# RSA-DWT BASED MEDICAL IMAGE WATERMARKING FOR TELEMEDICINE APPLICATIONS

**Article** *in* Journal of Theoretical and Applied Information Technology · August 2014



**1 author:**

P.V.V. Kishore
K L E F (Deemed - to - be -University)
**122** PUBLICATIONS **347** CITATIONS

SEE PROFILE

Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# RSA-DWT BASED MEDICAL IMAGE WATERMARKING FOR TELEMEDICINE APPLICATIONS

[1]N.VENKATRAM, [2]L.S.S.REDDY, [3]P.V.V.KISHORE, [4]CH.SHAVYA
[1, 2, 4]K.L.University, Dept of E.C.M, KL University, Vaddeswaram, Green Fields, GUNTUR, AP, INDIA
[3]K.L.University, Dept of E.C.E, KL University, Vaddeswaram, Green Fields, GUNTUR, AP, INDIA
E-mail: [1]nvenkatram@kluniversity.in, [2]lssreddy@kluniversity.in [3]pvvkishore@kluniversity.in, [4]ch.sravya@gmail.com

**ABSTRACT**

Medical images convey important information to the doctor about a patient's health condition. Internet transmits these medical images to remote locations of the globe to be examined by expert doctors. But data transmission through unsecured net invokes authentication problems for any image data. This problem of authentication of medical images is addressed in our research as medical image watermarking with patient images. Medical images contain very sensitive information. Watermarking medical images require careful modifications preserving the data in the images. This is being accomplished using RAS (Rivest, Shamir and Adleman) algorithm for patient image encryption and decryption. The host images are set of medical images such as MRI, CT and Ultrasound scans of patient body parts. These medical images are watermarked with encrypted patient image in transform domain using 2D Discrete Wavelet Transform (DWT). The host medical image and watermark image are transformed into wavelet domain and are mixed using two scaling factors alpha and beta. Finally these watermarked medical images are transmitted through the internet along with the secret key that will be used for decryption. At the receiving the embedded encrypted watermark is extracted using 2DWT and decryption key. The robustness of the proposed watermarking techniques is tested with various attacks on the watermarked medical images. Peak-Signal-to-Noise ratios and Normalized cross correlation coefficients are computed to accesses the quality of the watermarked medical images and extracted patient images. The results are produced for three types of medical images with one patient image watermarks using single key by using four wavelets (haar, db, symlets, bior) at four different levels (1,2,3,4).

**Keywords:** *Medical Image Watermarking, RAS (Rivest, Shamir and Adleman) algorithm, Discrete Wavelet Transform (DWT), MRI, CT and Ultrasound Images.*

## 1. INTRODUCTION

Medical image watermarking[1]-[4] plays an important role in assisting the patients all over the world by transmitted medical images of patients through unsecured networks such as World Wide Web. Watermarking of medical images provides secure transmission of medical images of patients to doctors around the globe for detailed analysis of their illnesses. This practice helps to expand the horizon of remotely stationed patients where no proper medical doctor is available to increase their chances of survival.

Trading medical images through unsecure internet networks is prone to undesirable alteration to the stuffing of the images. Medical images contain susceptible information pertaining to the life of a human being. General practitioner has to take paramount care to check that the images are not tampered before diagnosing the medical images of patients downloaded from the internet. For this reason, authentication of medical images such as Ultrasound scans, MRI scans, x-ray and Computer Tomography (CT) scans has to be watermarked. The host medical image can be watermarked with patient information before transmitting on the internet. At the physician's end it has to de watermarked before proceeding for diagnostics.

A digital watermark can be perceived as a visible or invisible detection code that is embedded inside a medical image. Medical image authentication calls for a non visible perfectly hidden watermark [5]. Medical image watermarking plays a prominent role in telemedicine applications [6]. Digital watermarks for medical images can be made by hiding patient information to make them unique to a particular patient [7]. Watermark is extracted to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

prove the authenticity that these medical images belong to a particular patient [8].

Watermarking is used extensively to protect every digital media contents such as text documents [9], images [10] and even audio and video data. Over the past decades the watermarking methods are developed based on image's spatial domain [11], transform domain [12], robust [13], semi-fragile [14] and fragile [15]. The last three methods are used to protect the watermark against malicious attacks while transporting images on unsecured networks such as internet. More or less all the watermarking techniques should satisfy three basic requirements for successful watermarking which are robustness, imperceptibility and competence.

*Coatrieux et al* enlightened that digital watermarks should be considered as a security tool in order to protect medical records[16]. Giakoumaki *et al* proposed a wavelet transform-based watermarking, which fulfills the strict requirements concerning the acceptable alterations of medical images [17]. This research paper proposes to find which wavelets are better for watermarking medical images and up to what level of decomposition will result in perfect watermarked image.

Irany et al proposes a high capacity reversible multiple watermarking scheme for medical images based on integer-to-integer wavelet transform and histogram shifting. The novelty of the proposed scheme is that it uses a scalable location map and incorporates efficient stopping conditions on both wavelet levels and different frequency subbands of each level to achieve high capacity payload embedding, high perceptual quality, and multiple watermarking capability. Results show that the proposed method attains high perceptual quality in high capacity rates for the medical images[18].

Lavanya et al proposed non region of intrest(NROI) based medical image watermarking schemes[19] where the patient details are embedded in non-ROI region of an image. The encrypted image is divided into non overlapping tiles to identify region of interest and non-region of interest. In examination site examiner embeds patient details in non-ROI of encrypted image using a data-hiding key. With an encrypted image containing patient details, a receiver may first defile and decrypt it using the encryption key, and the decrypted version is similar to the original image[20].

A watermarking algorithm should be reliable based on the following issues: Intelligibility: The most essential prerequisite for any Watermarking scheme shall be such that it is transparent to the end user. The watermarked content should be fragile at the projected user device without giving aggravation to the user.

Protection: Watermark information can only be available to the sanctioned users. Only approved user shall be able to modify the Watermark content. Encryption is used to prevent illicit access of the watermarked data.

Sturdiness: Watermarking must be vigorous enough to endure all kinds for image processing operations, "attacks" or unauthorized access. Any attempt that has a potential to modify the data content is considered as an attack. Sturdiness against attack is a key obligation for Watermarking and the accomplishment of this watermarking algorithm for protection depends on this .

