Journal of Engg. Research **Vol. 2 - (3) Sept. 2014** pp. 159-176

تحليل تفصيلي لتخطيط فعال لتحديد المواقع

[*]أ. أوما أاهيشفا آري و [**] لـ. ثناشكودي
[*]كلية سيري ساكثي للهندسة، جامعة أننا، كويمباتور، تاميلنادو، الهند
[**]كلية أكشايا للهندسة والتكنولوجيا، جامعة أننا، كويمباتور، تاميلنادو، الهند

الخلاصة

خدمات الطب عبر الهاتف والبنية التحتية للعناية الصحية تعتمد على أنظمة المعلومات في المستشفى (HIS)، وأنظمة معلومات لأشعة (RIS)، وأنظمة الأرشفة والاتصالات (PACS)، وذلك لأن هذه النقاط توفر طرقاً جديدة لتخزين وإطلاق وتوزيع المعلومات الطبية. وبنفس الدرجة هذه التطورات أضافت أخطار جديدة نتيجة تدفق المعلومات الطبية في الشبكات المفتوحة. الصور الطبية يجب أن تكون في المتناول في جميع الأحوال وقبل إجراء أية عملية حيث يجب الرجوع إليها للتأكد من صحة المعلومات. تحصلت الخوارزميات ذات المجال الترددي لتحديد المواقع أهمية نتيجة استخدامها الواسع. التخطيط المقترح لتحديد المواقع يستخدم النقل المزدوج والذي يحتوي التحويل الجذري المتقطع (DCT) والتحويل الموجي المتقطع (DWT). عدة أنواع من الهجمات تم إطلاقها مع فحص الأصالة. البرنامج المستخدم هو (مات لاب 7.9). فعالية تحديد المواقع تم قياسها بالمقارنة بالنتائج المخبرية.

A detailed analysis on effective watermarking scheme

A.UMAAMAHESHVARI* AND K.THANUSHKODI**

** Sree Sakthi Engineering College, Anna University, Coimbatore, Tamilnadu, India ums612@gmail.com*

*** Akshaya College of Engineering and Technology, Anna University,Coimbatore, Tamilnadu, India. thantan48@gmail.com*
**Corresponding Author:ums612@gmail.com*

ABSTRACT

Telemedicine and healthcare infrastructure depends on Hospital Information Systems (HIS), Radiology Information Systems (RIS) and Picture archiving and Communication Systems (PACS), as these provide new ways to store, access and distribute medical data. Equally, these developments have introduced new risks for unsuitable deployment of medical information flowing in open networks. Medical images need to be kept intact in any condition and prior to any operation needs to be checked and verified for integrity. In recent times, frequency domain watermarking algorithms have gained immense importance due to their widespread use. The proposed watermarking scheme makes use of hybrid transform, which combines Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In the proposed watermarking scheme, various types of attacks are given and checked for authenticity. The software used is Matlab 7.9 version. The effectiveness of the proposed watermarking scheme is demonstrated with the aid of experimental results.

Keywords: Digital watermarking; discrete cosine transform; discrete wavelet transform; hybrid transform; medical images.

Nomenclature

x1	1^{st} real number sequence	μ_x	Average of x
x2	2^{nd} real number sequence	μ_y	Average of y
xn	n^{th} real number sequence	σ_x^2	Variance of x
f1	1^{st} Complex Number of DCT	σ_y^2	Variance of y
f2	2^{nd} Complex Number of DCT	a_{xy}	Covariance of x and y
fn	n^{th} Complex Number of DCT	W	Binary Watermark Image
h0	First Daubauchie wavelet coefficient	V_I	Storage Vector

h1	Second Daubauchie wavelet coefficient	P_n	n^{th} Pixel Value
h2	Third Daubauchie wavelet coefficient	P_1	1^{st} Pixel Value
h3	Fourth Daubauchie wavelet coefficient	Iv	Immediate Vector
a[i]	Scaling Function	T_I	Transformed Image
c[i]	Wavelet Function	HT_I	Hybrid Transformed Image
I	Original Gray Scale Image	HTm	Hybrid Transformed Matrix
n×n	Size of Image		

INTRODUCTION

Environments and the transfer of multimedia documents across the Internet by the digital data owners have become simple. Thus, there is a rise in concern over copyright protection of digital contents (Piva *et al*., 2002; Wu & Cheung, 2010). Protection of digital images has gained remarkable significance with the omnipresence

The rapid advancement of the Internet and multimedia systems in distributed of internet and mobile. The introduction of image processing tools has amplified the susceptibility for illegal copying, alteration and dispersal of digital images. With this background, the data hiding technologies for digital data like digital watermarking have attracted massive attention recently (Tosihiro *et al*., 2006). Digital watermarking is utilized in order to prevent unauthorized duplication or exploitation of digital images (Thapa & Sood, 2011; Prachi, *et al*., 2011). Digital image watermarking is vital to all sorts of media, to prevent them from being asserted by other non related people, or from being edited or altered. Digital watermarking is a methodology that proffers a means to safeguard digital images from illegal copying and manipulation.

