International Journal ofComputing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 29-34

available at : www.ijcns.com
ISSN: 0976–1349

ENHANCING SECURITY IN MEDICAL IMAGE COMMUNICATION USING DIGITAL SIGNATURE

P. Antony raj, Mrs. A. Umamageswari
Department of Computer Science and Engineering
DMI College of Engineering
Palanchur, Chennai- 600 123, India
:antonyrajsite@gmail.com r.umaramesh@gmail.com

ABSTRACT

Medical image data require strict security, confidentiality and integrity when transmitted between open networks. Reversible or Lossless watermarking embedding the digital signature and information into medical images. In this paper, images are using Region of Interest (ROI) and try to embed data in Region of Non Interest. Before medical image is shared through network, proposed the JPEG Lossless algorithm for the purpose of compression and MD5 computing of the image to improve the authenticity hash value and encrypted using ACC-Advanced Classical Cipher to form the DS (Digital Signature). DS and Information is Watermark, it is embedded into Digital image communication images. Increase in authentication can be achieved when medical experts access secured medical images from web servers using Kerberos technique.

Keywords—JPEG Lossless image compression, Reversible watermarking, MD5, ACC, Kerberos.

1. INTRODUCTION

The security of Medical image communication image processing is a method to convert an image into the digital form and performs some operations like telesurgery and telediagnosis.Image compression is useful to reduce the size of an image during communication, so the bandwidth can be effectively utilized [1].The security of medical images, as for any medical information, derives from strict ethics and legislative rules, and can be declined in three mandatory characteristics,

-Confidentiality: means that only the authorized users, in the normally some conditions to access the information.

-Reliability: which has two aspects, i) Integrity: the information has not been modified by non authorized people; and, ii) Authentication: a proof that the information belongs indeed to the correct patient and is issued from the correct source.

- **Availability:** is the capability of an information system to be used by the entitled users in the normal scheduled conditions of access and exercise.

The main purpose of medical image is image enhancement, restoration, compression, recognition, retrieval of the images.

Watermarks are inseparable from the cover image in which they are embedded.

Data encryption techniques and Digital Signature algorithms are important on protecting confidential information. 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 [2]. The algorithm enables the integrity of a message to be determined and any change to the message with very high probability result in a different message Digest. Medical image knowledge digest consists of EPR, and EMR, procedures with doctor's information. Combination of medical image knowledge digest and digital signature of the medical image will be the watermark [3]. This watermark is embedded into the image which has to be shared by using lossless watermarking technique [4].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 [5].Reversible watermarking provide robustness, imperceptibility, high embedding capacity and readily retrieving capacity [6].

International Journal ofComputing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 29-34
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

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 [7].This paper discusses mainly on authenticity, i.e., providing knowledge digest belongs to the correct patient Information [8]. An unimportant area of an image (RONI) is watermarked. In this approach we leave the information of interest (ROI) for the diagnosis purpose after embedding the watermark into an image [9].

Compression Ratio = (Original Image Size / Compressed Image Size)

PSNR Calculation

The compressed and reconstruct images calculated to PSNR and MSE are the two error metrics used to compare image compression quality of MSE represents the cumulative squared error between the compressed and the original image the PSNR represents a measure of the peak error. The lower value of MSE is a lower error. To compute the PSNR and the block first calculates the mean-squared error values using the following equation:

$$MSE = \sum_{i=0,j=0}^{m,n} [I_1(i,j) - I_2(i,j)]^2 / m \times n \quad - (1)$$

In the previous equation, *m* and *n* are the number of rows and columns in the input images, $I_1(i,j)$ is the original image and $I_2(i,j)$ is the restored image the block computes the PSNR using the following equation:

$$PSNR = 10 \times \log_{10} ((R \times R)/MSE) \quad - (2)$$

In the previous equation, *R* is the maximum fluctuation in the input image data type. The input image is splitted into 8x8 block values of double-precision values then *R* is 1 this is a 8-bit unsigned integer 255 data values [10].

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.[11-12].

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. RELATED WORKS

The new approach of medical image security based on reversible Watermarking is very important to communicate medical images through internet to authenticate patient information. But the drawback is that security is low. If watermark is embedded in the ROI then sensitive information will get lost. Not considered any Authentication techniques when embedded images are shared through the Open Network.

DS will lost if the image file is converted to another format. In our paper we have enhanced the security level form the Digital signature using MD5 and ACC algorithms. The Kerberos techniques provide strict authentication accessing the medical images.

