Journal of Engg. Research **Vol. 2 - (3) Sept. 2014** pp. 87-108

نقل الصور الطبية بطريقة آمنة باستخدام التحديد المائي المبني على ROI والبصمة الرقمية الجديدة

أوماماجزواي[*] و [**]ج.ر.سوريش

[*]قسم الكمبيوتر، جامعة ساثها ياباما، تشيناي، الهند

[**]قسم الكمبيوتر، كلية ايسواري الهندسية، تشيناي، الهند

الخلاصة

إن حماية الصور الطبية مهم جداً في الاتصالات الطبية. أصبحت طريقة اللاخسارة الرقمية بالبصمة المائية هي الطريقة المعتمدة لنقل الصور الطبية بأمان. لزيادة الأمان تقترح هذه الورقة خوارزمية مجزئة آمنة أسمها خوارزمية رايفست – شامير. الخوارزمية الجديدة تجمع المعادلات الجزئية وبرامج تشفير متطورة لتستخدم بدل الخوارزمية الحالية وكذلك لإنتاج بصمة رقمية للوصول إلى درجة عالية من السرية والأصالة. يتم ضغط الصورة باستخدام مجموعة برامج الوصل الفوتوغرافي JPEG2000 باستخدام محولات المويجات المنفصلة للأجزاء تحت الاهتمام وباستخدام برامج الوصل الفوتوغرافي JPEG للاماكن غير ذات أهمية.

الصورة الطبية التي تحتوي المعلومات الإلكترونية عن سجلات المريض والبصمة الرقمية يتم تضمينها في الجزء غير ذي الأهمية باستخدام تقنية التحديد المائي اللاخساري. إن تقنية التحديد المائي تزيد من قيمة وأصالة الصور عند استخدامها من عدة جهات في الشبكة المفتوحة. إن نسبة الموجة الأعلى إلى التشويش تصل إلى 72 د.ب لجميع أنواع الصور والاتصالات الطبية. يمكن زيادة الأصالة عندما يطلق خبراء الطب صور طبية آمنة من ملقمات الشبكة باستخدام تقنية كيربيروس.

Secure medical image communication using ROI based lossless watermarking and novel digital signature

A.UMAMAGESWARI[*] AND G.R.SURESH[**]

[*]*Department of CSE, Sathyabama University, Chennai, India*

[**]*Department of ECE, Easwari Engineering College, Chennai, India*

ABSTRACT

Protection of medical image content is more significant in telemedicine. Digital lossless watermarking becomes the auspicious technique to secure the medical content in medical images. To enhance the security, this paper suggests secure hash algorithm , rivest- shamir- adlemen algorithm, novel algorithms additive hash function and advanced classical cipher for replacing the existing algorithm and the production of digital signature to achieve high confidentiality and authentication. An image is compressed using joint photographic experts group JPEG 2000 discrete wavelet transforms for region of interest and joint photographic experts group JPEG for region of non interest. The medical image content electronics patient record and digital signature is embedded in region of non interest of compressed image, using lossless watermarking technique. Watermarking technique increases the integrity and authenticity, when medical images are shared through open network. The peak signal to noise ratio value is up to 72dBs for all types of digital imaging and communications in medicine images. Increase in authentication can be achieved when the medical expert access secured medical images from the web servers using Kerberos technique.

Keywords: Authentication and confidentiality; JPEG 2000 compression; Kerberos; lossless watermarking; medical image security.

