Authentication of DICOM Medical Images using Multiple fragile watermarking Techniques in Wavelet Transform Domain

A.Kannammal[1*], Dr.S.Subha Rani[2]

[1] Assistant Professor
Department of Electronics and Communication Engineering
PSG College of Technology, Peelamedu, Coimbatore-641004
Tamil Nadu,India.

Professor and Head
Department of Electronics and Communication Engineering
PSG College of Technology, Peelamedu, Coimbatore-641004
Tamil Nadu,India.

ABSTRACT

A multiple, fragile image authentication scheme is proposed for DICOM images using discrete wavelet transform. This scheme addresses critical health information management issues, including source authentication, data authentication and transfer of patient diagnosis details. The robustness of the method is enhanced through a form of hybrid coding, which includes repetitive embedding of BCH encoded watermarks. The watermarked images were tested with common attacks to evaluate the behaviour of the algorithm. Conclusions were drawn based on the algorithms performance when the images were subjected to various attacks. The algorithm was also tested by changing the wavelet function used in the algorithm and the results show that the Haar wavelet is the most suitable wavelet. The experimental results on different medical images demonstrate the efficiency and transparency of the watermarking scheme, which fulfils the strict requirements concerning the acceptable alterations of medical images.

Key Words*- DICOM images, multiple watermarking, discrete wavelet transform.TAF.*

1. Introduction

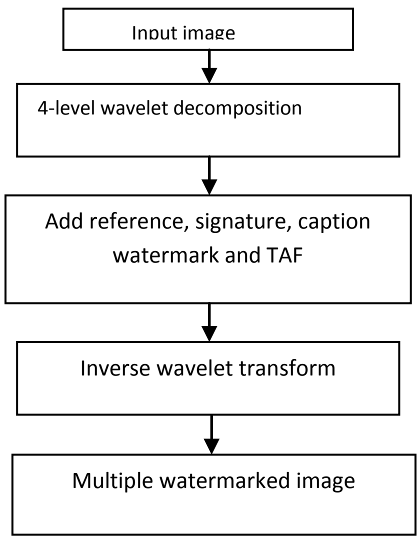
Digital watermarking has been used to increase medical image security, confidentiality and integrity. watermarked medical images should not differ perceptually from their original counterparts Digital data or images can be easily manipulated without leaving any trace of modification. Image authentication is the process of giving a legal validity to the data. By authentication technique, content tampering can be detected and we can indicate the true origin of the data [1]. Recent innovations in information and communication technologies have led to a new era in healthcare delivery and medical data management [2]. New challenges have arisen as a result of easier access and distribution of digital data, especially regarding security of sensitive medical information. The research community seeks complementary solutions to confront these challenges and to effectively deal with a range of substantial healthcare information management issues. Image authentication can be done using watermarking or encryption schemes.

The work is to watermark medical images [3] in an irreversible way and to use the watermarked data for authentication. The medical images used will be in DICOM (Digital Imaging and Communications in Medicine) format. Multiple watermarks [4] will be embedded in the image for source authentication, data authentication and transfer of patient diagnosis details. The watermarked images will be tested with common attacks to evaluate the behaviour of the algorithm. Conclusions will be drawn based on the algorithms performance when the images are subjected to various attacks. The performance of the algorithm will be measured using Peak Signal to Noise Ratio (PSNR) and a Tamper Assessment Factor (TAF).A good image authentication technique should satisfy the following criteria: It should be invertible and should support all data formats. It should be robust against incidental image processing operations, but it must detect malicious tampering The test images used are 256X256 size medical (DICOM) images.

2. Proposed algorithm

2. 1 .Watermark Embedding Algorithm:

In this method multiple watermarks such as, the reference watermark, TAF[6] of the watermarked image, patient diagnosis information and the physician's signature are embedded into wavelet transform domain.. The reference watermark is a fixed bit pattern that is used for tamper proofing or image authentication. The TAF value and patient diagnosis information act as caption watermark which gives additional information about the image. The physician signature is used for source authentication. All the data to be watermarked are represented in ASCII values. These values are BCH coded and embedded in many places to give additional robustness for the watermarking scheme. The steps involved in embedding the watermark are shown in Fig.1.



