ENHANCING SECURITY IN MEDICAL IMAGE COMMUNICATION USING NOVEL DIGITAL SIGNATURE WITH VARIOUS ATTACKS

A. Umamageswari[1] and G. R. Suresh[2]
[1]Sathyabama University, Chennai, India
[2]Easwari Engineering College, Chennai, India
E-Mail: grsuresh.@rediffmail.com

ABSTRACT

Medical image content authentication is very important, since medical image contents are more and more widely distributed. Reversible watermarking becomes a promising technique to embed the information into medical images. In this paper, we define the Region of Interest (ROI) in an image and trying to embed data in Region of Non Interest. When medical image shared through network, for the compression purpose we proposed the JPEG2000 algorithm and to improve the integrity and Authenticity hash value of the image is found by using MD5 and encrypted using RSA to form the DS (Digital Signature). DS and patient information is embedded into DICOM images. Strict authentication can be achieved by providing high security in accessing the secured medical images by medical experts which are available in the websites using Kerberos technique. The proposed method has been tested against various geometrical attacks to verity the robustness of the medical image and it has yields the fruitful results.

Keyword: medical image security, reversible watermarking, medical image compression, authenticity, integrity, RSA, HD5 hash function, JPEG2000 compression, Kerberos, attacks.

1. INTRODUCTION

Medical image communication is used in a variety of application like telesurgery and telediagnosis [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 MD5 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 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]. A reversible data hiding scheme and a reversible image authentication scheme can also be defined as the schemes which can recover the original image from the embedded image [14], [15]. Security can be defined in the term of integrity, authenticity, confidentiality and availability. This paper discusses mainly on authenticity, i.e. providing knowledge digest belongs to the correct patient information. An unimportant area of an image (RONI) is watermarked. In this approach we leave the information of interest (ROI) for the diagnosis purpose [16]. After embedding the watermark into an image, image quality can be calculated by peak signal to noise ratio, or PSNR, and the root mean square error (RMSE) and compression ratio (CR). Compression ratio should be minimum and PSNR should be maximum for better quality image. Compression ratio can be calculated by the ratio between the size of the image before compression and size of the image after compression.

$$\begin{aligned}&Compression\ Ratio\\&= (Original\ Image\ Size|Compressed\ Image\ Size)\end{aligned}$$

Here we make use of PSNR to quantify the distortion between the original image I and watermarked image Iw [17], [18].

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

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

The watermarked images are shared through the web sites. The medical experts who are accessing the images should be registered with the website with their user id and password. The strict authentication can be provided to those medical experts by using Kerberos. Kerberos introduces intermediate server which has the database all the medical experts should register their user id and passwords 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.

2. METHODLOLOGY USED

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: Pre-processing step will center the grayscale intensity values. We subtracted 127 from each intensity value in the image matrix.

Step-2: Transformation: JPEG2000 uses discrete wavelet Transformation (DWT). For lossless compression, we use the DWT in conjunction with the LeGall53 and perform the computation using lifting method. 2-3 iterations of the DWT were computed.

Step-3: Quantization: Above-mentioned two steps are enough for lossless compression.

Step-4: We simply used EBCOT to code the elements of the wavelet Transformation constructed with the LeGall filter. We can store the image using 215, 544 bits. The original image, in raw format requires 307, 200 bits of storage so the lossless method represents a saving of about 30%. The compression rate is 5.6bpp. Figure-1 shows the input US image of size 246x205 before compression and Figure-2 shows the same image after applying JPEG 2000 compression.

Figure-1. Image before compression.

Figure-2. Image after compression.

From the Figures 1 and 2 we can ensure that image size has been decreased from 41 KB to 4.64 KB, so compression ratio will be 0.113. When comparing the compression ratio of JPEG with JPEG2000, JPEG2000 giving better compression ratio with lossless compression.

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 DSA approach to generate the Digital Signature (DS). This signature can be produced with the Ticket created by the following Kerberos algorithm. This ticket is acts as the web server key to access the image from the Websites. Hash value of the input image is computed by using MD5 algorithm. MD5 accepts the image values and produces the 128 bit constant output as the hash value. This hash value will be encrypted using DSA approach.