INTRODUCTION

Distribution of medical image is used in various applications like remote diagnosis, tele-surgeries and tele-diagnosis department of telemedicine. (Lehmann *et al*., 2004). Safety can be achieved in Hospital information system (HIS) and picture archiving environment in communications (PACs) using digital image communication in medicine (DICOM) security standards as per health insurance portability and accountability act (HIPAA). Critically injured patients can be treated in the vicinity itself, by swapping their medical images between clinics located in different countries for giving best treatment to the patients by getting ideas from specialists available in various countries (Osbarne *et al*., 2006; Nisar Ahmed memon 2010). Medical industry expects high level security algorithms to maintain confidentiality, authenticity, integrity and information hiding techniques for data transmission (Pan *et al*., 2010). Enforcing content protection using classical access control mechanisms is no longer sufficient. It is essential to develop security mechanism that guarantees protection of medical image contents in an autonomous way, especially their integrity and traceability. Digital watermarking has been shown as a mechanism to enhance the medical image security (Zhou *et al*., 2001). Before images are made available in the open network, we should compress the medical images to effectively use the bandwidth. There are two major image compression algorithms - lossless and lossy methods. In lossless compression schemes, only the redundancy is exploited, and the image is recorded in more efficient manner. All the information is retained and hence the restored image is numerically identical to the original image. Lossy compression removes information, which seems irrelevant to the visual perception of the human observer and discarded. Therefore the compressed image cannot be perfectly reconstructed and distortion is introduced into the reconstructed image (Marcellin *et al*., 2000). Joint photographic experts group 2000 (JPEG2000) offers numerous advantages over the JPEG standard. It also offers both lossy and lossless compression. When high quality is needed, JPEG2000 using discrete wavelet transformation should be used, because it promises a high quality final image, even when using lossy compression and it also offers higher compression ratio. Digital signature algorithms are important in protecting confidential information (Qunkuang *et al*., 2009). To produce the digital signature (DS), hash value of the medical image is calculated using secure hash algorithm 1 (SHA-1) and additive hash function (AHF). The algorithm is an iterative, one way hash function that can process image to yield a condensed representation called message digest. This algorithm enables the integrity of a message to be determined and any change to the message will probably result in a different message digest (Jasni mohamad Zain 2012; Gaochang Zhaol *et al*., 2009). This message digest is then encrypted using rivest-shamir-adleman (RSA) and advanced classical cipher (ACC) to produce the Digital Signature. The DS is the encrypted hash value (William stallings 2010). Digital signature and medical content electronic medical record (EMR) are embedded in the region of non interest (RONI) using modified difference of expansion lossless watermarking technique. The basic principle of this approach is to share a medical image with knowledge digest (KD). The future KD gives the medical description and interpretation of the image content (Gouenou Coatrieux *et al*., 2009). To share the medical images with some extra header information, header files are prone to manipulation and information loss, which may occur during file format conversion. For example, most of the data contained in the header of a Digital imaging and communication (DICOM) 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. The main goal of digital lossless watermarking is to protect copyright and it can recover the original image (Chang *et al*., 2004). Lossless watermarking can also be defined on the schemes which can recover the original image form the embedded image (Chang *et al*., 2005; Mohammad Reza Keyvanpour & Farnoosh Merrikh-Bayat., 2010). There are three types of expansion based watermarking available. They are contrast mapping based, prediction error based and interpolation error based reversible watermarking schemes. Expansion based reversible watermarking achieves high embedding capacity and low computational complexity compared to the preceding techniques (Khan *et al*., 2014). The watermarked images are shared through the web servers. The medical experts who are accessing the images have to register with the web servers by their user id and password (Umamageswari & Suresh., 2013). Strict authentication can be provided to these medical experts by using kerberos. Kerberos introduces an intermediate server which has the database of all the medical experts. They should register their user id and password with this database. The intermediate authentication server produces a ticket to access the medical images, which are available in the websites, and therefore users who registered properly with the websites through this kerberos only can be able to access the message (Umamageswari & Suresh., 2013). After embedding the watermark inside into an image, the 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 high for better quality image (Baisa L.Gunjal & Suresh N.mali., 2012; Imen Fourati kallel *et al*., 2007). Compression ratio can be calculated as the ratio between the size of the image before compression and size of the image after compression (Ma Li,Xiaoshi Zheng *et al*., 2008; Saied QAmirgholipour kasmani & Ahmadreza naghsh-Nilchi., 2008; RC Gonzalez 2006). Proposed methodology introduces two novel algorithms advanced classical cipher (ACC) and additive hash function (AHF) to produce the digital signature (DS). Randomness can be included by changing the input value; hence the AHF algorithm works in a heterogeneous manner. Since it is heterogeneous in nature, constant examination leads to result being false. In ACC, the minimum probability of breaking the code is 36 million out of billion keys, which take a minimum of 1200 years for a single machine and a minimum of 200 years for 10 cluster systems.

METHODOLOGY USED

Existing methods used already existing algorithms for the generation of DS and embedding process. Following are the issues in the existing systems. Digital signature (DS) is transmitted with the image as a separate file or the image header, and hence there is a risk of losing the DS during transmission. If watermark is embedded in the ROI, then sensitive information will get lost. DS will be lost, if the image file is converted to another format. If we use DES, Block Ciphers, RC4, LFSR, RC5 etc. for creation of digital signature, then we cannot avoid some attacks like brute force attack etc. Attack tests like adding noise, signal distortion and different geometric operations (scaling, rotation, shearing etc.) performances were not satisfactory in existing methods.

Additive hash function (AHF)

This hash algorithm accepts the first row of the pixel mapped table of the original image as input and some confusion and diffusion are introduced mathematically to produce fixed length of output as a message digest value. The output message digest size will be of 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 H1024 into 8 parts (128 bits) namely z1 z2 z3 z4 z5 z6 z7 z8.

Step 6: Add alternate values, each value of H has 16 elements=128 bits

H1=z1+z5 H2=z2+z6 H3=z3+z7 H4=z4+z8

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, AHF has 16 elements=128 bits.

Where AHF= Additive Hash Value or Message Digest

Secure hash algorithm-SHA 1

This hash algorithm produces 160 bits in its output.

Step1: Appending padding bits. The original message is “padded” (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits less than a multiple of 512.

Step 2: Appending length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes. The rule of appending length follows:

- The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used.
- Break the 64-bit length into 2 words (32 bits each).
- The low-order word is appended first and it is followed by the high-order word.

Step 3: Preparing processing functions. SHA1 requires 80 processing functions

Step 4: Preparing processing constants. SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 $(0 <= t <= 19)$ K(t) = 0x6ED9EBA1 $(20 <= t <= 39)$

K(t) = 0x8F1BBCDC $(40 <= t <= 59)$ K(t) = 0xCA62C1D6 $(60 <= t <= 79)$

Step 5: Initializing buffers. SHA1 algorithm requires 5 word buffers with the following initial values:

H0 = 0x67452301 H1 = 0xEFCDAB89 H2 = 0x98BADCFE
H3 = 0x10325476 H4 = 0xC3D2E1F0

Step 6: Processing message in 512-bit blocks. This is the main task of SHA1 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, many operations are performed.

Step 7: Output. The contents in H0, H1, H2, H3, H4, and H5 are returned to sequence the Message Digest.

RSA Algorithm

The RSA scheme is a block cipher in which plaintext and ciphertext are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits.

Plaintext is encrypted in blocks, with each block having a binary value less than some number n. Key generation algorithm:

- Select two prime numbers, p and q
- Calculate n = pq
- Calculate □(n) = (p-1)(q-1)
- Select e such that e is relatively prime to □(n) .
- Determine d such that de=1 mod □(n) .

Cipher text, $C=M^e \bmod n$ and Plaintext $M=C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Creation of Digital signature

Authentication is maintained through the 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 reconstruction will indicate the information, which has been corrupted during communication. We planned a new approach named ACC or RSA to generate the DS hash value computed by SHA I (only first 128 bits of message digest) and AHF will be encrypted using ACC. The combination of electronic medical record (EMR) and DS is called watermark. This watermark is embedded inside the image using lossless modified difference of expansion technique at the sender side. At the receiver side the watermark is extracted from the suspected image.