Watermarking is described as the process of embedding data into a multimedia element, like image, audio or video. It is possible to extract this data from, or detected in, the multimedia element at a later stage for diverse purposes including copyright protection, access control and broadcast monitoring. A digital watermark is defined as an indiscernible signal included with digital data, called cover work, which can possibly be identified at a later stage for buyer/seller identification, ownership proof and the like (Cox *et al*., 2001). Image watermarking, video watermarking and audio watermarking are enlisted as categories of Digital watermarking in accordance with the range of application. Contemporary digital watermarking schemes primarily focus on image and video copyright protection (Wang & Hong, 2006). On the whole, a digital watermark is defined as a code that is embedded inside an image. It plays the role of a digital signature, providing the image with a sense of ownership or authenticity. It is possible for the embedded data (watermark) to be either visible or invisible. In visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such a manner that watermark is deliberately noticeable to a human observer while in the case of invisible watermarking the embedded data is not observable, but it is possible to extract it with the aid of a computer program (Huang *et al*., 2010; Darshana, 2010).

Watermarking techniques can be divided into two sub-domains: Robust watermarking, the one which encompasses the additional requirement of robustness against possible attacks, and Fragile watermarking, the one that is exceedingly susceptible to design changes. Robust watermarking techniques come with the feature of being infeasible to be removed or make them futile, devoid of destruction to the intellectual property (IP) at the same instant (Amr *et al*., 2008; Weng *et al*., 2008). When the IP is modified or altered, the fragile watermark is destroyed at once. Fragile watermarks can be employed to authenticate the integrity of the medical image. In the field of medical imagery, the extraordinary characteristics consequent from stringent ethics, legislative and diagnostic implications make the security of the integrity and confidentiality of content a vital issue. In any situation, medical images ought to be kept unharmed and they should be checked prior to any operation for (Vivien & Guillemot, 2004):

- Integrity: this verifies that unauthorized people have not modified the image
- Authentication: this verifies whether the image certainly belongs to the right patient.

In this paper, a novel and effective watermarking scheme is introduced for checking the integrity and authenticity of medical images using hybrid transform. The proposed scheme makes use of the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) to form a hybrid transform. The Daubechies 4 wavelet transform is chosen for DWT in the watermarking scheme. The watermark embedding and extraction are performed in a frequency domain with the help of hybrid transform. It is essential that the size of the original image be dyadic (2^n x 2^n) and the watermark image be a binary image. Initially, the DCT is applied into the original image and the resultant matrix is converted into hybrid transformed matrix with the aid of Daubechies 4 wavelet transform. A new scheme is proposed for embedding and extraction processes to be performed in the transformed image. In the proposed scheme, the size of watermark image is required for extraction of watermark. The effectiveness of the proposed scheme is tested for different attacks for different images and the experimental results are verified.

PREVIOUS RESEARCH

A number of earlier works available in the literature on digital image watermarking scheme that employs hybrid transform techniques for image processing, watermarking, image compression, image coding and denoising of digital images. Some of the recent motivating researches are briefly described below.

A non-subsampled contourlet and wavelet hybrid transform (NSCWHT) was built and its applications were studies by Yingkun *et al*. (2008). The construction of filtering banks was carried out on basis of the non-subsampled contourlet transform (NSCT) and wavelet transform (WT). The consequence was that point singularity and line singularity in image could possibly be represented simultaneously. They merged NSCT with WT to design filters that lead to a NSCWHT with enhanced singularity representation on comparison with single one of them. They offered a design framework on basis of the hybrid approach that permits a quick implementation based on NSCT and WT correspondingly. Besides, they designed an image watermarking algorithm based on the developed NSCWHT and assessed the performance of the NSCWHT in the image watermarking algorithm.

A family of non-redundant directional image transforms built with the aid of hybrid wavelets and directional filter banks (HWD) was presented by Eslami & Radha (2006). They built and assessed a HWD family algorithm for blind multiplicative watermarking. They approximated the watermarked coefficients through a generalized Gaussian distribution probability model and employed a locally optimal detector. Subsequently, they evaluated the performance of the HWD family against that of wavelet-based image watermarking.

(Lu *et al*., 2010) projected an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. It relies on row and column operations. Row operations involve pre-multiplying matrix and column operations involve post-multiplying matrix. The D component can be explored with a diagonal matrix.

WATERMARKING IN FREQUENCY DOMAIN

It is possible to categorize the digital image watermarking techniques into two classes: spatial-domain and frequency-domain watermarking techniques (Potdar *et al*., 2005). With the comparison of spatial domain techniques (Chan & Cheng, 2004), frequency-domain watermarking techniques proved to be more efficient with regard to achieving the imperceptibility and robustness requirements of digital watermarking algorithms (Lai & Tsai, 2010; Vivek, 2010). Discrete Wavelet Transform (Shital & Sanjeev, 2010), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) are some of the generally utilized frequency-domain transforms. Feature based watermarking is where the feature points of original image are extracted, based on which a watermark template is constructed and embedded adaptively into the local region of these points (Lu *et al*., 2011). Nevertheless, DWT (Wolfgang *et al*., 1999) has been employed in digital image watermarking often owing to its excellent spatial localization and multi-resolution characteristics, that are identical to the theoretical models of the human visual system (Tribhuwan & Vikas, 2010). Further performance enhancements in DWT-based digital image watermarking algorithms could be achieved with the combination of DWT with DCT (Xu & Li-qin, 2010).

