SECURITY IN MEDICAL IMAGE COMPRESSION USING COLOR MODELS

< S.Brindha>[1], <Kanimozhi>[2],<Senthilkumar>[3]

[1]Final Year, Department of Information Technology,
SKP Engineering College, Tiruvannamalai, Tamil Nadu
brindhasivakumar2014@gmail.com

[2] Final Year, Department of Information Technology,
SKP Engineering College, Tiruvannamalai, Tamil Nadu
Kanimozhikani92@gmail.com

[3]Assistant Professor, Department of Information Technology,
SKP Engineering College, Tiruvannamalai, Tamil Nadu
gsksuccess@gmail.com

Abstract: The main objective of the project is image compression.It explains how the image will be compressed and retrieved using the Arnold's cat map method.Reversible watermarking becomes a promising technique to embed the information into medical images.

Keywords: Reversible Watermarking, Medical Image Security, Medical Image Compression, Authenticity and Integrity, Arnold's cat map method, JPEG2000 Compression, Kerberos

1. Introduction

Medical image communication is used in a variety of application like telesurgery and telediagnosis[I][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 IPEG2000 image compression system has a rate distortion advantage over the original IPEG [4][5]. Arnold's cat map method, proposed by Vladimir Arnold in 1960 , is a chaotic map [6] which when applied to the digital image randomizes the original position of its pixels and the image becomes noisy. However it has a period p and if iterated p number of times, the original image reappears. The normal Arnold's cat map method uses the following equation for Transformation r = 'Where x,y € {(0,1,2,oo. N-l)} and N is the size of the input image. A new image will be produced when all the points in an image are manipulated by the equation (1). ACM is a simple but powerful transform [7] and digital image encryption can be achieved by applying this in the following manner. Let p be the transform period of an N x N digital image I. Applying ACM for a random iteration of t times (t € [I, p]) to I, a scrambled image [' is obtained which is completely different from I. Now [' can be transmitted over the communication channels without revealing any information to the unauthorized receivers [8,9]. At the receiving end the process is repeated for (p - t) times to obtain back the original image [10][11].Medical image knowledge digest consists of patient information like patient name, patient-ID , disease description, procedures with doctors information [12]. Medical image knowledge digest 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 Number of pixels change rate (NPCR). NPCR, Compression Ratio and Peak Signal to Noise Ratio should be maximum for high quality images.

a) Number of Pixel Change Rate (NPCR):

$$NPCR = \frac{\sum_{i,j} D(i,j) \times 100\%}{W \times H}$$

b) Peak Signal to Noise ratio (PSNR) is used as a quality parameter for reconstruction of compression images. Ere signal is the original data and the noise is the compressed data. Here we make use of PSNR to quantify the distortion between the original image I and watermarked image Iw [17][18].

$$PSNR(I, Iw) = 10\log_{10}(((2^{P} - 1)^{2} / MSE))$$

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

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. SYSTEM MODULES

2.1 JPEG 2000 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. IPEG2000 utilizes a new coding method called Embedded Block Coding with Optimized Truncation (EBCOT).

Step 1: Pre-processing: Pre-processing step will centre the greyscale 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. We compute2-3 iterations of the DWT.

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 Legal 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 I shows the input US image of size 246x205 before compression and figure 2 shows the same image after applying IPEG 2000 compression

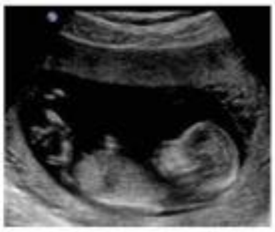


Figure 1 *Image Before Conversion*

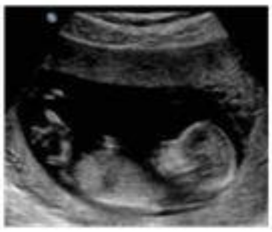


Figure 2 *Image After Conversion*

2.2 Encryption-Modified Arnold's Cat Map Transform:

It can easily be seen that the original Arnold transformations given by equation (1) can be modified to produce a sequence of Arnold transformations as given below:

$$\begin{bmatrix} x^{i} \\ y^{i} \end{bmatrix} - \begin{bmatrix} & i+1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \quad \text{......} (2)$$