Fig(1)Watermark Embedding Procedure

Initialization:

- Given f(m,n) – image to be watermarked.
- Given w(m,n) – watermark information to be embedded
  - ➢ The watermark information consists of the patient information, physician's signature and the TAF value of the watermarked image. All the watermark information is represented using ASCII values and BCH encoded.
  - ➢ These watermarks are improving the robustness and also used to indentify the tampered images

Step 1: *Decomposing the image into Wavelet Coefficients*

Perform the 4 level discrete Haar wavelet transform [7,8] on the image $f(m,n)$ to produce 12 detail coefficient images $f_{k,l}(m,n)$ where $k = h,v,d$ (horizontal, vertical or diagonal detail coefficient) and $l = 1,2,3,4$ is the particular detail coefficient resolution level, and a gross approximation at the lowest resolution level $f_{a,4}(m,n)$. That is,

$$\{f_{k,l}(m,n)\} = \text{DWT}_{\text{Haar}}\left[f(m,n)\right] \quad \text{--(1)}$$

Step 2: *Embedding watermark*

The multiple watermark such as patient information(PI),physician's signature(PS),Tamper assessment Factor(TAF).The reference watermark embedding locations in a four level wavelet decomposed image is shown in Fig.(5).All the data to be watermarked are represented in ASCII values. These values are BCH coded and embedded in many places to give additional robustness for the watermarking scheme. Perform quantization of the wavelet coefficients in places where watermark is to be embedded using the quantization function

$$Q(f) = \begin{cases} 0, & \text{if } r\Delta \le f < (r+1)\Delta \text{ for } r = 0, \pm 2, \pm 4.... \\ 1, & \text{if } r\Delta \le f < (r+1)\Delta \text{ for } r = \pm 1, \pm 3, \pm 5..(2). \end{cases}$$

where Δ - quantization parameter (positive real number)

- If $Q(f_{k,l}(m,n)) = w(i)$, then no change in the coefficient is required.
- Otherwise, change $f_{k,l}(m,n)$ such that we force $Q(f_{k,l}(m,n)) = w(i)$ using the following assignment:

$$z_{k,l}(m,n) = \begin{cases} f_{k,l}(m,n) + \Delta & \text{if } f_{k,l}(m,n) = \begin{cases} = 0 \\ \le -\Delta \end{cases} \\ f_{k,l}(m,n) + 2\Delta & \text{if } -\Delta < f_{k,l}(m,n) < 0 \\ f_{k,l}(m,n) - 2\Delta & \text{if } 0 < f_{k,l}(m,n) < \Delta \\ f_{k,l}(m,n) - \Delta & \text{if } f_{k,l}(m,n) \ge \Delta \end{cases} \quad -(3)$$

Step 3: Getting the Watermarked image

Perform the 4^{th} level inverse discrete Haar wavelet transform on the transformed wavelet coefficients $\{z_{k,l}(m,n)\}$ to produce the watermarked image $z(m,n)$. That is,

$$z(m,n) = IDWT_{Haar}\left[\{z_{k,l}(m,n)\} - (4)\right]$$

for $k = h, v, d, a$ and $l = 1,2,3,4$.

3. Testing for various attacks

The water marking procedure was done for twelve radiological images with different anatomy. The effect of various commonly occurring attacks [9] like Modification, Rotation and cropping, Brightness and Contrast adjustment, noises,[10] was observed. The various attacks for which the authentication effects were observed are listed below:

1. **Modification:** In modification, small area is removed from the image completely. The effect of this attack is tested at the center, top left, top right, bottom left and bottom right of the image.
2. **Rotation and Cropping:** The rotation operator performs a geometric transform which maps the position $(x_1.y_1)$of a picture element in an input image onto a position (x_2,y_2)in an output image by rotating it through user-specified angle ɵ about an origin o. In most implementations, output locations$(x_2,y_2\ )$which are outside the boundary of the image are ignored.
   The image was rotated for the angles 15°, 30°, 45° and 90°. The cropped corners after rotation were lost in the process.
3. **Brightness adjustment:** The brightness attack was performed using the formula,
   $$f(x,y) = g(x,y) + \beta \quad \text{--(5)}$$
   The various values added for testing are $\beta = 35, 600, 2500, 10000$.
4. **Contrast adjustment:** The contrast attack was performed using the formula,
   $$f(x,y) = g(x,y)^{\gamma} \quad \text{--(6)}$$
   The various exponents used were, $\gamma = 0.5, 0.8, 1.2, 3.0$ when γ <1, the image contrast decreases otherwise it increases.
5. **Horizontal flip and Vertical flip**
   Here the image is flipped about its horizontal axis by interchanging the rows above and below the horizontal axis. Here the image is flipped about its vertical axis by interchanging the columns to the left and right of the verticals axis
6. **Blurring:**
   Here a frequency domain Gaussian Low Pass Filter with standard deviation of 0.2, 0.5, 0.8 and 2 were used to blur the edges of the image.
7. **Sharpening**
   The sharpening of the image was carried out using Laplacian high pass filter with standard deviation of 0, 0.3, 0.7 and 1. The edges of the sharpened image were enhanced during the process.
8. **Averaging filter**
   Averaging filter was implemented using two dimensional spatial masks of sizes: 3×3, 5×5, 7×7 and 9×9. When size of the mask is increased the blurring caused also increases.
9. **Addition of Salt & Pepper Noise**
   Salt and pepper noise is also known as impulse noise or shot noise. Salt and pepper noise with variance of 0.01, 0.05, 0.1 and 0.5 were added to the image
10. **Addition of Gaussian Noise**
    Gaussian Noise is the most common form of noise encountered in most of the communication channels. The Gaussian noise with variance of 0.01, 0.05, 0.1 and 1 were added to the image.
11. **High Boost filtering**

    In high boost filtering a blurred version of the image is subtracted from the image to obtain a sharpened image. The weight given to the center pixel in the mask is varied using an alpha factor which is given the values 0.2, 0.5, 0.8 and 1.

4. Quality measure of proposed algorithm:

Any algorithm should be evaluated on basis of certain quality measures. Here we have used two quality measures: Peak Signal to Noise Ratio (PSNR) and Tamper Assessment Factor (TAF).

4.1. Peak Signal to Noise Ratio (PSNR)

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is most easily defined via the mean squared error (MSE) for which two $M \times N$ images f and z where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(f(x,y) - z(x,y)\right)^2 \quad \text{---(7)}$$

The PSNR is defined as:

$$PSNR = 10 \times \log_{10} \frac{MaxBits^2}{MSE} dB \quad \text{----(8)}$$

Here, $MaxBits$ is the maximum possible pixel value of the image. When samples are represented using B bits per sample, $MaxBits$ is 2^B-1.

4.2. Tamper Assessment Factor (TAF):

It gives the difference between the actual embedded watermark and the reconstructed watermark. It is given by the expression

$$TAF(w, \tilde{w}) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} w(x,y) \oplus \tilde{w}(x,y) \quad -(9)$$

where M, N - dimensions of the image

w - embedded watermark

$\tilde{w}$ - reconstructed watermark

$\oplus$ - denotes exor operation

The value of TAF ranges between zero and one.

5. Results and Discussion about various attacks and wavelet transforms:

The water marking procedure was done for different radiological images and the overall results were tabulated in Table.2. Figure(2) shows the original Image.Figure(3) shows the four level wavelet decomposed image.Figure(5) shows the location of four different watermarks(TAF,physical signature,patient information,,reference watermark) in four level wavelet coefficients. After applying all the watermarks in the wavelet coeffiecients the inverse wavelet transform are applied ,then the multiple watermarked image was obtained is shown in Figure (4) .Then the watermarked image is analysed for differenent attacks and the results are shown in Table.1