Discrete cosine transform

The Discrete Cosine Transform is a renowned coding technique employed in image and video compression algorithms. It is capable of carrying out decorrelation of the input signal in a data-independent manner (Ezhilarasan & Thambidurai, 2008). The DCT is a methodology for the transformation of a signal into elementary frequency components. The sequences of n real numbers are converted into the sequence of n complex numbers by the DCT (Xu *et al*., 2010) in accordance with the following formula:

$$f_i = \sum\nolimits_{k=0}^{n-1} xk \left[\cos \frac{\pi}{n} j \left(K + \frac{1}{2} \right) \right] \tag{1}$$

Discrete wavelet transform

Wavelets can be described as functions defined over a finite interval and having an average value of zero. The fundamental idea of the wavelet transform is to denote any arbitrary function as a superposition of a set of such wavelets or basis functions (Ezhilarasan & Thambidurai, 2008). These wavelets are acquired from a single mother wavelet through multiplicative scaling and translational shifts. The large number of known wavelet families and functions provides a rich space in a variety of applications. Biorthogonal, Coiflet, Haar, Symmlet, Daubechies wavelets (Daubechies, 1992) and the like, are some of the wavelet families.

Daubechies-4 wavelet transform

(Daubechies, 1990) created a set of most elegant ortho-normal wavelet basis function. These wavelets are efficiently supported in the time-domain and possess superior frequency domain decay. This denotes the motivation behind our choice of Daubechies wavelet transform. Daubechies-4 wavelet, the one that consists of only 4 coefficients, is considered to be the simplest member of the Daubechies family. The coefficients are,

$$h_0 = \frac{1+\sqrt{3}}{4\sqrt{2}}, h_1 = \frac{3+\sqrt{3}}{4\sqrt{2}}, h_2 = \frac{3-\sqrt{3}}{4\sqrt{2}}, h_3 = \frac{1-\sqrt{3}}{4\sqrt{2}} \tag{2}$$

The Daubechies D4 wavelet transform has four wavelet and scaling function coefficients.

Scaling function,

$$a[i] = h_0 s[2i] + h_1 s[2i+1] + h_2 s[2i+2] + h_3 s[2i+3] \tag{3}$$

Wavelet function,

$$c[i] = g_0 s[2i] + g_1 s[2i+1] + g_2 s[2i+2] + g_3 s[2i+3] \tag{4}$$

Hybrid transform

A number of watermarking algorithms that utilize either the DCT or the DWT exist in frequency domain. Major benefits of the hybrid DWT-DCT transform algorithm include the following

- Combined transforms recompense for the disadvantages of each other.
- Produce an effective image watermarking.
- Enhanced Peak Signal to Noise Ratio (PSNR).
- Structural Similarity Index Measure (SSIM)

Effective watermarking scheme using hybrid transform (DCT-DWT)

There are numerous important requirements needed into the medical image watermarking which should not affect the quality of the medical image. In the medical field, the qualities of the biomedical images are crucial, treated strictly and the image shall not be altered in any way. Digital watermarking in medical images is very important to prevent modification of medical images by any parties. Because of the importance of the security issues in the management of medical information, we have presented a novel and effective watermarking scheme for checking the integrity and authenticating medical images using hybrid transform. Our proposed scheme makes use of the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) to form a hybrid transform. For DWT, the Daubechies 4 wavelet transform is chosen in our watermarking scheme. Here various types of attacks are added and checked for the integrity of the image. The novel watermark embedding and extraction are performed in a frequency domain with the help of hybrid transform. The following subsections portray the steps involved in the watermark embedding and extraction processes.

Watermark embedding

The embedding of watermark image into the original image is detailed in this subsection. It is essential that the size of the original medical image be dyadic (2^n x 2^n) and the watermark image be a binary image. The proposed watermark embedding process is performed in a frequency domain with the help of hybrid transform. Initially, the DCT is applied into the original image and the resultant transformed image is converted into the hybrid transformed image with the aid of Daubechies 4 wavelet transform. Consequently, the extraction process proceeds as, the Least Significant Bit (LSB) value of every two bytes of the hybrid transformed image is computed and followed by the XOR operation is performed for those LSB values. The resultant XOR value is compared with each pixel value of the binary watermark image to obtain a modified embedded transformed image. Then, the watermark embedded transformed matrix is mapped back to its original position. Subsequently, inverse Daubechies 4 wavelet transform and inverse DCT are applied respectively to obtain the watermarked image. To the watermarked image attacks like JPEG, Rotation, low pass filter, sharpening, scaling and Gaussian noise are added and immunity verified. Figure 1 depicts the block diagram of the watermark embedding process.

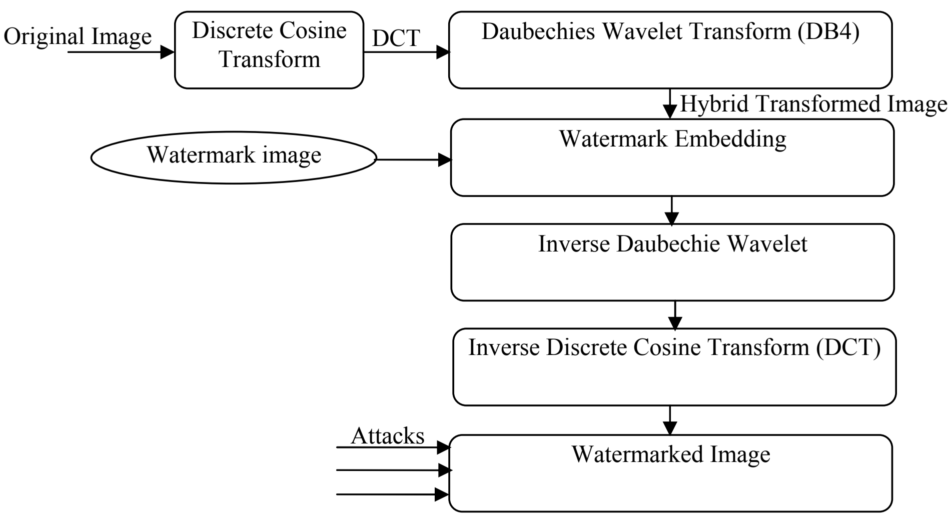

Fig. 1. Block diagram of Watermark Embedding

Watermark embedding steps

Input: Original Image (I), Binary Watermark Image (W)

