# Improved RSA Encryption based Medical Image Compression using Fractional Fourier Transform and Modified SPIHT Encoding Scheme

Vasanthi Kumari P
Assistant Professor, Department of CSE,
Coimbatore Institute of Engineering and Technology, Coimbatore.

K. Thanushkodi, Ph.D
Director of Akshaya College of Engineering and Technology, India.

## ABSTRACT
Medical image data generally need a huge amount of resources for storage and transmission. In recent years, due to the extensive popularity of medical imaging applications in healthcare settings and the increased interest in telemedicine technologies, it is important to minimize both storage and transmission bandwidth necessities required for archival and communication of related data, preferably by employing compression techniques. The security of the compressed image has also become an essential part in medical image analysis. This research focuses on providing efficient compression of the DICOM images with better security and authentication. The DICOM images are encrypted using Improved RSA Variant for better overall performance. This approach uses efficient fractional Fourier Transform and Block based Pass-Parallel SPIHT for compressing the DICOM images. The performance of the proposed approach is compared with the existing approaches and is observed to provide better PSNR and lower MSR values.

## Keywords
DICOM, Block based Pass-Parallel SPIHT, Fractional Fourier Transform, Magnetic Resonance Imaging (MRI).

## 1. INTRODUCTION
Medical image analysis has become an essential aspect in the field of image processing and a number of research works have been carried out in securing the medical image data [1]. Hospitals and medical centers produce large volume of digital medical image sequences and these sequences need substantial storage space. So, medical image compression is playing a vital role in the field of medical sciences [2]. This research work focuses on compressing Digital Imaging and Communication in Medicine (DICOM) for better storage and compatibility [3]. Compressed medical images have to protect all the original data details when they are restored for image presentation. That is, medical image compression and uncompression must be lossless.

Discrete Cosine Transform (DCT) has been widely used in image and video processing applications. DCT is considered as a discrete time version of the Fourier Cosine series [4]. DCT has been in close association with Discrete Fourier Transform (DFT) and it has been effectively used in the field of signal processing, image processing, communications and data compression applications.

This paper uses Fractional Fourier Transform (FrFT) for transformation approach [5]. Fractional Fourier transformation based image compression has extra degree of freedom that is provided by its fractional orders. FrFT poses a number of significant attributes of the regular Fourier transform and has a free parameter ‘a’ which is its fraction [6]. So, instead of wavelet domain the fractional Fourier domain approach is used in this approach.

An improved form of SPIHT algorithm is used in this research work for better compression efficiency. SPIHT algorithm produces a pyramid structure based on a fractional Fourier decomposition of an image. The original SPIHT algorithm processes the transformed coefficients (Wavelet/Fourier) in a dynamic order that is based on the values of the coefficients. Therefore, it is very tedious to process multiple coefficients in parallel and thus the throughput of the original SPIHT is degraded. Hence, this research work used Block-Based Pass-Parallel SPIHT Algorithm for the compression approach [7] to overcome the drawbacks of the original SPIHT algorithm.

In the present scenario, besides compression, the security of the medical image is also considered as an important aspect in medical image analysis. In recent years, the transmission of medical data has become an essential process and it is important to identify an effective and secure approach to transmit them over networks. Therefore, security problem occurs when sending medical image data over the network. Therefore, encryption has become a probable potential solution to provide security to the medical image data [3].

Encryption is the efficient technique to ensure security in the image data. When sending medical image data (DICOM) over wider networks for diagnosis, security of the image is under risk. This research work uses an efficient genetic algorithm based encryption approach for encrypting the medical image data. Then, the encrypted image is compressed using FrFT and Block-Based Pass-Parallel SPIHT algorithm.

