CHAPTER IV

MIW with RSA-DWT
4.1 Introduction

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 about 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 chapter is organized as follows. Section 4.2 gives a brief introduction of RSA algorithm. Section 4.3 deals with the proces of watermarking with RSA and DWT. Section 4.4 of this chapter gives medical image watermark extraction algorithm along with the decryption using inverse RSA.

Section 4.5 introduces measurable parameters that can judge the watermarking procedures with results and discussion that present an insight into the use of multiresolution wavelet transform with RSA encryption and decryption for medical image watermarking.

Finally conclusions are drawn on the medical image watermarking procedure discussed in this chapter in section 4.6.
4.2 RSA Algorithm of Watermark ImageEncryption

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

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

$$n = pq$$ (4.1)

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

$$\Psi(n) = \Psi(p)\Psi(q) = (p-1)(q-1)$$ (4.2)

where $\Psi$ 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 $\Psi(n)$ 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 $0 \leq m < n$ which is accomplished using padding scheme. The cipher text ‘$C$’ is computed as

$$C = m^e \pmod{n}$$ (4.3)

S7. Decryption:

Destination receives the encrypted message along with the secret key and decrypts the message ‘$m$’ using,

$$m = C^d \pmod{n}$$ (4.4)
The DWT has already been discussed extensively in the previous chapters. Hence a brief discussion about 2D DWT filter bank model is provided here. 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 level 1.

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

Further in level 2 decomposition the low frequency information is divided into LL and high frequency information LH. The high frequency component in level 1 is decomposed to low frequency information HL and high frequency HH. The wavelet decomposition process is shown in the figure 4.1. The results of wavelet decomposition using 2D Daubechies two wavelets for level 2 on a video frame is shown in figure 4.2.

Figure 4.1: Wavelet Decomposition based on Discrete WT
4.3 RSA Encrypted MI Watermark Embedding

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 produce an encrypted patient watermark image.

**S2.** Save the encrypted patient image and KEY. The KEY will accompany the watermarked image for decryption.
**S3.** Carry out $n^{\text{th}}$ level 2D Discrete Wavelet Transform (DWT) on the Medical Image (Cover Image) [29] and decompose into 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

$$W(i, j) = W^{\text{Sub}}(i, j) + (2\sigma + \delta)(2w^\varepsilon(k) - 1) \quad (4.5)$$

Where $W(i,j)$ is watermarked medical image with encrypted patient image. $W^{\text{Sub}}(i,j)$ is $n^{\text{th}}$ level wavelet sub-bands 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. $w^\varepsilon(k)$ is the encrypted patient image at $k^{\text{th}}$ position.

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

$$I^{WMi} = (W^{(n)})^{-1} \quad (4.6)$$

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.
4.4 Decrypted Patient Image Extraction Algorithm

The watermarked medical image $I_{RMi}$ 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 from 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.

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

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

(4.7)

Where $W_{RMi}(i, j)$ is the transformed 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.

**S3.** 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.
4.5 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 grayscale images, it is intended to consider grayscale patient image as watermark.

The dynamic standard deviation ratio factor $\sigma$ 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) as defined in eq’s 3.17 and 3.18 respectively. These parameters 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. Psnr
is the peak signal to noise ratio in db which range between 40db to 60 db generally for good watermarking. The values of normalized cross correlation coefficients (ncc) range from 0 to 1. Larger values of ncc are preferred for better watermarking.

Figure 4.3 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 medical image(256×256) is used as cover image for watermarking in figure 4.4(a) and Lena image is used as patient image(64×64) in figure 4.4(b).

RSA-DWT watermarking procedure proposed in this chapter embeds RSA encrypted patient image into brain MRI cover image as shown in figure 4.4(c).

Figure 4.4(d) shows the extracted encrypted watermark of patient image. Figure 4.4(e) shows decrypted patient watermark image. Visually figure 4 shows that the watermarked image and extracted image match stalwartly as per the human visual system.
The figure 4.4 shows the robustness of RSA-DWT algorithm. Similar results are acquired using Magnetic Resonance Imaging (MRI) in figures 4.5 and 4.6, and Ultrasound (US) Medical images, figures 4.7 and 4.8 as cover images. The watermark is a RSA encrypted patient image in grayscale.

**Figure 4.4:** (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 4.4 shows the robustness of RSA-DWT algorithm. Similar results are acquired using Magnetic Resonance Imaging (MRI) in figures 4.5 and 4.6, and Ultrasound (US) Medical images, figures 4.7 and 4.8 as cover images. The watermark is a RSA encrypted patient image in grayscale.

**Figure 4.5:** Discrete Wavelet Transform of Level -1 using ‘Haar’ mother wavelet (a) Original Brain MRI Medical Image (b) its 2D DWT
Figure 4.6: (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 4.7: Discrete Wavelet Transform of Level -1 using ‘Haar’ mother wavelet (a) Original pregnant ultrasound (US) Medical Image (b) its 2D DWT

Figure 4.8: (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
From figure 4.4, 4.6 and 4.8 it can visually be observed that the watermarking process proposed in this chapter 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 4.9 shows MRI Medical image in wavelet transformed domain up to level-1 and figure 4.10 shows watermarked medical image and extracted patient watermark image both encrypted and decrypted using db2 wavelet at level-1.