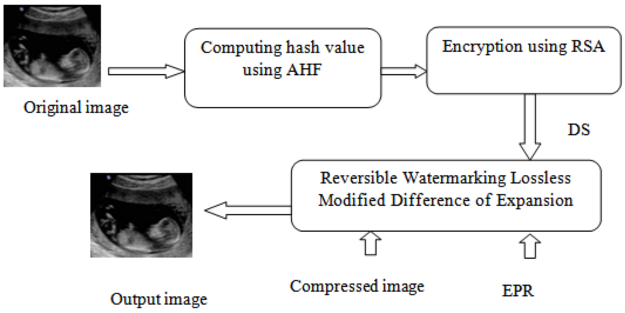

Original image
Computing hash value using AHF
Encryption using RSA
DS
Reversible Watermarking Lossless Modified Difference of Expansion
Output image
Compressed image
EPR

Figure-3. Embedding procedure and authentication procedure.

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 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.

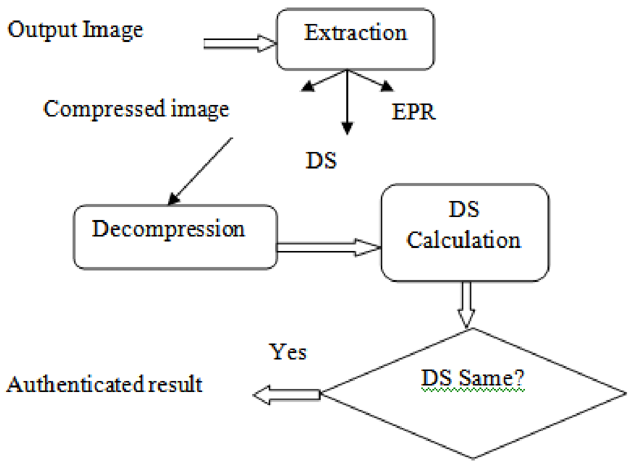


Figure-4. Watermark extraction and authentication verification.

Reversible/lossless watermarking

In reversible 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 method we will embed the watermark in the difference of the pixel values. For a pair of pixel values (x, y) in a greyscale image, 0≤x, y≤255, define their (integer) average l and difference h as

$$l = \lfloor (x+y)/2 \rfloor$$
$$h = x - y$$

where x and y are two adjacent pixels.

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)

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 DISCUSSIONS

The proposed methodology has been simulated in C# .Net using around 100 digital Ultrasonic images (US) images. These images were taken from public databases. The images in the databases were in different formats. We brought it to the various sizes of medical US images, 8 bits per pixel and represented in PNG format. We have taken only five images for discussions. Table 1 shows the PSNR and Compression ratio (CR) of those five images when JPEG is used for compression and Reversible watermarking with DSA approach and Kerberos is used for authentication, reliability and integrity maintenance Table 2 shows the PSNR and Compression ratio (CR) of the proposed algorithms mentioned in methodologies used. When we are comparing the compression ratio of the existing and proposed algorithms our proposed method only gives better CR. When CR of the first US image taken into consideration from Table-1 and Table-2, it is 3.03 in previous algorithms but it is 4.11 in proposed algorithm. So our proposed method giving better results for compression. This JPEG2000 is lossless compression only so sensitive information in the medical image will not get lost. 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. For this paper we didn't take capacity ratio for Discussions.

When we take the second parameter PSNR, PSNR is also best in our proposed methodology. PSNR value in our existing method is only 52.63 dB but in our proposed methodology it is 60.72 dB. It is applicable for all the messages used for our discussions. From the Tables 1 and 2 we can say that the PSNR values of the existing algorithm is better in proposed algorithm.

Table-1. PSNR and CR of existing algorithm in [3] [5] [18].

Sample images	PSNR value in dB	CR value
I1	52.63	3.03
I2	53.19	2.90
I3	48.51	2.97
I4	48.23	2.88
I5	50.45	2.89

Table-2. PSNR and CR of proposed algorithm.