## 2. METHODOLOGY
This approach comprises of 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.

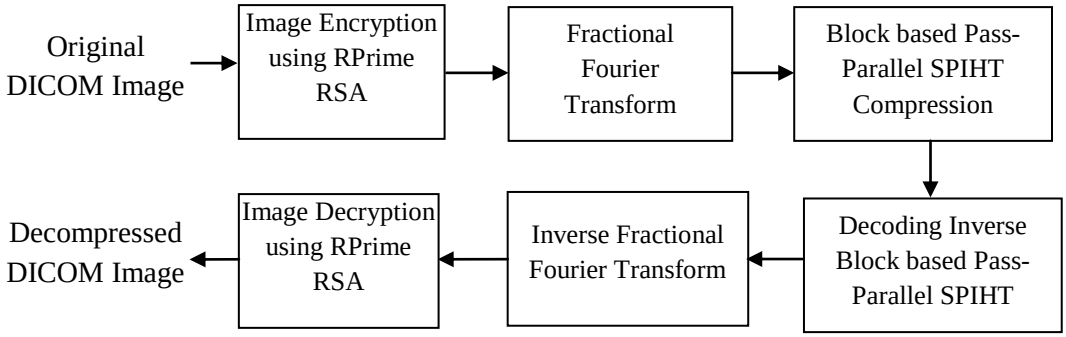



**Fig 1: Overall Flow of the Proposed Image Compression Approach**

## 2.1 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 [8].

In RSA, encryption keys are public, while the decryption keys are not, so 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 [9].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 be hacked and the RSA is broken [10].

### *2.1.1 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 of the RSA algorithm [11].

There are four variants of RSA namely Batch RSA, Mprime RSA, Mpower RSA and Rebalanced RSA [12]. In this paper only two variants of RSA namey Mprime and Rebalanced RSA are taken into consideration with the goal of reducing the decryption and signature generation times of the original cryptosystem. Then the two variants are integrated to attain a more efficient RSA approach. As a result, a new variant RPrime RSA is faster than plain RSA [13].

### *2.1.2 Mprime (Multi-Prime) RSA*

Mprime RSA was introduced by Collins et al. [14]. It generates moduli with k prime factors ($n = p1, p2, \cdots pk$) 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. But, a linear raise in the number of exponentiations 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.

### *2.1.3 Rebalanced RSA*

Rebalanced RSA is based on comments by Wiener [15] on 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. But, this choice of d results in large values of e. It is obvious that $dp, dq$ have $s$ bits each (hence $log\ dp = log\ dq = O(s)$). The cost of modular multiplications is the same as that of QC RSA, so the only difference is the number of multiplications computed during each modular exponentiation. Rebalanced RSA is theoretically 6.4 times faster than QC RSA.

### *2.1.4 RPRIME RSA*

The Rebalanced RSA and Mprime RSA approaches can be efficiently integrated for better performance [11]. 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 therefore about 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 $\lfloor lg(n)/kc \rfloor$ bits in size, with $gcd(p_1 - 1, \ldots, p_k - 1) = 2$, and compute $n = \prod_{i=1}^{k} pi$ ; Generate k random s-bit integers $dp_1, \ldots, dp_k$ such that $gcd(d_{p_1}, p_1 - 1) = \ldots = gcd(dpk, pk - 1) = 1\ and\ dp1\_\ldots\_dpk\ (mod\ 2)$;

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

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

The public key is $\langle n, e \rangle$, while the private key is $\langle p_1, \ldots, p_k, dp_1, \ldots, dp_k \rangle$.

[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 and Shacham [12]. The proposed RSA algorithm is about 27 times faster than the original cryptosystem.

## 2.2 Fractional Fourier Transform

After the quasi group encryption, the DICOM image is encrypted and the encrypted image is given as input to the Fractional Fourier transform block.

Discrete Fractional Fourier Transform (DFrFt) is applied to the encrypted image to obtain the transformed coefficients. It is analyzed that by altering the value of fractional order "a" to different value, the DFrFT can provide significant results in terms of PSNR [16].

The extra degree of freedom provided by the fractional orders of DFT and this 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 this paper, the encrypted DICOM images are compressed by DFrFT [16].

### *2.2.1 Discrete Fractional Fourier Transform*

FrFT is a class of time–frequency representations that have been widely used in domain of signal processing. The calculation of DFrFT is formulated by means of the Eigen-decomposition of the DFT kernel matrix [17]. The kernel matrix of DFT has only four distinct Eigen values [l, *- j,* -1, *j*] shown in [18].

A vector space same Eigen value is formulated by the Eigen vectors as these Eigen vectors of DFT kernel is not obtained exclusively. A matrix S is formulated to evaluate the Eigen vectors of F with real values [19]. The matrix S is defined as follows:

$$s = \begin{bmatrix} 2 & 1 & 0 & 0 & \dots & 1 \\ 1 & 2cos\omega & 1 & 0 & \dots & 0 \\ 0 & 1 & 2cos2\omega & 1 & \cdots & 0 \\ 1 & 0 & 0 & 0 & \cdots & 2\cos(N-1)\,\omega \end{bmatrix} \quad (2)$$

Where $\omega = \frac{2\pi}{N}$. It satisfies the following commutative property.