Digital image communication Data Header

In sharing of medical images communication, security can be applied with the addition of extra header information into the file format. The header files are prone to manipulation and information loss may occur. For example in DICOM system[13], in which the image file will be lost during the conversion of file format to provide security for healthcare systems and to protect the medical information system(MIS) from un authorized users using watermarking which ensures the system with confidentiality and reliability[14].Mainly for applications like e-diagnosis or image sharing through PACS and also done embedding of the description of the identified pathology within an image. Authentication is provided by issuing the DICOM header format in which watermark allows verifying the header raw data association and digital signature is used to ensure integrity of the medical image. The main drawback is that data hiding was not explored in healthcare systems properly and with reliability of the medical images.

The Reversible Technique:

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.

There are three basic reversible watermarking classifications

Reversible Watermarking by Data Compression

To embed more data into the original image, we have to compress the embedding data. The robustness of this type is very weak. Due to most

International Journal ofComputing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 29-34
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

data compression, distortions cannot be restricted. The complexity is more.

Reversible Watermarking by Difference Expansion

It usually generates small values to represent the features of original image. The generated values are expanded to embed the bits of watermark information. The embedding capacity is high. But it lacks robustness. We need additional information to determine the pair of pixels to be embedded.

Reversible Watermarking by using histogram shifting

To enhance the robustness, embedding target is replaced by the histogram of a block. The embedding capacity is lower but the robustness is the major advantage of this type of reversible watermarking.

Classical encryption techniques:

The technique enables us to illustrate the basic approaches to conventional encryption today. The two basic components of classical ciphers are substitution and transposition. Then other systems described that combines both substitution and transposition.

Substitution techniques

In this technique letters of plaintext are replaced by or by numbers and symbols. If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

3. PROPOSED FUCTIONAL MODULES

This work presents a high efficient Reversible or Lossless watermarking to embed the watermark into a Medical Image scheme using difference of expansion techniques.

Medical Image Transmission using JPEG Lossless Image Compression

Image compression addresses the problem of reducing the amount of data required to represent a digital image. In this process intended to yield a compact representation of an image thereby, reducing the image storage/transmission requirements.

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 JPEG Lossless using DWT for compression because no need to block the image More robust under transmission errors. Facilitates progressive transmission of the image (Scalability) in medical images and calculated to PSNR values.

Figure..1 Original Image:

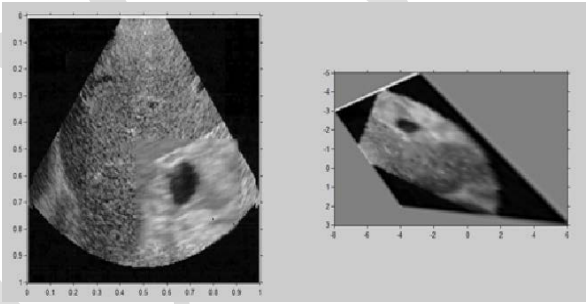
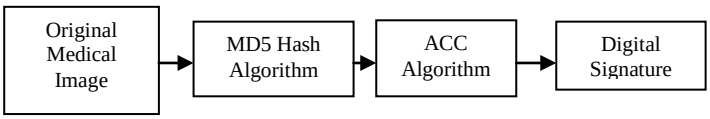


Figure.2 After compression MD5&Discrete Wavelet Transformed Image

Digital Signature Computed Using MD5 and ACC

Authentication is maintained through the Digital Signature (DS).This is computed over the input medical image use this signature to verify the reliability of the information. We used MD5 algorithm to generate the Digital Signature (DS).Fig.3.3.



MD5 algorithm: Accepts the input of any length values and produces the 128 bit constant output as the hash value. This hash value is will be encrypted using ACC algorithm. 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[20].The Receiver side the signature and patient and disease information is extracted from the suspected image and hash value of the original image

International Journal ofComputing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 29-34

available at : www.ijcns.com
ISSN: 0976–1349

is also computed in the receiver side because we used reversible watermarking, the hash value is encrypted using ACC approach to find the digital signature then this DS is compared with the signature extracted from the suspected image, if these two signature are same we can say that no alteration in the suspected image during transmission.

Embedding Reversible or Lossless watermarking

The goals of the reversible watermarking are to protect the copyrights and can recover the original image.

Conventional Watermarking Vs Reversible Watermarking:

- In reversible watermarking the assigned watermark is embedded into the original image 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.
- In conventional watermarking we can get the watermark back but we cannot get the original image.