Step 1: Obtain random number from server.

Step2: Obtain hash from the image by using AHF.

Step 3: Use the random number as vignere substitution value.

Step4: Change the hash key with respect to the random number.

Step 6: Now use this hash key as a prime text for play fair algorithm.

Step7: Encrypt the patient details with the play fair algorithm.

Step 8: Use the encrypted hash key as digital signature.

In the actual execution, all values are 128 bit, which are 16 characters

Vignere Vector = {1 2 3} Hash Value = {a b c}

a->1=b; b->2=d; c->3=f First level of encryption = BDF

B	D	F	A	C
E	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

DATA = NSCHAR NS ->SX CH->FK AR->DT

Second Level of Encryption (Digital Signature) = **SXFKDT**

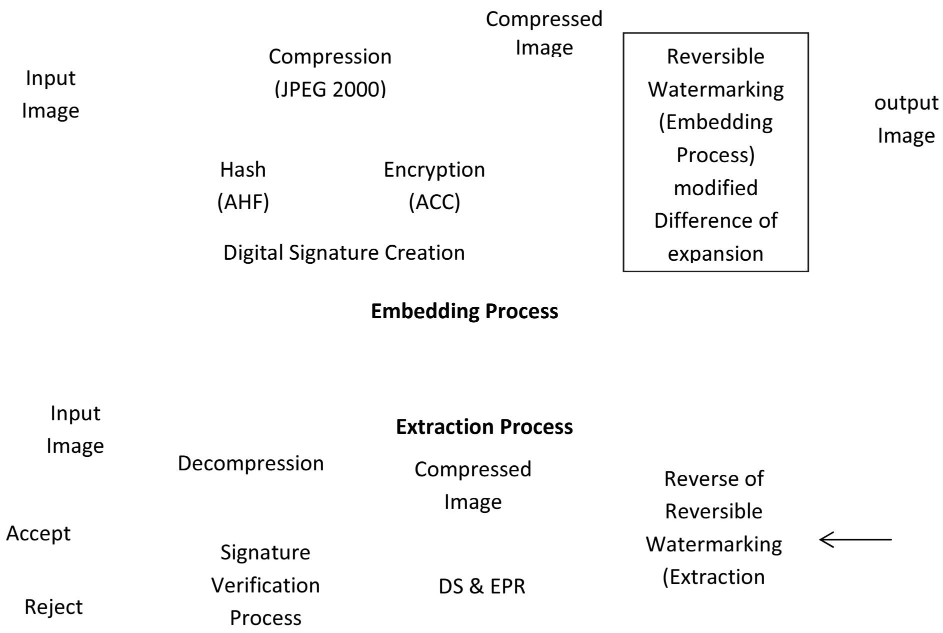


Fig. 1. Block diagram of proposed methodology

Hash value of the original image is also computed at the receiver side and then this hash value is encrypted using ACC or RSA to find the digital signature.

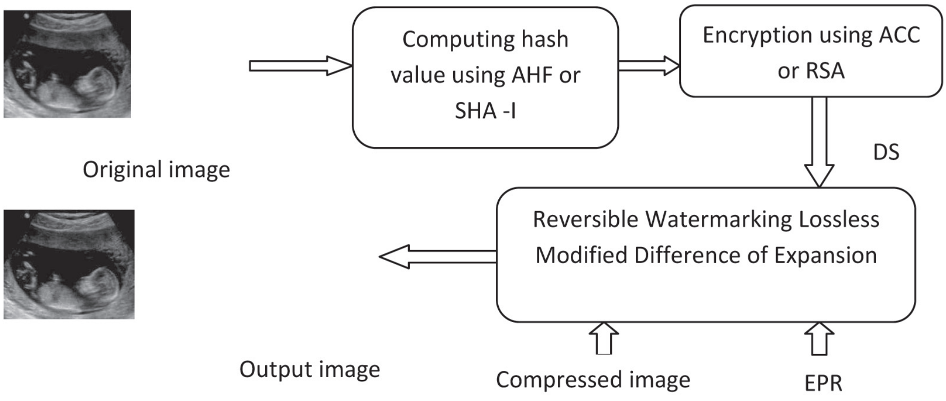

Computing hash value using AHF or SHA -I
Encryption using ACC or RSA
DS
Original image
Reversible Watermarking Lossless Modified Difference of Expansion
Output image
Compressed image
EPR

Fig. 2. Embedding procedure

If the computed DS is same as the digital signature extracted from the suspected image's watermark, then there is no alteration during the communication.

Lossless modified difference of expansion

In lossless watermarking, we embed a watermark in a digital image I, and obtained 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 have sensitive information.

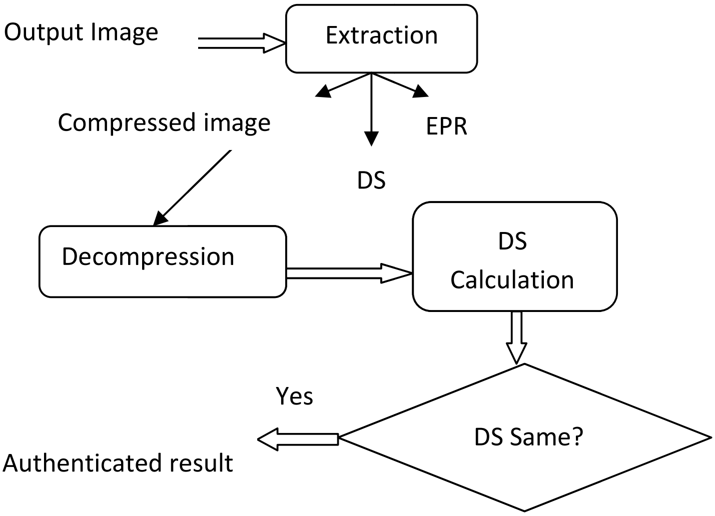


Fig. 3. Extraction procedure

These images should not be altered during embedding process. For this purpose only, we proposed the reversible watermarking.