This research proposes to use wavelet transform [21]-[23] and RSA algorithm for medical image watermarking. The watermark in this case is a patient image that is first treated with RSA encryption with the help of KEY. The encrypted patient image watermark is then embedded into to the medical image using 2D DWT. But seeing the scale of wavelets, it is decided to test different wavelets with multiple levels of decomposition and arrive at a conclusion that which type of wavelet at what level best compliments medical image watermarking. Finally the extracted watermark is decrypted using KEY and RSA decryption algorithm. The rest of the paper is organized as follows. Section 2 gives a brief introduction of RSA algorithm and discrete wavelet transform. Section 3 deals with the process of watermarking. Section 4 gives medical image dewatermarking algorithm. Section 5 introduces measurable parameters that can judge the watermarking procedures. Results and discussion in section 6 present insight into the use of multiresolution wavelet transform with RSA encryption and decryption for medical image watermarking. Finally conclusions are made on the medical image watermarking procedures in section 7.

## 2. RSA AND WAVELET THEORY

This research proposes the use of two most popular techniques used in data encryption and image processing in computer communications for copyright protection. RSA algorithm is used to generate KEY and encrypt the patient image that is the watermark. The watermarking of the encrypted patient image watermark into a medical image is accomplished using 2D discrete wavelet transform.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This section provides the basics of RSA algorithm and DWT used for medical image watermarking.

### 2.1 RSA

RSA is a public key cryptosystem named after Ron Rivest, Adi Shamir and Leonard Adleman in 1997 for their research at MIT[24]. RSA is being used since then for secure data transmission in computer networks such as internet. In this the encryption key is public and the decryption key is private which is secret and transmitted along with the encrypted data[25]. RSA is a asymmetric algorithm because of its two different keys. The intricacy augments when size of prime numbers enlarges beyond a certain limit. Any person can encrypt the message by means of public key but cannot decrypt unless the secret key is known. Decoding would be easy if the prime factors are known apriori. RSA algorithm is presented briefly.

**S1.** Choose two prime numbers p and q distinctly. For security, the prime integers p and q must be chosen at random of similar bit length.

**S2.** Then compute n which is given by

$$n=pq \quad (1)$$

and n is used in calculating both public and private key. 'n' is number of bits defining the length of the public KEY.

**S3.** Compute

$$\Psi(n)=\Psi(p)\Psi(q)=(p-1)(q-1) \quad (2)$$

where Ψ is Euler's totient function.

**S4.** Choose an integer e which satisfies $1<e<\Psi(n)$ and $\gcd(e,\Psi(n))=1$ where e and Ψ(n) are co prime. e is public key exponent. It is having short bit length and small Hamming weight in more efficient encryption.

**S5.**compute d which is given by $d\equiv e^{-1} \pmod{\Psi(n)}$ ,d is multiplicative inverse of e. d is also given as $d\cdot e\equiv 1 \pmod{\Psi(n)}$. 'd' is known as private key exponent.

**S6.** Encryption:

Source transmits public key (n,e) (which means it consists of modulus n and public or encryption exponent e) is transmitted to destination computer. Source turns message into an integer in such a way that the values of integers lies between $0\le m<n$ which is accomplished using padding scheme. The ciphertext 'C' is computes as

$$C \equiv m^e \pmod{n} \quad (3)$$

**S7.** Decryption:

Destination receives the encrypted message along with the secret key and decrypts the message 'm' using,

$$m \equiv C^d \pmod{n} \quad (4)$$

### 2.2 Discrete Wavelet Transform

Wavelet transform can be applied to image decomposition and reconstruction [26-28]. Wavelet transform provide a structure in which an image is decomposed, with each level corresponding to a lesser resolution.

This multi resolution analysis of 2D DWT permits to decompose a video frame into approximations and details. The 2D discrete wavelet transform divides the image into low frequency (L) and high frequency components (H) at level1.

The 2D medical image $I^{Mi}(x,y)$ passes through low pass filter and a downsampler of level 2 to produce approximate image at level-1 wavelet decomposition. Similarly 2D medical image $I^{Mi}(x,y)$ is applied to a high pass filter and downsampler to create detailed image at level-1 wavelet decomposition.

Further in level2 decomposition the low frequency information is divided into LL and high frequency information LH. The high frequency component in level1 is decomposed in to low frequency information HL and high frequency HH. The wavelet decomposition process is shown in the figure 3. The results of wavelet decomposition using 2D Daubechies two wavelets for level2 on a video frame is shown in figure 3.9.

The notion $L^2(R^2)$, where R is a set of real numbers, denote the finite energy function $I^{Mi}(x,y)$ in $R^2$; and $x,y$ in R. In two dimension wavelet transform, a 2D scaling function $\varphi(x,y)$, and three two dimensional wavelets, $\varphi^H(x,y)$, $\varphi^V(x,y)$ and $\varphi^D(x,y)$ are produced as shown in figure 3.8.

The above functions represent gray level variations along different directions such as horizontal variations, vertical variations and diagonal variations. The DWT of $I^{Mi}(x,y)$ of size $M\times N$ is

$$W_\varphi(j_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}I^{Mi}(x,y)\varphi(j_0,m,n) \quad (5)$$

Where j, m, n, M, N are integers, i= {H, V, D}, $j_0$ is an arbitrary starting scale and the coefficients $W_\varphi$ define an approximation of $f$ at scale $j_0$.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$W_{\varphi}^{i}(j_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}I^{Mi}(x,y)\psi_{j,m,n}^{i} \quad (6)$$

The coefficients in the above equation add horizontal, vertical and diagonal details as shown in figure.3.8 for scales $j \geq j_0$. The $\varphi_{j,m,n}$ and $\psi_{j,m,n}^{i}$ denote scaled and translated basis functions as shown below,

$$\varphi_{j,m,n}(x,y)=2^{j/2}\varphi(2^{i}x-m,2^{j}n-1)$$
$$\psi^{i}{}_{j,m,n}(x,y)=2^{j/2}\psi^{i}(2^{i}x-m,2^{j}n-1) \quad (7)$$

Given $W_{\varphi}$ and $W_{\psi}^{i}$, $I^{Mi}(x,y)$ is obtained via inverse DWT as:

$$I_{Mi}^{W}=\frac{1}{\sqrt{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left(W^{j_0}\varphi_{j_0}+\sum_{i}\sum_{j=j_0}^{\infty}W_{\psi^i}^{j}W_{j}^{i}\right) \quad (8)$$

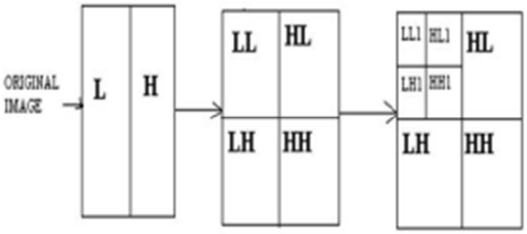



*Figure 1: Wavelet Decomposition based on Discrete WT*

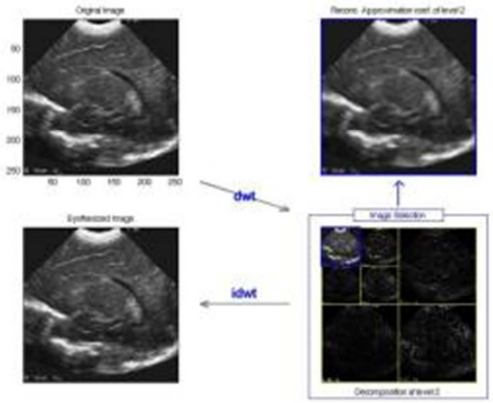



*Figure 2: Daubechies 2 Wavelet Transform of Level 2*

## 3. WATERMARK EMBEDDEDING

Medical Images are watermarked with their analogous encrypted patient image using RSA is accomplished using the following steps.

