CHAPTER 4

IMPROVED RSA ENCRYPTION BASED MEDICAL IMAGE COMPRESSION USING FRACTIONAL FOURIER TRANSFORM AND MODIFIED SPIHT ENCODING SCHEME

4.1. CRYPTOGRAPHIC ENCRYPTION SCHEMES

In Cryptography, encryption is the process of concealing information to build it in an unreadable form without any particular knowledge. This is generally made for privacy and in confidential communication. Encryption may be used for various purposes like digital signatures, authentication and digital cash as discussed by Kostas & Andreas (2005).

Cryptography is related to more than one branch of knowledge. Even before the time of computers, it was closely associated to linguistic variables. At present, the importance of the computers has shifted the use of Cryptography in a wide range of technical areas such as Mathematics, particularly those areas called as Discrete Mathematics. It consists of topics from Number theory, Information theory, calculation complexity, statistics and Combinatorics. The securities of all the practical encryption schemes like symmetric and asymmetric schemes remain unverified. For symmetric ciphers, confidence gained in an algorithm is generally subjective. For example, there is no successful attack that has been reported on an algorithm
for several years in spite of intensive analysis. Such a cipher might also have provable security besides a restricted class of attacks. Intended for asymmetric schemes, it is found to rely on the complexity of the related mathematical problem, but it is also not provably secure. Unexpectedly, it is demonstrated that Cryptography has only one secure cipher that is the one-time pad. In this case, the keys are needed at least as long as the plaintext. It was therefore always too bulky to utilize (Kostas & Andreas 2005).

Sequences of well defined steps are taken as a procedure for performing encryption and decryption. A cipher is an algorithm for doing encryption and decryption process in Cryptography. The original information is known as plaintext and the encrypted form is called as ciphertext. Kostas & Andreas (2005) described that, the ciphertext message is built with all the information contained in the plaintext. However, the message is not in the readable format and it cannot be read by the humans.

Ciphers are typically parameterised by a piece of supplementary information, called a key. The encrypting procedure is varied based on the key which changes the complete operation of the algorithm. Without the key, the cipher cannot be used to encrypt, or to decrypt (Beker & Piper 1982).

In non-technical practice, a "cipher" is the similar thing as a "(secret) code". However, in technical negotiations, they are differentiated into two concepts, codes work at the level of meaning; that is, words or phrases are transformed into something else, whereas ciphers work at a lower level: the level of individual letters or small groups of letters or in modern ciphers as individual bits.

There are several different types of encryption are presented. Algorithms used previously in the history of Cryptography are considerably
different than the recent methods and the modern ciphers can be classified according to the key usage of one or more keys to operate.

Encryption methods can be divided into symmetric key algorithm. A symmetric-key algorithm is an algorithm for Cryptography that uses a similar cryptographic key to encrypt and decrypt the message. In fact, it is easy to calculate the decryption key from the encryption key and vice versa. In cryptography, an asymmetric key algorithm makes use of a pair of different, cryptographic keys to encrypt and decrypt. The two keys are associated scientifically, that a message encrypted by the algorithm by means of one key can be decrypted by the same algorithm (RSA), there are two separate keys: a public key is available and enables any sender to perform encryption, whereas a private key is set aside secret by the receiver and enables to perform decryption.

Symmetric key ciphers can be differentiated into two types, based on their work on blocks of symbols typically of a fixed size (block ciphers), or on a continuous stream of symbols (stream ciphers). In this chapter, an efficient and widely used cryptographic encryption technique is analyzed.

4.2. AN OVERVIEW OF RSA

In 1978, Ron Rivest, Adi Shamir & Leonard Adleman (1977) introduced a Cryptographic algorithm, which effectively replaced the less secure National Bureau of Standards (NBS) algorithm. Mainly, RSA implements a public-key cryptosystem, in addition to digital signatures. RSA is annoyed by the available works of (Diffie & Hellman 1976) from several years before, who illustrated the thought of such an algorithm, but never truly developed it.
At the time when the period of electronic email was likely to immediately arise, RSA implemented two significant ideas. They are,

1. Public-key encryption. This idea excludes the requirement for a courier to deliver keys to recipients in excess of an additional secure channel before transmitting the originally-intended message. In RSA, the encryption keys are public, whereas the decryption keys are not, so only the person with the accurate decryption key can decode an encrypted message. One and all have their own encryption and decryption keys. The keys must be ended in such a way that the decryption key may not be easily construed from the public encryption key.