Output: Watermarked Image (W_I)

Let I be an original grayscale medical image of size $n \times n$ be represented as:

$$I = \{x_{i_j} | 0 \leq i < n, 0 \leq j < n\}; \; x_{i_j} \in \{0, 1, ..., N\} \quad (5)$$

Apply the DCT into the original image I and generate a resultant transformed matrix T_I.

$$T_I = \{x'_{ij} | 0 \leq i < n, 0 \leq j < n\} \tag{6}$$

$$T_I = \begin{bmatrix} p_{11} & p_{12} & \dots & P_{1n} \\ P_{21} & P_{22} & \dots & P_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ P_{n+1} & P_{n+2} & \dots & P_{nn} \end{bmatrix} \tag{7}$$

Subsequently, the resultant matrix is altered by means of the daubechies 4 wavelet transform in order to get the hybrid transformed image.

$$HT_I = \{x''_{ij} | 0 \leq i < n, 0 \leq j \leq n\} \tag{8}$$

Then, the LSB value of every two bytes of the hybrid transformed matrix HT_I is taken out and stored in an intermediate vector I_V. In order to find the LSB value of every two bytes, the pixel values must be in whole number so that the whole number and the mantissa part are separated out.

$$HT_I = [P_1 P_2 P_3 ... P_N] \tag{9}$$

$$I_v = LSB[P_i, P_{i+1}]; I \leq i \leq N \tag{10}$$

Then, the XOR operation is performed for the resulted LSB values of every two bytes in the I_V.

$$C = XOR[I_{v,(i,i+D)}] \tag{11}$$

If the XOR value is equal to every pixel of the binary watermark image W, then embed the summation of XOR values and the mantissa part to attain the watermarked image W_I . If the value is not equal, then any of the LSB value is adjusted to get the same value as the pixel value of the watermark image W.

$$Watermarked\ image, W_I = \begin{cases} C + M_P & ; if\ C == W_i \\ I_v = LSB(P_{i+1}, P'_{i+1} & \\ C = XOR[I_{v(i,i+1)}; otherwise & \\ \quad C + M_p & \end{cases} \tag{12}$$

Then, the watermark embedded transformed matrix is mapped back to its original position. Subsequently, inverse Daubechies 4 wavelet transform and inverse DCT are applied respectively to obtain the watermarked image W_I .

Watermark extraction

The extraction of binary watermark image from the watermarked image is explained in this section. As the watermarking scheme is blind, it requires the watermarked image and size of watermark image for extraction. To begin with, the DCT is applied into the watermarked image as a result of the DCT transformed image. Then, the Daubechies 4 wavelet transform is applied into the transformed matrix to attain the hybrid transformed image. Afterward, the XOR operation is performed for Least Significant Bit (LSB) values of every two bytes present in the hybrid transformed image. Eventually, the binary watermark image is extracted with the help of hybrid transformed image by utilizing the size of the watermark image. The recovered watermark and the Image are checked for the confidentiality through the corresponding value of the PSNR and SSIM values. Figure 2 shows the block diagram of the watermark extraction process.

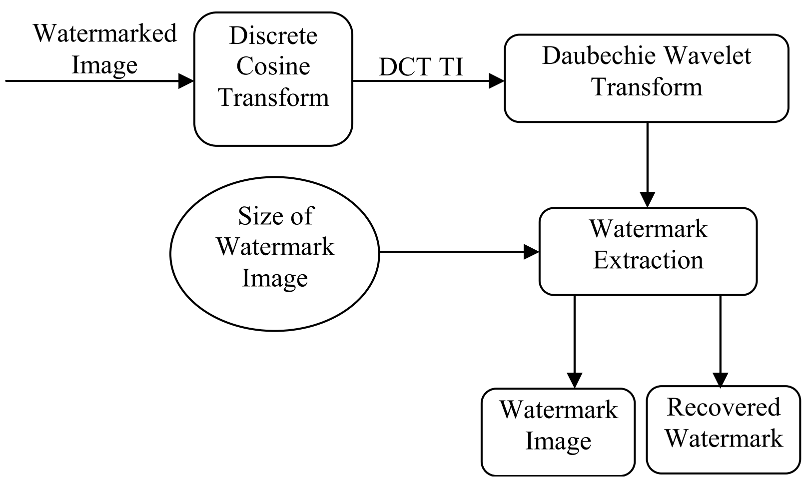

Fig. 2. Block diagram of Watermark extraction

Watermark extraction steps

Input: Watermarked Image (W_I), Size of watermark image ($|W|$)

Output: Watermark Image (W)

Initially, the DCT is applied into the watermarked image W_I which produces the resulted transformed matrix TW_I.

$$TW_I = \{y_{i_j} | 0 \leq i < n, 0 \leq j < n\} \tag{13}$$

Then, the Daubechies 4 wavelet transform is applied into the transformed matrix TW_I and resulted as a hybrid transformed matrix HT_M.

$$HT_M = \{y'_{ij} | 0 \leq i < n, 0 \leq j < n\} \quad (14)$$

Subsequently, the LSB of every two pixel values of the hybrid transformed matrix HT_M is taken out and stored in a vector V_I.

$$V_I = LSB[HT_{M(i,i+1)}] \quad (15)$$

Eventually, the XOR values are computed from the stored values and placed in a matrix with the size of the watermark image in order to extract the binary watermark image W.

$$W = XOR(V_{I(i,i+1)}) \quad (16)$$

The watermark and the corresponding image is recovered without any degradation.

