortunately header files are prone to manipulation and information loss may occur during file format conversion. For Example, most data contained in the header of a DICOM (Digital Imaging and Communication) image file will be lost after conversion into another multimedia format. The combination of Medical image knowledge digest and Digital Signature (DS) of the medical image will be the watermark. The data hiding scheme should have a large embedding capacity to carry more information. Main goal of Digital Lossless watermarking is to protect the copyright and can recover the original image [14]. Lossless watermarking can also be defined on the schemes which can recover the original image form the embedded image [15] [16]. An unimportant area of an image (RONI) is watermarked. In this approach we leave the information of interest (ROI) for the diagnosis purpose .The watermarked images are shared through the web servers. The medical experts who are accessing the images should be registered with the web servers through their user id and password [17]. The strict authentication can be provided to these medical experts by using Kerberos. Kerberos introduces intermediate server which has the database all the medical experts should register their user id and password with this database. The intermediate authentication server produces ticket to access the medical images which are available in the websites, so the doctors registered properly with the websites through this Kerberos only can able to access the message [18][19]. 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 [20] [21]. Compression Ratio can be calculated by the ratio between the size of the image before compression and size of the image after compression [22] [23].

$$Compression\ Ratio = \frac{Size\ of\ the\ Original\ Image}{Size\ of\ the\ Compressed\ image} \quad (1)$$

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 given by

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

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

Where f (m, n) is pixel gray values of the original image.f1 (m, n) is pixel gray values of watermarked image.

The rest of this paper is organized as follows. In section 2 algorithms used for proposed is described 2.1.JPEG2000 Image compression algorithm, 2.2. Additive Hash algorithm-AHF, 2.3.Advanced Classical Cipher-ACC, 2.4.Lossless Watermarking- 2.5 Modified Difference of Expansion, 2.6. Algorithm for Kerberos] and then results and discussion for this proposed work is discussed in section 3. The paper concludes in section 4.

2. METHODOLOGY USED

2.1 JPEG2000 Image Compression

The JPEG 2000 image compression consists of four basic steps in the algorithm-pre-process, transformation. In our work we implemented JPEG2000 compression without quantization because medical images contains sensitive information, these information should not get lost during compression. JPEG2000 utilizes a new coding method called Embedded Block Coding with Optimized Truncation (EBCOT).

Step 1: Pre-processing: Image is decomposed to components to maximum of 256. These components are decomposed into rectangular tiles.
Step 2: Transformation: JPEG2000 uses discrete wavelet Transformation (DWT). Each tile is decomposed into different resolution levels, these levels are made up of sub bands of coefficients.
Step 3: Quantization: Sub bands of coefficients are quantized and collected as blocks.
Step 4:Entropy Encoding: The bit planes of the coefficients in a code block are entropy encoded. Encoding can be done in such a way that certain ROI can be coded at a higher quality than the background.
Figure 1 shows the input MRI image of size 512×512 before compression and figure 2 shows the same image after applying JPEG 2000 compression.

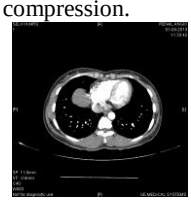


Fig. 1 Before Compression

Fig. 2 After Compression

2.2 Additive Hash Function (AHF)

This Hash algorithm accepts first row of the pixel mapped table of the original image as input and do some confusion and diffusion mathematically to produce the fixed length of output as a message digest value. The output message digest size will be 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 the H1024 into 8 parts 16 elements=128 bits namely z1 z2 z3 z4 z5 z6 z7 z8.
Step 6: Add alternate values

H1=z1+z5 H2=z2+z6
H3=z3+z7 H4=z4+z8 each value of H has 16 elements=128 bits

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

Where AHF= Additive Hash Value or Message Digest
AHF has 16 elements=128 bits.

2.3 Digital Signature Using RSA Approach

Authentication is maintained through the Digital Signature (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 reconstructed will indicate the information has been corrupted during transmission. We used.RSA approach to generate the Digital Signature (DS).Hash value of the input image is computed by using above mentioned AHF algorithm. AHF accepts the image values and produces the 128 bit constant output as the hash value. This hash value will be encrypted using RSA approach.The combination of Patient information, Disease information 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.

