International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 4328-4337

Reduction of Image Transmission Resources and Improvement In Image Security Using SPIHT, Fractional Fourier Transform and RSA Algorithm

Shaık Afsar Basha[1], Dr. Ayyem Pillai V[2]

Medical images require large amount of resources for transmission and storage. Over the last few years, due to increase in popularity of medical imaging applications, it is very important to minimize both storage and the transmission bandwidth for communication of data. The resources can be minimized by using compression. Security of medical images is also very important. So it is essential to find a secure and effective approach to transmit the data over the networks. One of the best suitable solutions for secure transmission is encryption of medical image data. Discrete Fractional Fourier Transform (DFRFT) is used for reducing the dimensions of an image. Wavelet decomposition is used for the image Compression and RSA algorithm for encryption and decryption of image. In this paper novel approach is used which combines SET PARTIONING IN HIERARCHIAL TREES (SPIHT) and RSA for the image encryption and compression which enhances both the security and transmission rate. All the results are simulated in MATLAB software

Keywords: *Block Based Pass-Parallel SPHIT,Fractional Fourier Transform (FRFT), Mean Square Error, Peak Signal To Noise Ratio (PSNR)*

1 Introduction:

Image analysis in medical area has become a crucial aspect and a lot of research works are carried out in that field to securely transmit the research data. Many hospitals and research centres are producing a large number of image data which needs a huge storage space. So image compression in the medical field plays a key role in reducing the percentage of data for representation of an image. This Paper focuses on lossless compression of digital images.

There are many techniques in image and video processing and Discrete Cosine Transform (DCT) is one of them. It is considered as the discrete time version of Fourier Cosine series [10]. The DCT technique is very closely related with Discrete Fourier Transform (DFT) and has been very effective in the field of image processing, signal processing, data compression and communication applications.

This paper uses Fractional Fourier Transform (FRFT) for the transformation approach [10]. Fractional Fourier Transform image compression technique has similar attributes to a regular Fourier Transform and has an extra free parameter "a" which is the fraction [18]. By varying this parameter FRFT can achieve high PSNR [14] and low MSE.So instead of normal approach, Fractional Fourier transform approach is used. In this paper, an improved SPIHT algorithm is used for the better image compression. SPIHT algorithm has a structure of pyramid which is based on the Fractional Fourier decomposition of the image. The fundamental SPIHT algorithm will processes the transformed coefficients which are Wavelet/Fourier in a dynamic order which is based on the value of the transformed coefficients. So it is laborious process to process multiple coefficients at a time and thus the output of fundamental SPIHT is degraded. So this paper focuses on the Block-Based Pass –Parallel SPIHT algorithm for the image compression approach [11] to overcome the disadvantages of the Fundamental SPIHT algorithm.

At present in the field of medical images [14] not only compression but also the security of the image is very important. So it very crucial to choose an effective and secure image transmission method to transmit an image over the network. So for this purpose encryption has become a suitable solution to

ISSN: 2005-4238 IJAST

provide security for the medical image data [14]. This paper focuses on using an efficient algorithm for encrypting the medical image data and for this purpose RSA is used. In this after encrypting the image it is compressed using the FRFT and the Block-Based Pass-Parallel SPIHT algorithm.

2 Proposed Method

In the proposed method we are giving a digital image as an input. Then the image is encrypted using RSA algorithm. Then on the encrypted image we are applying FRFT to reduce the dimensions of an image. In this we are using discrete fractional Fourier transform for this purpose. After the FRFT transformed image we are applying SPIHT by using wavelets. Then inverse SPIHT and FRFT is applied. After this image is decrypted using key generated using RSA.