Types of attacks

JPEG: Joint Photographic Experts Group. The JPEG is the commonly used method of lossy compression. There is a tradeoff between storage size and image quality. This is considered as one type of attack and image is tested. With the combined watermarking method, the output quality of the image is best compared with other methods.

LOW pass Filter: The low pass filter eliminates the frequencies above the cutoff frequency. It passes only the low frequency signals. When images pass through network, sometimes it may undergo filter under cutoff frequency. But with this algorithm, the LPF has not that much impact on the image.

Median Filter: This filter considers each pixel in the image in turn and looks at its nearby neighbors to decide whether or not it is representative of its surroundings. As a substitute of simply replacing the pixel value with the *mean* of neighboring pixel values, it replaces it with the *median* of those values. The median is calculated by first sorting all the pixel values from the surrounding region into numerical order, and then replacing the pixel being considered with the middle pixel value. The median is a more robust and preserves the edge quality.

Blur filter: It wraps around the edges of an image to reduce edge effects when a pattern is created by tiling multiple copies of the image side by side. If the image is blurred, then this filter removes the leakage of colors from the unblurred area.

Sharpening: The sharpening is a type of attack and the image is tested in sharpening form also. It is a type of transformation to bring out the image details. The edges are emphasized, so that eye can pick up the image very quickly. Blurriness of the image is reduced.

Rotation: It is considered as a type of attack. The image is rotated to 90° and tested. The result is tabulated.

Gaussian noise: It is statistical noise that has its probability density function equal to that of the normal distribution. It is also known as the Gaussian distribution. In many applications, Gaussian noise is most commonly used as additive white noise to yield additive white Gaussian noise.

Scaling: It is the ability of a system, network or process to handle a growing amount of work in a capable manner. The image is scaled to 0.25 ,0.5,0.6,0.8 and performance is tabulated below.

Cropping: It refers to the removal of the outer parts of an image to improve framing. Depending on the application, this may be performed on a physical photograph, artwork or film footage. It is considered as a type of noise in the network and analysis is done.

Salt and Pepper Noise: This is a form of noise typically seen on images. It represents randomly occurring white and black pixels. It creeps into images when there is a transient.

EXPERIMENTAL RESULTS AND DISCUSSION

The experimental results of the proposed effective watermarking scheme is for checking the integrity and authenticating medical images using hybrid transform (DCT-DWT). The proposed watermarking scheme is programmed in Matlab (Matlab7.9) and tested with different sizes of medical images. The proposed watermarking scheme discussed in this paper effectively embedded the watermark image into the original image, and extracted it back from the watermarked image. The watermarked images possess superior Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and visual quality. The watermark and watermarked images of medical and lena image is shown in Figures 3,4 and 5.

Structural similarity index measure (SSIM)

The Structural SIMilarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index can be viewed as a quality measure of one of the images being compared, provided the other image is regarded as of perfect quality. The SSIM metric is calculated on various windows of an image. The measure between two windows *x* and *y* of common size $N \times N$ is

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \qquad (17)$$

Where μ*x* the average of *x* , μ*y* the average of *y*; σ*x*2 the variance of *y*; σ*y*2 the variance of *y*; σ*xy* the covariance of x and y; *c*1=(*k*1*L*)2, c2=(*k*2*L*)2 two variables to stabilize the division with weak denominator; L the dynamic range of the pixel-values (typically this is 2#*bits per pixel* -) *k*1=0.01 and *k*2=0.03 by default.

Peak signal to noise ratio (PSNR)

In the case of watermarking, PSNR indicates the quality of the watermarked image. Higher the PSNR, higher will be the quality. Quality of the watermarked image should be higher to the quality. Quality of the watermarked image should be higher to make the secret data invisible to attackers. The PSNR is given in Decibesl as

$$PSNR = 10log10\frac{65025}{MSE} \tag{18}$$

Correlation coefficient

R= corrcoef(x) Returns a matrix R of correlation coefficients calculated from an input matrix X, whose rows are observations and whose columns are variables. The matrix *R= corrcoef(X)* is related to the covariance matrix *C=cov(x)* by

$$R(i,j) = \frac{c(i,j)}{\sqrt{c(i,i).c(j,j)}} \tag{19}$$

Table 1. Showing the corresponding PSNR ,MSE,SSIM AND CORRELATION VALUES of the Medical Images.