In reversible watermarking, we embed a watermark in a digital image I, and obtain the watermarked image Iw. The authentication can remove the watermark from Iw to restore the original image and also the watermark we have embedded

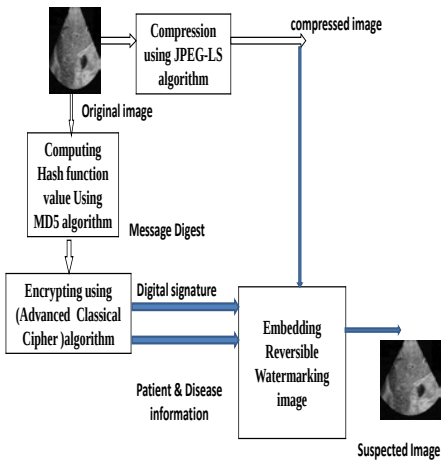


Figure. 3SENDER SIDE – Embedding procedure and authentication procedure

In lossless compression techniques, the original image can be perfectly recovered from the compressed image. These are also called noiseless since they do not add noise to the signal. It is also known as entropy coding since it use decomposition techniques to minimize redundancy The extracted image is same as the original image, because medical images having sensitive information these images should be altered during embedding process, As a result of our algorithm, the watermark embedded in the medical images can be recovered completely without any data loss during embedded or recovery process. The information is protected by encryption. Peak Signal to Noise Ratio (PSNR) testing confirms the reliability of the algorithm.for this purpose only we proposed reversible watermarking.

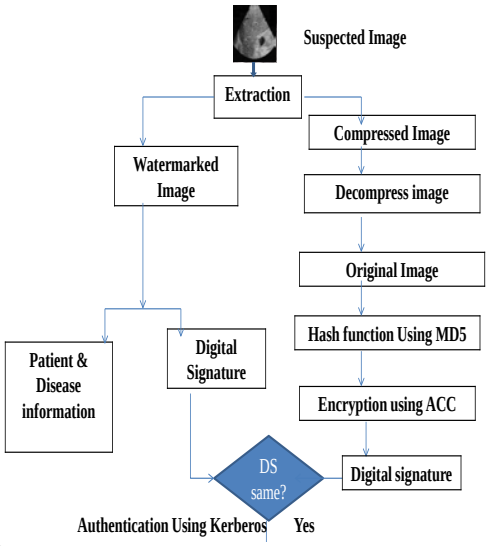


Figure. 4 RECEIVER SIDE – Watermark extraction and authentication verification

Authentication Scheme for Kerberos Algorithm

The Kerberos authentication models use a secret key encryption to provide strong network authentication for client/server applications.

Firewalls make a risky assumption that attacker are coming from the outside for attacks frequently come from Kerberos assumes that network connections (rather than servers and workstations) are the weak link in network security

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

Step 2:The user system is 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 unauthentication.

International Journal ofComputing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 29-34
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

Step 3: The initial ticketing service to creates a unique session key(K session) and sends back to the user a dual-encrypted ticket-granting ticket and session key in the form
{{Ttgs, Ksession} Ktgs, Ksession}Kuser
Step 4: 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,cession}Ktgs
Step 5: 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 personal can access the watermarked image and original medical images available in the websites through this Ticket granting services are reusable.

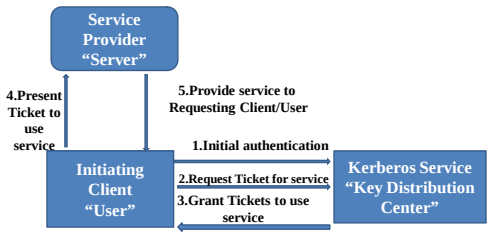


Figure.5 .Kerberos authentication model

4. RESULTS AND DISCUSSIONS

The proposed methodology has been simulated in MATLAB using digital Ultrasonic images (US).These images were taken from public databases like community. The images in the databases were in different formats data. We use it to the various sizes of medical US images, 8 bits per pixel and represented in PNG format of medical images to calculate PSNR values..The compression ratio (CR) of JPEG is used for compression and reversible with ACC approach and Kerberos is used for authentication, reliability and integrity of maintenance in proposed methodologies are used. The compression ratio of the existing and proposed algorithms our proposed method only gives better CR.

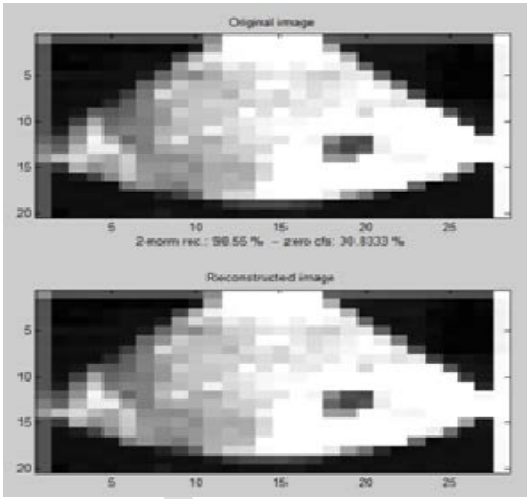


Figure6. Comparison for Original image and Reconstructed Image

This JPEG Lossless compression image is sensitive information in the medical image will not get lost so medical image is compressed with lot then we can insert more amount of information into an image clearly the Capacity Ratio will be increased.