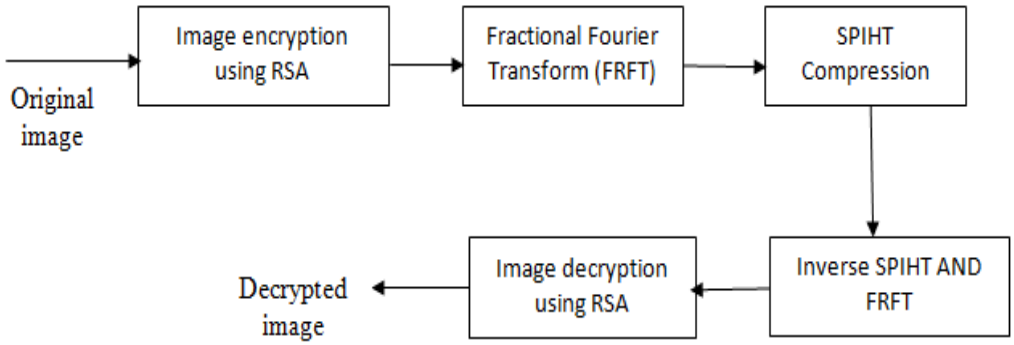

Fig 1: Flow of Proposed Method

2.1 Encryption Using RSA

Cryptography is an art of using mathematics to encrypt and decrypt digital data which assures for the storage and transmission of crucial data through a very secure manner. RSA is one of the most widely used algorithms in the field of public key cryptography [11].

RSA algorithm has two keys one for encryption which is a public key and the other is a decryption key which is a private key. In the RSA decryption key is designed such that it will not be easily decrypted from the encryption key [19]. RSA algorithm consists of a modulus n which is a product of two prime numbers x and y in which bit length is the key length. So if these numbers x and y are identified then the decryption key i.e. private key can be hacked [12].

2.1.1 Improvised RSA

The main disadvantage of using the fundamental RSA is the time taken for encryption and decryption will increase. So to tackle this problem variants for RSA are used which increases the speed of RSA [11]. Totally there are four variants for RSA which are M-prime RSA, Batch RSA, Rebalanced RSA and M-power RSA. In this research paper only two variants are used namely M-prime and Rebalanced RSA with a goal of reducing the signature generation time and decryption time of the cryptosystem. Finally these two variants are integrated to create a more efficient RSA. Due to this the new R-prime RSA approach is faster than the standard RSA.

2.1.2 Rebalanced RSA

Rebalanced RSA depends on remarks by Wiener[20] on the weakness in the utilization of private exponent d. This variant will improve the performance of decryption at the expense of performance of encryption. This is performed by selecting d such that d mod x-1 and d mod y-1 are small. But this selection of d results in large values of e. so it is obvious that dx, dy have s bits each (hence log dx= log dy= O(s)). Here the cost of modular multiplications is same as QC RSA and the only difference is number of multiplications computed for each modular exponentiation.

2.1.3 M-prime (Multi-Prime) RSA

Collins introduced the M-prime RSA [5]. It creates moduli with n prime factors instead of two which was the case of plain RSA. M-prime RSA accomplishes a decryption speed similar to plain and QC RSA by limiting the size of moduli and exponents at the expense of modular exponentiations. In any case a direct rise in the number of exponentiations causes a cubic decrease in the expense of each exponentiation for the overall speedup i.e. quadratic in the number of factors n of the modulus.

2.1.4 R-prime RSA

The M-prime RSA and Rebalanced RSA approaches can be effectively integrated for better performance [4]. The key generation procedure of Rebalanced RSA is carried out together with decryption procedure of M-prime RSA. For the image encryption applications which require high decryption and marking performance, the R-prime RSA has shown an improvement of 30% over Rebalanced RSA for 2048bits moduli. Hence it is 27 times quicker than the plain RSA and about eight times quicker than the QC RSA.

The proposed method uses a good combination of two variants of the RSA cryptosystem which are analysed by Shacham and Boneh [21]. This method is approximately 27 times faster than the original cryptosystem.

2.2 Fractional Fourier Transform

FRFT is a class of time frequency-representation and is an extension of classical Fourier Transform. It was introduced by Victor Namias [22] in the year 1980. FRFT is defined by transformation kernel K_α

$$k_{\alpha(t,u)} = \begin{cases} \delta(t-u) & if\ \alpha\ is\ a\ multiple\ of\ 2\pi \\ \delta(t+u) & if\ \alpha+\pi\ is\ a\ multiple\ of\ 2\pi \\ \frac{\sqrt{1-jcot\alpha}}{2\pi} e^{j\left(\frac{(u^2+t^2)}{2}\right)cot\alpha - jutcosec(\alpha)} & if\ \alpha\ is\ a\ multiple\ of\ \pi \end{cases} \quad \text{eq(1)}$$

