© May 2016 | IJIRT | Volume 2 Issue 12 | ISSN: 2349-6002

Medical Image Authentication using Combination of Cryptography and Watermarking

Mamta Mangtani[1], Narendrasinh Limbad[2]
[1]*PG Scholar, Computer Engineering, L.J.I.E.T*
[2]*Asst.Professor, Computer Engineering, L.J.I.E.T*
Ahmedabad, India

***Abstract*— In this paper, we propose a combined encryption and reversible watermarking system for the purpose of protecting medical information. The method uses modified quantization index modulation scheme for watermark embedding. The encryption is done using RC4: a stream cipher algorithm and AES: a block cipher algorithm in cipher block chaining (CBC) mode of operation. Watermarking will protect the ownership identity and everything it is supposed to but encryption will be highly desirable in the case of medical images to ensure authenticity of the same. The security analysis of our system and experimental results achieved on ultrasound images which one is 8-bit as well as on 16-bit encoded positron emission tomography(PET)images demonstrate the capability of our system to securely make available security attributes.**

***Index Terms*— Image watermarking, Encryption Algorithm, Medical image security, PSNR, MSE,NCC**

I.INTRODUCTION

In recent years the growth of the digital multimedia technology and the successful development of the internet raise the issue to protect copyright ownership. A digital watermarking is better solution. Embedding the specific information in digital content such as a picture, animation or sound without any perceptual changes in digital watermarking technology [1]

Digital data is widely used in various characteristics of human life because it offers cost-efficiency and flexibility on data manipulation, storage and transmission. Medical imaging systems (such as Computed Tomography, Magnetic Resonance Imaging, X-ray imaging, Ultrasonography) require reliable security in storage and transmission of digital images. In medical image, the patient information has been embedded into the image as watermark image. As the doctor diagnose from medical images, special care is required to hide the information in medical images[2][3]

The rapid evolution of modern communication technologies offers different means of exchange the medical images between hospitals has become usual practice nowadays. This exchange of medical images inflicts three restraints for medical images [4]

1.Confidentiality:Only authorized person have right to use patient data

2.Availability:There should be guarantees medical information has to be access

3.Reliability:Reliability is based on integrity and authentication

- Integrity: Patient information is not altered or modified by unauthorized user
- Authentication: A proof of information origin and of its attached to one patient

Among the security mechanism, encryption is used to ensure the confidentiality. Encryption appears as an "a priori"protection mechanism .watermarking is proposed as a complementary mechanism to improve the security of medical image. Nowadays, combine encryption and watermarking in order to benefit of their complementarily in terms of a priori/a posteriori protection [4]

II.CRYPTOGRAPHIC AND WATERMARKING ALGORITHM

This research paper proposes the two most popular type of cryptographic algorithm: Stream cipher algorithm and block cipher algorithm

RC4 is used to manipulate the stream in stream cipher algorithm and AES (advanced encryption standard) is used to operate on block of data in block cipher algorithm [6]

A Stream Cipher Algorithm

RC4 algorithm includes the following major steps[5]:

1. Key scheduling algorithm
2. The pseudo random generation algorithm

3. XOR operation between the key and plaintext message.

The pseudo random generator (PRNG) generate key stream of bit/bytes

The basic step in RC4 PRNG is:

1.Initialization: In which, with the repetition keys, 256 bytes of table is filled

2.Permutation: To generate key stream the elements of table are combined and addition are applied

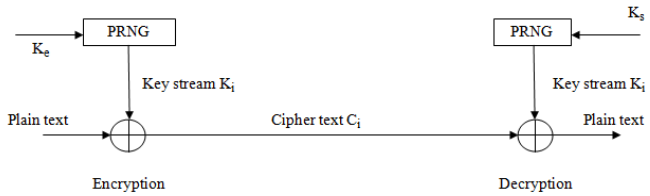
Now generation of PRNG key stream, which are multiplied with plaintext through XOR operation