**S1.** Apply RSA on the 64×64 resolution patient image. Prime numbers are selected randomly between 1 and 200 for every new encryption. Public KEY is generated n bit long that is sent to the destination for decryption. The encryption is carried on each pixel to producing a encrypted patient watermark image.

**S2.** Save the encrypted patient image and KEY. The KEY will accompany the watermarked image for decryption.

**S3.** Carry out n$^{th}$ level 2D Discrete Wavelet Transform (DWT) on the Medical Image (Cover Image) [29] and decompose in to following sub-bands (LL, LH, HL, HH). Where n is the number of levels a wavelet is supposed to be decomposed. In our research we tried with four different levels i.e. n=1, 2, 3 and 4.

**S4.** The watermark is embedded using the formula

$$W(i,j)=W^{Sub}(i,j)+(2\sigma+\delta)(2w^{e}(k)-1) \quad (9)$$

Where $W(i,j)$ is watermarked medical image with encrypted patient image. $W^{Sub}(i,j)$ is n$^{th}$ level wavelet subbands of medical image. $\sigma$ is the ratio of standard deviation of wavelet coefficient block and the maximum standard deviation of all the coefficient blocks. $\delta$ is the fixed embedding watermark strength which is fixed at 0.05 in this paper. $w^{e}(k)$ is the encrypted patient image at k$^{th}$ position.

**S5.** Finally, assemble all the modified sub-bands and apply inverse 2D Wavelet Transform (IDWT) and is formulated as

$$I^{WMi}=\left(W^{(n)}\right)^{-1} \quad (10)$$

Where 'n' represents 4 sub-bands for n=1, LL, LH, HL, HH. is the watermarked medical image. The watermarked medical image $I^{WMi}$ is obtained which contains the RSA encrypted patient image. This watermarked medical image is transmitted to unsecured networks to servers of major hospitals around the world to expert medical practitioners.

## 4. WATERMARK EXTRACTION PROCESS

The watermarked medical image $I^{WMi}$ is sent distantly through unsecured internet servers to expert medical doctors from remote parts of the world. At the doctor's place the system decouples the attacked watermarked medical image form the watermark for authentication. The following extraction process is incorporated at the doctor's side to extract the encrypted watermark patient image and decrypt the patient watermark image.

**S1.** The possibly attacked watermark medical image is treated with 2D Discrete wavelet transform (DWT) and decomposed to n$^{th}$ level with n sub-bands LL, LH, HL and HH.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

**S2.** Medical image is decoupled from the patient watermark image using the inverse expression

$$I^{ep}(x,y)=\frac{2(W^{RMi}(i,j)-W^{Mi}(i,j))}{(2\sigma+\delta)+1} \quad (11)$$

Where $W^{RMi}(i,j)$ is transformed the received watermarked medical image at i[th] and j[th] location. $W^{Mi}(i,j)$ is the subbands of original cover image that is received with the transmitted watermarked image. $I^{ep}(x,y)$ is the recovered watermark patient image which encrypted with RSA.

**S4.** Extracted watermark patient image is an encrypted image. The watermarked medical image is accompanied by a KEY. This public KEY is used to decrypt the watermark patient image at the destination computer. Finally authentication of the medical image is identified by extracted patient image.

## 5. RESULTS AND DISCUSSION

The proposed watermarking process is implemented on MATLAB 13.0.1 software with three different types of medical images which are considered as cover images. MRI, CT and Ultrasound medical (US) images are used as cover images of standard resolution 256×256. Watermark is a patient image of resolution 64×64. Since medical images are gray scale images, it is intended to consider grayscale patient image as watermark. The dynamic standard deviation ratio factor σ is used for watermarking in our experiments which is computed from wavelet coefficients. The other scaling factor $\delta$ is chosen as 0.05. Here there is no fixed bound for $\delta$ as it can be varied within 0.01 to 0.09 for medical image watermarking.

The performance of the proposed medical image watermarking is judged by computing peak signal to noise ratio (psnr) and normalized cross correlation coefficient (ncc). These parameters will decide the robustness of the watermarking method using RSA-DWT watermarking process. Watermarking of medical images is relatively susceptible process as the medical images contain information related to life changing scenarios of human subject. Corruption of the original medical image by watermarking process should be within the acceptable confines of human perception. The visual sensitivity of the watermarked and extracted images is mathematically represented by calculating psnr and ncc.

### 5.1 Embedded Peak Signal to Noise Ratio (psnr)

Embedded psnr [29] is the measure of peak error between original image and watermarked image and is computed using the following expression

$$psnr=10\log_{10}\left(\frac{MN\left(\max(\max(I^{M}(x,y)\right)^{2}}{\sum_{x\in N}\sum_{y\in M}\left(I^{M}(x,y)-W^{MI}\right)^{2}}\right) \quad (12)$$

Where N and M represent image resolution. $I^{M}(x,y)$ is the original medical image and $W^{Mi}$ is the watermarked medical image. psnr is the peak signal to noise ratio in db which range between 40db to 60 db generally for good watermarking.

### 5.2 Extracted Normalized Cross Correlation Coefficient (ncc)

Normalized cross correlation [29] is mostly used by pattern recognition research for measuring similarity between a query image and the images from the database. The cross correlation is normalized by subtracting the mean and dividing by standard deviation. Embedded normalized cross correlation coefficient gives the measure of closeness between watermarked image and original medical image.

