A Survey on Security in Medical Image Communication

A.Umamageswari
Assistant Professor
Department of CSE
DMI College 0f Engineering
Palanchur, Chennai-600123

M.Ferni Ukrit
Assistant Professor
Department of CSE
DMI College 0f Engineering
Palanchur, Chennai-600123

Dr.G.R.Suresh
Professor
Department of IT
Easwari Engineering College
Ramapuram, 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. This paper discusses the need for reversible watermarking techniques and security related problems in medical images. Here we are comparing the lossless watermarking techniques for various medical image modalities like MRI (Magnetic resonance imaging), US (Ultrasonic), PET (Positron emission tomography), Endoscopic and angiographic images. For the discussions we can take ROI supporting lossless watermarking systems. This lossless watermarking is responsible for recovering the altered medical image content of the system.

General Terms

Medical Image Security, Security using SHA-256, Compression Techniques and performance analysis of various algorithms.

Keywords

Reversible Watermarking, Integrity, Confidentiality, Authentication, Medical Image Compression, Medical Imaging.

1. INTRODUCTION

The security of the medical images is purely based on the following things. (i) Confidentiality (ii) Integrity (iii) Authentication [1][2][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 the correct patient.

Medical image sharing through internet becomes very popular nowadays to make telediagnosis, telesurgeries and teleconsultation. When sharing the medical images with patient information we should provide very high security (Integrity, Authentication, Confidentiality) to the contents presents in the covering image.[3].

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 prepared to overcome the disadvantages of the previous methods. In conventional watermarking we can get the watermark (embedded patient information) back 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].
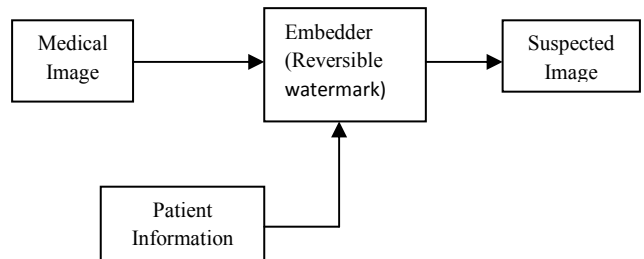

Figure 1: Simple reversible watermarking Process

2. AUTHENTICATION VERIFICATION BY USING LOSSLESS ATERMARKING

Strict authentication can be achieved by using cryptographic hash functions.[5].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. This hash code also referred as a message digests 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 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).
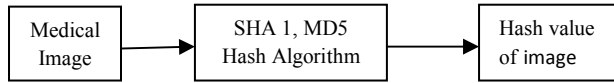
Figure 2: Generation of hash value

3. CONFIDENTIALITY VERIFICATION USINGPUBLICKEYCRYPTOGRAPHY

The RSA (Rivest-Shamir-Adelman) algorithm [6] 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.[7][8], 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.[9]. A digital signature is actually 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. To avoid this loss of image only we are introducing Reversible or lossless watermarking.
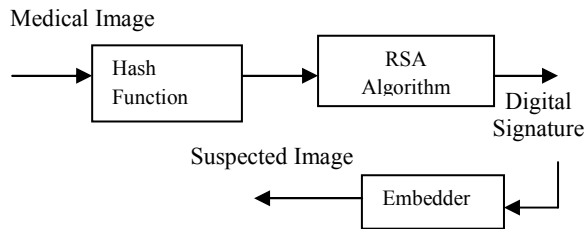
Figure 3 : Sender
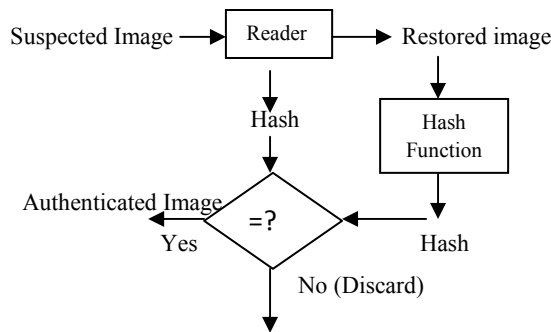
Figure 4 : Receiver

4. IMPORTANCE OF COMPRESSION IN MEDICAL IMAGE TRANSMISSION

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 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.[10].

JPEG2000 is an emerging standard for medical image compression. We believe it is more amenable to a compact description.[11]. This promises a higher quality final image, even when using lossy compression. Since the JPEG2000 format includes much richer content than existing JPEG files. This can able to offer higher compression ratios for lossy compression. Compression efficiency for lossy compression is typically measured using the Peak Signal to Noise Ratio (PSNR) and Root Mean Square Error (RMSE).

$$PSNR(dB) = -20\log\left(\frac{RMSE}{2^b - 1}\right)$$

Where b is the bit depth of the original image.

5. REVERSIBLE WATERMARKING OF MEDICAL IMAGE

Lossless watermarking has a special feature that the original digital watermark can be completely restored.[12]. 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.