Ci=ti(XOR)ki

Where C=[c1…ci…cn] called cipher text

T=[t1…ti…tn] is plaintext

K=[k1…ki…kn] is key stream



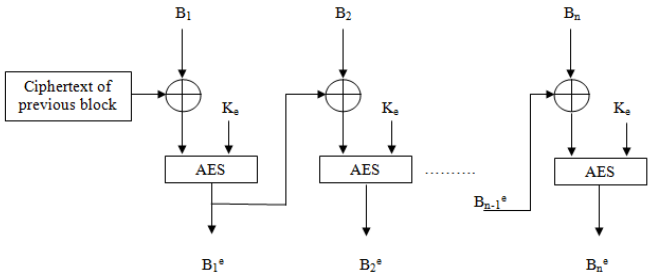
(a)

B Block Cipher Algorithm

In Block Cipher Algorithm the AES(Advanced Encryption Standard) algorithm is used in CBC (Cipher Block Chaining) mode of operation

When CBC(Cipher Block Chaining) mode is applied the plaintext block is combined with previous cipher text block through XOR operation

when the CBC(Cipher Block Chaining) mode is applied, a plaintext block is combined, with the previous cipher text block through a XOR operation before being encrypted with the AES. If we denote *Be i* the encrypted version of a block *Bi* and *Bei*−1 the previous encrypted block, *Be i* is thus given by *Bei*= AES(*Bi* ⊗*Bei*−1,*Ke* where *Ke* is the encryption key



(b)

Figure 2.1 (a) RC4 stream cipher Algorithm (b)AES block cipher Algorithm in CBC mode

C Watermarking Algorithm

The modified QIM (quantization index modulation) technique is used for embed the medical information of patient in medical image.A modified QIM based watermarking method of medical image is proposed in this work where each watermark bit is spreaded over N-mutually orthogonal signal points. First cover signal is projected on *N*-mutually orthogonal signal points in *N*-dimensional signal space. The projection may be accomplished in down sampling the cover by a factor of *N*. The cover (***X***) can mathematically be represented as $\boldsymbol{X = \{X_1, X_2 ,\ldots, X_N\}}$where$\{X_i\}$ is the signal coefficients corresponding to complete orthogonal basis function set[7]

Watermark Insertion:

a) Generation of Binary Dither for QIM: Two dither sequences, with length *n*, are generated pseudo randomly using a '*key'* with step sizes (*Δ*) as follows:

$$d_q(0)=\{key\times\Delta\}-\Delta/2 \qquad 0<=q<=n-1$$

$$d_q(1) = d_q(0)+\Delta/2 \quad if \quad d_q(0)<0$$
$$d_q(1) =d_q(0) - \Delta/2 \quad if \quad d_q(0)<1$$

Where (*key*) is a random number generator. Dither *d* (0) and *d*(1)are used for embedding watermark bit '0' and '1',respectively

b) Watermark bit Insertion: In QIM watermarking host signal points are quantized, using a quantizer Q_Δ (.), based on the message bit (*m).* The watermarked signal, ($\boldsymbol{X'_N}$) is considered as a *N*-dimensional vector $\boldsymbol{\{X'_1, X'_2, X'_3\ldots X'_N\}}$ and may be written as follows:

$$\boldsymbol{X'_N} = Q_\Delta (\boldsymbol{X_N} +k\times d\ (m)) - d\ (m);\ m \in\{0, 1\}$$

Where, 'Δ' is a fixed quantization step size, *d* (.) is the used dither for embedding watermark bit. The factor *k* represents the degree of quality degradations for the image. The value of *k* is set to 2 in this paper as that amount of distortion is sufficient for access control of image. The numerical value of 'k' in Equation .has been determined from independent experimentations conducted over large number of benchmark images having varied image characteristics

Watermark Decoding:

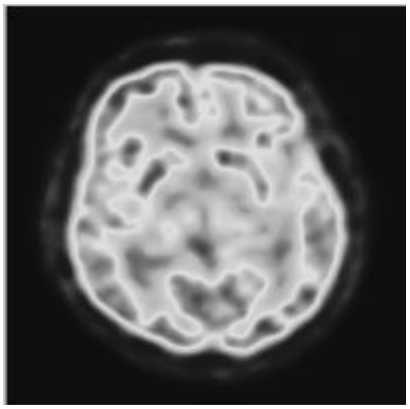
The steps for watermark decoding process are described as follows:

Step1: watermark encoding to generate binary dither, using the same step size (Δ) and key that were used at the time of watermark embedding

Step 2: Watermark Bit Extraction: The received watermarked signal is first projected onto *N*-orthogonal signal points and requantized using m^{th} dither resulting in $r^m=\{r_1,r_2,r_3,\ldots r_N\}$

The decision variable for the m^{th} dither at n^{th} signal point is denoted by r_n and can be written as follows:

$$r_n=|X'_N- Q_\Delta(X'_N+d(m))-d(m)|;m\in\{0,1$$



(a)

(b)

Figure 2.2 sample test image(a)PET image (b)Ultra sound image

III.PROPOSED JOINT WATERMARKING AND CRYPTOGRAPHIC ALGORITHM

A) *Embedding Algorithm:*

In this paper medical information is embedded in medical image using join watermarking and encryption algorithm.

At sender side, patient data is converted into ASCII form then apply encryption AES algorithm using cipher block chaining mode for encrypt the data. For embedding the encrypted data into medical image first apply the data hiding method on that image. In this paper modified QIM method is proposed for embed the data. In modified QIM method N-mutually orthogonal signal used for projection of image and dither is used for embed the'0 and'1' bit into medical image. After that SHA-512 algorithm is used for integrity check, and watermark image is send to receiver side.

Step1: First Convert Patient Data into Binary form

Step2: Apply Encryption Algorithm on Patient's Data Using Cipher Block Chaining (CBC) mode of AES (blocked-cipher) algorithm

Step3*:* Then apply modified QIM method on medical image

Step4*:* Calculate hash value using SHA-512

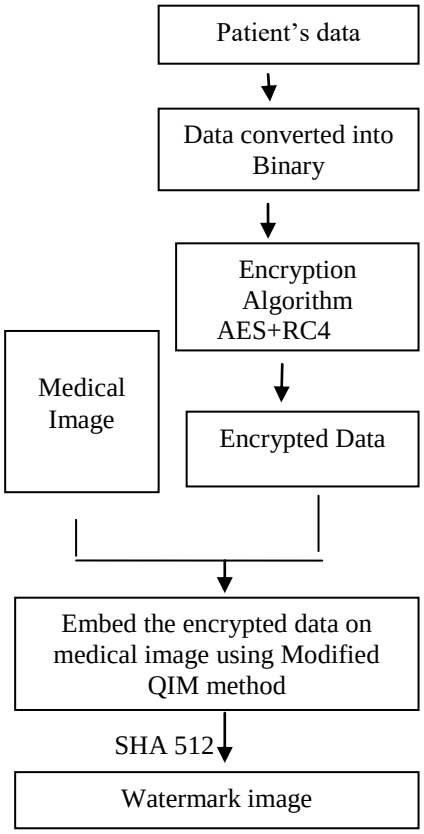


Figure:3.1 Embedding process of proposed method

B) Extraction Algorithm:

The watermark medical image is now ready to send through network to doctor at another locations

At receiver side, the hash of the received medical image is calculated and compared with the extracted hash value. If they both match then the received medical image is accepted and proof that the medical information will not be destroy else the medical image has been tampered. After that for decode the encrypted medical data from watermarked medical image, apply the watermark decoding method of modified QIM using same step size and key that were used at the time of watermark embedding. In last decrypt the patient data using AES decryption and RC4 decryption algorithm. After extraction of watermark the original image was recovered and same watermark was also recovered.