2. Digital signatures. The receiver may require verifying that a transmitted message really originates from the sender (signature) and not from there (authentication). This is done by means of the sender's decryption key and the signature can afterward be public encryption key. Therefore, Signatures cannot be fictitious. Moreover, no signatory can later reject having signed the message.

RSA is well-known as an Asymmetric cryptographic system. This encryption technique is essentially a one-way function. Hence, a message encrypted with a public key can only be decrypted with the equivalent private key. This technique makes the problem of key distribution rather simpler; as there is only one key to deal out and it can be openly published (Stinson 2006). It is the primary algorithm known to be appropriate for signing with encryption and was extensively used in electronic commerce protocols, and is supposed to be protected given adequately long keys and the use of up-to-date implementations (Diffie & Hellman 1976). The RSA algorithm can be used for both public key encryption and digital signatures. RSA was one of the
initial immense advances in Asymmetric Cryptography and the algorithm depends on the integer factorization issues (RSA Laboratories 2007).

The RSA Algorithm is a general concept of Public key cryptography, which allows two parties who have never met and who can converse only on an insecure channel, to send protected and verifiable messages to each other. The Internet at present is an insecure communication channel with an apparent use for such technologies. Certainly, the greatest estimated growth for public key approaches is in Internet-related communication.

Among public key techniques, each user has two types of keys, one key is made public and the other key is to kept as secret. One of the keys is used to encrypt a message, and the other is used to decrypt the message.

4.3. THE RSA IMPLEMENTATION OF PUBLIC KEY ENCRYPTION AND DIGITAL SIGNATURES

The RSA system uses multiplication in modular arithmetic. The RSA system multiplies one number (called the base) by itself a number of times. The number of times a base is multiplied by itself is called the exponent,

\[ 16 = 2 \times 2 \times 2 \times 2 \]
\[ 16 = 2^4 \]

In this example, the number (2) is the base, and is multiplied by itself four times, making the exponent the number (4).

The RSA Algorithm may then be divided, into three steps
(1) Key generation: The key generation in which the factors of the modulus (n) (the prime numbers (p) and (q)) are selected and multiplied simultaneously to form (n), an encryption exponent (e) is chosen, and the decryption exponent (d) is computed by means of (e), (p), and (q).

(2) Encryption: Here, the message(M) is increased to the power(e), and then reduced modulo(n).

(3) Decryption: Here, the ciphertext(C) is increased to the power(d), and then reduced modulo(n).

In the RSA encryption formula, the message (denoted by a number M) is multiplied by itself (e) times called raising (M) to the power (e), and the product is after that divided by a modulus (n), leaving the remainder as a ciphertext (C) was studied by Patrick & James (1997)

\[ C = M^e \mod n \]  \hspace{1cm} (4.1)

This is a tedious operation to undo, when (n) is very large (200 digits or so) even the best computers by means of the fastest known methods could not possibly recuperate the message (M) simply from knowing the ciphertext (C) and the key used to create the message ((e) and (n)).

In the decryption operation, a different exponent, (d) is used to transform the ciphertext back into the plain text,

\[ C = M^d \mod n \]  \hspace{1cm} (4.2)

The modulus(n) is a composite number, build up by multiplying two prime numbers (Patrick & James 1997) (p) and (q), together,

\[ n = p \ast q \]  \hspace{1cm} (4.3)
The encryption and decryption exponents, (d) and (e), are associated with each other and the modulus (n) in the subsequent way as,

\[ d = e^{-1} \mod ((p-1)(q-1)) \]  

(4.4)

To compute the decryption key, one should know the numbers (p) and (q) (called the factors) used to determine the modulus (n). When (n) is an adequately large number, it is not feasible, by means of known algorithms and the fastest computing techniques to compute the prime number factors of (n).

4.4. ENCRYPTION USING RSA

RSA is effective on the basis of multiplication of two prime numbers. Consequently, number factorization is a serious intimidation next to RSA. Nowadays, the large numbers factorization is a main problem for humankind. On the other hand, there are a lot of ineffective algorithms presented today which will properly factor the big numbers. The design of RSA has been clearly described (Majid & Mohd 2012).

By considering the RSA, cryptosystem works on a given modulus “n” that is the product of two prime random numbers “p” and “q”, a public exponent "e", and an element \( C \in Z_n \), users find “m” such that \( C = m^e \mod n \) and a private exponent “d” that should satisfy \( m = c^d \mod n \).