$$SF=FS \quad (3)$$

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:

$$s = \sum_{k=0}^{N-1} \gamma_k v_k \quad (4)$$

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:

$$F = \sum_{k\in E1} v_k v_k^* + \sum_{k\in E2} (-j) v_k v_k^* + \sum_{k\in E3} (-1) v_k v_k^* + \sum_{k\in E4} (j) v_k v_k^* \quad (5)$$

where*E1,E2,E3* and *E4* denotes the set of indices for Eigen vectors which belongs to Eigen values [l, *- j,* -1, *j* ] respectively. From equation 5 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,

$$R^{\alpha} = F^{\frac{2\alpha}{\pi}} \quad (6)$$

$$\begin{cases} \sum_{k=0}^{N-1} e^{-jN\alpha_{v_k v_k^*}} & N \text{ is odd} \\ \sum_{k=0}^{N-2} e^{-jN\alpha_{v_k v_k^*}} + e^{-jN\alpha_{v_{N-1} v_{N-1}^*}} & N \text{ is even} \end{cases} \quad (7)$$

Where $v_k$ is the Eigen vector obtained from matrix **S**. The DFrFT of signal *x(n)*can be computed through equation

$$X_{\alpha}(n) = R_{\alpha}x(n) = F^{\frac{2\alpha}{\pi}}x(n) \quad = VD^{\frac{2\alpha}{\pi}}V^{*}x(n) \quad (8)$$

The signal *x(n)* is also recovered from its DFrFT through an operation with parameter *(-α)* as

$$x(n) = R_{-\alpha}X_{\alpha}(n) = VD^{\frac{-2\alpha}{\pi}}V^{*}X_{\alpha}(n) \quad (9)$$

Several properties of DFrFT are discuss in Table 1

Table 1.Properties of DFrFT

| | | |
|---|---|---|
| 1 | Unitary | $R_{\alpha}^{*} = R_{\alpha}^{-1} = R_{-\alpha}$ |
| 2 | Angle Additivity | $R_{\alpha}R_{\beta} = R_{\alpha+\beta}$ |
| 3 | Time inversion | $R_{\alpha}x(-n) = X_{\alpha}(-n)$ |
| 4 | Periodicity | $R_{\alpha+2\pi} = R_{\alpha}$ |
| 5 | Symmetric | $R_{\alpha}(\alpha, b) = R_{\beta}(b, \alpha)$ |

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 [20]:

$$R_{(\alpha,\beta)} = R_{\alpha} \otimes R_{\beta} \quad (10)$$

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

$$X_{(\alpha,\beta)}(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} x(p,q)R_{(\alpha,\beta)}(p,q,m,n) \quad (11)$$

$$x(p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} X_{(\alpha,\beta)}(m,n)R_{(-\alpha,-\beta)}(p,q,m,n) \quad (12)$$

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 [21]. The cutoff of the transform coefficients can be tuned to bring out a negotiation between image quality and compression factor. In order to use this approach, an image is initially partitioned into non-overlapped $n \times n$ (generally taken as 8x8 or 16×16) 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 cutoff selected. At Decoder, the process of encoding is simply reversed.

## 2.3 SPIHT

Then the image is compressed using the SPIHT algorithm. SPIHT is the image compression technique [22].

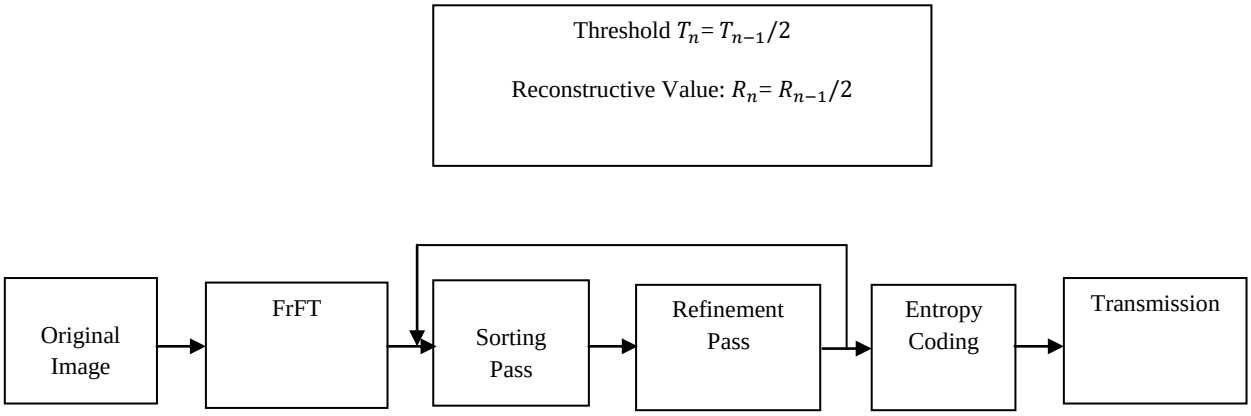



**Fig 2: SPIHT Algorithm**

The overall flow of the SPIHT algorithm is shown in figure 2. 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