**Figure 4.9:** Discrete Wavelet Transform of Level -1 using ‘bd2’ mother wavelet (a) Original Brain MRI Medical Image (b) its 2D DWT using db2 at level-1

**Figure 4.10:** (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 for ‘db2’ at Level-1
Figure 4.11: Discrete Wavelet Transform of Level -2 using 'bd2' mother wavelet (a) Original Brain MRI Medical Image (b) its 2D DWT using db2 at level-2

Figure 4.12: (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 for 'db2' at Level-2

Figure 4.13: Discrete Wavelet Transform of Level -3 using 'bd2' mother wavelet (a) Original Brain MRI Medical Image (b) its 2D DWT using db2 at level-3
Figure 4.14: (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 for ‘db2’ at Level-3

Figure 4.15: Discrete Wavelet Transform of Level -1 using ‘bd2’ mother wavelet (a) Original Brain MRI Medical Image (b) its 2D DWT using db2 at level-4

Figure 4.16: (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 for ‘db2’ at Level-4
Level-2 db2 watermarking for the same MRI medical image is shown in figure 4.11 and figure 4.12 shows watermarked medical image and extracted watermark patient image. Level-3 and Level-4 are shown in figures 4.13, 4.14, 4.15 and 4.16 show wavelet transformed medical images and watermarked medical images and extracted watermarks.

Visually comparing the watermarked medical images from figures 4.10, 4.12, 4.14 and 4.15(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 4.10(c) and 4.12(c) produce good watermarked medical images and their extractions in figure 4.10(e) and 4.12(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 4.14(c) and 4.16(c), the watermarked medical images have deformed considerably.

Similarly the extracted watermarks for level-3 and level-4, form figures 4.14(e) and 4.16(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 4.17 and 4.18 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-VIII: psnr and ncc for Medical Cover Images

<table>
<thead>
<tr>
<th>Cover Medical Image</th>
<th>PSNR(db)</th>
<th>NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRI</td>
<td>49.8998</td>
<td>0.9835</td>
</tr>
<tr>
<td>CT</td>
<td>48.3565</td>
<td>0.9823</td>
</tr>
<tr>
<td>Ultrasound(US)</td>
<td>46.3454</td>
<td>0.9812</td>
</tr>
</tbody>
</table>

From Table-VIII 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 should be restricted to a maximum value of 3. Level-1 and 2 produce excellent results.
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 chapter.

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 from 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-IX.

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 completeuncorrelation 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 IX: Comparison of Extracted watermarks

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

Eleven different types of attacks on the watermarked MRI image are shown in figure 4.17. Figure 4.17(a) gives 3×3 window mean attack, 4.17(b) median attack, figure 4.17(c)-4.17(f) rotation attacks, figure 4.17(g)-4.17(j) noise attacks and figure 4.17(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 4.18. Figure 4.19 shows attacks on watermarked CT images and figure 4.20 shows the extracted watermarks after attacks. Finally the US watermarked images are attacked and watermark extracted are shown in figure 4.21 and 4.22 respectively.
Figure 4.17: 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 0.1 for salt & pepper noise, and (k) shows crop attacks with area of [100,100].
Figure 4.18: Extracted and Decrypted Patient images from MRI Watermarked Images with ‘db2’ after (a) 3x3 window mean attack, (b) median attack, (c)-(f) rotation attacks, (g)-(j) noise attack, and (k) shows crop attacks.
Figure 4.19: 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.

Figure 4.20: 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.
Figure 4.21: 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.
104

Figures 4.17 and 4.19 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 4.17-4.20. One prominent conclusion is that the medical watermarked images get affected by noise in a notable manner compared to other attacks.

Table-X presents ncc values for Gaussian and salt & pepper noise for all densities with very poor results. Visually also 4.17(c)-4.17(f) and 4.19(c)-4.19(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.

Figure 4.22: 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
Table X: Comparison of Extracted watermarks

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

Except noise attack, remaining attacks does not affect the proposed RSA-DWT watermarking and extraction processes. Figures 4.21 and 4.22 provide visual information on attacks for Ultrasound Medical Images.

From figures 4.18, 4.20 and 4.22, 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 method proposed in this chapter prevails due to the RSA based encryption and decryption applied before and after transmission.
4.6 Conclusions

In this chapter 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 chapter. 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.

The next chapter gives exclusive discussion on two non linear models and their application to medical image watermarking. The two non linear models used are Artificial Neural Networks and optimization algorithm known as BAT algorithm.

These two algorithms may aid in providing exceptionally good watermarked medical images and are restraint to attacks for real time telemedicine applications.