4.5. DRAWBACKS OF RSA

The main disadvantage of RSA algorithm is that it takes higher encryption and decryption time. To overcome the problem of RSA algorithm, variants of RSA algorithm are used to get better speed of the RSA algorithm.

RSA is an extremely secure algorithm. The only well-known way to attack it is to carry out a "brute-force" attack on the modulus. This attack
can be simply overcome by increasing the key size (Rivest et al 1978). However, this approach can show the way to a number of problems namely,

- Increased processing time – as a rough guide, decryption time increases 8-fold as key sizes double.
- Computational Overheads – the computation need to perform the public key and private key transformations.
- Increased key storage constraint – RSA key storage (private keys and public key) requires important amounts of memory for storage.

In addition, key generation is difficult and time consuming (The time increases extensively as the key size increases). In each of the systems (RSA – DSS) substantial computational investments can be made. In RSA, a short public model can be employed (even though this does acquire some security risks) to speed up signature verification and encryption. In DSS, a large proportion of the signature generation and encrypting transformations can be pre-computed. Memory constrained devices cannot generate RSA keys effortlessly and so may need to have keys generated by another system. Conversely, this means that the non-repudiation service may not be possible (Burt 2006).

4.6. A NOVEL MEDICAL IMAGE DATA COMPRESSION AND SECURITY APPROACH

An enormous number of medical images are available in electronic format for effortless storage, maintenance, and retrieval. Omnipresent wired and wireless networks make it possible to access and share data among medical personnel, to promote high quality of care for patients. However, the handiness of data access and distribution creates a huge threat on the privacy of patients’ information.
A number of efforts are being made to offer solutions ensure the security of the data. Preserving patient’s privacy is the most important concern for medical data processing systems. The distribution of data in excess of a grid makes data control much more difficult than on closed systems. Data on grids may be simulated but all storage sites are not attributed to take delivery of medical data. Therefore, their administrators should not have access to read the data contented. A number of identifying metadata are not available to non attributed users as well. Attaining a high security level is compulsory but security is always a trade-off between trouble for the users and the preferred level of protection. Hence, much functionality such as the following needs to be provided to the users to use grids for their data storage and processing.

- Reliable authentication of users.
- Secure transfer of data from one grid element to another.
- Secure storage of data on a grid element.
- Access control for resources such as data, storage space or computing power.
- Anonymization of medical records to make them available for research.
- Tamper-proof logging of operations performed on medical files.
- Robustness against denial-of-service attacks

Thus, due to the importance of the security of the medical image data, cryptographic techniques are employed to offer security through their encryption process.
Thus, this approach uses an efficient cryptographic technique for encrypting the medical image data. The proposed image compression and encryption approach comprises of the following phases namely Encryption, Domain Transformation, Block based Pass-Parallel SPIHT Compression, Decoding through Inverse Block based Pass-Parallel SPIHT and Inverse Fractional Fourier Transform and finally Decryption.

![Diagram of the proposed image compression approach]

**Figure 4.1 Overall Flow of the Proposed Image Compression Approach**

### 4.6.1. RSA Based Encryption

Cryptography is the science of using Mathematics to encrypt and decrypt data that assures the storage and transmission of sensitive data in a secure manner. RSA is a widely used algorithm for public-key cryptography as discussed by Mare et al (2011).

In RSA, the encryption keys are public, while the decryption keys are not. Hence, only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key (Gaochang et al 2010). In RSA, the public key consists of the modulus n which is a large integer number, a product of two prime numbers p and q, whose bits length is the key size. If these numbers are identified, then the private key can then be hacked and the RSA is broken (Anane et al 2010).
4.6.2. Improved RSA

A disadvantage of using RSA algorithm is that it takes higher encryption and decryption time. To overcome the problem of RSA algorithm, variants of RSA algorithm are used to improve the speed, as explained by Cesar & Decio (2003).

There are four variants of RSA namely Batch RSA, Mprime RSA, Mpower RSA and Rebalanced RSA as discussed in Boneh & Shacham (2002). In the present research, only two variants of RSA, Mprime and Rebalanced RSA are considered with the goal of reducing the decryption and signature generation times of the original cryptosystem. The two variants are then integrated to attain a more efficient RSA approach. As a result, a new variant RPrime RSA, which is faster than plain RSA has been developed as discussed by Quisquater & Couvreur (1982).