Table .1 for PSNR and CR of proposed algorithm

Sample images	PSNR Value	CR value
I1	60.72	5.11
I2	59.28	4.17
I3	54.58	4.49
I4	58.52	3.22
I5	54.45	3.18

5. CONCLUSION

A medical image security system based on lossless watermarking to achieve authentication, reliability and integrity was designed and implemented in this paper. Strict authentication was achieved through Kerberos. The Digital signature, patient information and disease information also embedded inside the image. It has completely solves the problem of, reliability and authentication of medical image by using integrity, reliability 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.Moreover, thes keys are tickets generated by the authenticated web server by using Kerberos algorithm, so it has high security.

6. FUTURE ENHANCEMENT

In future we can achieve higher Compression ratio (CR) by introducing another JPEG algorithms for compression, so we can embed more information

inside an image Result of our work is enhanced security comparing the previous papers.

REFERENCES

[1].Gouenou coatrieux, Clara Le Guillou,Jean-Michel Cauvin,Christian Roux:"Reversible watermarking for knowledge Digest Embedding and Reliability Control in Medical Images:,IEEE Transactions on IT in BM,Vol.13.N0.2.March-2009.

[2].C.Le.Guillou, J.M.Cauvin, G.Coatrieux,"Enhancing shared medical image functionalities with medical image knowledge digest and watermarking" presented at the IEEE conference-2006.

[3].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.

[4].A.Umamageswari, Dr.G.R.Suresh, "Security in Medical Image Communication with ROI Based Lossless watermarking and Digital Signature "Proceeding of NCIEEE'13(Feb- 2013).

[5].Xiaoping Zheng, Jidong Jin"Research for the Application and Safety of MD5 Algorithm in Password Authentication" ICFSKD (FSKD-2012).

[6].B.Brindha, G.Raghuraman**"**Region Based Lossless Compression For Digital Images in Telemedicine Application" ICCSP,(April - 2013)India.

[7].Jen-Bang.feng,Iron-ChangLin,Chewi-ShoyongsaiandYen-PingChu:"Reversible watermarking: current status and key issues", vol.2, no.3, pp.161-171, May2006.

[8].Jingbing Li, Chunhua Dong, Mengxing"The Medical Images Watermarking Using DWT and Arnold" IEEE-2012.

[9].Li-qun Kuang,Yuan zhang,xi" A Medical Image Authentication System Based on Reversible digital Watermarking"ICISE-2009.

[10].G.Sudha, R.Ganesan"Secure Transmission Medical Data for Pervasive Healthcare System using android"ICCSP, April-2013,India

[11].M.FerniUkrit, G.R.Suresh"Effective Lossless Compression forMedicalImageSequencesUsingCompositeAlgorithm"ICCPCT-2013.

[12].Shantanu D.Rane and Guillermo sapiro"Evaluation of JPEG-LS,the New Lossless and Controlled-Lossy Still Image Compression Standard,for Compression of High-Resolution Elevation Data"IEEE GRS.VOL 39,NO.10.OCT .

[13].Li-qun Kuang, Yuan zhang, xie han"A Medical Image Authentication System Based on Reversible digital Watermarking"ICISE-2009.

[14].Zhuo wei, zhong shu,yajuan xie"Image lossless Compression and Secure Transmission System based on Integer Wavelet Transform"ICMIT-2010.

[15].A.Umamageswari,G.R.Suresh"Security in Medical Image Communication with Arnold's Cat map method and Reversible Watermarking".

[16].Aparna Mohanty&Asutosh kar"A Novel Approach For Spatial Domain Authentication System Design in Telemedicines"ICCCI-2012,Jan.10-12-Coimbatore,India

[17].G.Coatrieux, E.Chazard, R.Beuscart"Lossless Watermarking of Categorical attributes for Verifying Medical Data Base Integrity"ICIEEE EMBS-September 3-2011-USA

[18]. A.Umamageswari, M.FerniUkrit, Dr.G.R.Suresh"A survey on Security in Medical Image Communication" IJCA (0975-8887) Volume 30-No.3, September 2011.

[19].G.Sudha, R.Ganesan"Secure Transmission Medical Data for Pervasive Healthcare System using android" ICCSP,April 3-5,2013,India.

[20].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 , 2009, Version 1- 14 Jan 2010.

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