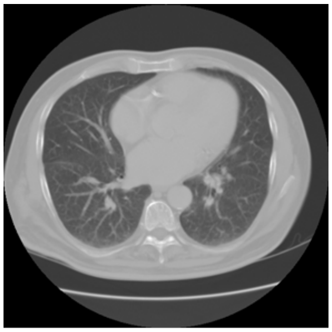
5.1.Different Attacks

1. *Modification attack*: The embedded information was retrieved in most of the cases and the average TAF was at least 19% more than the actual TAF of the watermarked image.
2. *Rotation and Cropping attack*: The embedded information was lost completely when the image is subjected to Brightness attack
3. *Brightness attack:* The embedded information was retrieved when Beta is between 100 and 4000. TAF was at least 70% more than the actual TAF of the watermarked image.
4. *Contrast attack:* The embedded information was lost completely when the image is subjected to Contrast attack.
5. *Flip:* The flipped image when seen by a person may be mistaken to be the actual radiological image that was taken. But on retrieving the embedded watermark we can observe the effect of flipping very clearly.
6. *Blurring:* The reference watermark is modified completely even though Blurring of the image is very less and the image cannot be differentiated from the actual image by the human eye.
7. *Sharpening:* The Sharpened image may appear to be the actual image but on seeing the recovered reference watermark we can say that the image has been subjected to modification
8. *Averaging*: The reference watermark is modified completely even though Blurring of the image is very less and the averaged image is difficult to differentiate from the original image by the human eye.
9. *Salt and pepper Noise:* The embedded reference watermark is lost completely when the image is corrupted by Salt & Pepper Noise.
10. *Gaussian Noise:* The embedded reference watermark is lost completely when the image is corrupted by Gaussian Noise.
11. *High boost filtering:* The Laplacian sharpened image can be easily differentiated by the human eye. The drastic increase in TAF and decreased PSNR further confirm that the image has undergone some modification.

5.2 .Performance of the algorithm for various wavelet functions

The embedded TAF value was retrieved in most of the cases is shown in Table.3.. The TAF was retrieved for all cases when using Haar, Symlet and Integer wavelet. But the patient information and the physician signature were retrieved only when using the Haar wavelet in the algorithm. Thought the PSNR of the image watermarked using Integer wavelet transform is more than the PSNR of watermarked image using Haar wavelet, the TAF is considerably high. So from the results we can say that the Haar wavelet is best suitable for algorithm used for watermarking the DICOM images.

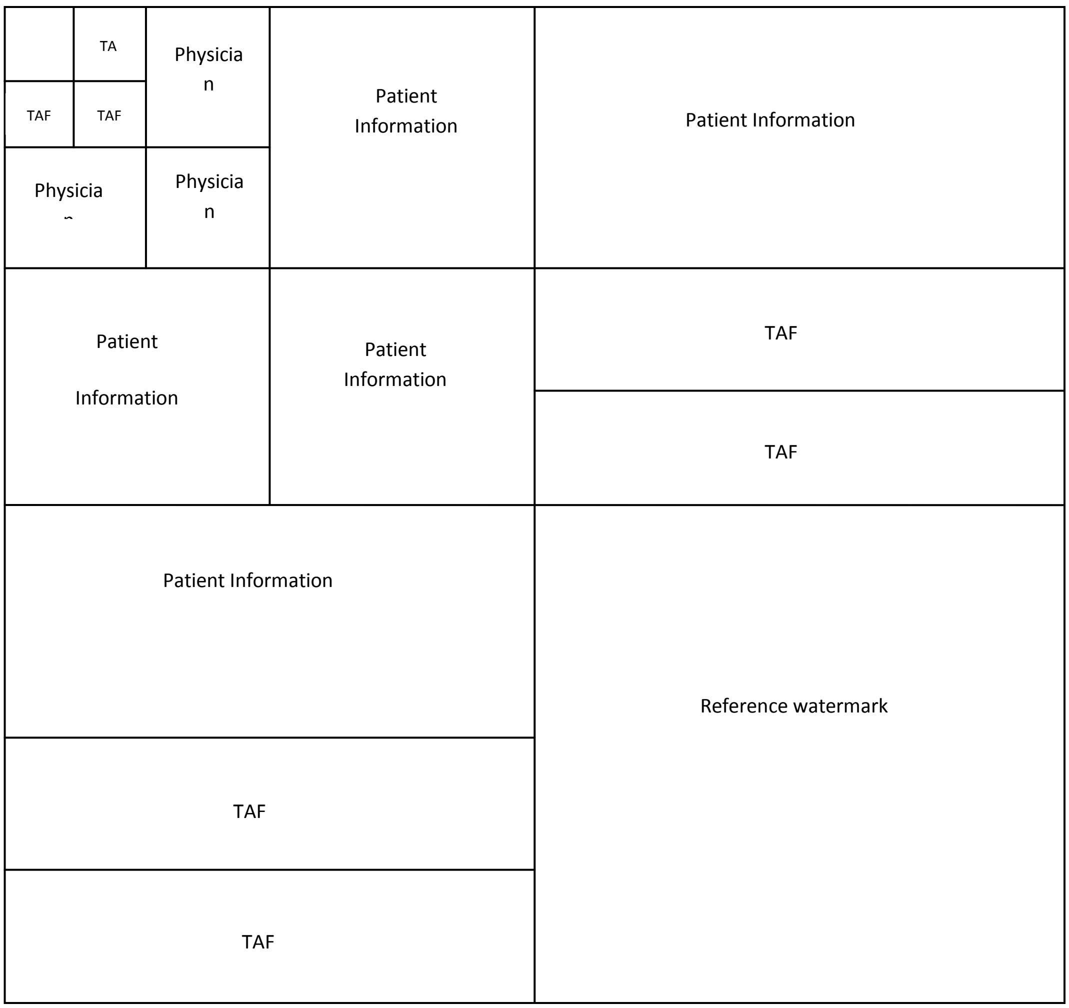
IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011
ISSN (Online): 1694-0814
www.IJCSI.org