$$s_n(T) = \begin{cases} 1, & \max_{w(i)\in T}(|w(i)|) \geq 2^n \\ 0, & otherwise \end{cases} \qquad (13)$$

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 subsets and its significances in turn are to be tested again. Based on the zero tree hypothesis [2], SPIHT encodes given set T and its descendants denoted by D (T) together by verifying the significance of T ∪ D(T ) (the union of T and D(T )) and by denoting T ∪ D(T ) as a single symbol "zero" if T ∪ D(T ) is insignificant. On the other hand, if T ∪ D (T) is significant, T is partitioned into subsets, each of which is tested independently.

### *2.3.1 Limitations of SPIHT Coding Scheme*

Slow processing speed due to its dynamic processing order that depends on the image contents

## 2.4 High Throughput Image Coding

This section presents a modified SPIHT algorithm, called the Block-based Pass-parallel SPIHT (BPS). The proposed algorithm mainly concentrates to speed up both encoding and decoding times.

### *2.4.1 Block-Based Pass-Parallel SPIHT*

BPS processes each bit-plane from the most significant bitplane just like the original SPIHT algorithm. However, the processing order of the pixels in each bit-plane is not same as the original SPIHT algorithm. BPS first decomposes the whole bitplane into 4 × 4 bit blocks and processes each 4 × 4-bit block at a time. After one 4 × 4-bit block is processed, the next 4×4 bit block is processed in the Morton scanning order [23].

The encoded stream in the original SPIHT is comprises of three kinds namely sorting bit, magnitude bit and sign bit. The sorting bit is the result of the significance test for a 2 × 2 or 4 × 4 set showing whether the set is significant or not. The magnitude and sign bits indicate the magnitude and sign of each pixel, respectively. The magnitude and sign bits output in IPP and SPP are called "refining bit," but the magnitude and sign bits output in ISP are called the "first refining bit" as these bits are the refining bits formed initially for each pixel. The proposed BPS algorithm is formulated for a single 4 × 4-bit block. The 4 × 4-bit block is represented by *H* that is decomposed into four 2 × 2 blocks.

BPS comprises of three passes they are output refining bits, sorting bits, and first refining bits, respectively. Based on the type of generated bits, these three passes are called Refinement Pass (RP), Sorting Pass (SP), and First Refinement Pass (FRP), respectively.

The RP is a integration of the IPP and SPP from the original SPIHT and visits each 2 × 2 block which is significant in the previous bit-plane (i.e., $S_{n+1}(Q) = 1$ as the condition in line 2 of the algorithm. Then, RP outputs the *n*th magnitude bit of the significant 2 × 2 bit block. Moreover, the sign bit of a pixel is output if the pixel becomes significant in the *n*th bit-plane (i.e. $S_{n+1} + (w(i)) = 0 \wedge S_n(w(i)) = 1$. The order of pixels processed in BPS is different from that in original SPIHT as the two passes IPP and SPP from the original SPIHT algorithm are integrated as a single pass RP in the proposed Block based Pass parallel SPIHT algorithm.

The ISP pass in the original SPIHT is decomposed into SP and FRP passes in BPS. The SP categorizes a block as either significant or insignificant and transmits the sorting bits. The initial step of the SP is to transmit and produce the significance of the 4 × 4-bit block. This is processed when two constraints are met. The initial condition is that the 4×4-bit block is insignificant in the (*n* + 1)th bit-plane (i.e., $S_{n+1}(H \cup D(H)) = 0$). The second condition $\sim (parent(H) \wedge S_n(parent(H)) = 0$ implies that it is not mandatory to construct the significance of the set if the 4×4-bit

block has a parent whose descendants are insignificant as the insignificance of the parent already shows that the 4 × 4-bit block is insignificant. SP is the only pass that processes a 4×4-bit block. The other two passes RP and FRP process a 2 × 2 bit block as the processing unit.