4.6.3. Mprime (Multi-Prime) RSA

Mprime RSA was introduced by Collins et al (1997). It generates moduli with k prime factors \((n = p_1, p_2, \ldots, p_k)\) rather than two as such in RSA. Mprime RSA attains a decryption speedup relative to plain and QC RSA by minimizing the size of exponents and moduli, at the cost of extra modular exponentiations. However, a linear raise in the number of exponentiation results in a cubic decrease in the cost of each exponentiation, for an overall speedup that is quadratic in the number of factors \(k\) of the modulus.

4.6.4. Rebalanced RSA

Rebalanced RSA is based on the comments by Wiener (1990) about the weakness in the use of the private exponent \(d\). This variant improves decryption performance at the expense of encryption performance. This is carried out through selecting \(d\) such that \(d \mod p - 1\) and \(d \mod q - 1\) are small. However, this choice of \(d\) results in large values of \(e\). It is obvious that
dp, dq have s bits each. The cost of modular multiplication is the same as that of QC RSA. Hence, the only difference is the number of multiplications computed during each modular exponentiation. Rebalanced RSA is theoretically 6.4 times faster than QC RSA.

### 4.6.5. RPRIME RSA

The Rebalanced RSA and Mprime RSA approaches can be efficiently integrated for better performance as explained by Cesar & Decio (2003). The key generation process of Rebalanced RSA (modified for k primes) is carried out together with the decryption procedure of Mprime RSA. For image encryption applications which require high decryption and signing performance, the RPrime RSA, which for 2048-bits moduli showed an improvement of 30% over Rebalanced RSA, being 27 times faster than plain RSA and about 8 times faster than QC RSA.

#### Key generation

Generate k random primes $p_1, \ldots, p_k$, each $\lceil lg(n)/kc \rceil$ bits in size, with $gcd(p_1 - 1, \ldots, p_k - 1) = 2$, and compute $n = \prod_{i=1}^{k} p_i$.

Generate k random s-bit integers $d_{p_1}, \ldots, d_{p_k}$ such that $gcd(d_{p_1}, p_1 - 1) = \ldots = gcd(d_{p_k}, pk - 1) = 1$ and $d_{p_1} \ldots d_{p_k} (mod 2)$;

Apply the CRT to obtain d such that $d \equiv d_{p_i} (mod p_i - 1)$ for $1 \leq i \leq k$.

Calculate $e = d^{-1} mod \varphi(n)$

The public key is $\langle n, e \rangle$, while the private key is $\langle p_1, \ldots, p_k, d_{p_1}, \ldots, d_{p_k} \rangle$.

#### Encryption

Apply the encryption procedure of plain RSA. As was the case in Rebalanced RSA, we have $e = O(n)$ instead of $O(1)$ as in plain RSA, leading to more costly public-key operations.
The proposed scheme uses an efficient combination of two variants of the RSA cryptosystem MPrime and Rebalanced RSA analyzed by Boneh & Shacham (2002). The proposed RSA algorithm is about 27 times faster than the original cryptosystem. Once, the encryption process is completed, the encrypted image data is given as input to the Fractional Fourier transform block.

4.6.6. **Fractional Fourier Transform**

Discrete Fractional Fourier Transform (DFrFt) is applied to the encrypted image to obtain the transformed coefficients. It is found that by altering the value of fractional order “a” to different value, the DFrFt can provide significant results in terms of PSNR as discussed by Ma Jing et al (2011).

The extra degree of freedom provided by the fractional orders of DFT becomes the main aspect of the DFrFT. FrFT share several valuable properties of the regular Fourier transform and has a free parameter “a”, its fraction. When the fraction is zero, the Fourier modulated version of the input signal is obtained. When it is unity, conventional Fourier transform is obtained. As the fraction alters from 0 to 1, different forms of the signal are obtained, which interpolate between the Fourier modulated form of the signal and its FT representation. In the present research, the encrypted DICOM images are compressed by DFrFT.