	PSNR		SSIM		CORRELATION	
MRI ULTRA	MRI	ULTRA	MRI	ULTRA	MRI	ULTRA
No Attack	53.076	49.536	0.9999	1	1	1
JPEG 100	51.288	50.889	0.9998	0.9999	1	1
JPEG 80	47.300	42.976	0.9952	0.9974	0.9990	0.9988
JPEG 60	41.910	42.554	0.9845	0.9936	0.9975	0.9973
JPEG 40	36.034	34.900	0.9570	0.9608	0.9959	0.9954
Low pass Filter	37.058	43.308	0.9938	0.9958	0.9885	0.9893
Median Filtering	38.7326	37.4321	0.9934	0.9911	0.9213	0.9154
Blur Filtering	37.8734	36.9342	0.9241	0.9190	0.9156	0.9067
Sharpening	31.178	33.595	0.9145	0.9644	0.9650	0.9565
Rotation 90	53.076	49.536	0.2250	0.3825	0.3906	0.2878
Gaussian Noise	25.882	25.259	0.4997	0.3932	0.8465	0.8033
zero mean noise with 0.01 variance	33.8034	33.1312	0.9141	0.9110	0.9196	0.9161
0.5 mean noise with 0.02 variance	30.9754	29.9393	0.9124	0.9088	0.9188	0.9167
0.6 mean noise with 0.05 variance	27.7304	26.4278	0.9011	0.8990	0.9061	0.9011
Scaling 0.25	54.095	52.470	0.9997	0.9999	1	1
Scaling 0.5	53.076	49.536	0.9999	1	1	1
Scaling 0.6	53.076	49.536	0.9999	1	1	1
Scaling 0.8	53.076	49.536	0.9999	1	1	1

The above Table 1 shows the results of MRI and ULTRA sound images. When there is no attack, the PSNR of the image is maximum and we get the actual image. With JPEG 40 the PSNR is 36.034. For Gaussian noise attack the PSNR reduces to 25.88 and results in a clear image . In the previous work the PSNR of the image is calculated (Kothari *et al*., 2010) and the work is continued for all types of attacks. Table 2 shows the PSNR,SSIM and CORRELATION values of the recovered watermark. Table 3 shows the corresponding values for general Images. Table 4 gives the corresponding values of recovered watermark.

Table 2. Showing the corresponding PSNR ,SSIM AND CORRELATION VALUES of the Recovered Watermark from the Medical images.

Recovered watermark	PSNR		SSIM		CORRELATION	
	MRI	ULTRA	MRI	ULTRA	MRI	ULTRA
No Attack	48.27609	48.26891	0.9671	0.9687	0.5294	0.5309
JPEG 100	48.28643	48.26577	0.9648	0.9694	0.5430	0.5575
JPEG 80	48.27609	48.29229	0.9671	0.9635	0.5333	0.5468
JPEG 60	48.26891	48.27385	0.9687	0.9676	0.5210	0.5679
JPEG 40	48.26936	48.27519	0.9686	0.9673	0.5580	0.5435
Low pass Filter	48.26891	48.26667	0.9687	0.9692	0.5502	0.5248
Sharpening	48.27205	48.27699	0.9680	0.9669	0.5488	0.5334
Rotation 90	48.26533	48.27429	0.9695	0.9675	0.5479	0.5643
Gaussian Noise	48.27564	48.27923	0.9672	0.9664	0.5559	0.5554
Scaling 0.25	48.2734	48.27474	0.9677	0.9674	0.5552	0.5497
Scaling 0.5	48.28013	48.26667	0.9662	0.9692	0.5333	0.5563
Scaling 0.6	48.26219	48.27879	0.9702	0.9665	0.5536	0.5359
Scaling 0.8	48.26936	48.27519	0.9686	0.9673	0.5399	0.5392

Fig. 3. (a) Original Image (b) DWT of Image (c) Watermarked Input DWT Image (d)Watermarked Input

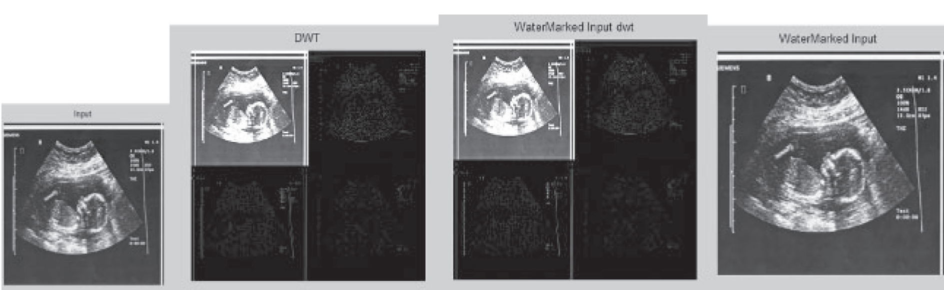

Fig. 4. Images under various attacks

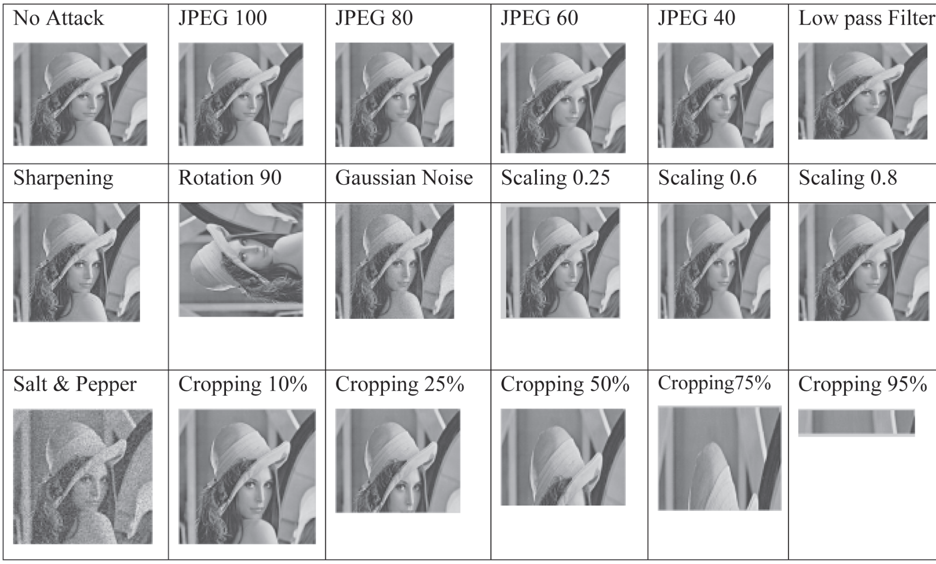

Fig. 5. Extracted Watermarks from the Watermarked Images

Table 3. Showing the corresponding PSNR, SSIM AND CORRELATION VALUES of the UMA AND LENA Images.