Fig(2)Original Image

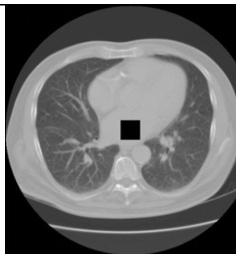
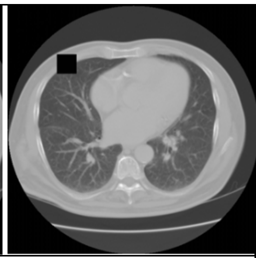
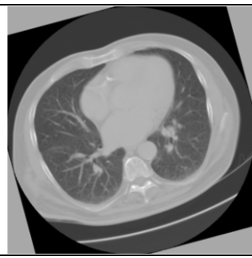
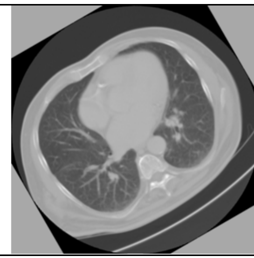
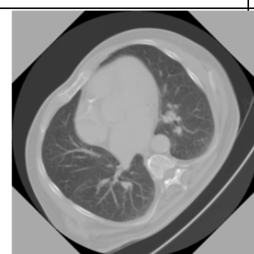
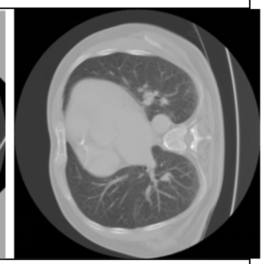
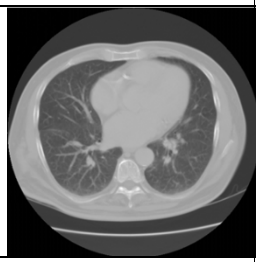
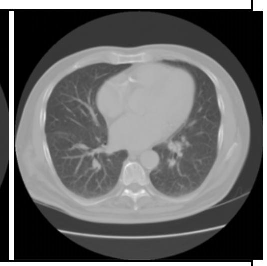
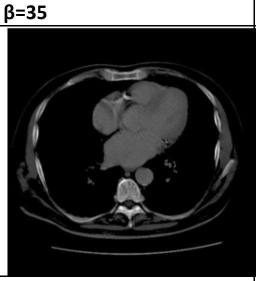
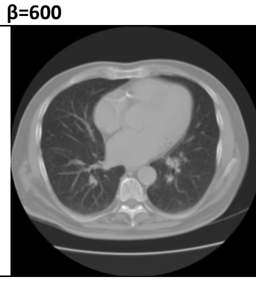
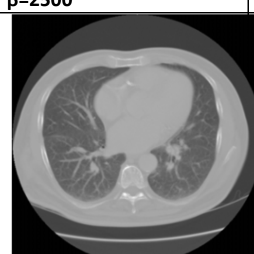
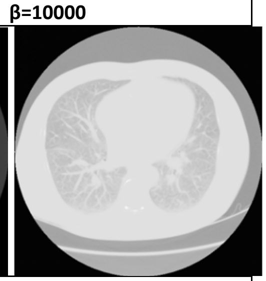
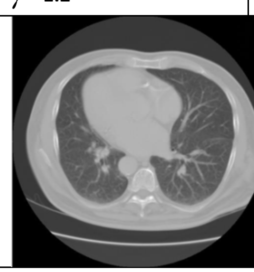
Fig(3) Four level Wavelet decomposed image