4.6.7. **Discrete Fractional Fourier Transform**

FrFT is a class of time–frequency representations that have been widely used in the domain of Signal processing. The calculation of DFrFT is formulated by means of the Eigen-decomposition of the DFT kernel matrix as described in Pei and Yeh (1996). The kernel matrix of DFT has only four distinct Eigen values \([1, -j, -1, j]\) shown in McClellan & Parks (1972).
The same vector space Eigen value is formulated by the Eigen vectors as these Eigen vectors of DFT kernel is not exclusively obtained. A matrix S is formulated to evaluate the Eigen vectors of F with real values as discussed in Dickinson & Steiglitz (1982). The matrix S is defined as follows,

\[
s = \begin{bmatrix}
2 & 1 & 0 & 0 & \ldots & 1 \\
1 & 2\cos(\omega) & 1 & 0 & \ldots & 0 \\
0 & 1 & 2\cos(2\omega) & 1 & \ldots & 0 \\
1 & 0 & 0 & 0 & \ldots & 2\cos(N-1)\omega
\end{bmatrix}
\]  

(4.11)

where, \( \omega = \frac{2\pi}{N} \). It satisfies the following commutative property.

\[SF=FS\]  

(4.12)

The Eigen vectors of S matrix are identical to that of the eigenvectors of F with different corresponding Eigen values. Due to the symmetric property of S matrix, all Eigen values of S matrix are real and the eigenvectors are orthonormal to each other. The Eigen-decomposition of matrix S is formulated as below,

\[s = \sum_{k=0}^{N-1} \gamma_k v_k\]  

(4.13)

where, \( v_k \) is the Eigen vector of the matrix S corresponding to the Eigen value \( \gamma_k \). The Eigen-decomposition of DFT kernel matrix F is written as,

\[F = \sum_{k \in E_1} v_k v_k^* + \sum_{k \in E_2} (-j)v_k v_k^* + \sum_{k \in E_3} (-1)v_k v_k^* + \sum_{k \in E_4} (j)v_k v_k^*\]  

(4.14)

where \( E_1, E_2, E_3 \) and \( E_4 \) denotes the set of indices for Eigen vectors which belongs to the Eigen values \([1, -j, -1, j]\) respectively. From Equation (4.15)
the Eigen values of DFT kernel is determined. The transform kernel of DFrFT is obtained by means of the fractional powers of these Eigen values,

\[ R^\alpha = F^{\frac{2\alpha}{\pi}} \]  \hspace{1cm} (4.15)

\[ \sum_{k=0}^{N-1} e^{-j\frac{2\pi N}{N}N} \text{ N is odd} \]

\[ \sum_{k=0}^{N-2} e^{-j\frac{2\pi N}{N}N} + e^{-j\frac{2\pi N}{N}N} \text{ N is even} \]  \hspace{1cm} (4.16)

where, \( v_k \) is the Eigen vector obtained from matrix \( S \). The DFrFT of signal \( x(n) \) can be computed through the following equation,

\[ x_\alpha(n) = R_\alpha x(n) = F^{\frac{2\alpha}{\pi}}x(n) = VD^{\frac{2\alpha}{\pi}}V^*x(n) \]  \hspace{1cm} (4.17)

The signal \( x(n) \) is also recovered from its DFrFT through an operation with parameter \( (-\alpha) \) as,

\[ x(n) = R_{-\alpha} X_\alpha(n) = VD^{\frac{-2\alpha}{\pi}}V^*X_\alpha(n) \]  \hspace{1cm} (4.18)

Several properties of DFrFT are discussed in Table 4.1

<table>
<thead>
<tr>
<th></th>
<th>Properties of DFrFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unitary</td>
</tr>
<tr>
<td>2</td>
<td>Angle Additivity</td>
</tr>
<tr>
<td>3</td>
<td>Time inversion</td>
</tr>
<tr>
<td>4</td>
<td>Periodicity</td>
</tr>
<tr>
<td>5</td>
<td>Symmetric</td>
</tr>
</tbody>
</table>
Two-Dimensional DFrFT is needed for the study of (2D) signals such as images. For a $M \times N$ matrix, the 2D DFrFT is calculated by applying 1D DFrFT to each row of matrix and then to each column of the resultant matrix. The 2D transformation kernel is defined with separable form as discussed by Pei & Yeh (1998),

$$ R_{(\alpha, \beta)} = R_\alpha \otimes R_\beta $$  \hspace{1cm} (4.19)

The 2D forward and inverse DFrFT are computed from above 2D transformation kernel as,

$$ X_{(\alpha, \beta)}(m, n) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} x(p,q) R_{(\alpha, \beta)}(p,q,m,n) $$  \hspace{1cm} (4.20)

$$ x(p,q) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} X_{(\alpha, \beta)}(m,n) R_{(-\alpha,-\beta)}(p,q,m,n) $$  \hspace{1cm} (4.21)

In two-dimensional DFrFT, two angles of rotation have to be considered: $\alpha = a\pi/2$ and $\beta = b\pi/2$ and if one of these angles is zero, the 2D transformation kernel minimizes to the 1D transformation kernel.