FRFT belongs to a class of transformations which are sometimes called as quadratic phase-transforms or linear canonical transforms. Transformations belonging to this class can be broken into a succession of smaller operations such as *chirp convolution*, *chirp multiplication*, *Scaling and Fourier Transformation*. The one-dimensional(1D) FRFT is useful in processing of single-dimension signals such as speech waveforms. For the processing of two-dimensional signals such as images 1D FRFT is applied on each row of the matrix and then to each column of matrix. After the encryption of quasi group, the image is encrypted and given as input to the Fractional Fourier Transform block. To obtain the transformed coefficients from encrypted image DFRFT (Discrete Fractional Fourier Transform) is applied on it. By utilizing FRFT enormous amount of data is packed into smallest no transformed coefficients, and hence a smaller compression is achieved at this stage.

Fractional orders of DFT are providing an extra degree of freedom which become the main aspect of the DFRFT. FRFT have many valuable properties of regular Fourier Transform and has a free parameter "a" i.e. its fraction. Now when the fraction is zero, the Fourier modulated version of the input signal is

ISSN: 2005-4238 IJAST

obtained, and when it is unity conventional Fourier Transform is obtained. The free parameter i.e. the fraction when alters from o to 1 different forms of signal are obtained, which interpolates between the Fourier modulated form of the signal and its Fast transform representation. In this paper, images are compressed by DFRFT [14].

2.2.1 Discrete Fractional Fourier Transform

FrFt belongs to a class of time-frequency representations which have been widely used in the domain of signal processing. The calculations of DFrFt is obtained by means of Eigen decomposition of DF kernel matrix [16]. A matrix S is formulated to evaluate the values of F with the real values [15].

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

Here the matrix S is computed to evaluate the Eigen vectors of F and computing the Eigen decomposition of DFT kernel. After this compute DFrFt by the fractional powers of the Eigen values. The next step is to compute 2D forward and inverse DFrFt from 2D transformation for 2D images. All these efforts are to reduce the dimensions of the image so to have better compression efficiency.

2.3 SPIHT

SPIHT algorithm is an efficient image coding method developed by Said and Pearlman. This is an enhanced version of Embedded Zero Tree Wavelet (EZW) by Shapiro. It is one of the efficient image compression techniques [21]. SPIHT algorithm works in three steps. SPIHT defines the following function which shows whether the set T has pixels greater than a given threshold.

$$H_n(T) = \begin{cases} 1\,, max_{(i,j)\epsilon T}\{|i,j|\} \geq 2^n \\ 0 \qquad\qquad otherwise \end{cases} \quad \text{Eq(3)}$$

Here when $H_n(t)$ is "0" T is called as insignificant set else T is referred as a significant set. A significant set is partitioned into subsets and its significance are tested again where as an insignificant set can be denoted as a single bit "0". SPIHT algorithm encodes given set T and its descendants denoted by O(T). If the significance of T υ O(T) is insignificant then if it is given by single symbol zero where as if T υ D(T) is significant, T is partitioned into subsets to test each of them independently. SPIHT algorithm consists of three passes Significant Pixel Pass(SPP),Insignificant Pixel Pass(IPP) and Insignificant Set Pass(ISP).

2.3.1 Disadvantages Of SPIHT Coding

SPIHT algorithm has slow processing speed due to its dynamic processing order which depends on the contents of the image.

2.4 Efficient Image Coding

The following section deals with a modified SPIHT called as Block-based Pass-Parallel SPIHT(BPS). This proposed algorithm concentrates on speeding up both the encoding and decoding times.

2.4.1 Block Based Pass-Parallel SPIHT

ISSN: 2005-4238 IJAST

is insignificant in the (n+1)th bit plane. The second condition is it is not compulsory to construct the The BPS processes the bit-plane similar to the original SPIHT where the processing starts from the most significant bit plane. The main difference is the processing order of bit-plane is not same as original SPIHT. In this the BPS first decomposes the total bit-plane into 4×4 bit blocks and processes each 4×4 bit block at a time. After processing one 4×4 bit block the next 4×4 bit block is processed in a Morton scanning order [8].