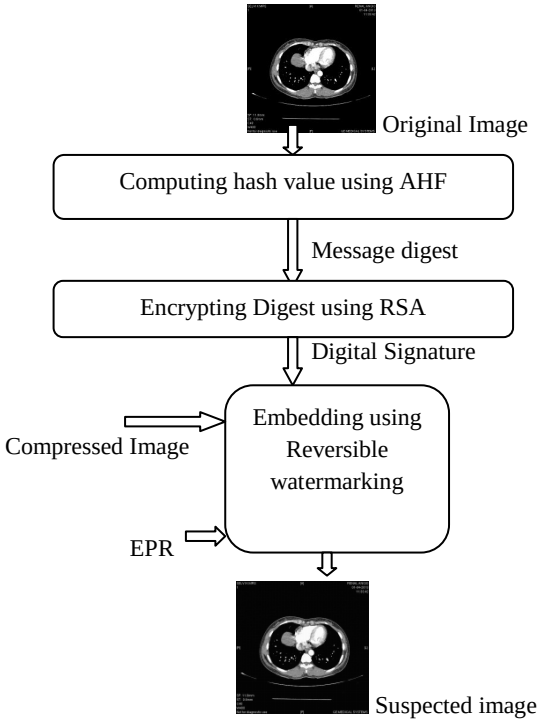


Fig. 3 Embedding and Authentication Procedure

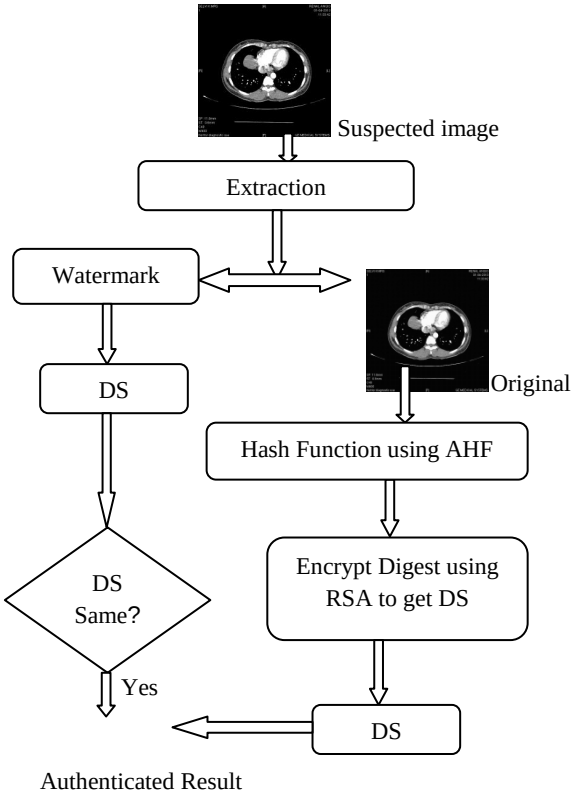


Fig. 4 Extraction and Authentication Verification

and hash value of the original image is also computed in the receiver side because we used reversible watermarking, the hash value is encrypted using RSA approach 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.

2.4 Lossless Modified Difference of Expansion

In lossless watermarking, we embed a watermark in a digital image I, and obtain the watermarked image Iw.The authenticator can remove the watermark from Iw to restore the original image and also the watermark we have embedded. The extracted image is same as the original image, because medical images having sensitive information these images should not be altered during embedding process, for this purpose only we proposed reversible watermarking. A basic idea of reversible watermarking is to select an embedding area in an image, and embed both the payload and the original values in this area into such area. If the amount of information need to embed is larger than the embedding area, most of the techniques rely on lossless compression on the original values in the embedding area, and the space saved from compression will be used for embedding the watermark. We are using difference expansion method for reversible watermarking. This scheme usually generates some small values to represent the features of the original image. Then we expand the generated values to embed the bits of watermark information. The watermark information is embedded in the LSB parts of the expanded values. Then the watermarked image is reconstructed by using the modified values.In our proposed modified difference of expansion method we will embed the watermark in the differnce of the pixel values. For a pair of pixel values (x,y) in a grey scale image, $0 \le x,y \le 255$, Define their average l and difference h as

$$L=((x+y)/2) \quad (4)$$

$$h = x - y \quad (5)$$

where x and y are two adjacent pixel.

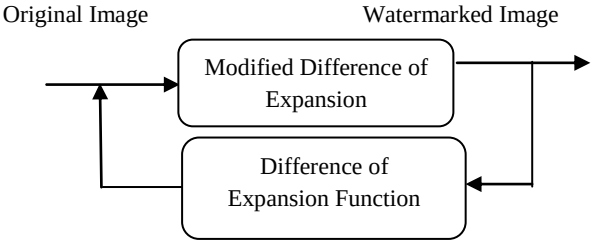


Fig. 5 Modified Difference of Expansion

Embedded value h=2×h+b (6)
Where h1=Embedded Pixel
h=Original Pixel
b=Payload (Binary value of watermark to be embed)

2.5 Algorithm for Kerberos

The Kerberos authentication model relies on a secret key symmetric encryption scheme and the concept of dual encryption to provide secure authentication across a possibly insecure network. Authentication tickets are delivered to Kerberos medical experts encrypted in two keys.