Where, i € {I, 2, 3. .. }

Transformations given by equations (2) is periodic as abs (det (A)) is 1 in both the cases where, A = [a, b; c, d] is the Arnold transf orm matrix. Equations (2) , given above, produce a sequence of different Arnold transforms with different periodicity values Pk. Figure 3 shows the step by step work of sender side, Input image is compressed using JPEG2000 better compression ratio and predefined quality of an image then the compressed image is encrypted using Arnolds cap map method. Patient and disease information is embedded into an encrypted image using reversible watermarking techniques which has specified in the following section. From the Lossless watermarking method we will get the suspected image, suspected image will be send to the receiver side medical experts through the web servers. To increase the authenticity we have proposed Kerberos technique. Kerberos introduces new authentication server between web server and an user. All the users like doctors and medical experts should register their information with Authentication server to get the Ticket. By using ticket only the medic al experts can able to send and receive the images through the web servers. So we can maintain integrity, authenticity and Reliability over medical images during communication. The combination of Patient information, Disease information is called as Watermark.

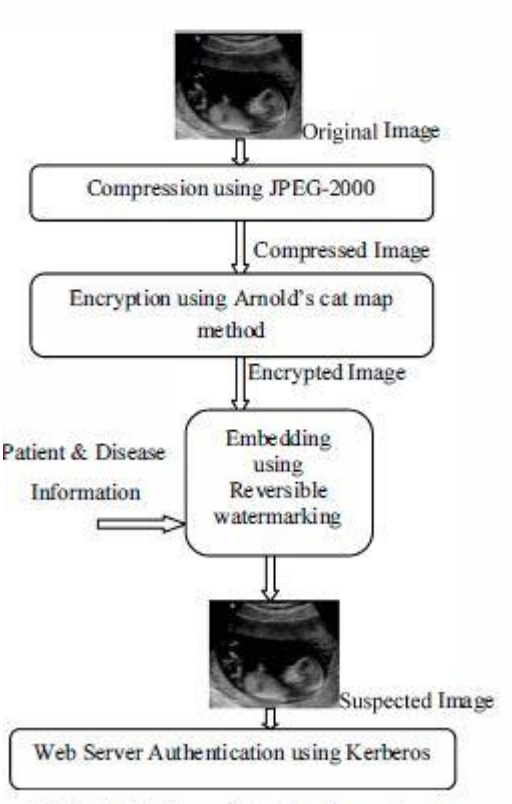

Original Image
Compression using JPEG-2000
Compressed Image
Encryption using Arnold's cat map method
Encrypted Image
Patient & Disease Information
Embedding using Reversible watermarking
Suspected Image
Web Server Authentication using Kerberos

Fig 3 Sender Side Process (Encryption, Compression and Authentication)

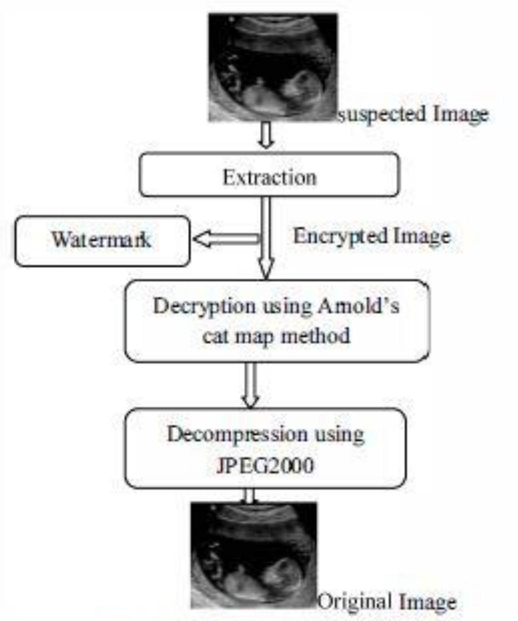

suspected Image
Extraction
Watermark
Encrypted Image
Decryption using Arnold's cat map method
Decompression using JPEG2000
Original Image

Fig 4 Receiver Side Process (Decryption and Decompression)

2.3 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 basie 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, O<Sx, y<::255 ,define their (integer) average l and difference h as