The remaining operation of the SP is based on the significance of the 4×4-bit block. If the block is significant, it is decomposed into four 2 × 2-bit blocks. The significance of each 2 × 2 block is generated if it is insignificant in the $(n + 1)$th bit-plane. According to its significance, each 2 × 2-bit block is classified either as an insignificant block to be processed by the SP for the $(n-1)$th bit-plane or as a significant block to be processed by the FRP pass in the current bit-plane. To be processed by the FRP, a 2 × 2 block $Q$ requires its significance $S_n(Q)$ to be set to 1. The significant block processed by the FRP is called the new-significant block. When $(H \cup D(H))$ is insignificant, all four 2 × 2-bit blocks in $H$ are categorized as insignificant blocks for the $(n-1)^{th}$ bit-plane. The FRP pass processes the new-significant 2×2-bit blocks categorized by the SP. FRP outputs the *n*th magnitude bit of the pixels in the new-significant blocks. If the magnitude bit is significant in the FRP, this shows that the magnitude bit is significant in the first time for the pixel. Therefore, the sign bit is also output. It is to be noted ISP in the original SPIHT is decomposed into SP and FRP in the BPS algorithm. The separation of SP and FRP facilitates each pass to be processed in a single cycle. It should be noted that the process of FRP is based on the results of SP, so that parallel execution is not possible. In the implementation, FRP is delayed by one cycle, thus it can be executed in parallel with the RP and SP of the next 4 × 4-bit block. Parallel execution is possible as the FRP in the current 4 × 4-bit block is not dependent on the RP and SP of the next 4 × 4-bit block. Thus, for each cycle, the bitstream of a single 4 × 4-bit block for a given bit-plane is produced.

The compression efficiency can be obtained by a small adjustment in the selection of FNZB. When the size of the Fractional Fourier transformed image is relatively small (e.g., 16 × 16), the root pixel(s) has a much better absolute value than the other pixels in the image. Thus, only the root pixel(s) is significant for many very essential bit-planes. Therefore, the FNZB is obtained from the pixels excluding the root pixel(s). Then bit-plane coding initiates from this FNZB. As a result, the number of encoded bitplanes can be minimized. For the root pixel(s), the value from MSB to FNZB-1 is stored in the header.

Initialization before the algorithm is essential for the FNZBth bit-plane which is the most significant bit-plane to be processed. Initially, the 2 × 2 set that comprises the root pixel(s) is categorized as a significant block. All other blocks are categorized as insignificant. For any 2×2 set $Q$, the parameter $dsig$ is derived. This parameter is used to compute the significance $S_n(Q \cup D(Q))$. Moreover, for any 4×4 set $H$, significance $S_n(Q \cup D(Q))$ is also computed in advance. The initial derivation of $dsig$ makes the significance evaluation simple in such a way that it can be processed in a single cycle.

### *2.4.2 Bitstream Generation for a Fast Decoder*

In this scenario, improving the speed of a decoder is very complicated than that of an encoder. Since RP and SP are independent encoder can process them in parallel. However, in decoder, parallel execution of RP and SP is not possible as their independency of each other is not sufficient for parallel execution. Another constraint for parallel execution is the precalculation of the start bit of each pass in the bitstream. This constraint is very evident as a decoder cannot start to process a pass till the start bit of the pass is known prior to the start of the pass. It is very difficult for a decoder to identify the start bit of each pass as the length of each pass is not constant, and the length can be identified by the decoder only after the pass is completely decoded. Thus, in order to facilitate parallel execution of multiple passes in a decoder, the bitstream should be formatted in such a way that it should look ahead for the length of the bitstream for each pass.

Thus, before start of the RP, the end bit of the RP magnitude (and the start bit of the next SP sorting) is identified this in turn facilitates the decoding of both RP magnitude bits and SP sorting bits in parallel. Alternatively, the number of sign bits in the RP can be identified only after the magnitude bits of the equivalent RP are decoded. Therefore, the sign bits of RP are decoded in one cycle later than the decoding of the equivalent magnitude bits. For FRP, the number of sorting bits transmitted by the SP is known only after SP is completed. Therefore, FRP magnitude bits can be decoded one cycle later than SP. The number of magnitude bits from FRP is identified by the outcome of the SP in the same bit-plane. Therefore, the length of the FRP can be computed in advance before the FRP begins. This shows that the start bit of the RP of the next 4 × 4-bit block is also identified before the FRP starts. Therefore, both the RP and SP of the next 4×4-bit block is carried out in the same cycle as FRP. Hence, the RP and SP can be processed in parallel with the FRP of the previous 4 × 4-bit block.