The 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. 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 different expansion methods 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. Figure 1 shows the complete block diagram of proposed methodology. Figure 2 shows the step by step procedure of secure watermarking and figure 3 shows the extraction procedure to get the embedded watermark with original image and integrity checking process in deatail. In our proposed modified difference of expansion method, we embed the watermark in the differnce of the pixel values. For a pair of pixel values (x,y) in a grey scale image, $0 \leq x,y \leq 255$, define their average l and difference h as

$$l = \lfloor (x + y) / 2 \rfloor \quad (1)$$

$$h = x - y \quad (2)$$

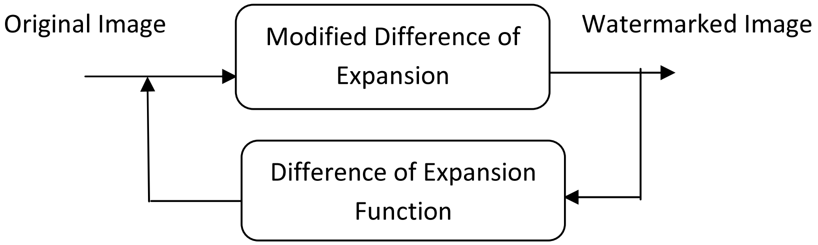
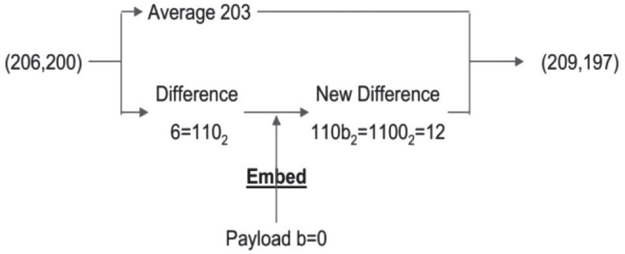

Original Image
Modified Difference of Expansion
Watermarked Image
Difference of Expansion Function

Fig. 4. Modified difference of expansion

where x and y are two adjacent pixels. Figure 4 shows the modified difference of expansion.



$$h' = 2\times h + b = 2\times 6 + 0 = 12$$

Embedded value = h^1=2×h+b

Where h^1=Embedded Pixel, h=Original Pixel b=Payload (watermark to be embed)

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.

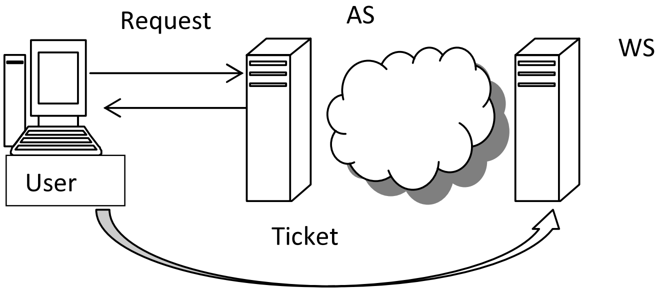
Step 2: The user system sends a request to the Kerberos initial ticketing service requesting a ticket-granting ticket for the user.

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

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.

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

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.



AS: Authentication Server WS: Web Server

Fig. 5. Involvement of kerberos in authentication

The medical experts can access the watermarked medical images available at the websites through this ticket, produced by the ticket granting ticket (TGT). Figure 5 shows the involvement of Kerberos in higher authentication for this medical environment.

EXPERIMENTAL RESULTS AND DISCUSSION

Performance analysis

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 high for better quality image (Baisa L.Gunjal & Suresh N.mali., 2012; Imen Fourati kallel *et al*., 2007). Compression ratio can be calculated by the ratio between the size of the image before compression and size of the image after compression (Ma Li,Xiaoshi Zheng *et al*., 2008; Saied QAmirgholipour kasmani *et al*., 2008; RC Gonzalez 2006).

$$Compression\ Ratio = \frac{Size\ of\ the\ Original\ Image}{Size\ of\ the\ Compressed\ Image} \tag{3}$$

The quality of the watermarked image is measured by PSNR. If the PSNR value is high, the quality of watermarked image will be good. PSNR for image with size M×N is given by

$$PSNR(I, Iw) = 10log_{10}(((2^{p} - 1)^{2}|MSE)) \tag{4}$$

$$MSE = \frac{1}{MN}\left[\sum_{i=0}^{M}\sum_{j=0}^{N}\left[\tilde{f}(m,n) - f(m,n)\right]^{2}\right] \tag{5}$$

where f (m, n) is pixel gray values of the original image and f^{1} (m, n) is pixel gray values of watermarked image. PSNR value is based on the capacity rate (watermark size). Number of pixels change rate (NPCR) also should be high for high quality images.

$$NPCR = \frac{\sum_{i,j} D(i,j) \times 100\%}{W \times H} \tag{6}$$

The proposed methodologies have been simulated in Matlab, using more than 500 DICOM format image archives in various modalities and tests are conducted. Some of the real-time images are collected from SMF-Sundaram Medical Foundations, Chennai and Krishna Scanning Centre Chennai. Experiments with these algorithms were conducted only with three modalities like ultrasound (US), magnetic resonant images (MRI) and computed tomography (CT) images and are saved in our database with a size of 512×512 JPG images. We tested our database with the proposed and existing methodology.