Fig (4) Multiple watermarked image



Fig(5) Watermark embedding locations in a 4-level wavelet decomposed image

Table.1.Output of Different attacks outputs

Modification attacks				
				
At center	**At top left**	**At top right**	**At bottom left**	**At bottom Right**
Rotation and cropping				
	θ=15	**θ=30**	**θ=45**	**θ=90**
Brightness				
	β=35	**β=600**	**β=2500**	**β=10000**
Contrast				
	γ **=0.5**	γ **=0.8**	γ **=1.2**	γ **=3.0**
Flip		Horizontal		Vertical

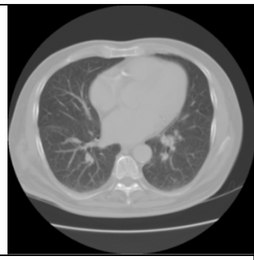
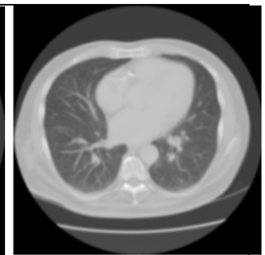
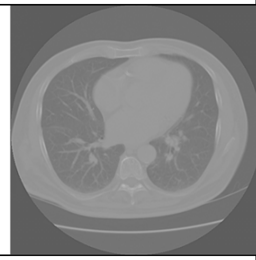
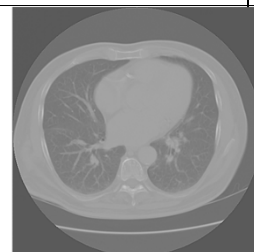
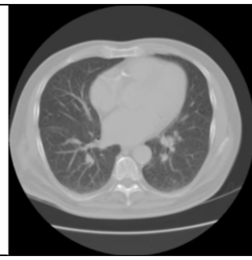
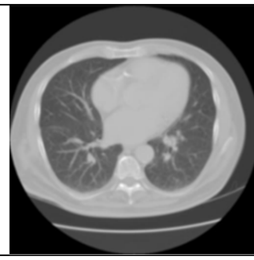
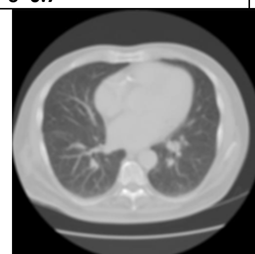
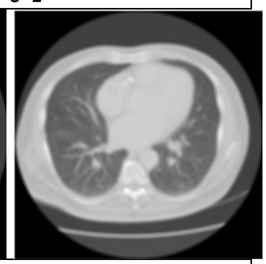
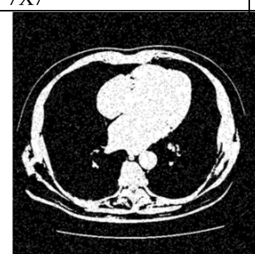
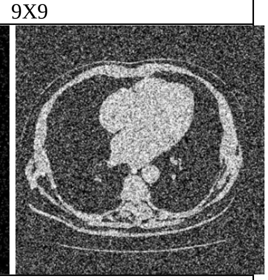
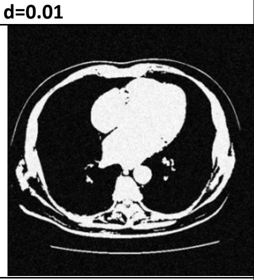
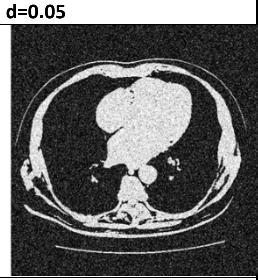
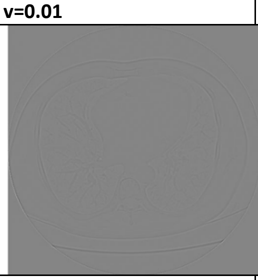
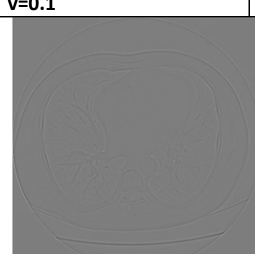
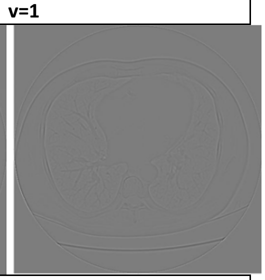
Blurring(Gaussian LPF)				
	σ=0.2	**σ=0.5**	**σ=0.8**	**σ=2.0**
Sharpening(Laplacian HPF)				
	σ=0	**σ=0.3**	**σ=0.7**	**σ=1**
Averaging(Spatial Averaging Filter)				
	3X3	5X5	7X7	9X9
Salt and pepper Noise				
	d=0.01	**d=0.05**	**d=0.1**	**d=0.5**
Gaussian Noise				
	v=0.01	**v=0.05**	**v=0.1**	**v=1**
High boost filtering				
	α=0.2	**α=0.5**	**α=0.8**	**α=1**