Sign bits are stored from the right of the bitstream. The length of the sign bits transmitted by RP is not known before the RP is completed as it is identified by the RP based on the magnitude bit. Thus, the sign bits are processed by the decoder one cycle after the equivalent magnitude bits. The sign bits of FRP can only initiate after the magnitude bits of the FRP are decoded. Thus, the decoding of FRP sign bits is carried out one cycle after the decoding of FRP magnitude bits. It is to be observed that the FRP sign bits can be processed in the same cycle as the RP sign bits of the next 4 × 4-bit block.

## 3. DECOMPRESSION

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

## 3.1 RPrime RSA Decryption

This process is highly alike the process of encryption which has just been discussed. The key point to be considered is the need of secret key by computing once again the modular exponentiation to recover the original image.

[Decryption]

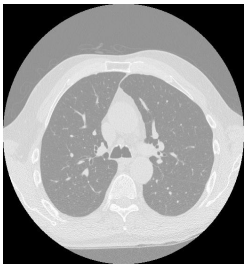
Compute $M_i = C^{dp_i} mod\ p_i\ for\ 1 \leq i \leq k$;

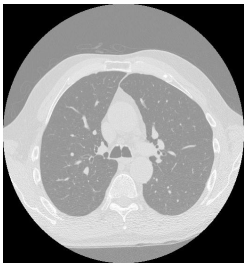
Apply the CRT to the $M_i's$ to obtain $M = Cd\ mod\ n$.

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

## 4. EXPERIMENTAL RESULTS

The experiment is carried out in MATLAB 7.0. The performance of the proposed approach is evaluated based on the PSNR value. The proposed approach is compared with the image compression using Haar transform. DICOM images of Lungs of size 256x256 are taken for experimentation.


Lung 1


Lung 2

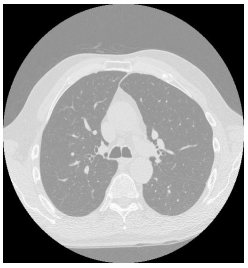

Lung 3

**Fig 3: DICOM Lung Test Images**

**Table 2: Encryption and Decryption Time Comparison**

| Standard Images | Bit Per Pixel (Bpp) | Encryption Time | | Decryption Time | |
|---|---|---|---|---|---|
| | | RSA | RPrime RSA | RSA | RPrime RSA |
| Lung 1 | 0.5 | 2.37 | 1.6 | 28.45 | 20.14 |
| | 1 | 3.89 | 1.75 | 39.58 | 29.28 |
| | 2 | 4.98 | 2.19 | 58.24 | 47.82 |
| Lung 2 | 0.5 | 2.40 | 1.65 | 29.68 | 21.04 |
| | 1 | 3.95 | 1.81 | 40.82 | 30.21 |
| | 2 | 4.96 | 2.14 | 60.45 | 47.05 |
| Lung 3 | 0.5 | 2.41 | 1.67 | 29.75 | 20.52 |
| | 1 | 3.94 | 1.79 | 39.80 | 29.8 |
| | 2 | 4.95 | 2.11 | 59.55 | 47.5 |

It is observed from the table that the proposed RPrime RSA consumes lesser encryption and decryption time when compared with the traditional RSA approach. This is mainly due to the hybrid nature of Rebalanced and Mprime RSA. For all the three Lung images taken for consideration, the encryption and decryption time for different bpp.

**Table 3: PSNR (DB) Comparison**

| Standard Images | Bit Per Pixel (Bpp) | Wavelet Transform with SPIHT | D2 Wavelet Transform with Modified SPIHT | Fractional Fourier Transform with BSP SPIHT |
|---|---|---|---|---|
| Lung 1 | 0.5 | 29.48 | 31.89 | 36.6 |
| | 1 | 33.56 | 34.33 | 37.10 |
| | 2 | 36.62 | 37.29 | 38.20 |
| Lung 2 | 0.5 | 20.10 | 21.7 | 23.97 |
| | 1 | 27.69 | 29 | 32.85 |
| | 2 | 33.11 | 35.76 | 37.19 |
| Lung 3 | 0.5 | 20.3 | 21.75 | 24.26 |
| | 1 | 27.83 | 29.36 | 33.17 |
| | 2 | 33.81 | 35.88 | 38.16 |

Table 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 when compared with the existing technique.

The MSE value comparison is shown in figure 4. It is observed from the figure that the MSE value of the proposed DFrFT approach is very less when compared with the existing transformation approaches.