Proposed work 1

When joint photographic experts group (JPEG2000) for ROI and JPEG for RONI are used for compression, lossless watermarking with DS created using SHA I and ACC approach and Kerberos is used for authentication, reliability and maintenance of integrity. Table 1 shows the PSNR and payload of existing and proposed methodology. If the medical image is compressed a lot, then we can insert more amount of information into an image. So obviously, capacity rate will be increased. Beyond the integrity control, if the aim is to insert more amount of information into an image,

Table 1. PSNR of existing and proposed work 1[Gouenou Coatrieux *et al*.,2009]

Image	**Payload(bpp)**	**Proposed Method**	**Existing Method**
		(SHA I, ACC & Modified Difference of Expansion)	(MD5,RSA & LSB)
	0.324	74.21	58.77
US	0.432	72.02	55.46
	0.513	69.13	53.23
	0.343	78.32	68.84
MRI	0.429	76.17	67.72
	0.542	68.02	64.02
	0.551	60.75	49.32
CT	0.429	65.23	52.17
	0.343	72.29	45.49

Table 1 proves that the PSNR value of proposed method is better than existing.

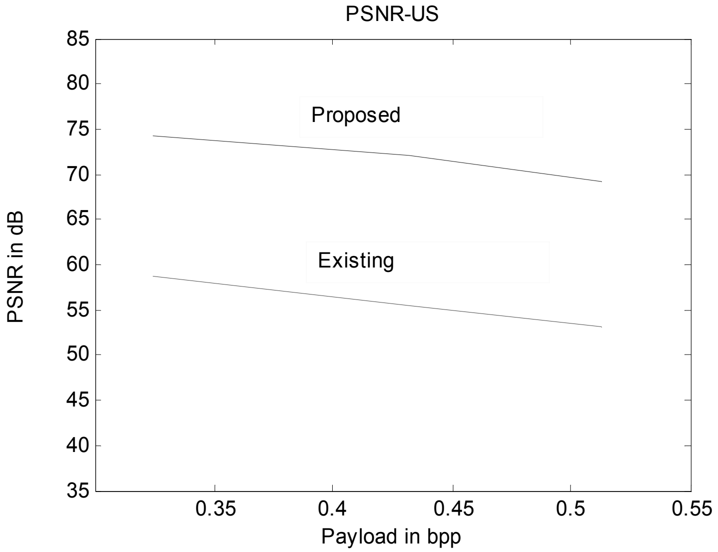


Fig. 6. PSNR of existing (MD5, RSA & LSB method) and proposed in US images with respect to payload

our methodology offers a compromise of 0.3432 bpp/78.32 dB for MRI, 0.4329 bpp/69.02 dB for US and 0.55 bpp/60.75 dBs Almost in all of our 512×512 medical images with the embedding size of greater than 15000 bits, we got 60.4 dB to 78.9 dB as the PSNR value with less distortion in reconstructed image; that too of JPEG2000 compression, not of watermarking.

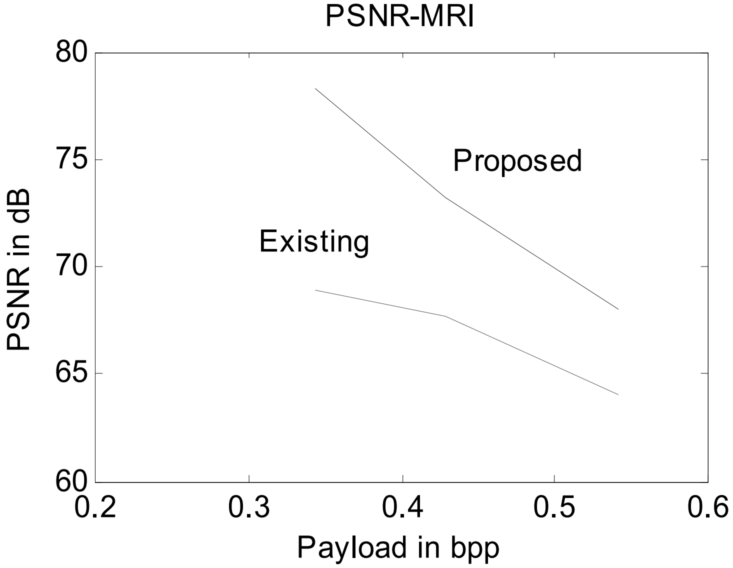


Fig. 7. PSNR of existing (MD5,RSA & LSB method) and proposed in MRI with respect to payload

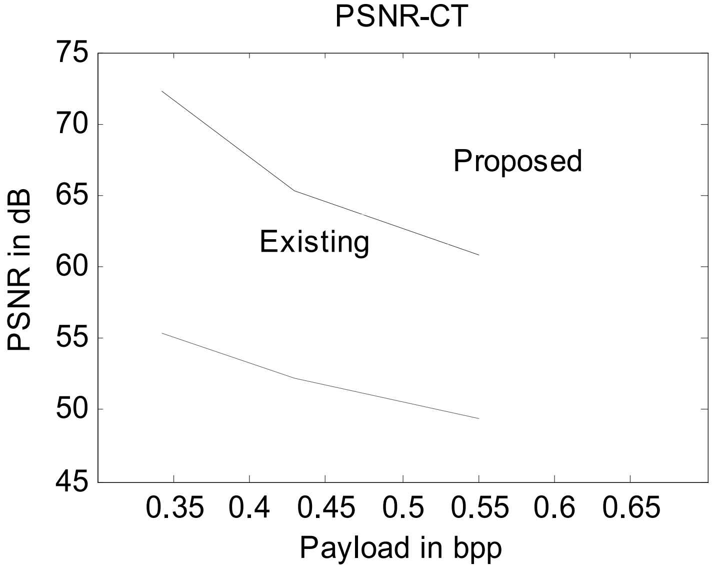


Fig. 8. PSNR of existing (MD5, RSA & LSB method) and proposed in US

Figure 6 shows that if we increase the payload length in ultrasonic images, then PSNR starts to decrease. When compared to MRI slices and CT images, the embedding capacity of US images are very high. Our proposed method achieved better PSNR value with very high embedding capacity and less distortion in a reconstructed image. Distortion in a reconstructed image is only because of the compression.