Sample images	PSNR value	CR value
I1	60.72	4.11
I2	59.28	3.57
I3	54.58	4.49
I4	58.52	3.92
I5	54.45	3.78

The following graphs in Figure-5 and Figure-6 also show the comparison of PSNR value of the existing and proposed methodology and Compression Ratio (CR) of the existing and proposed methodology respectively. From these two figures we can definitely conclude that our proposed algorithm giving better PSNR value and Compression Ratio (CR) value.

Figure-5 shows the PSNR comparison of previous algorithm and proposed algorithm. From the Figure we can say that the PSNR value is more in proposed algorithm only. Figure-6 shows the Compression ratio of previous algorithm and proposed algorithm. From the figure we can say that the CR is more in proposed algorithm only.

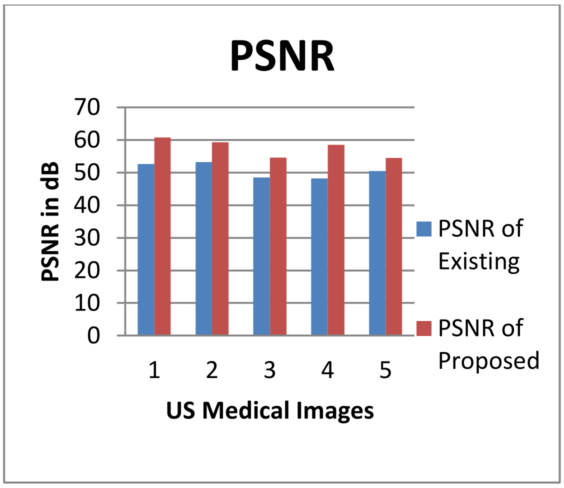


Figure-5. Comparative results of PSNR for existing and proposed.

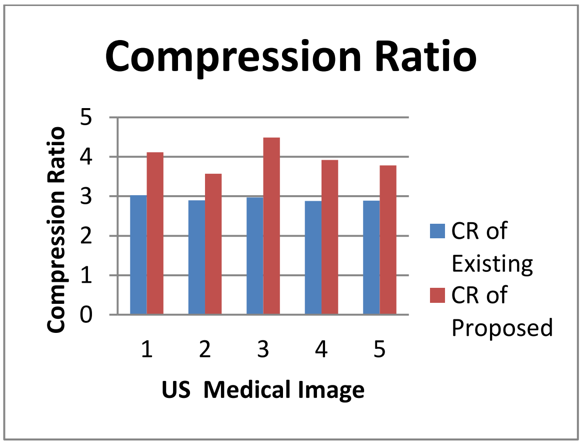
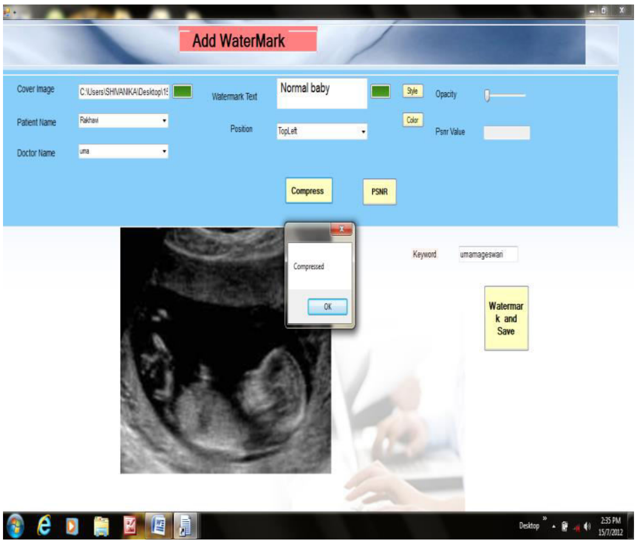
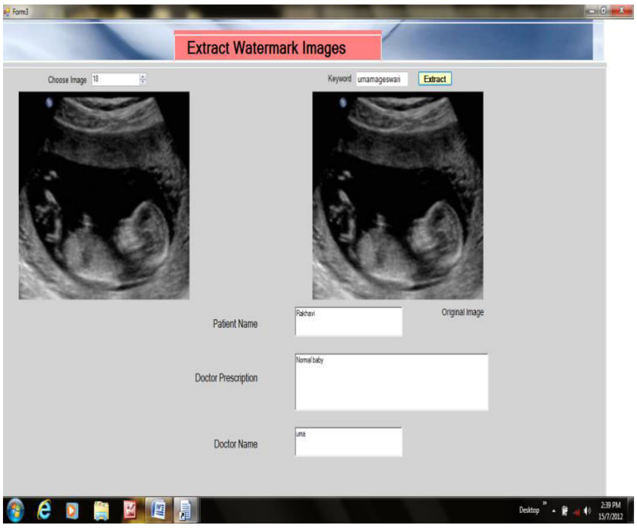