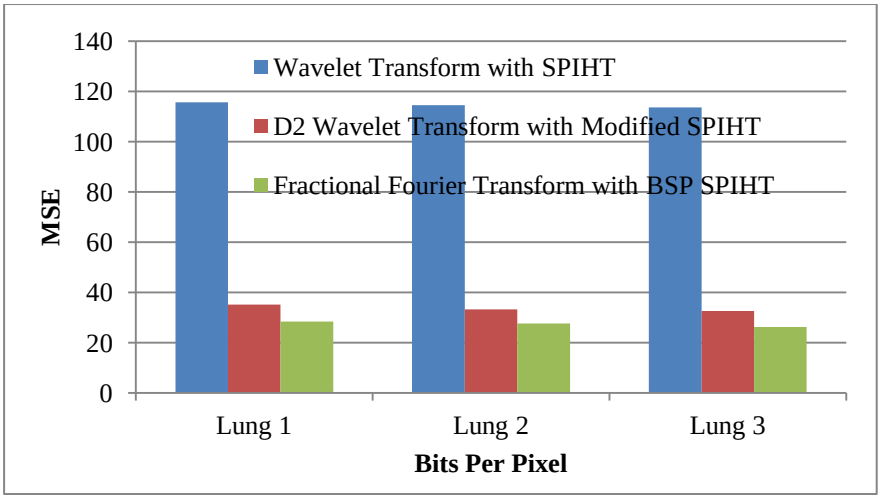
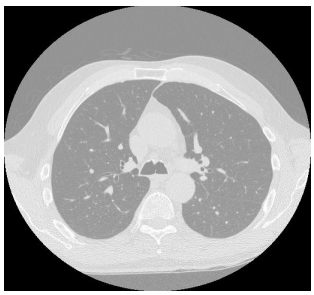
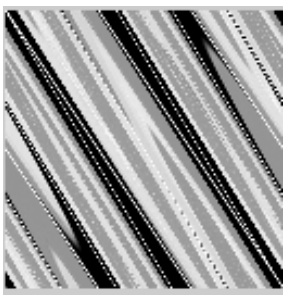



**Fig 4: MSE Evaluation of the Image Compression Techniques for DICOM Images for 2 (Bpp)**

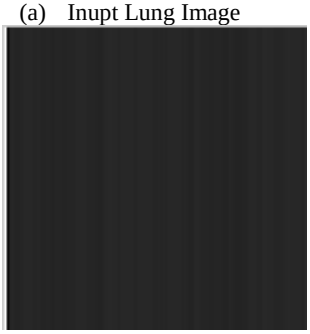


(a) Inupt Lung Image



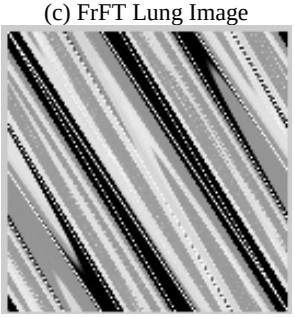
(b)RPrime RSA Encrypted Image

(c) FrFT Lung Image

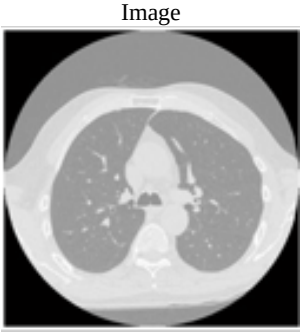


(d) Parallel SPIHT Encoding Lung Image

(e) Parallel SPIHT Decoding Lung Image



(f) Inverse FrFT Lung Image



(g) RPrime RSA Decrypted Lung Image

**Fig 5: Evaluated DICOM Lung Images using the Proposed Image Compression Approach**

Figure 5 shows the output images of the proposed Image compression technique which uses RPrime encryption and pass parallel SPIHT encoding algorithm.

## 5. CONCLUDING REMARKS

A novel image compression technique is introduced in this approach for providing better security and visual quality. Quasi group encryption technique is used in this approach for providing encryption. Fractional Fourier Transform is used in this approach for compression. It is observed that the DFrFT provides better compression efficiency when compared with the wavelet transformation. The performance of the proposed approach is evaluated with DICOM images of Lungs. This approach also uses the pass parallel SPIHT encoding scheme which provides better significance when compared with the SPITH coding approach. It is observed from the result that the proposed DFrFT with approach provides high PSNR values. Moreover, MSE value of the proposed approach is also very less when compared with the existing technique.