Step1: Receive the watermark medical image
Step2: Check hash value, if hash value is same than proof that no medical information is destroy
Step3: Decode the medical data using modified QIM method
Step4:Decrypt the medical data using AES and RC4 algorithm

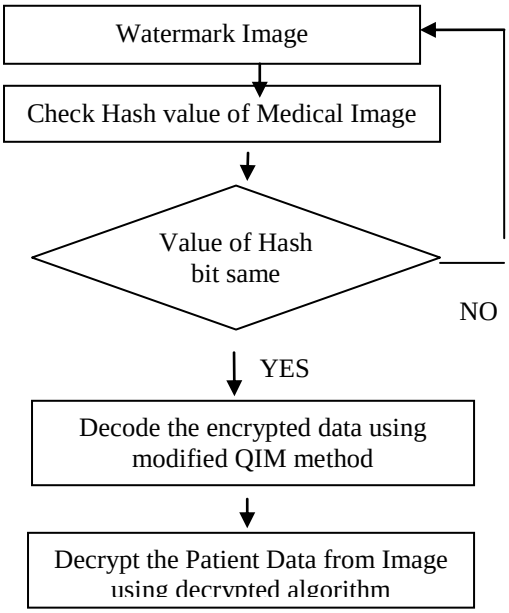
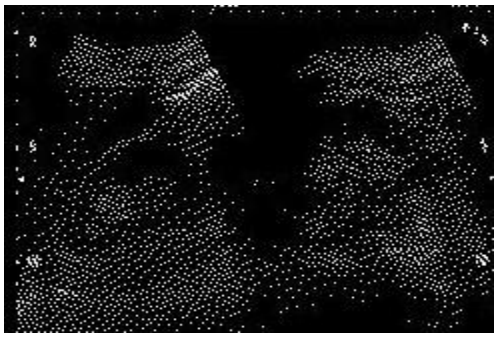


Figure:3.2 Extraction process of proposed method

(a)



(b)

(c)

Figure:3.3 (a) original ultra sound image (b) join watermark /ciphered (dither image) (c) Decrypted image

IV. EXPERIMENTAL RESULTS

Type of Image	QIM Method paper[6]	Modified QIM Method
	PSNR	
Ultra Sound Image	60.85	75.13
PET Image	52.59	60.10

Table4.1 PSNR Result

Type of image	Entropy of original image		Entropy of Encrypt image		Entropy of Watermark image	
	Paper [6]	Propose method	Paper [6]	Propos method	Paper [6]	Propose method
PET	5.66	5.66	7.99	7.27	7.99	7.27
Ultra Sound	6.21	6.21	7.98	7.10	7.98	7.11