Figure-6. Comparative results of Compression Ratio (CR) for existing and proposed.



Cover Image C:\Users\SHIVANIKA\Desktop\1
Patient Name Rakhavi
Doctor Name uma
Watermark Text Normal baby
Position TopLeft
Opacity
Psnr Value
Compressed
Keyword umamageswari

Figure-7. Implementation of watermark embedding.



Choose Image 18
Keyword umamageswari
Patient Name Rakhavi
Doctor Prescription Normal baby
Doctor Name uma

Figure-8. Implementation of watermark extraction.

Figures 7 and 8 shows the implemented results of watermark embedding and extraction process respectively.

Evaluating robustness with attacks

The robustness of proposed algorithm has been evaluated with various geometrical attacks. The medical image of 512x512 x16 sizes with a capacity of 0.5 bpp is tested against various attacks like salt and pepper noise addition, compression, rotation, cropping and scaling etc. The proposed methodology is evaluated by using PSNR and NCC (Normalized correlation coefficient) which is used to measure the similarity between the cover image and the watermarked image.

a) Effect of compression

Figure-9 shows the original image, watermarked image with PSNR 75.6 dB, and compressed images with PSNR 69.2 dB. This has produced hign PSNR with less distortion.

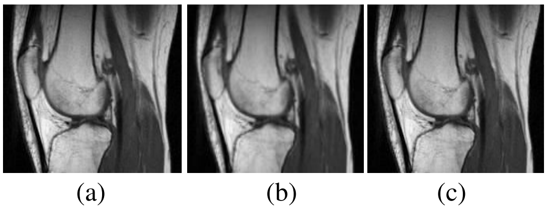


Figure-9. (a) Original image (b) Watermarked image PSNR 75.6 dB (c) Wavelet compressed image PSNR 69.2 dB.

b) Effect of salt and pepper noise

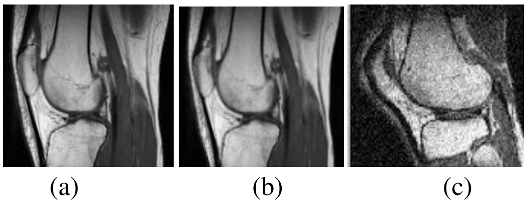


Figure-10. (a) Original image (b) Watermarked image PSNR 75.6Db (c) Salt and pepper noise attacked image PSNR 62.9 dB.

Figure-10 shows the original image, watermarked image with PSNR 75.6 dB, and 40% of salt and pepper noise image with PSNR 62.9 dB. The experimental result shows that the algorithm is robust to salt and pepper noise attack because PSNR value is better after adding noise.

c) Effect of rotation attack

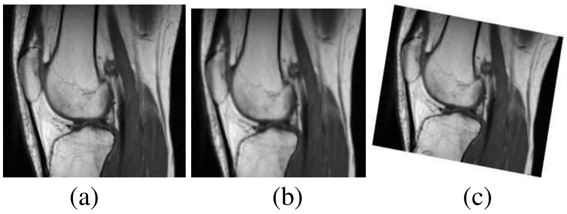


Figure-11. (a) Original image (b) Watermarked image with PSNR 75.6 dB (c) Rotated with 20° Image with PSNR 66.7 dB.