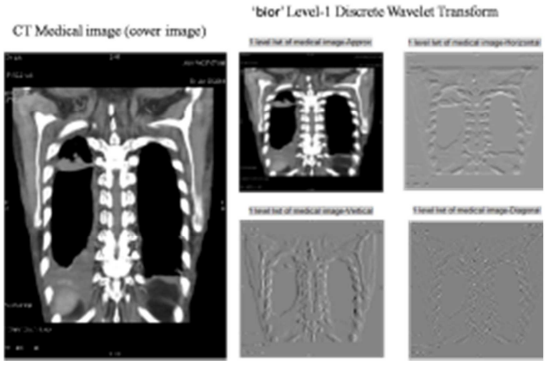
$$ncc=\frac{\sum_{x\in N}\sum_{y\in M}I^{M}(x,y)\times W^{Mi}(x,y)}{\sqrt{\sum_{x\in N}\sum_{y\in M}\left[I^{M}(x,y)\right]^{2}}\sqrt{\sum_{x\in N}\sum_{y\in M}\left[W^{Mi}(x,y)\right]^{2}}} \quad (13)$$

The values of normalized cross correlation coefficients (ncc) range from 0 to 1. Larger values of ncc are preferred for better watermarking.

Figure 3 shows a patient's abdomen CT along with its 2D discrete wavelet transform. DWT decomposes the medical image using haar mother wavelet to level-1 decomposition. CT brain medical image(256×256) is used as cover image for watermarking in figure 4(a) and lena image is used as patient image(64×64) in figure 4(b). RSA-DWT watermarking procedure proposed in this paper embeds RSA encrypted patient image into brain MRI cover image as shown in figure 4(c). Figure 4(d) shows the extracted encrypted watermark of patient image. Figure 4(e) shows decrypted patient watermark image. Visually figure 4 shows that the watermarked image and extracted image match stalwartly as per human visual system.

Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195




(a) (b)

*Figure 3: Discrete Wavelet Transform of Level -1 using 'bior' mother wavelet (a) Original abdomen CT Medical Image (b) its 2D DWT*

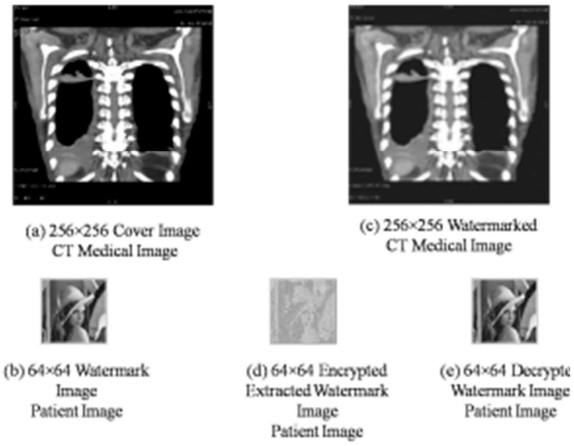
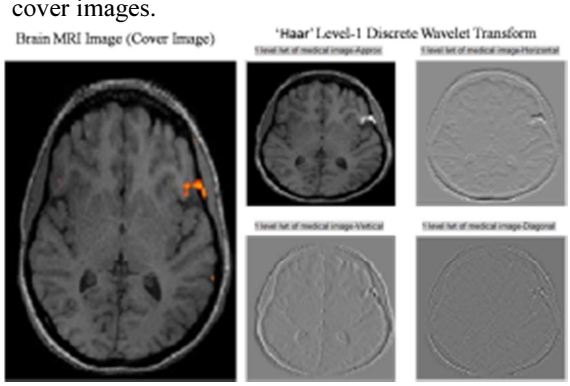



*Figure 4: (a) CT Cover Image (b)Watermark Patient Image (c) CT Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY*

The figure 4 shows the robustness of RSA-DWT algorithm. Similar results are acquired using Computer Tomography (CT), figures 5 and 6, and Ultrasound (US) Medical images, figures 7 and 8 as cover images.




(a) (b)

*Figure 5: Discrete Wavelet Transform of Level -1 using 'haar' mother wavelet (a) Original Brain fMRI Medical Image (b) its 2D DWT*

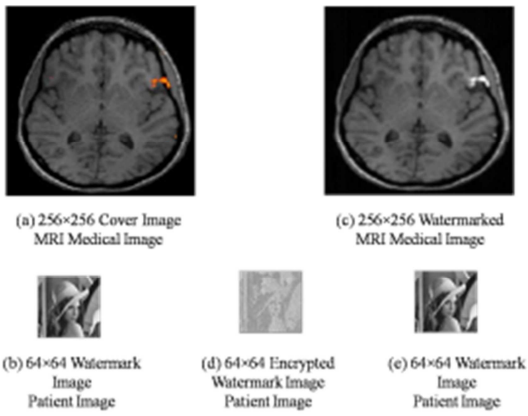



*Figure 6: (a) MRI Brain Cover Image (b) Watermark Patient Image (c) MRI Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY*

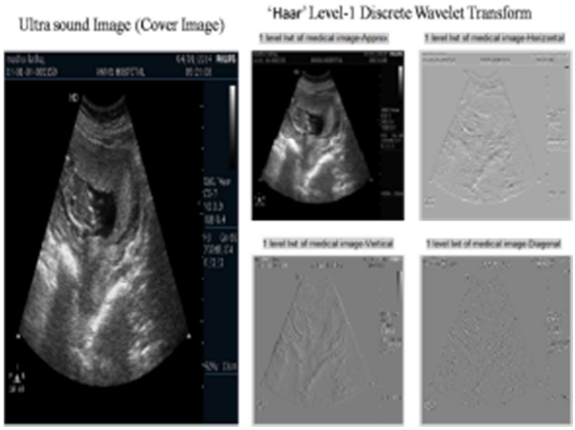



*Figure 6: Discrete Wavelet Transform of Level -1 using 'haar' mother wavelet (a) Original pregnant ultrasound(US) Medical Image (b) its 2D DWT*

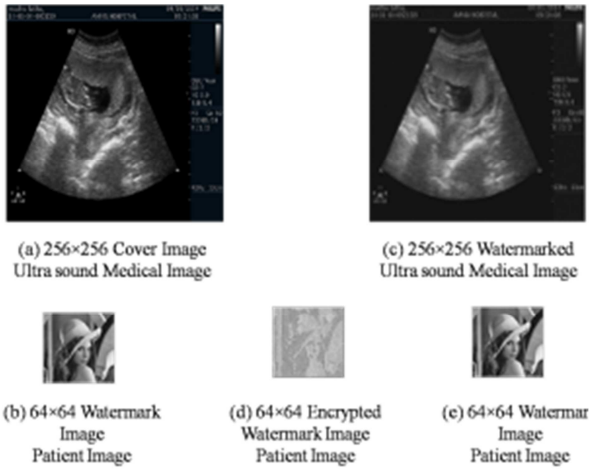



*Figure 8: (a) Pregnant US Cover Image (b) Watermark Patient Image (c) US Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY*

Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From figure 8 it can visually be observed that the watermarking process proposed in this paper has actually removed noise from the ultrasound image.