Figure 7 shows that if we increase the payload length in MRI slices, then PSNR starts to decrease. When compared to US images and CT images, the embedding capacity in MRI slices are moderate. Figure 8 shows that, if we increase the payload length in CT images, then PSNR starts to decrease. When compared to US images and MRI slices, the embedding capacity in CT images are much less. Compression ratio is also better in our JPEG 2000 compression algorithm, as it is up to 3.57. Hence, we can definitely use the bandwidth effectively for communication. For networking communication, we have used Java socket programming to implement the Kerberos operation.

Proposed work 2

When JPEG2000 is used for compression, lossless watermarking with DS is created using AHF and RSA approach and Kerberos is used for authentication, reliability and integrity maintenance. Table 2 shows the PSNR of existing and proposed methodologies of these 3 images, when capacity is 0.1 bpp, 0.25 bpp and 0.5 bpp. The parameter PSNR and NPCR are best in our proposed methodology, because in our 69.6 dB, almost in all of our 512×512 medical images with the embedding size of 64×64 images, we got 68.4 dB to 78.9 dB as the PSNR value and average NPCR is 98.9 %. From Table 2, we observe that the PSNR value of proposed method is better than existing, for increase in capacity rate. From figure 9 we can conclude that PSNR value is decreasing, when increasing the capacity rate. However, 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.

Table 2. PSNR of existing and proposed work 2 [Gouenou Coatrieux *et al*.,2009, Baisa L.Gunjal *et al*.,2012]

Image (MRI)	Payload(bpp)	Proposed Method (AHF,RSA,Modified)	Existing Method (MD5,RSA & LSB)	NPCR %
1	0.1	78.32	68.84	98.5
	0.25	76.17	67.72	99.8
	0.5	68.02	64.02	99.0
2	0.1	74.21	58.77	99.8
	0.25	72.02	55.46	99.7
	0.5	69.13	53.23	99.7
3	0.1	60.75	49.32	98.6
	0.25	65.23	52.17	99.2
	0.5	72.29	45.49	98.6

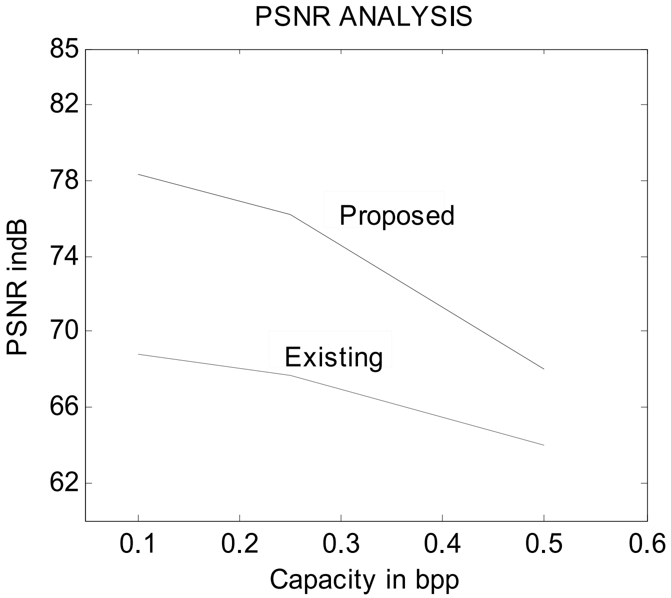


Fig. 9. Comparative results of PSNR for existing (MD5,RSA & LSB method) and proposed for a single MRI image

Proposed work 3

When JPEG2000 is used for compression, lossless watermarking with DS is created by using ACC and AHF approach and Kerberos is used for authentication, reliability and integrity maintenance.

Table 3. PSNR of existing and proposed work 3 [Gouenou Coatrieux *et al.*,2009]

Image	**Payload(bpp)**	**Proposed Method**	**Existing Method**
(MRI)	**(AHF,ACC & Modified**	**(MD5,RSA & LSB Method)**	
	Difference of Expansion)		
1	0.1	69.6	60.7
	0.25	67.2	60.1
	0.5	66.1	59.2
2	0.1	69.3	61.2
	0.25	68.6	60.8
	0.5	65.8	57.2
3	0.1	75.9	62.4
	0.25	71.2	60.2
	0.5	68.4	57.8
4	0.1	72.4	58.2
	0.25	68.2	55.4
	0.5	65.3	53.2

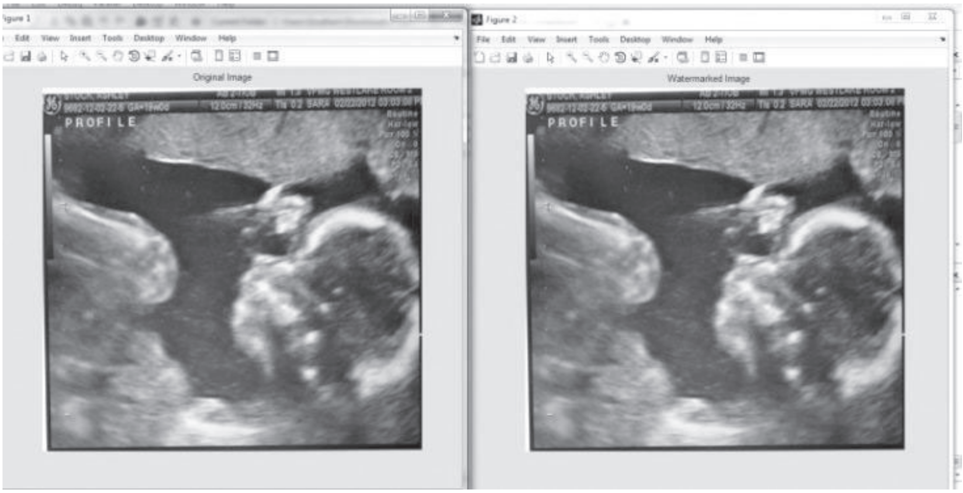


Figure 1
Edit View Insert Tools Desktop Window Help
Original Image
PROFILE
Figure 2
File Edit View Insert Tools Desktop Window Help
Watermarked Image
PROFILE

Fig. 10. Watermarking process.