Table 4.2 Entropy Result

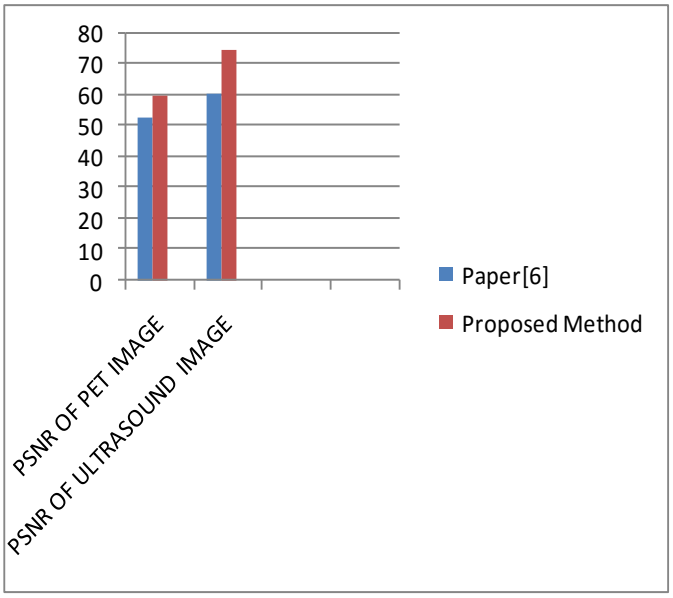
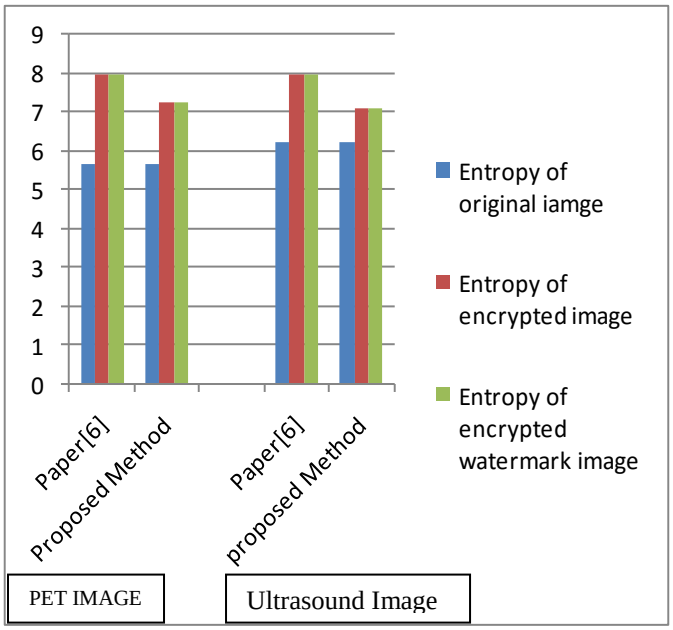


Figure 4.1 Comparison Graph of PSNR Value



V. CONCLUSION

In this paper, we have proposed a joint watermarking and cryptography algorithm, which guarantees a priori and *a* posteriori protection of medical images. It merges the reverse watermarking technique modified QIM method and a stream cipher algorithm and a block cipher algorithm. Modified QIM method for data embedding to achieve the robustness of medical information. In this paper also achieve the integrity of data using SHA-512 hash algorithm is use. Using the modified OIM method also achieve the quality of image

REFERENCES

[1]Toshiki Ito,Ryo Sugimura,Hyunho Kang, Keiichi Iwamura,Kitahiro Kaneda,Isao Echizen,Niijuku, Katsushika-ku, Hitotsubashi, Chiyoda-ku"A New Approach to ReversibleWatermarking"2014 IEEE pp.455-458

[2]Nelmiawati,Mazleena Salleh, MalekNajib Omar" Pixel-Based Dispersal Scheme for Medical Image Survivability and Confidentiality"2014 IEEE pp.298-303

[3]Md.Moniruzzaman, Md.Abul Kayum Hawlader andMd.FoisalHossain"Wavelet BasedWatermarkingApproach of Hiding Patient Information in Medical Image for Medical Image Authentication"2014 IEEE pp.374-378

[4]D. Bouslimi, G. Coatrieux" Combination of Watermarking and Joint Watermarking-Decryption for Reliability Control and Traceability of Medical Images"2014IEEE

[5] Mehbooba P Shareef, Divya T v, Nimisha Abraham,Tina Babu and Reshma KV" Encryption-Enhanced Reversible Watermarking for Medical Images via Prediction and RC4 Encryption" 2014 IEEE

[6]Suganya G, Amudha K" Medical Image Integrity Control Using Joint Encryption and Watermarking Techniques" 2014 IEEE Pages: 1 – 5

[7]Amit Phadikar, Himadri Mandal, Goutam Kr. Maity, Tien-Lung Chiu"A New Model of QIM Data Hiding for Quality Access Control of Digital Image" IEEE International Conference on Soft Ccomputing and Network Security ISDN-978-1-4799-1752-5,pp.1-5,2015