The CT, MRI and US medical cover images are watermarked using mother wavelet 'db2'. Different levels for the mother wavelet 'db2' are also computed. Figure 9 shows MRI Medical image in wavelet transformed domain up to level-1 and figure 10 shows watermarked medical image and extracted patient watermark image both encrypted and decrypted using db2 wavelet at level-1. Level-2 db2 watermarking for the same MRI medical image is shown in figure 11 and figure 12 shows watermarked medical image and extracted watermark patient image. Level-3 and Level-4 are shown in figures 13,14, 15and 16 show wavelet transformed medical images and watermarked medical images and extracted watemarks.

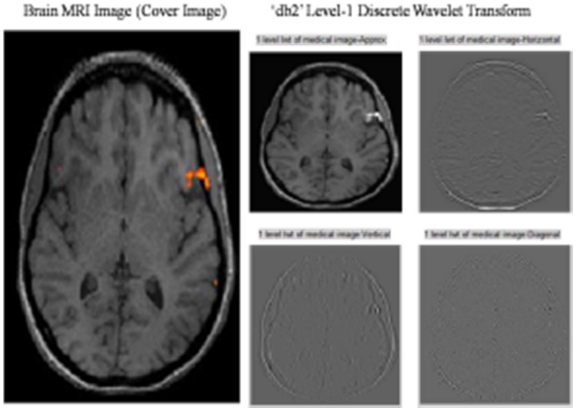



*Figure 9: Discrete Wavelet Transform of Level -1 using 'bd2' mother wavelet (a) Original Brain fMRI Medical Image (b) its 2D DWT using db2 at level-1*

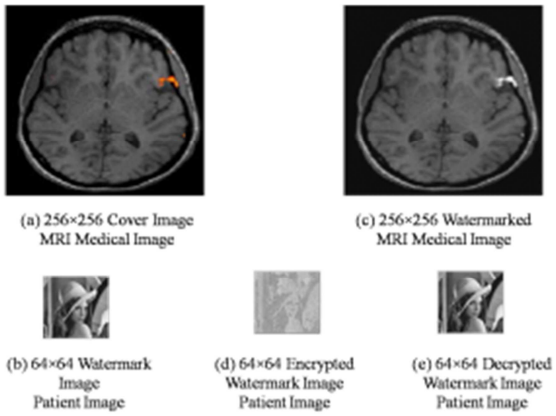



*Figure 10: (a) fMRI Brain Cover Image (b) Watermark Patient Image (c) fMRI Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY for 'db2' at Level-1*

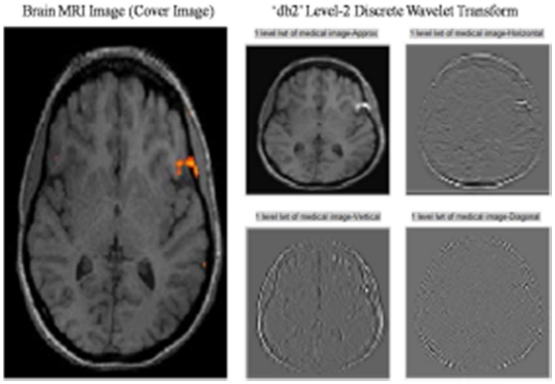



*Figure 11: Discrete Wavelet Transform of Level -2 using 'bd2' mother wavelet (a) Original Brain fMRI Medical Image (b) its 2D DWT using db2 at level-2*

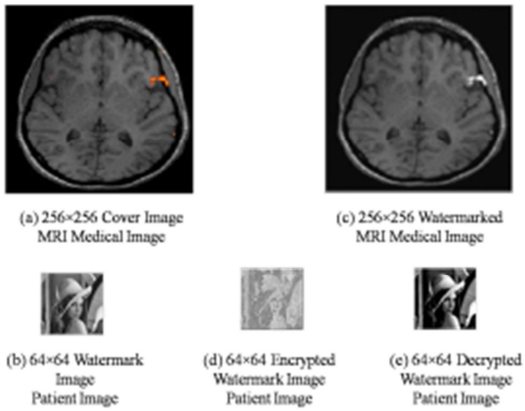



*Figure 12: (a) fMRI Brain Cover Image (b) Watermark Patient Image (c) fMRI Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY for 'db2' at Level-2*

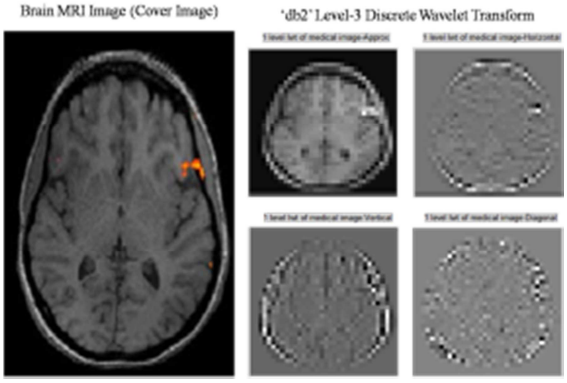



*Figure 13: Discrete Wavelet Transform of Level -3 using 'bd2' mother wavelet (a) Original Brain fMRI Medical Image (b) its 2D DWT using db2 at level-3*

Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

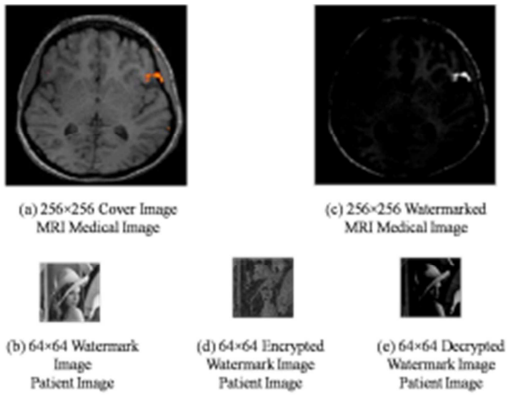



*Figure 14: (a) fMRI Brain Cover Image (b) Watermark Patient Image (c) fMRI Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY for 'db2' at Level-3*