In medical image processing, compression plays a very important role. This means minimizing the dimensions of the images to a processing level. Image compression using transform coding provides significant results, with fair image quality as discussed by Yetik et al (2001). The cut-off of the transform coefficients can be tuned to bring about a negotiation between image quality and compression factor. To use this approach, an image is initially partitioned into non-overlapped $n \times n$ (generally taken as 8x8 or 16x16) sub images. A 2D-DFrFT is applied to each block to transform the gray levels of pixels in the spatial domain into coefficients in the frequency
domain. The coefficients are normalized by various scales based on the cut-off selected. At Decoder, the process of encoding is simply reversed.

4.6.8. SPIHT

The image is then compressed using the SPIHT algorithm. SPIHT is the image compression technique as explained by Hualiang et al (2010).

The overall flow of the SPIHT algorithm is shown in Figure 4.3. For a given set $T$, SPIHT defines a function of significance which shows whether the set $T$ has pixels larger than a given threshold. $S_n(T)$, the significance of set $T$ in the $n$th bit-plane is defined as,

$$S_n(T) = \begin{cases} 1, & \max_{w(i) \in T} \min(||w(i)||) \geq 2^n \\ 0, & \text{otherwise} \end{cases}$$ (4.22)

when $S_n(T)$ is “0,” $T$ is called an Insignificant set; if not, $T$ is referred as a significant set. An insignificant set can be denoted as a single-bit “0,” but a significant set is partitioned into sub-sets and its significances in turn are to be tested again. Based on the zero tree hypothesis, SPIHT encodes the given set $T$ and its descendants denoted by $D(T)$ together by verifying the significance of $T \cup D(T)$ (the union of $T$ and $D(T)$) and by denoting $T \cup D(T)$ as a

Figure 4.2 SPIHT Algorithm
single symbol “zero” if $T \cup D(T)$ is insignificant. On the other hand, if $T \cup D(T)$ is significant, $T$ is partitioned into sub-sets, each of which is tested independently.

4.6.9. **Decompression**

This process is the reverse to the compression technique. After SPIHT, it is necessary to transform the data to the original domain (spatial domain), to do this the Inverse Fractional Fourier Transform is applied first in columns and then in rows.

4.6.10. **Decryption**

RPrime RSA Decryption is carried out in this section to retrieve the original image. This process is highly similar to the process of encryption which has just been discussed. The key point to be considered is the need for secret key by computing once again the modular exponentiation to recover the original image.

Decryption

Compute $M_i = C^{d_{p_i}} \mod p_i$ for $1 \leq i \leq k$;

Apply the CRT to the $M_i$’s to obtain $M = Cd \mod n$.

Thus, the entire process of DICOM image compression is carried out with Fraction Fourier Transform domain and BSP SPIHT approach.

4.7. **Experimental Results**

For the experimental evaluation, three DICOM lung images are taken. The performance of the proposed approach is evaluated based on the PSNR value, MSE, encryption and decryption time.
Figure 4.3  DICOM Lung Test Images

Table 4.2  Comparison of the RPrime Encryption and Decryption Time

<table>
<thead>
<tr>
<th>Standard Images</th>
<th>Modulus (bits)</th>
<th>Encryption Time (seconds)</th>
<th>Decryption Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RSA</td>
<td>RPrime Encryption</td>
</tr>
<tr>
<td>Lung 1</td>
<td>2048</td>
<td>3.105</td>
<td>2.892</td>
</tr>
<tr>
<td></td>
<td>1024</td>
<td>1.965</td>
<td>1.721</td>
</tr>
<tr>
<td></td>
<td>512</td>
<td>1.510</td>
<td>1.326</td>
</tr>
<tr>
<td>Lung 2</td>
<td>2048</td>
<td>2.901</td>
<td>2.512</td>
</tr>
<tr>
<td></td>
<td>1024</td>
<td>1.789</td>
<td>1.493</td>
</tr>
<tr>
<td></td>
<td>512</td>
<td>1.443</td>
<td>1.224</td>
</tr>
<tr>
<td>Lung 3</td>
<td>2048</td>
<td>2.936</td>
<td>2.352</td>
</tr>
<tr>
<td></td>
<td>1024</td>
<td>1.839</td>
<td>1.462</td>
</tr>
<tr>
<td></td>
<td>512</td>
<td>1.493</td>
<td>1.021</td>
</tr>
</tbody>
</table>