Table 3 shows the PSNR of existing and proposed methodologies of 4 US images out of 500 DICOM images tested in our work. The parameter PSNR is best in our proposed methodology, because in our existing method the value is 61.58 dBs, but in our proposed methodology it is 72.4.6 dBs

Almost in all of our 512×512 medical images with the embedding size of 64×64 images, we got 68.4 dB to 75.9 dB as the PSNR value. From Table 3, we observe that the PSNR value of proposed method is better than existing.

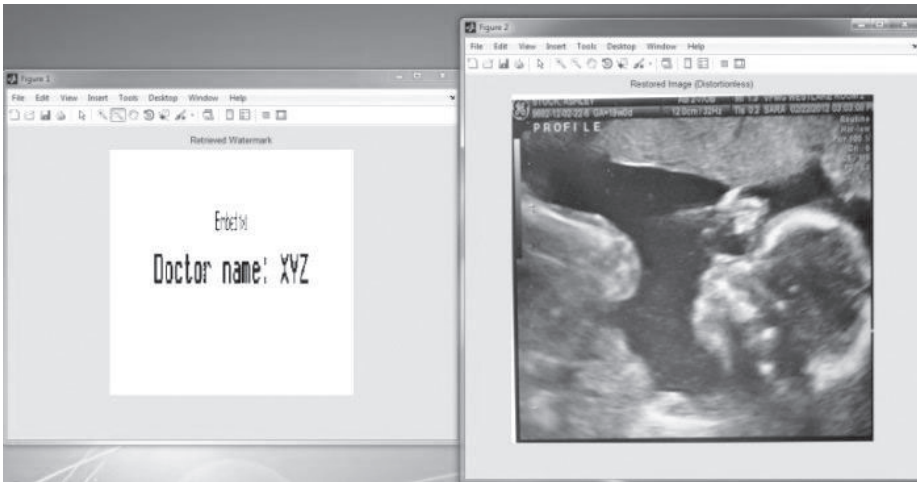
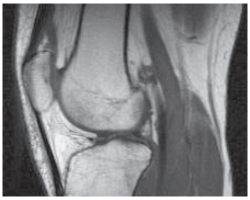
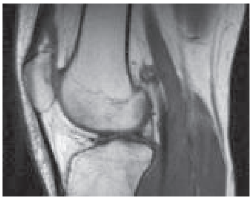
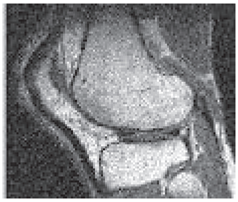
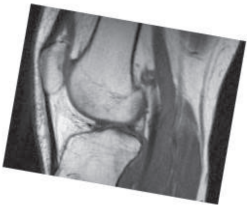


Figure 1
File Edit View Insert Tools Desktop Window Help
Retrieved Watermark
Embedded
Doctor name: XYZ
Figure 2
File Edit View Insert Tools Desktop Window Help
Restored Image (Distortionless)
PROFILE

Fig. 11. Extraction process.

Figure 10 shows original image and watermarking Process. Figure 11 shows the extraction process and embedded watermark of the proposed work 3.

Table 4. Results for various attacks.

	
Watermarked image PSNR=65.6 dB	Wavelet compressed image PSNR=59.2 dB
	
Salt and pepper noise PSNR= 52.9 dB	Rotation attack PSNR= 56.7 dB

The medical image of 512×512 sizes is tested against various attacks like salt and pepper noise addition, compression rotation and scaling etc, in table 4. This shows the watermark recovery is satisfactory under various attacks.

COMPARISON OF ALGORITHM

Breaking of data encryption standard (DES):

- Encryption takes computer's process time.
- Encryption keys can be 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 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 do not have the tools to "read" the image.

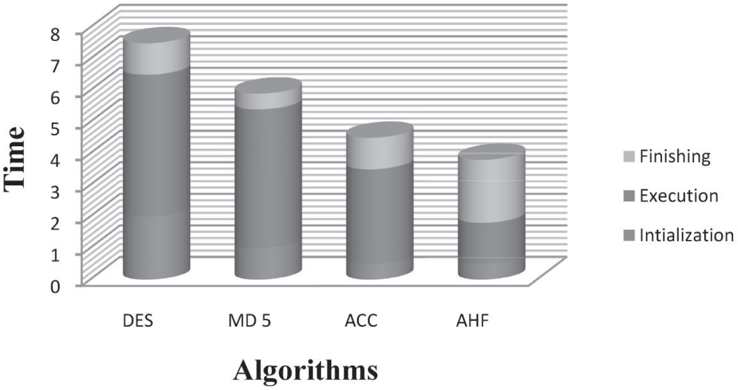


Fig. 12. Performance analysis of various algorithms

Figure 12 shows the performance analysis of various algorithms. Performance is recorded by using CPU-Z and the program was executed in matlab. So we have only proposed novel algorithms like ACC and AHF. It's execution time is less when compared to message digest 5 (MD5) and data encryption standard (DES).