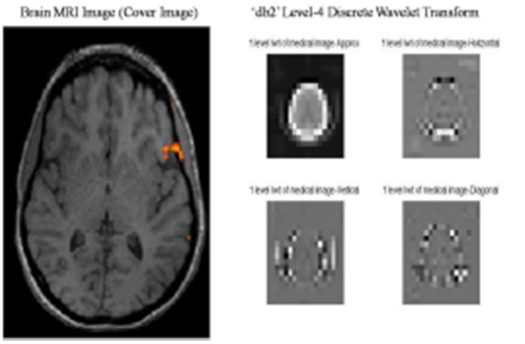



*Figure 15: Discrete Wavelet Transform of Level -1 using 'bd2' mother wavelet (a) Original Brain fMRI Medical Image (b) its 2D DWT using db2 at level-4*

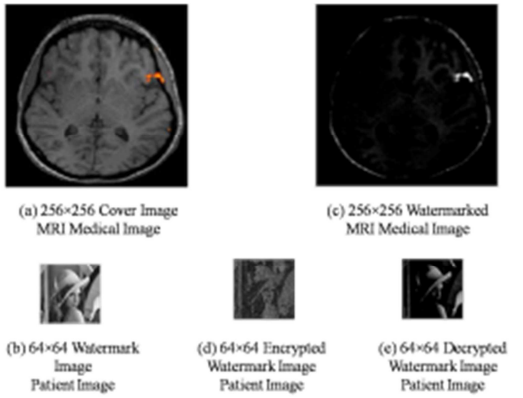



*Figure 16: (a) fMRI Brain Cover Image (b) Watermark Patient Image (c) fMRI Watermarked Medical Image (d) Extracted RSA Encrypted Watermark (e) Decrypted Watermark patient Image With KEY for 'db2' at Level-4*

Visually comparing the watermarked medical images from figures 10, 12, 14 and 15(c) with patient image reveal that there is remarkable deviation in case of MRI for 'db2' at various levels. Level-1 and level-2 from figure 10(c) and 12(c) produce good watermarked medical images and their extractions in figure 10(e) and 12(e) are also near to the original patient image. But as we attempt level-3 and level-4 it can be observed from the figures 14(c) and 16(c), the watermarked medical images have deformed considerably. Similarly the extracted watermarks for level-3 and level-4, form figures 14(e) and 16(e), show very less coincidence to original patient image watermarks. Hence it is understood that as the wavelet decomposition level increases further the proposed watermarking process for medical images fails to make an impact.

Results are also formulated using equations 17 and 18 in Table-I for the embedded watermark and original medical image for all three different medical images. The data analysis highlights the usefulness of the RSA-DWT watermarking process for medical image watermarking with patient image as consignment.

*Table-1: PSNR and ncc for Medical Cover Images*

| Cover Medical Image | PSNR(db) | NCC |
|---|---|---|
| MRI | 49.8998 | 0.9835 |
| CT | 48.3565 | 0.9823 |
| Ultrasound(US) | 46.3454 | 0.9812 |

From Table-1 psnr in db for MRI, CT and US watermarks are 49.8998db, 48.3565db and 46.3454db respectively. Comparing with psnr values of dwt based watermarking in [29] our proposed RSA-DWT on medical images are better and within the prescribed values of watermarking. Normalized Cross Correlation (ncc) coefficient is good for MRI and CT with 0.9835 and 0.9823 compared to US at 0.9812. Again the values are within the permissible range as proposed by RSA-DWT watermarking and compared to results in [29].

Four wavelets, 'Haar', 'db2', 'sym' and 'bior' are used in medical image watermarking and at four different levels. Visually the watermarked medical images in RSA-DWT watermarking process are excellent for all wavelets. RSA-DWT watermarking process is independent of mother wavelet. But the only constraint is in the level of the wavelet transform which according to this paper should be restricted to a maximum value of 3. Level-1 and 2 produce excellent results.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The watermarked medical images are transmitted on unsecured networks and are most likely be attacked from various unlawful elements present on the network. Hence attacks are simulated for testing the watermarking model proposed in this paper. For this purpose six different types of commonly used attacks with common values are simulated making the total number of attacks to eleven. Computing normalized cross correlation coefficient form equation 13 for the extracted watermark patient images reveals the performance of the RSA-DWT medical Image watermarking process. The values are put up in Table-2.

Generally the ncc coefficient for better watermark is something above 0.75[16]. For remarkably excellent correlation the value of ncc should be around 0.9999 or 1. A value of zero for ncc indicates a complete uncorrelation between the original cover image and the watermarked image. Table-2 ncc values are computed for 'db2' wavelet for sub band HH at level-1 of watermarked image. The watermarked medical image is subjected to six attack categories such as a 3×3 window mean filtering, a 3×3 window median filtering, 45˚, 90˚, 135˚ and 180˚ rotation, Gaussian noise and salt & pepper noise of noise densities 0.001,0.005,0.01 and 0.1 and finally crop with crop area [100,100]. Table-2 shows the robustness of RSA-DWT under these attacks.

*Table 2: Comparison of Extracted watermarks*

| Attacks | (MRI) | (CT) | (US) |
|---|---|---|---|
| Mean Filtering (3×3) | 0.9899 | 0.9789 | 0.9765 |
| Median Filtering (3×3) | 0.8026 | 0.7916 | 0.7892 |
| Rotation (45˚) | 0.9776 | 0.9666 | 0.9642 |
| Rotation (90˚) | 0.9653 | 0.9543 | 0.9519 |
| Rotation (135˚) | 0.953 | 0.942 | 0.9396 |
| Rotation (180˚) | 0.9407 | 0.9297 | 0.9273 |
| Gaussian Noise (density=0.001) | 0.6007 | 0.6097 | 0.6073 |
| Gaussian Noise (density=0.005) | 0.6084 | 0.6074 | 0.605 |
| Gaussian Noise (density=0.01) | 0.6061 | 0.6051 | 0.6027 |
| Salt & Pepper Noise (density=0.1) | 0.6038 | 0.6028 | 0.6004 |
| Crop(100,100) | 0.7456 | 0.7346 | 0.7322 |

Six different types of attacks on the watermarked MRI image are shown in figure 17. Figure 17(a) gives 3×3 window mean attack, 17(b) median attack, figure 17(c)-17(f) rotation attacks, figure 17(g)-17(j) noise attacks and figure 17(k) shows crop attack on watermarked MRI image with RSA encrypted patient data of size 64×64. The extracted watermark after attacks are shown in figure 18. Figure 19 shows attacks on watermarked CT images and figure 20 shows the extracted watermarks after attacks. Finally the US watermarked images are attacked and watermark extracted are shown in figure 21 and 22 respectively.