Table2.Anaylsis of Different attacks and different watermarks

Attacks	Types	Average TAF	Average PSNR	Patient info	Physician sign	Embedded TAF
Modification	At center	0.0084	55.58894167	Retrieved	Retrieved	Retrieved
	At top left	0.0084	59.18993333	Retrieved	Not Retrieved	Retrieved
	At top right	0.0083	59.30213	Retrieved	Retrieved	Retrieved
	At bottom left	0.0083	58.20526	Retrieved	Retrieved	Retrieved
	At bottom right	0.0083	58.54638	Retrieved	Retrieved	Retrieved
Rotation and Cropping	θ=15	0.1406	42.49909	Error	Error	Error
	θ =30	0.1406	40.86071	Error	Error	Error
	θ =45	0.1405	40.28192	Error	Error	Error
	θ =90	0.1407	43.19115	Error	Error	Error
Brightness	β=35	0.0134	65.4288	Not Retrieved	Not Retrieved	Retrieved
	β=600	0.0142	40.76633	Retrieved	Retrieved	Retrieved
	β=2500	0.009	28.37064	Retrieved	Retrieved	Retrieved
	β=10000	0.0241	16.32948	Not Retrieved	Not Retrieved	Not Retrieved
Contrast	γ =0.5	0.14	39.35022	Error	Error	Error
	γ =0.8	0.1398	41.35969	Error	Error	Error
	γ =1.2	0.1229	30.87605	Error	Error	Error
	γ =3.0	0.1245	86.40327	Error	Error	Error
Flip	Horizontal	0.086392	44.66864	Error	Error	Error
	Vertical	0.068108	48.08443	Error	Error	Error
Blurring(Gaussian LPF)	σ=0.2	0.14	39.35022	Error	Error	Error
	σ =0.5	0.1398	41.35969	Error	Error	Error
	σ =0.8	0.1229	30.87605	Error	Error	Error
	σ =2.0	0.1245	86.40327	Error	Error	Error
Sharpening(Laplacian HPF)	σ=0	0.1478	53.81487	Error	Error	Error
	σ =0.3	0.10985	55.48749	Error	Error	Error
	σ =0.7	0.149167	56.78416	Error	Error	Error
	σ =1	0.115308	57.33012	Error	Error	Error
Averaging (Spatial averaging filtering)	hsize=3	0.207967	65.837	Error	Error	Error
	hsize=5	0.213008	61.77748	Error	Error	Error
	hsize=7	0.210958	59.28639	Error	Error	Error
	hsize=9	0.21455	57.57739	Error	Error	Error
Salt and pepper noise	d=0.01	0.2203	39.22999	Error	Error	Error
	d=0.05	0.2203	39.22978	Error	Error	Error
	d=0.1	0.2203	39.22954	Error	Error	Error
	d=0.5	0.2203	39.22757	Error	Error	Error
Gaussain Noise	v=0.01	0.2203	39.22964	Error	Error	Error
	v=0.05	0.2203	39.22915	Error	Error	Error
	v=0.1	0.2203	39.2288	Error	Error	Error
	v=1	0.2203	39.2269	Error	Error	Error
High Boost filtering	α=0.2	0.111525	38.86525	Error	Error	Error
	α=0.5	0.137925	38.91058	Error	Error	Error
	α=0.8	0.139192	38.93458	Error	Error	Error
	α=1.0	0.149333	38.94469	Error	Error	Error