In the case of additive insertion, the watermark w to be embedded is embedded in to the original image (host). $I_w = I + w$ (It is fully based on signals).

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. The following table shows that capacity rate and PSNR values of medical images with various algorithms implemented by using MAT lab.

From the following table we can discuss that the capacity rate and PSNR values for various medical images by using reversible watermarking algorithms. Normal reversible watermarking without using any additional security techniques having least capacity rate [1] and PSNR values. Reversible watermarking with DSA approach [9] having better capacity rate and PSNR
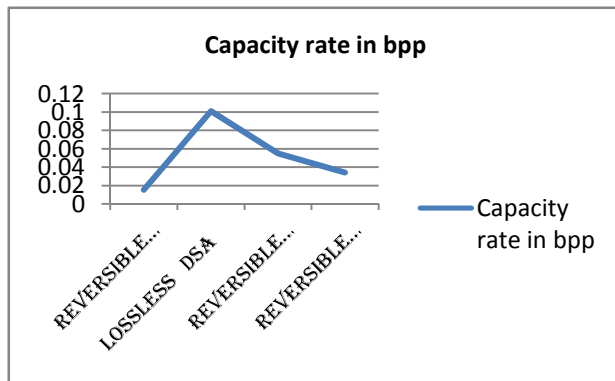
value. When compared to reversible watermarking with SHA-256 [7] having good capacity rate, but PSNR value in low because extra information embedded inside the image, Finally reversible watermarking with RSA approach [3] having best capacity rate and maximum PSNR value when compared to another algorithm.

Table 1: Capacity rate and PSNR values for various reversible watermarking algorithms.

Algorithm used	Capacity Rate in bpp	PSNR in dB
Reversible Watermarking [1]	0.15	49.11
Lossless watermarking with DSA Approach [9]	0.10	48.51
Reversible watermarking with SHA-256 [7]	0.05	41.00
Reversible watermarking with RSA approach [3]	.034	51.5
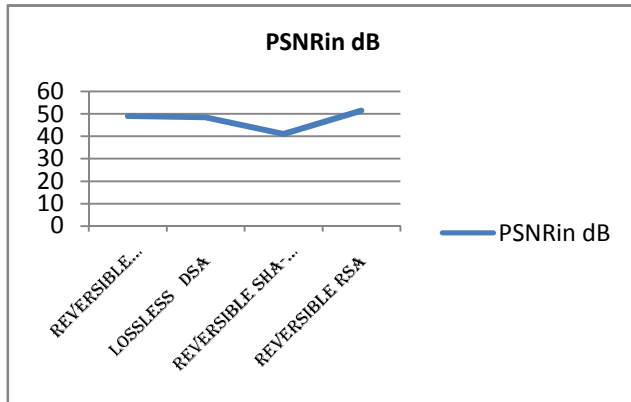
Figure 5 : PSNR in dB

Figure 6 : Capacity rate in bpp

6. COMPARITIVE RESULTS

Performances of the various algorithms in reversible watermarking can be compared with various modalities like MRI (Magnetic resonance imaging), US (Ultrasonic), PET (Positron emission tomography), Endoscopic and angiographic images by using their capacity rate (c) and Peak to Signal Noise Ratio (PSNR) value.[13].

6.1 Capacity Rate

Capacity Rate is number of bits in the image divided by the number of pixels in the image.

$$CapacityRate(c) = \frac{No.ofembeddedbit \sin theimage}{No.ofPixels}$$

C should be minimum for better quality Image.

6.2 Peak to Signal Noise Ratio

The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR.One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

$$PSNR(I, I_w) = 10\log_w \left((2^p - 1)^2 \Big/ MSE \right)$$

P   =   No of bits used to represent a Pixel
MSE =   Mean Square Error
I   =   Original image
I_w =   Watermarked Image

PSNR should be maximum for better quality image.

Table 2 compares the capacity rate and PSNR values of the reversible watermarking techniques in various modalities. When we considering about the information embedding by means of reversible watermarking with authenticated and encrypted approach, the above table discusses that, MRI images allows PSNR value to the maximum of 73 dB for 0.26 bpp capacity rate, PET images allows 67.87-97.98 dB for the capacity rate 0.13 – 0.2 bpp, Ultrasonic's allows 40.08 – 52.6 dB, Endoscopic and Angiographic images giving least PSNR & capacity rates values only. Generally PET (Positron emission tomography) images are allowing more information with low distortion when compared to the MRI (Magnetic resonance imaging), US (Ultrasonic), PET (Positron emission tomography), Endoscopic and angiographic images. The number of images used for experimentation also specified in the following table.