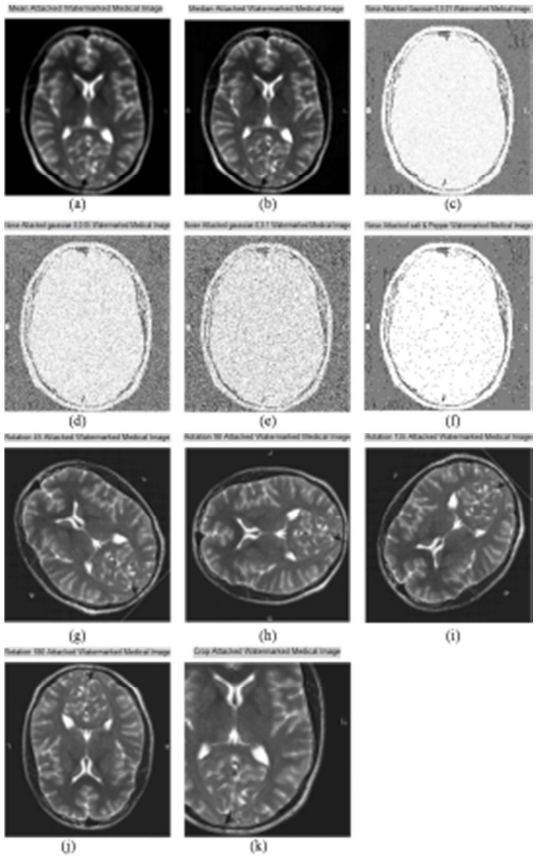


*Fig.17. MRI Watermarked Images with 'db2' after (a) 3×3 window mean attack,(b) 3×3 window median attack, (c,d,e,f) rotation attack with rotation angles of 45˚, 90˚, 135˚ and 180˚, (g,h,i,j) noise attack noise densities 0.001,0.005,0.01 for Gaussian and 0.1for salt & pepper noise, and (k) shows crop attacks with area of [100,100].*

Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Fig.18. Extracted and Decrypted Patient images from MRI Watermarked Images with 'db2' after (a) 3×3 window mean attack,(b) median attack,(c)-(f) rotation attacks,(g)-(j) noise attack, and (k) shows crop attacks*

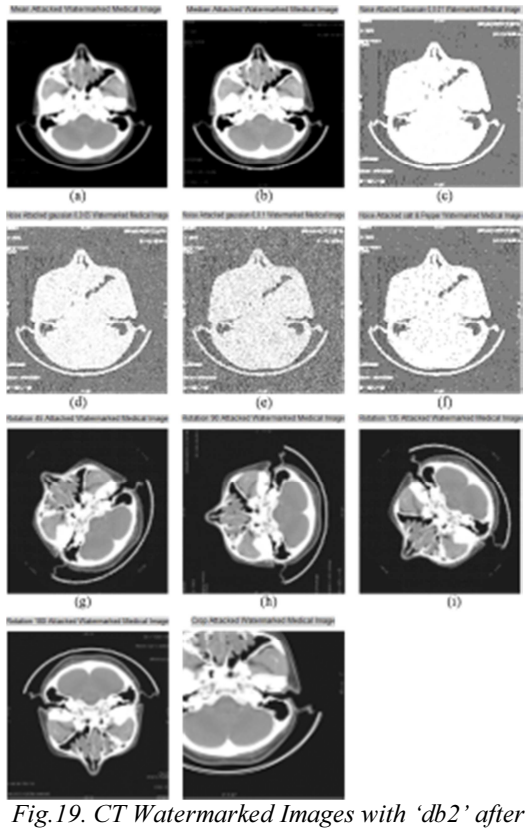


*Fig.19. CT Watermarked Images with 'db2' after (a) 3×3 window mean attack,(b)median attack, (c,d,e,f) rotation attacks, (g,h,i,j) noise attacks, and (k) shows crop attack.*

*Fig.20. Extracted and Decrypted Patient images from CT Watermarked Images with 'db2' after (a) 3×3 window mean attack,(b) median attack,(c)-(f) rotation attacks,(g)-(j) noise attack, and (k) shows crop attacks*

Figures 17 and 19 show a remarkable restraint towards attacks except for noise attacks. The proposed RSA-DWT watermarking procedure for medical images is visually effective as can be understood from the figures 17-20. One prominent conclusion is that the medical watermarked images get affected by noise in a notable manner compared to other attacks. Table-2 presents ncc values for Gaussian and salt & pepper noise for all densities with very poor results. Visually also 17(c)-17(f) and 19(c)-19(f), the watermarked medical image is completely lost except for the edges. At the same time the extracted watermark from the noise attacked watermarked image is in good condition visually and the ncc is around 0.8223. Except noise attack, remaining attacks does not affect the proposed RSA-DWT watermarking and extraction processes. Figures 21 and 22 provide visual information on attacks for Ultrasound Medical Images.

From figures 18, 20 and 22, the RSA-DWT medical image watermarking scheme has a good quality of extracted medical images even under attacks. For noise attacks medical images loose most of the information but the watermarking process RSA-DWT retains the watermark patient image with minimum damage. The reason where normal DWT based watermarks fail, the proposed in this paper prevails due to the RSA based encryption and decryption applied before and after transmission.

Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

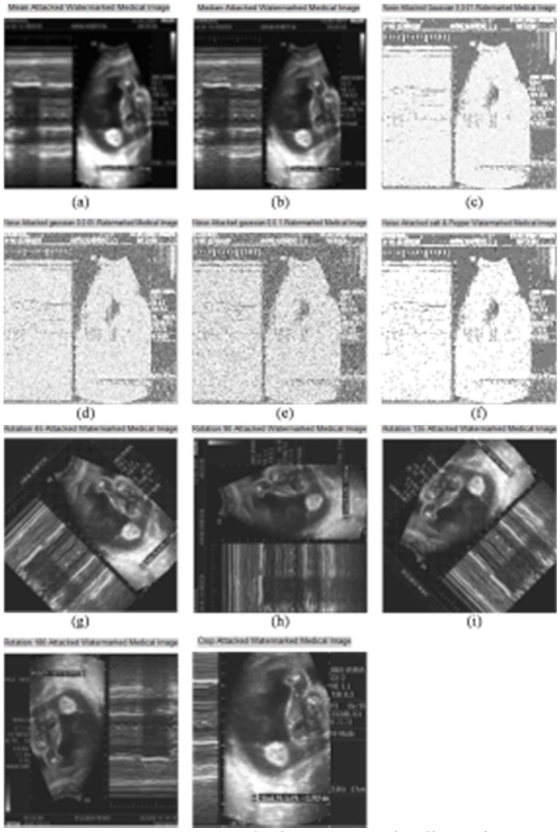


*Fig.19. US Watermarked Images with 'db2' after (a) mean attack,(b)median attack, (c,d,e,f) rotation attacks, (g,h,i,j) noise attacks, and (k) crop attack.*