Advantages of rivest-shamir-adleman (RSA):

Though the RSA algorithm is the strongest, it cannot withstand the test of time. In fact, no encryption technique is even perfectly secure from an attack by a realistic cryptanalyst. Methods such as brute-force are simple, but lengthy and may crack a message; it is not likely an entire encryption scheme. We must also consider a probabilistic approach, meaning there is always a chance that someone may get the one key out of a million. So far, we do not know how to prove whether an encryption scheme is unbreakable. If we cannot prove it, we will at least see if someone can break the code. This is how the NBS standard and RSA were essentially certified.

Advantages of additive hash function (AHF):

- Simple to implement and require less process utilization.
- Randomness can be included by changing the input value; hence the algorithm works in a heterogeneous manner. Since it is heterogeneous by nature, constant examination leads to false result.

Advantages of advanced classical cipher (ACC):

- New algorithm is easy to execute and it requires less computation time.
- It does not have backtracked decrypting technique. But has another algorithm to decrypt.
- Since two different classical ciphers are chosen, the minimum probability of breaking the code is 36 million out of billion keys, which take a minimum of 1200 years for a single machine and a minimum of 200 years for 10 cluster system.
- Imagine that we have a device which encrypts data with a hard-wired secret key and imagine furthermore that we do not have the tools to “read” the image.

CONCLUSION

Medical image security system based on lossless watermarking to achieve higher authentication, reliability and integrity was designed and implemented in this paper with various algorithms. It solves the problem of integrity, reliability and authentication of medical image by using SHA-1 and ACC, AHF and RSA and AHF and ACC methods. We can also embed large amount of data inside the medical image with less distortion in an image. Since it requires secret key for both embedding and extraction process, it gives better authentication to our medical images. Medical images are authenticated in web server by using Kerberos algorithm. In future we can use better lossless compression algorithm like JPEG-LS.

REFERENCES

Baisa L.Gunjal & Suresh N.Mali 2012. ROI based embedded watermarking of medical images for secured communicationin telemedicine. The international journal of computer and communication engineering:293-298.

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

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

Digital imaging and communication in medicine (DICOM) standard 2007. [online]. Available:www.nema.org.

Gaochang Zhaol, Xiaolin Yang, Bin Zhoul & Wei Wei 2009. RSA based digital image encryption algorithm in wireless sensor networks. Proc. second international conference on signal processing systems:640-643.

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

Imen Fourati kallel, Mohamed Salim Barehlel & Jean-Christophe Lapayre 2007. Improved Tian's Method for Medical Image Reversible Watermarking.GVIP.7(2):1-7.

ISO 2000. JPEG2000 image codingsystem.ISO/IEC FCD 15444-1. JPEG2000 part I Final Committee Draft Version 1.0.

Jasni mohamad zain 2012. Strict authentication watermarking with JPEG compression(SAW-JPEG) for medical images. Europian journal of scientific research.42:232-241.

Lehmann T, M.Guld, C.Thies, B.Fischer, K.Spitzer, D.Keysers, H.Ney, M.Kohnen & B.Wein 2004. Content based image retrieval in medical applications. Methods inf.med..**43**(4):354-361.

Li.Qunkuang, Yuan Zhang & Xie han 2009. A medical image authentication system based on reversible watermarking. IEEE 1St international conference on information science and engineering:1047-1050.

Ma Li, Xiaoshi Zheng, yanling Zhao, Huimin wu & Shifeng li 2008. Robust algorithm of digital image watermarking based on discrete wavelet transform. Electronic commerce and security international symposium:942-945.

Micheal W.Marcellin, Micheal J.Garmish, Ali Bilgin & Martin P.Bolick 2000. An overview of JPEG2000. in proc IEEE data compression conference: 523-541.

Mohammad Reza Keyvanpour & Farnoosh Merrikh-Bayat 2010. A new encryption method for secure embedding in image watermarking.Proc. of third int. conference on advanced computer theory and engineering.2:402-407.

Nisar Ahmed memon 2010. Watermarking of medical images for content authentication and copyright protection.PhD thesis. GIK institute of engineering sciences and technology. Pakistan.

Osbarne D, D.Rogers, J.Muzumdar, R.Coutts & D.Abbott 2009. An overview of wavelets for image processing for wireless applications. Proceedings of SPIE smart structures devices and systems. University of Melbourne.Australia.4935:427-435.

Pan W, G.Coatrieux, N.Cuppens Boulahia, F.Cuppens & 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.

Khan A, A.Siddiqa, S.Munip & S.A.Malik 2014. A recent survey on reversible watermarking techniques. DOI:10.1016/j.ins.2014.03.118, Information sciences.

RC Gonzalez, RE Wood 2006: Digital Image Processing.2nd Ed.New Delhi. India.

Saied QAmirgholipour kasmani & Ahmadreza naghsh-Nilchi 2008. A new robust digital image watermarking technique based on Joint DWT-DCT transformation. Convergence and hybrid information technology. **2**: 539-544.

Umamageswari A & G.R.Suresh 2013. Security in medical image communication with ROI based lossless watermarking and digital signature. The proceedings of NCIEEE'13.

Umamageswari A & G.R.Suresh 2013. Enhancing security in medical image communication with JPEG2000 compression and lossless watermarking. The proceedings of the fourth international conference on signals and image processing. Lecture notes in electrical engineering 221,DOI.10.1007/978-81-322-0997-3-36. Springer. India: 399-408.

Umamageswari A & G.R.Suresh 2013. Security in medical image communication with arnold's cat map method and reversible watermarking. The proceedings of international IEEE conference circuits, power and computing technologies.

William stallings 2010. Cryptography and network security. New delhi. India.

Zhou X.Q, H.k huang & S.L.Lou 2001. Authenticity and integrity of digital mammography images. IEEE transactions on medical imaging. **20**(8):784-791.

Submitted: 12/01/2014

Revised: 26/05/2014

Accepted: 30/06/2014