The experimental result shows that the algorithm is robust to rotation attack. The original image, watermarked image with PSNR 75.6 dB, and watermarked image and 20◦ rotation attack with PSNR 66.7 dB are shown in the Figure-11.

d) Effect of cropping attack

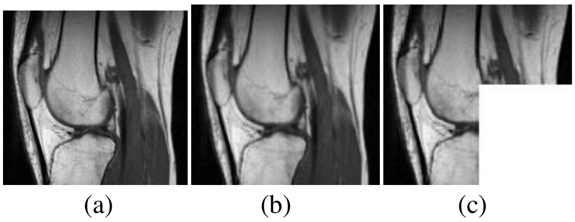


Figure-12. (a) Original image (b) Watermarked image with PSNR 75.6 dB (c) 25% cropped image PSNR 64.6 dB.

The experimental results show that the algorithm is robust to cropping attack. The original image, watermarked image with PSNR 75.6 dB, and watermarked image and cropping with the PSNR 64.6 dB are shown in the Figure-12.

4. CONCLUSIONS

We have proposed novel algorithms used to maintain an authentication while communicating medical images with the watermark through the open network. Medical image security system based on lossless watermarking to achieve higher authentication, reliability and integrity was designed and implemented in this thesis with various algorithms. It solves the problem of integrity, reliability and authentication of medical image by using AHF, RSA and ACM methods. We can also embed large amount of data inside the medical image with less distortion in an image because the medical image has been compressed before the embedding process and medical images are authenticated in web server by using Kerberos algorithm. The proposed systems provides exact authentication, geometric transform resistant watermarking system for exact recovery of original image in the receiver side, are proven to be robust according to intensive experiments with various properties. The proposed system is expected to be effective for medical images in the sense that it is able to completely recover the original image at the receiving end after the authenticity of image is verified.

5. FUTURE ENHANCEMENT

The watermarking technique that is given in this thesis can be further improved to increase the hiding capacity of images without affecting the imperceptibility of the images. The other future scope is that our technique can be enhanced to embed color watermark in colored image. Further it can be improved by proposing a new algorithm for selecting multiple Region of Interest (ROI) in an image.

REFERENCES

[1] Gouenou Coatrieux, Clara le Guillou, J. Cauvin and Ch, Roux: 2009. Reversible watermarking for knowledge digest embedding and reliability control in medical images. IEEE Transaction on information technology in biomedicine. 13(2).

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

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

[4] Micheal W. Marcellin, Micheal J. Garmish, Ali Bilgin and Martin P. Bolick. 2000. An overview of JPEG-2000. In proc IEEE data compression conference. pp. 523-541.

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

[6] Li-Qun Kuang, Yuan Zhang, Xie Han. 2009. 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 Mohammad Zain. 2012. Strict Authentication watermarking with JPEG compression (SAW-JPEG) for medical images. In European Journal of Scientific Research, ISSN 450-216X. 42(2): 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. 1978. A method for obtaining digital signatures and public-key cryptosystems. Communication of ACM. 21.2: 120-126.

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

[11] Lein Harn, jian Ren. 2008. Efficient identity-based RSA multisignatures computer r s and security. 27: 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.

[13] C.C. Chang and I.C. Lin. 2004. Remarks in fingerprint-based remote user authentication scheme using smart cards. ACM operating system review. 38(3): 91-100.

[14] C.C. Chang, W.L. Tai and M.H.Lin. 2005. A reversible data hiding scheme with modified side match vector quantization. In proc of the international conference on advanced information networking and applications. 1: 947-952, Taiwan.

[15] Mohammad Reza Keyvanpour, farnoosh Merrikh-Bayat. 2010. A new encryption method for secure embedding in image watermarking. In proc third international conference on advanced computer theory and engineering. 2: 402-407.

[16] Gouenou Coatrieux, Catherin Quantin, julien Montagner, Manianne Fazza Francois-Andre Allert and Ch. Roux. 2008. Watermarking medical images with anonymous patient identification to verify authenticity. In eHealth beyond the horizon. pp. 667-672.

[17] A. Umamageswari, M. Ferni Ukrit, Dr. G.R. Suresh. A survey on security in medical image communication. International journal of computer application.

[18] M. FerniUkrit, A. Umamageswari, Dr. G.R. Suresh. A survey on lossless compression techniques for dynamic images. International journal of computer application.

[19] William Stallings. 2010. Cryptography and network security.