Table 2: Capacity rate and PSNR values for various reversible watermarking algorithms

MRI[14][15]			PET[14][15]			US[14][15]			Endoscopic image[3]			Angiographic image[16]		
No of Images	C bpp	PSNR (dB)	No of Images	C bpp	PSNR (dB)	No of Images	C bpp	PSNR (dB)	No of Images	C bpp	PSNR (dB)	No of Images	C bpp	PSNR (dB)
79	0.021	72.40	79	0.13	97.27	79	0.22	48.44		0.01	36.48		0.043	48.13
80	0.199	44.62	80	0.21	67.87	80	0.49	40.58	1500	0.026	38.84	160	0.082	48.53
99	0.26	73.00	99	0.2	97.98	99	0.05	52.6		0.022	39.71		0.188	49.11
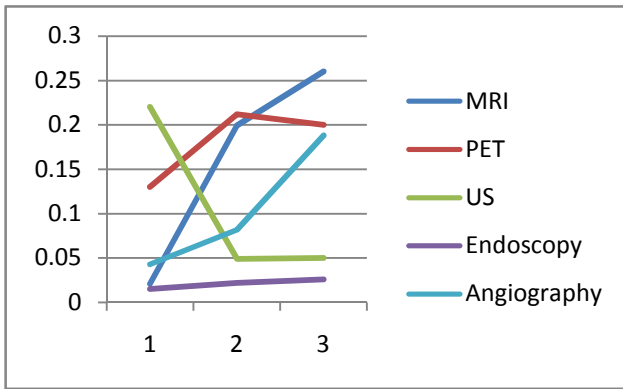
Figure 7: Capacity Rate (bpp)
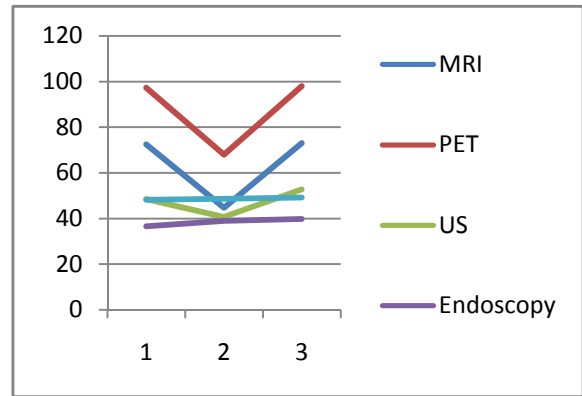
Figure 8: PSNR (dB)

7. CONCLUSIONS

Medical image security based on reversible watermarking is very important to communicate medical images through internet to authenticate patient information. This paper analyzed many important parameters for reversible watermarking and compared image qualities for various modalities with their capacity rate and peak noise to signal ratio. So reversible watermarking is important for medical image communication.

8. ACKNOWLEDGEMENTS

9. REFERENCES

[1] G.coatrieux, H.Maitre, B.Sankur, Y.Rolland and R.collorec:"relevance of watermarking in medical imaging:, in proc, IEEE Int. Conf. ITAB, Arlington, VA, 2000. PP-250-255

[2] G.coatrieux, L.Lecornu,B.Sankur,and.Roux:"A review of image watermarking applications in health care:, in proc, IEEE EMBS Annual international conf, New York City,USA,Aug 30-sept 3,2006, PP-4691-4694

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

[4] G.Coatrieux, M.lamard, w.Daccache, J.puentes and 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, pp.2224-2227.

[5] Jansi mahammad Zain: "Strict authentication watermarking with JPEG compression for medical images".European journal of scientific research ISSN 1450-216X vol.42,No.2010,pp 233-241.

[6] 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

[7] Shrikannde Rohini, Vinayak Bairagi:"lossless medical image security", International journal of applied engineering research, Dindigul, vol-1, No.3, 2010, pp.536-541.

[8] William stallings,2010, Cryptography and network security.

[9] 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

[10] C.Kim:"Compression of color medical images in gastrointestinalendoscopy: A.review", Med.Informatics, vol.9, pp.1046-1050, 1998.

[11] M.W.marcellin,m.J.Gormish,Ali.Bilgin,M.p.Boliel:"An overview of JPEG 2000",in proc.of the IEEE data compression conference,pp.523-541,2000

[12] Jen-Bang.feng, Iuon-Chang Lin, Chewi-Shoyong Tsai and Yen-Ping Chu:"Reversible watermarking: current status and key issues", International Journal of network security, vol.2, no.3, pp.161-171, May2006.

[13] 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.

[14] D.M.Thodi and J.j.Rodriquez:"Expansion embedding Technique for reversible watermarking", in IEEE Trans, Image Processing, vol.16, No.3, pp.721-730, March 2007.

[15] G.R.Xyan, Y.Q.Shi, C.Y, Yang, Y.Z.Zhang, D.K.Zou, P.Q.Chai:"Lossless Data Hiding using Integer wavelet Transform and threshold embedding Technique", in proc.of Int.Conf.Multimedia and Expo, 2005, pp.1520-1523.

[16] .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