Step 1: The medical expert wishing access to an authenticated target service provides his/her username and password to the system he/she is using. The system used by the medical expert has no record of the user's username and password.

Step 2: The user system sends a request to the Kerberos initial ticketing service requesting a ticket-granting ticket for the

user whose user name it has been given. This request is totally unauthenticated.

Step 3: The initial ticketing service creates a unique session key (Ksession) and sends back to the user a dual-encrypted ticket-granting ticket and session key in the form

{{Ttgs, ksession} Ktgs, Ksession}Kuser

The user attempts to decrypt the TGT using his/her password as a key. If the decryption succeeds, The user can be certain that the user is authentic.

Step 4: When the medical expert attempts to use a particular target service, the user sends a service ticket request to the Kerberos ticket granting service.

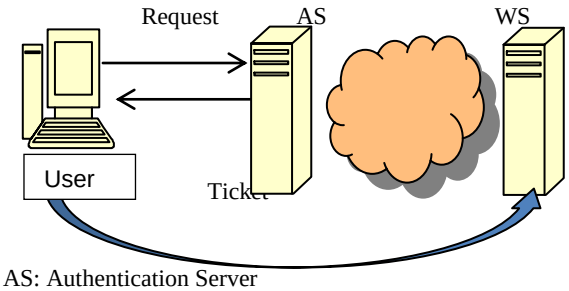
{TGT, {request, User ID, Time} Ksession}

Where TGT= {Ttgs, ksession} Ktgs

Step 5: The Kerberos ticket granting service uses its own secret key (Ktgs) to decrypt the TGT in the request it has received, then uses the session key (Ksession) in that TGT to decrypt the rest of the request.

Step 6: The user decrypts the service ticket it has received using the session key provided to yield the service session key and an encrypted service ticket.

({Tservice, kservice-session} Kservice)



AS: Authentication Server

WS: Web Server

Fig. 6 Involvement of Kerberos in Authentication

The medical experts can access the watermarked medical images available in the websites through this Ticket produced by the ticket granting ticket. These tickets are reusable.

3. RESULTS AND DISCUSSION

3.1 Performance Analysis

The proposed methodology has been simulated in Matlab with more than 500 digital medical images of various sizes collected from various scanning centers(Krishna Scanning Centre, Chennai), Hospitals (Sundharam Medical Foundation) and Medical databases available in the Internet in the raw format. In our project these images were resized to 512×512. We have taken only 3MRI images for discussions. The following table 1 shows the PSNR of existing and proposed methodologies of these 3 images when capacity is 0.1,0.25 bpp and 0.5bpp when JPEG2000 is used for compression, Lossless watermarking with ACC approach and Kerberos is used for authentication, reliability and integrity maintenance. If our medical image is compressed a lot then we can insert more amount of information into an image. So obviously capacity ratio will be increased. The parameter PSNR and NPCR is best in our proposed methodology because in our existing method the value is 60.72dB but in our proposed methodology it is 69.6dB.Almost in all of our 512×512 medical images with the embedding size of 64×64 bicubic images, we got 68.4dB to 78.9dB as the PSNR value and average NPCR is 98.9 %.Beyond the integrity control, if our aim is to insert more amount of information into an image, our methodology offers a compromise of 0.1bpp/78.32dB for image, 0.25bpp/72.02bB for US and 0.5bpp/60.75dB.

Table 1. PSNR of existing and proposed [18][20]

Image (MRI)	Payload (bpp)	Proposed (AHF+RSA+Lossless Watermarking)	Existing [12][18]
		PSNR(dB)	PSNR(dB)
1	0.1	78.32	68.84
	0.25	76.17	67.72
	0.5	68.02	64.02
2	0.1	74.21	58.77
	0.25	72.02	55.46
	0.5	69.13	53.23
3	0.1	60.75	49.32
	0.25	65.23	52.17
	0.5	72.29	45.49

From the Table 1, we observe that the PSNR value of proposed is better than existing for increase in capacity rate.