It is observed from the Table 4.2 that the proposed RPrime Encryption consumes lesser encryption and decryption time than the traditional RSA approach. This is mainly due to the hybrid nature of Rebalanced and Mprime RSA. The evaluation is carried out for three different bits such as 2048, 1024 and 512 bits. For all the three Lung images taken for consideration, the encryption and decryption time of the proposed RPrime encryption is lesser.
Table 4.3 shows the PSNR value comparison of the proposed DFrFT with the existing approaches such as Wavelet Transform with SPIHT and D2 Transform Modified SPIHT. It is observed that the proposed approach provides better PSNR value than the existing technique.

Table 4.3 Comparison of PSNR of Fractional Fourier Transform with Modified SPIHT

<table>
<thead>
<tr>
<th>Standard Images</th>
<th>Bit Per Pixel (Bpp)</th>
<th>Wavelet Transform with SPIHT</th>
<th>D2 Wavelet Transform with Modified SPIHT</th>
<th>Fractional Fourier Transform with Modified SPIHT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lung 1</td>
<td>0.5</td>
<td>29.48</td>
<td>31.89</td>
<td>34.6</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>33.56</td>
<td>34.33</td>
<td>35.50</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>36.62</td>
<td>37.29</td>
<td>37.70</td>
</tr>
<tr>
<td>Lung 2</td>
<td>0.5</td>
<td>20.10</td>
<td>21.7</td>
<td>22.34</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>27.69</td>
<td>29</td>
<td>30.85</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>33.11</td>
<td>35.76</td>
<td>36.19</td>
</tr>
<tr>
<td>Lung 3</td>
<td>0.5</td>
<td>20.3</td>
<td>21.75</td>
<td>22.45</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>27.83</td>
<td>29.36</td>
<td>31.57</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>33.81</td>
<td>35.88</td>
<td>36.86</td>
</tr>
</tbody>
</table>

Figure 4.4 PSNR Evaluation of the Image Compression Techniques for DICOM Images for 0.5 (Bpp)
The Figures 4.5, 4.6 and 4.7 have been drawn for PSNR evaluation of the Image Compression Techniques for DICOM Images. From the figures, it is observed that the PSNR value of the proposed DFrFT algorithm approach is higher than that of the existing transformation approaches.
The comparison of the MSE value is shown in Table 4.4.

### Table 4.4 Comparison of the MSE values of Fractional Fourier Transform with Modified SPIHT

<table>
<thead>
<tr>
<th>Standard Images</th>
<th>Bit Per Pixel (Bpp)</th>
<th>Wavelet Transform with SPIHT</th>
<th>D2 Wavelet Transform with Modified SPIHT</th>
<th>Fractional Fourier Transform with Modified SPIHT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lung 1</td>
<td>2</td>
<td>115.68</td>
<td>35.11</td>
<td>30.41</td>
</tr>
<tr>
<td>Lung 2</td>
<td>2</td>
<td>114.52</td>
<td>33.14</td>
<td>29.25</td>
</tr>
<tr>
<td>Lung 3</td>
<td>2</td>
<td>113.54</td>
<td>32.54</td>
<td>28.4</td>
</tr>
</tbody>
</table>

**Figure 4.7 MSE Evaluation of the Image Compression Techniques for DICOM Images for 2 (Bpp)**

The MSE value comparison is shown in Figure 4.8. It is observed from the figure that the MSE value of the proposed FrFT approach is much less than that of the existing transformation approaches.
Figure 4.8 shows the output images of the proposed Image compression technique which uses RPrime encryption and pass parallel SPIHT encoding algorithm.
4.8 SUMMARY

This chapter clearly discusses about the proposed Improved RSA Encryption based Medical Image Compression Using Fractional Fourier Transform and Modified SPIHT Encoding Scheme. The detailed process about the proposed technique is explained in this chapter. The performance evaluation of the proposed approach has also been discussed. The performance of this proposed approach is compared with the various image compression techniques on parameters like PSNR, MSE, and encryption and decryption time. It is observed from the experimental results that the proposed Improved RSA Encryption Scheme provides the best results.