## 6. REFERENCES

[1] V. Sanchez, R. Abugharbieh, and P. Nasiopoulos, 2009. "Symmetry-Based Scalable Lossless Compression of 3D Medical Image Data", IEEE Transactions on Medical Imaging, Vol. 28, No. 7.

[2] Sandeep Kumar, 2011. "Image Compression Based on Improved Spiht and Region of Interests", 2011.

[3] R. Tamilselvi and G. Ravindran, 2011. "Encryption and Security Analysis Using Modified Advanced Encryption Standard Based Algorithm in DICOM Images Using Histogram and Encryption Quality", European Journal of Scientific Research ISSN 1450-216X Vol.54 No.4 (2011), pp.569-575.

[4] Andrew B. Watson, 1994. "Image Compression Using the Discrete Cosine Transform", Mathematica Journal, 4(1), 1994, p. 81-88.

[5] Namias, V. 1980. "The fractional order Fourier transform and its application to quantum mechanics", Journal of Institute of Mathematics and its Applications,no. 25, 241-265.

[6] Rajinder Kumar, Kulbir Singh and Rajesh Khanna, 2012. "Satellite Image Compression using Fractional Fourier Transform", International Journal of Computer Applications (0975 – 8887) Volume 50 – No.3, 2012.

[7] Ma, Jing; Fei, Jindong; Chen, Dong, 2011. "Rate-distortion weighted SPIHT algorithm for interferometer data processing", Journal of Systems Engineering and Electronics, Volume: 22, Issue: 4 Page(s): 547 – 556.

[8] Mare, S.F. ; Vladutiu, M. ; Prodan, L., 2011. "Secret data communication system using steganography, AES and RSA", IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME).

[9] Gaochang Zhao ; Xiaolin Yang ; Bin Zhou ; Wei Wei, 2010. "RSA-based digital image encryption algorithm in wireless sensor networks", 2nd International Conference on Signal Processing Systems (ICSPS).

[10] Anane, N. ; Anane, M. ; Bessalah, H. ; Issad, M. ; Messaoudi, K., 2010. "RSA based encryption decryption of medical images", 7th International Multi-Conference on Systems Signals and Devices (SSD).

[11] Cesar Alison Monteiro Paixao and Decio Luiz Gazzoni Filho, 2003. "An efficient variant of the RSA cryptosystem",

[12] Boneh, D. and Shacham, H. (2002). Fast variants of RSA. *RSA Laboratories.*

[13] Quisquater, J.-J. and Couvreur, C. (1982). Fast decipherment algorithm for RSA publickey cryptosystem. *Eletronic Letters*, 18:905–907.

[14] Collins, T., Hopkins, D., Langford, S., and Sabin, M. (1997). Public key cryptographic apparatus and method. US Patent #5,848,159.

[15] Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558.

[16] Ma, Jing; Fei, Jindong; Chen, Dong, 2011, "Rate-distortion weighted SPIHT algorithm for interferometer data processing", Journal of Systems Engineering and Electronics, Volume: 22, Issue: 4 Page(s): 547 – 556.

[17] Pei, S.C. andYeh, M. H. 1996. "Discrete fractional Fourier transform" IEEE International Symposium onCircuits and Systems,vol. 2, 536 – 539.

[18] McClellan, J. H. and Parks,T. W. 1972. "Eigenvalue and Eigen vector decomposition of the discrete Fourier transform", IEEE Transaction on Audio and Electroacoustics, AU-20, 66-74, (Mar. 1972).

[19] Dickinson,B. W. and Steiglitz,K. 1982."Eigenvectors and functions of the discrete Fourier transform", IEEE Transaction Acoustic., Speech, and Signal Processing., vol. ASSP-30, 25-31, (Feb. 1982).

[20] Pei, S.C.andYeh, M. H. 1998."Two dimensional discrete fractional Fourier transform", Signal Processing, vol. 67, 99-108.

[21] Yetik, I. S., Kutay, M.A. and Ozaktas,H.M. 2001."Image representation and compression using fractional Fourier transform", Optical Communication., vol. 197, 275-278.

[22] Hualiang Zhu, Chundi Xiu and Dongkai Yang, 2010. "An improved SPIHT algorithm based on wavelet coefficient blocks for image coding", International Conference on Computer Application and System Modeling (ICCASM),

[23] V. R. Algazi and J. Estes, 1995. "Analysis-based coding of image transform and subband coefficients", in Proc. SPIE Vis. Commun. Image Process. Conf., pp. 11–21