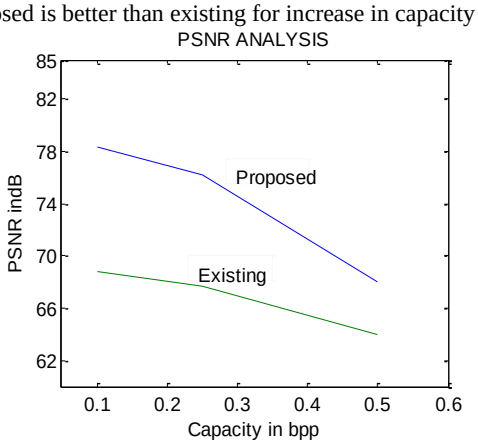


Fig. 7 Comparative Results of PSNR for existing and proposed for a single MRI image

From the figure 7 we can conclude that PSNR value is decreasing when increasing the Capacity rate bur 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.So we can definitely use the bandwidth effectively for communication. For networking communication we have used Java Socket Programming to implement the Kerberos operation. The following figure8 shows original image and watermarking Process, figure 9 shows the Extraction process and embedded watermark.

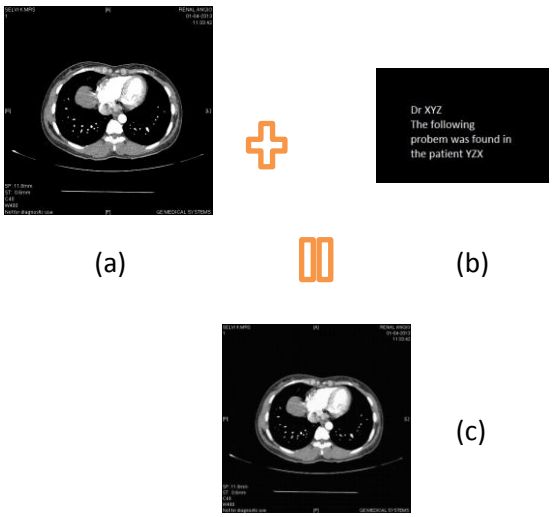


Fig. 8 (a) Original Image (b) Watermark (c) Watermarked Image

3.2 Comparison of Algorithms

DES algorithm and Breaking of DES:

- Encryption takes computer's process time.
- Encryption Keys can become lost.
- Encryption that is managed by the user can become a problem in a managed network by rendering necessary file inaccessible to the network manager.
- In 1990, Biham and Shamir, two Israeli cryptographers working at the Weitzman Institute, have invented a new generic technique to break symmetric algorithm called the Differential Cryptanalysis. It was the first time, that the method could break DES in less time than an exhaustive search.
- Imagine that we have a device which encrypts data with a hard-wired secret key and imagine furthermore that we don't have the tools to "read" the image.

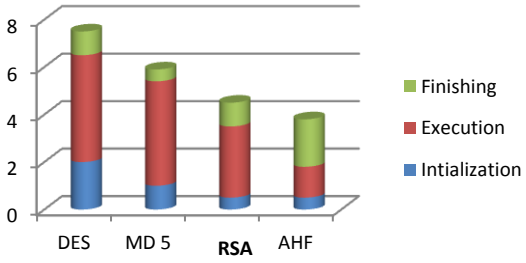


Fig. 9 Performance Analysis of various algorithms

4. CONCLUSION

Medical image security system based on lossless watermarking to achieve authentication, reliability and integrity was designed and implemented in this paper. A strict authentication was achieved through Kerberos. An EMR (Electronic Medical Record). It has completely solves the problem of integrity, reliability and authentication of medical image by using AHF and RSA method and also we can embed large amount of data inside the medical image without any distortion in an image. Since it requires secret key for both embedding process and extraction process it gives more authentication to our medical images. Medical images are authenticated in web server by using Kerberos algorithm, so it has high security. In future we can use better lossless Compression algorithm like JPEG-LS and new Lossless Watermarking Technique to improve the embedding Capacity.

5. REFERENCES

[1] Gouenou Coatrieux,Clara le Guillou,J.Cauvin and Ch,Roux: "Reversible watermarking for knowledge digest emedding and reliability control in medical images',IEEE Ransaction on information technology in biomedicine,vol.13,No.2,March 2009.

[2] G.Coatrieux,M.lamard,W.Daccache,j.Puentes, and C.Roux,"A low distortion and reversible watermark application in angiographic images of the retina," in proc.IEEE IEEE-EMBC Conf.,Shanghai,China,2005,pp.2224-2227.