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

$$h = x - y$$

2.4 Algorithm For Kerberos:

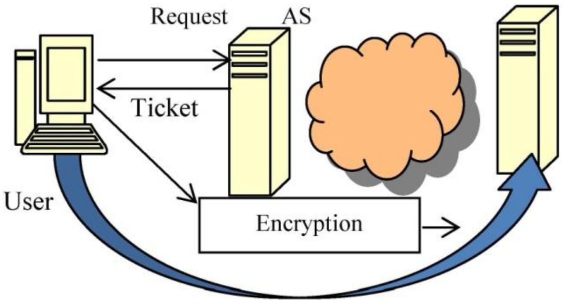
The Kerberos authentication model relies on a secret key symmetrie encryption scheme and the concept of dual encryption to provide seeure authentication across a possibly insecure network. Authentication tickets are delivered to Kerberos medical experts encrypted in two keys.

Step 1: The me die al 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



Figure

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)

3. CONCLUSIONS

The proposed methodology has been simulated in Java Beans using around 100 digital Ultrasonic images (US) images. These images were taken from public databases like. 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 I shows the PSNR and Compression ratio (CR) of those five images when JPEG is used for compression and Reversible watermarking with Digital Signature Approach. Table 11 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 OUf proposed method only gives better CR. When CR of the first US image taken into consideration from table I and table 11 it is 3.43 in previous algorithms but it is 4.56 in proposed algorithm. So OUf 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

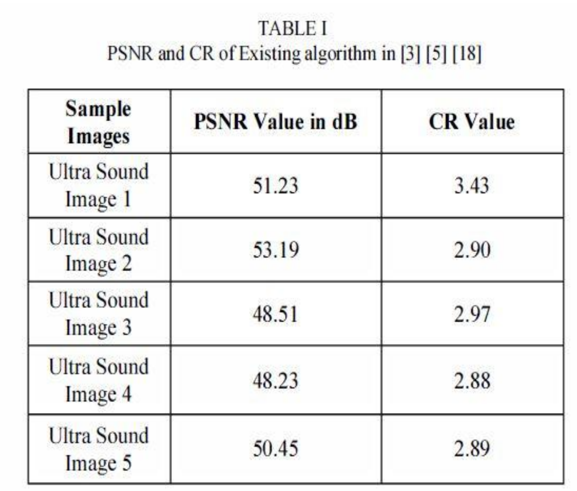


TABLE I
PSNR and CR of Existing algorithm in [3] [5] [18]

Sample Images	PSNR Value in dB	CR Value
Ultra Sound Image 1	51.23	3.43
Ultra Sound Image 2	53.19	2.90
Ultra Sound Image 3	48.51	2.97
Ultra Sound Image 4	48.23	2.88
Ultra Sound Image 5	50.45	2.89

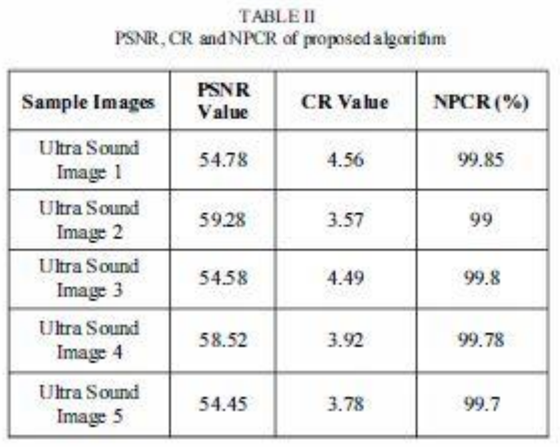


TABLE II
PSNR, CR and NPCR of proposed algorithm

Sample Images	PSNR Value	CR Value	NPCR (%)
Ultra Sound Image 1	54.78	4.56	99.85
Ultra Sound Image 2	59.28	3.57	99
Ultra Sound Image 3	54.58	4.49	99.8
Ultra Sound Image 4	58.52	3.92	99.78
Ultra Sound Image 5	54.45	3.78	99.7

4. FUTURE SCOPE

In future we can achieve higher compression ratio (CR) by introducing IPEG-LS algorithm for compression, so we can embed more information inside an image. Implementation of Arnold's cat map approach is difficult so we can introduce other security algorithm.

References

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

[2]G.Coatrieux, M.lamard, WDaccache, j.Puentes, and C.Roux,"Alow distortion and reversible watermark application in angiographic images of the retina," in proc.lEEE-EMBC, 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 Drajt Version 1.0,2000.

.