*Fig.20. Extracted and Decrypted Patient images from US Watermarked Images with 'db2' after (a) 3×3 window mean attack,(b) median attack,(c)-(f) rotation attacks,(g)-(j) noise attack, and (k) shows crop attacks*

## 6. CONCLUSION

In this paper a RSA-DWT based medical image watermarking scheme is proposed. Patient image is used as a watermark to load the medical image. Three types of medical images such as MRI, CT and US are used for testing the proposed RSA-DWT watermarking procedure. In this method the patient watermark image is encrypted with KEY generated using RSA algorithm. The encrypted patient image is used as a payload which is embedded into a Medical Image in wavelet domain. Experimental results show that the RSA-DWT scheme demonstrates superior protection on unsecured networks compared to normal DWT based watermarking scheme in [29]. The experimental results prove this fact visually and mathematically in this paper. Robustness of the RSA-DWT scheme is proved by subjecting the watermarked images to various attacks and extracting the payload. The proposed method does not put constraints on the resolution of the watermarks used.

## REFRENCES:

[1] Hsieh, Ming-Shing, Din-Chang Tseng, and Yong-Huai Huang. "Hiding digital watermarks using multiresolution wavelet transform." Industrial Electronics, IEEE Transactions on 48.5 (2001): 875-882.

[2] Xia, Xiang-Gen, Charles G. Boncelet, and Gonzalo R. Arce. "A multiresolution watermark for digital images." Image Processing, 1997. Proceedings., International Conference on. Vol. 1. IEEE, 1997. pp. 101-111.

[3] Antonini, Marc, et al. "Image coding using wavelet transform." Image Processing, IEEE Transactions on 1.2 (1992): 205-220.

[4] Wei, Z. H., P. Qin, and Y. Q. Fu. "Perceptual digital watermark of images using wavelet transform." Consumer Electronics, IEEE Transactions on 44.4 (1998): 1267-1272.

[5] Swanson, Mitchell D., Bin Zhu, and Ahmed H. Tewfik. "Transparent robust image watermarking." Image Processing, 1996. Proceedings., International Conference on. Vol. 3. IEEE, 1996.

[6] Kundur, Deepa, and Dimitrios Hatzinakos. "A robust digital image watermarking method using wavelet-based fusion." Image Processing, 1997. Proceedings., International Conference on. Vol. 1. IEEE, 1997.

[7] Wong, Ping Wah, and Nasir Memon. "Secret and public key image watermarking schemes for image authentication and ownership

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

verification."Image Processing, IEEE Transactions on 10.10 (2001): 1593-1601.

[8] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on. IEEE, 2005.

[9] Maity, Santi P., and Claude Delpha. "Optimization in digital watermarking techniques." vol., Adv. techn. in multimedia watermarking: Image, video and audio appl., IGI Global Pub., USA (2010): 369-406.

[10] Bors, Adrian G., and Ioannis Pitas. "Image watermarking using DCT domain constraints." Image Processing, 1996. Proceedings., International Conference on. Vol. 3. IEEE, 1996.

[11] Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia."Image Processing, IEEE Transactions on 6.12 (1997): 1673-1687.

[12] Bi, Ning, et al. "Robust image watermarking based on multiband wavelets and empirical mode decomposition." Image Processing, IEEE Transactions on 16.8 (2007): 1956-1966.

[13] Ganic, Emir, and Ahmet M. Eskicioglu. "Robust DWT-SVD domain image watermarking: embedding data in all frequencies." Proceedings of the 2004 Workshop on Multimedia and Security. ACM, 2004.

[14] Chandra, DV Satish. "Digital image watermarking using singular value decomposition." Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on. Vol. 3. IEEE, 2002.

[15] Mohamad Jansi, "PhD thesis 2005: Digital Watermarking in Medical Images", school of information systems, computing and Mathematics, Brunel University.

[16] Coatrieux, G., H. Maitre, B. Sankur, Y. Rolland, and R. Collorec. "Relevance of watermarking in medical imaging." In Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference on, pp. 250-255.

[17] Irany, Behrang Mehrbany, Xin Cindy Guo, and Dimitrios Hatzinakos. "A high capacity reversible multiple watermarking scheme for medical images." In Digital Signal Processing (DSP), 2011 17th International Conference on, pp. 1-6. IEEE, 2011.

[18] Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. Image Processing, IEEE Transactions on, 16(3), 721-730.

[19] Lavanya, A., and V. Natarajan. "Watermarking patient data in encrypted medical images." Sadhana 37.Part 6 (2012).

[20] Inoue, H., Miyazaki, A., Yamamoto, A., & Katsura, T. (1998, October). A digital watermark based on the wavelet transform and its robustness on image compression. In Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on (Vol. 2, pp. 391-395). IEEE.

[21] Boscher, Arnaud, Robert Naciri, and Emmanuel Prouff. "CRT RSA algorithm protected against fault attacks." Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems. Springer Berlin Heidelberg, 2007. 229-243.

[22] Barrett, Paul. "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor." Advances in cryptology—CRYPTO'86. Springer Berlin Heidelberg, 1987.

[23] Washington, Lawrence C., and Wade Trappe. *Introduction to cryptography: with coding theory*. Prentice Hall PTR, 2002.

[24] Nozaki, Hanae, et al. "Implementation of RSA algorithm based on RNS Montgomery multiplication." Cryptographic Hardware and Embedded Systems—CHES 2001. Springer Berlin Heidelberg, 2001.

[25] Huh, Mi-Suk, et al. "Security system using RSA algorithm and method thereof." U.S. Patent No. 7,421,074. 2 Sep. 2008.

[26] Kishore, P. V. V., & Rajesh Kumar, P. (2012). A Video Based Indian Sign Language Recognition System (INSLR) Using Wavelet Transform and Fuzzy Logic. International Journal of Engineering & Technology (0975-4024), 4(5).

[27] Kishore, P. V. V., & Kumar, P. R. (2012). A Model For Real Time Sign Language recognition System. International Journal of Advanced Research in Computer Science and Software Engineering, vol.2,(6).

[28] Kishore, P. V. V., Kumar, P. R., Kumar, E. K., & Kishore, S. R. C. (2011). Video Audio Interface for Recognizing Gestures of Indian Sign. International Journal of Image Processing (IJIP), 5(4), 479.

[29] N.Venkatram, L.S.S.Reddy, P.V.V.Kishore, Multiresolution Medical Image Watermarking for Telemedicine Applications, CiiT International Journal of Digital Image Processing, Vol(6),Issue 1, Jan 2014,pp6-15.