	PSNR		SSIM		CORRELATION	
UMA LENA	UMA	LENA	UMA	LENA	UMA	LENA
No Attack	55.10	55.00	0.9999	1	1	1
JPEG 100	55.51	57.27	0.9997	0.9999	1	1
JPEG 80	51.85	50.72	0.9938	0.9929	0.9995	0.9980
JPEG 60	45.66	46.58	0.9851	0.9849	0.9991	0.9968
JPEG 40	39.37	41.97	0.9742	0.9757	0.9985	0.9957
Low pass Filter	48.58	36.89	0.9976	0.9898	0.9989	0.9944
Sharpening	32.78	39.80	0.9357	0.8978	0.9839	0.9535
Rotation 90	55.10	50.00	0.3082	0.2302	0.2308	-0.0849
Gaussian Noise	31.81	38.30	0.5202	0.5937	0.9045	0.8835
Scaling 0.25	56.55	49.73	0.9998	1	1	1
Scaling 0.5	53.82	49.68	0.9996	1	1	1
Scaling 0.6	56.43	49.93	0.9995	1	1	1
Scaling 0.8	55.44	49.77	0.9999	1	1	1
Cropping 10%	26.47	31.17	0.4275	0.4930	0.5251	0.6968
Cropping 25%	20.12	26.36	0.3537	0.4267	0.0811	0.2754
Cropping 40%	22.98	23.95	0.4718	0.4011	0.3815	0.1313
Cropping 50%	22.07	24.41	0.4297	0.4047	0.2497	0.1764
Cropping 75%	19.84	24.64	0.3260	0.3832	0.1953	0.0295
Cropping 90%	20.72	24.15	0.2532	0.2826	0.1945	0.0765
Cropping 95%	22.42	23.17	0.1782	0.2138	0.0352	0.1176
Salt & Pepper	25.85	31.13	0.1912	0.2706	0.5723	0.5362

Table 4. Showing the corresponding PSNR, SSIM AND CORRELATION VALUES of the Recovered Watermark from the UMA AND LENA images

Recovered watermark	PSNR		SSIM		CORRELATION	
	Uma	Lena	Uma	Lena	Uma	Lena
No Attack	48.270	48.279	0.9684	0.9664	0.4182	0.4032
JPEG 100	48.278	48.265	0.9666	0.9695	0.3876	0.4269
JPEG 80	48.273	48.274	0.9677	0.9676	0.4186	0.3672
JPEG 60	48.263	48.258	0.9701	0.9711	0.4037	0.3989
JPEG 40	48.265	48.262	0.9696	0.9703	0.3767	0.3837
Low pass Filter	48.264	48.275	0.9698	0.9673	0.4031	0.3985
Sharpening	48.266	48.266	0.9693	0.9694	0.3756	0.3636
Rotation 90	48.260	48.280	0.9706	0.9663	0.4121	0.3632
Gaussian Noise	48.270	48.277	0.9684	0.9670	0.3694	0.3882
Scaling 0.25	48.268	48.267	0.9690	0.9692	0.3854	0.4257
Scaling 0.5	48.275	48.268	0.9674	0.9688	0.3811	0.4254
Scaling 0.6	48.278	48.259	0.9667	0.9710	0.3731	0.4084
Scaling 0.8	48.257	48.266	0.9713	0.9694	0.3895	0.4186
Cropping 10%	48.278	48.273	0.9666	0.9677	0.3876	0.3
Cropping 25%	48.260	48.268	0.9706	0.9689	0.4064	0.3715
Cropping 40%	48.270	48.281	0.9684	0.9660	0.4182	0.3876
Cropping 50%	48.273	48.264	0.9677	0.9698	0.4186	0.3743
Cropping 75%	48.263	48.270	0.9701	0.9684	0.4037	0.4182
Cropping 90%	48.264	48.269	0.9698	0.9686	0.4031	0.3946
Cropping 95%	48.281	48.275	0.9660	0.9673	0.3876	0.3900
Salt & Pepper	48.274	48.271	0.9675	0.9682	0.3809	0.3924

Table 5. Comparison of the proposed method with the existing Method

S.no	Type of Image	Kothari *et al*	Proposed
1	Lena	47.7707	55
2	ultra	-	49.536
3	Hima/Uma	47.4048	55.10

The proposed method is compared with the existing method. The PSNR of the Lena image is 47.7707 with reference to Kothari *et al*. and in the proposed method it is exactly same as the input image. For a general image, the peak signal to noise ratio is 55dB and the method is good. The same when applied with the advanced version of Matlab may result in very good quality and clarity. Each method is good in its own way. In digital watermarking method, no two images are similar. On applying same method on different images, the peak signal to noise ratio of each image varies. So watermarking is an evergreen area where research can be done for improving the robustness.