Table .3.Performance of the algorithm for various wavelet functions

Wavelet function	Average TAF	Average PSNR	Embedded TAF	Patient info	Physician sign
Haar	0.0075	87.44158	Retrieved all	Retrieved all	Retrieved all
Biortogonal	0.0379	85.57798	Retrieved	Error	Error
Coiflet	0.0507	86.32846	Retrieved	Error	Error
Symlet	0.0354	86.5734	Retrieved	Error	Error
Meyer	0.0776	86.89085	Retrieved	Error	Error
Integer	0.0116	90.47334	Retrieved	Error	Error

6. Conclusion

Almost all the images responded in a similar way to the various attacks. The embedded watermarks were retrieved when the image is subjected to Modification and Brightness attack, within certain limits. But the watermarks were completely destroyed in Rotation and Cropping and Contrast Attacks. In the Modification and Brightness attack the embedded TAF value was found to be significantly higher than the retrieved TAF value from the tampered image. So we can conclude that a image is tampered when the reconstructed TAF is greater than the actual embedded TAF, as in Modification and Brightness attack or when the TAF value is not at all recovered from the image, as in Contrast, Rotation and Cropping attack.

References

[1]José Alberto Martínez Villanueva, Claudia Feregrino Uribe and Jezabel Z. Guzmán Zavaleta, "Watermarking algorithms analysis on radiological images," *International Conference on Electrical Engineering, Computing Science and Automatic Control*, pp. 298-303, 2008.

[2]A. Giakoumaki, S. Pavlopoulos, D. Koutsouris "Secure and efficient health data management through multiple watermarking on medical images" *Med Bio Eng Comput* pp. 619–631, 2006.

[3]M. Kutter, F. Hartung, "Introduction to watermarking techniques. In: Katzenbeisser S, Petitcolas FAP (eds) Information hiding techniques for steganography and digital watermarking," Artech *House, Norwood* pp 97–120, 2000

[4]C.S. Woo, J. Du, and B. Pham "Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images" *WDIC2005 pages* pp. 59-64, Australia, February, 2005.

[5]J. Nayak, P. Subbanna Bhat, R. Acharya U and Niranjan UC "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study" *BioMedical Engineering OnLine*, pp. 3-17, 2004.

[6]D. Kundur, D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proc IEEE Vol. 87*, pp. 1167–1180, 1999.

[7]A. Giakoumaki, S. Pavlopoulos, D. Koutsouris "A medical image watermarking scheme based on wavelet transform" *IEEE EMBS Annual International Conference, Cancun, Mexico* pp. 17-21, September, 2003

[8]P. Meerwald, A. Uhl, "A survey of wavelet-domain watermarking algorithms". *Proc of the SPIE security and watermarking of multimedia contents*, Vol. 4314, San Jose, pp. 505–516, 2001.

[9]D. Kundur, D. Hatzinakos, "Diversity and attack characterization for improved robust watermarking", *IEEE Trans Signal Process Vol.49*, pp. 2383–2396, October, 2001

[10]W. Puech, JM. Rodrigues, "A new crypto-watermarking method for medical images safe transfer," *Proc of the 12th European signal processing conference, Vienna, Austria*, pp. 1481–1484, 2004.

Mrs.A.Kannammal *registered Ph.D. in Engineering from Anna University coimbatore in the year 2008, M.E. degree from Thiagarajar college of Engineering , Madurai,Tamilnadu,India in 2004. B. E degree in Electronics and communication engineering, in 2002. In 2004, she joined the Deptt. of ECE,Thiagarajar college of Engineering as Lecturer. She joined PSG College of Technology, India as a Lecturer in the Deptt. of Electronics and Communication in 2007. She is presently working as Assistant Professor in the Deptt. of Electronics and Communication Engineering at PSG College of Technology ,Coimbatore,Tamilnadu, India. Her interests include, Medical Image Processing and Soft computing Techniques. She has contributed 6 technical papers in various journals and conference.*

Dr.S.Subha Rani *received Ph.D. in Engineering from Bharathiar University in the year 2000. M.E. degree from* Anna University*, in 1987. B. E degree in Electronics and communication engineering, in 1984. In 1988, she joined the Deptt. of Electronics and communication engineering as Lecturer. She is presently working as Professor and Head in the Deptt. of Electronics and Communication Engineering at PSG College of Technology, Tamil Nadu, India. Her interests include, Optimal Control, Wireless ystems.MEMS and Soft computing Techniques. She has contributed more than 67 technical papers in various journals and conference. She is a life member of IEEE and IETE, she has completed 04 sponsored projects.*