[3] W.Pan, G.Coatrieux, N.Cuppens-Boulahia, F.Cuppens and Ch.Roux:"medical image integrity control combining digital signature and lossless watermarking",published in 2nd SSETOP international workshop on autonomous and spontaneous security,Saint malo:France,2009,Version 1-14 Jan 2010

[4] Micheal W.Marcellin,micheal J.Garmish,Ali Bilgin and Martin p.bolick,"An overview of JPEG-2000," in proc IEEE data compression conference,pp.523-541,2000.

[5] ISO,"JPEG2000 image codingsystem",ISO/IEC FCD 15444-1,JPEG2000 part I Final Committee Draft Version 1.0,2000.

[6] Li-QunKuang,Yuan Zhang,Xie Han:"A medical image authentication system based on reversible digital watermarking",in IEEE, 1st international conference on information science and engineering (ICISE 2009),pp 1047-1050.

[7] Jasni mohamad Zain,"Strict Authentication watermarking with JPEG compression(SAW-JPEG) for medical images,"in Europian journal of Scientific Research ISSN 450-216X vol.42 no.2(2012),pp.232-241

[8] Gaochang Zhaol,Xiaolin Yang,Bin Zhoul and Wei Wei,"RSA-Based digital image encryption algorithm in wireless sensor networks,"in proc second international conference on signal processing systems,Version 2,pp.640-643.

[9] R.Rivest,A.Shamir,l.Adleman: "A method for obtaining digital signatures and public-key cryptosystems",Communication of ACM.vol.21.2,pp120-126,1978

[10] Kuo Wen-Chung, Chen Ming-Yang. A modified(t,n) threshold proxy signature scheme based on the RSA cryptosystem.In information technology and applications,ICITA 2005,2,pp.576-579.

[11] Lein Harn,jian Ren.Efficient identity-based RSA multisignatures computer r s& security,2008,27,pp.12-15.

[12] Gouenou Coatrieux,Clara le Guillou,J.Cauvin,L.locarnu and Ch,Roux: "Enhancing shared medical image functionalities with image knowledge digest and watermarking",presented in the IEEE EMBC

conf.Int.Tech-nol.Appl.Biomed.(ITAB 2006).Joannina,Greece,Oct.

[13] Digital imaging and Communication in Medicine (DICOM) standard.(2007) [onlinr].Available:www.nema.org.

[14] C.C.Chang and I.C.Lin,"Remarks in fingerprint-based remote user authentication scheme using smart cards,"ACM operating system review, vol.38, no.3, pp.91-100,oct 2004.

[15] C.C.Chang, W.L.Tai and M.H.Lin,"A reversible data hiding scheme with modified side match vector quantization,"in proc of the international conference on advanced information networking and applications, vol.1), pp.947-952, Tai-Wan, mar 2005.

[16] Mohammad Reza Keyvanpour, farnoosh Merrikh-Bayat,"A new encryption method for secure embedding in image watermarking," in proc third international conference on advanced computer theory and engineering, v2, pp.402-407, 2010.

[17] A.Umamageswari, Dr.G.R.Suresh,"EnhancingSecurity In Medical Image Communication With JPEG2000 Compression And Lossless Watermarking", in the proceedings of the fourth international conference on Signals and image processing 2012 -ICSIP2012,Lecture notes in Electrical Engineering 221,DOI:10.1007/978-81-322-0997-3_36, Springer India 2013, pp 399-408.

[18] A.Umamageswari, Dr.G.R.Suresh "Security in Medical Image Communication with ROI based Lossless watermarking and Digital Signature" in the Proceedings of NCIEEE'13(ISBN:978-81-924031-9-9) 21st and 22nd February 2013.

[19] A.Umamageswari, Dr.G.R.Suresh,"Security in Medical Image Communication with Arnold's Cat map method and Reversible Watermarking," in the proceedings of International IEEE Conf.Circuits,poer and Computing Technologies(ICCPCT-13),(ISBN:)21st and 22nd March 2013.

[20] 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,pp.293-298,June 2012

[21] Imen Fourati kallel, Mohamed Salim Barehlel and Jean-Christophe Lapayre,"Improved Tian's Method for Meedical Image Reversible Watermarking",GVIP,vol.7,Issue 2,pp.1-7,August 2007.

[22] 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,Volume,Issue,3-5 August 2008,pp.942-945.

[23] Saied QAmirgholipour kasmani,Ahmadreza 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,11-13,no 2008,vol:2,pp.539-544.

[24] RC Gonzalez, RE Wood: Digital Image Processing, 2nd Ed, PHI, New Delhi, 2006.