SUMMARY AND CONCLUSION

In this paper, an effective watermarking scheme is presented for the integrity and authenticity verification of medical images and General images. The proposed frequency domain watermarking scheme make use of hybrid transform, in which Discrete Cosine Transform is combined with Daubechies 4 wavelet transform. The watermark embedding and extraction are done in the frequency domain, using the presented watermarking scheme. The proposed watermarking scheme has been experimented with different images and the experimental results revealed the efficiency of the proposed watermarking scheme. In this, the image is tested for JPEG, rotation, scaling, sharpening, low pass filter, median filter,blur filter,cropping, Gaussian noise with different mean ,variance , salt and pepper noise.

REFERENCES

Amr,T. Abdel-Hamid & Sofiene,T. 2008. Fragile IP watermarking techniques, NASA/ESA Conference on Adaptive Hardware and Systems.

Chan, C. & Cheng, L. 2004. Hiding data in images by simple LSB substitution, Pattern Recognition, 37(3): 469-474.

Cox, I. J., Miller, M. J. & Bloom, J. A. 2001. Digital watermarking, Morgan Kaufmann, San Francisco, Calif, USA.

Darshana, Mistry. 2010. Comparison of digital water marking methods. (IJCSE) **02**(09).

Daubechies, I. 1992. Ten lectures on wavelets , SIAM, Philadelphia.

Daubechies, I. 1990. The wavelet transform, time-frequency localization and signal analysis, IEEE Trans. on Information Theory. **36**(5) pp: 961-1005.

Eslami, R. & Radha, H. 2006. Image watermarking using hybrid wavelets and directional filter banks, in Proceedings of the 40th Annual Conference on Information Sciences and Systems, 464 - 467.

Ezhilarasan, M. & Thambidurai, P. 2008. A hybrid transformation technique for advanced video coding, UbiCC Journal, 3(8).

Huang, W. T., Tan, S. Y., Chang,Y. J. & Chen, C. H. 2010. A robust watermarking technique for copyright protection using discrete wavelet transform, WSEAS Trans. Computers, **9**(5): 485-495.

Kothari, A. M., Suthar, A. C. & Gajre, R. S. 2010. Performance analysis of digital image watermarking-combined DWT-DCT over individual DWT, International Journal of Advanced Engineering and Applications pp.177-180

Lai, C. C. & Tsai, C. C. 2010. Digital image watermarking using discrete wavelet transform and singular value decomposition, Instrumentation and Measurement, IEEE Transactions on **59**(11),3060 – 3063.

Lu, K. Uehira. & Yanaka, K. 2010. Practical evaluation of illumination watermarking technique using orthogonal transforms, Journal of Display Technology, **6**(9),pp.351-358. doi:10.1109/JDT.2010.2049336

Lu, W. Lu, H. & Chung, F. L. 2011. Feature based watermarking using watermark template match," Applied Mathematics and Computation, **177**(1), pp. 886-893.

Piva, A. Bartolini, F. & Barni, M. 2002. Managing copyright in open networks, IEEE Transactions on Internet Computing. 6(3): 18–26.

Potdar, V., Han, S. & Chang, E. 2005. A survey of digital image watermarking techniques, in Proceedings of the IEEE International Conference on Industrial Informatics, 709-716,

Prachi, Khanzode, Siddharth Ladhake & Shreya. 2011. Digital watermarking for protection of intellectual property" IJCEM,12.

Shital, G. & Sanjeev, J. 2010. A Robust algorithm of digital image watermarking based on discrete wavelet transform . Special issue on IJCCT, **1** (2,3,4)

Thapa, M. & Sood, S. 2011. On secure digital image watermarking techniques, Journal of Information Security, 2(4), pp. 169-184. doi: 10.4236/jis.2011.24017.

Tosihiro, A. Fumiaki, M. Osamu, U. & Shohachiro, N. 2006. Hybrid digital watermarking for color images based on wavelet transform.IADIS International Conference on Applied Computing,548-551.

Tribhuwan, Kumar, T. & Vikas, S. 2010. An improved and robust DCT based digital image Watermarking Scheme, International Journal of Computer Applications (0975 – 8887) 3(1).

Vivek, T. 2010. A Statical comparison of Digital Image Watermarking Techniques.

Vivien, C. & Guillemot, C. 2004. Slavica Marinkovic, Image coding with iterated contourlet and wavelet transforms, in Proceedings of the International Conference on Image Processing, **5**: 3157- 3160.

Wang, X. Y. & Hong, Z. 2006. A novel synchronization invariant audio watermarking scheme based on DWT and DCT, IEEE Transactions On Signal Processing, 52006, **4**(12)

Weng, S. Yao, Z. & Jeng-Shyang, P. 2008. A novel reversible data hiding scheme¨, International Journal of Innovative Computing, Information and Control, **4** (2): 351-358.

Wolfgang, R. Podilchuk, C. Delp, E. 1999. Perceptual watermarks for digital images and video, Proc. of the IEEE, 87(7): 1108-1126.

Wu, H. T. & Cheung, Y. M. 2010. Reversible watermarking by modulation and security enhancement, IEEE Trans. Instrum. Meas., **59**(1), pp.221 -228,

Xu Yan-Ping & Li-qin, J. 2010. Research of a Digital Watermarking Algorithm Based on Discrete Cosine Transform, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS '10) Guangzhou. 373-375

Yingkun, H. C. Mingxia, Z. & Liu, D. Y. 2008. The Nonsubsampled Contourlet-Wavelet Hybrid Transform: Design and Application to Image Watermarking, in Proceedings of the International Conference on Computer Science and Software Engineering, **3**: 627-630.

Submitted: 14-9-2013

Revised: 13-1-2014

Accepted: 17-3-2014