In the original SPIHT the encoded stream consists of three kinds namely Magnitude bit, Sorting bit and Sign bit. The magnitude and the sign bit indicates magnitude and sign of each pixel and the sorting bit is a result of significance test for a 4×4 or 2×2 set presenting whether set is significant or insignificant. The sign and magnitude bits output in IPP and SPP are called as "refining bits", where as magnitude and sign bits output in and ISP are called as First Refining bits as these bits are refining bits formed initially from the each pixel of an image. The BPS algorithm proposed is designed for a single 4×4 bit block. The 4×4 bit block is represented by I which is decomposed into four 2×2 blocks.

BPS consists of three passes which are output refining bits, Sorting bits and first refining bits. According to the type of generated bits these passes are called as Refinement Pass(RP), First Refinement Pass(FRP), Sorting Pass(SP).The RP is a combination of SPP and IPP from the original SPIHT algorithm and take each 2×2 block which is significant in the previous bit plane(i.e.$H_{N+1}(Q)=1$). Then RP outputs the nth magnitude of significant 2×2 bit block. The order in which pixels are processed in BPS is different from the original SPIHT where IPP and SPP are combined as a single refinement pass in the BPS.

The ISP pass in fundamental SPIHT is decomposed into FRP and SP, in the BPS. The SP divides a block as either significant or insignificant and transmit the sorted bits. The first step of SP is transmit and produce the significant bits of 4×4 bit block. SP is processed when two constraints are met where the first condition is that 4×4 bit block significance of set if 4×4 bit block has a parent whose descendants or insignificant as insignificance of the parent shows 4×4 bit block is insignificant. SP is the only pass which processes the 4×4 bit blocks. The remaining passes RP and FRP process a 2×2 bit block.

The balance operation of the SP is based on significance of 4×4 bit block, and if the block is significant it will be decomposed into four 2×2 blocks. The significance of each 2×2 bit block is generated only if it is insignificant in $(n+1)^{th}$ bit plane. Depending on the significance each 2×2 bit block is classified as either as an insignificant block to be processed by the SP for the $(n-1)^{th}$ bit plane or as a significant block processed by the FRP pass in the current bit plane. For the processing by the FRP a 2×2 bit block Q requires its significance $H_n(Q)$ to be set to 1. The significant block which is being processed by the FRP is called the new significant block. When (I υ D(I)) is insignificant, all the four 2×2 bit blocks in I are considered as insignificant block for the $(n-1)^{th}$ bit plane. The FRP is going to process the new significant 2×2 bit blocks which are categorised by the SP. Now if the magnitude bit is significant for the FRP, then it shows that this bit significance for the first time for the pixel. Hence sign bit is also an output. The separation of FRP and SP help each pass to be processed in a single cycle. We should also keep in mind that the process of FRP is based on the result of SP, so that the parallel execution is not possible. In this implementation FRP is delayed by one cycle such that it can execute in parallel with the RP and SP of the next 4×4 bit block. Here the parallel execution is possible because the FRP in the current 4×4 bit block is not depending on the RP and SP of next 4×4 bit block. Hence for each cycle, the bit-stream of a single 4×4 bit block for a given bit-plane is produced.

The efficiency for the image compression can be obtained by adjustment in selection of FNZB(First Non-Zero Bit Plane). Then the size of FrFT image is relatively small then the root pixels of the image has an much absolute value then the other pixels of the image. Hence only root pixels are significant for many essential bit planes. Hence the FNZB is achieved from the pixels excluding root pixels. Now bit-plane coding initiates from this FNZB. Due to this the no of encoded bit-planes can be minimized. The value

from MSB to FNZB-1 is stored in header of root pixel. The initialization of FNZB bit-plane of the algorithm is essential as it is the most significant bit-plane to be processed. The initial 2×2 set which comprises of root pixels is considered as a significant block. All the remaining blocks are categorised as insignificant.

2.4.2 Generation of Bit-stream For a Fast Decoder

In the present scenario improving the speed of decoder is very difficult than that of an encoder. As RP and SP are independent, encoder can process them in parallel, but where as in case of decoder parallel execution of SP and RP is not possible as their independency is not sufficient for the parallel execution. The other constraint for parallel execution is pre-calculation of start bit of each pass in the bit stream. This factor is very clear as a decoder cannot start to process a pass until the start bit of pass is known prior to start of the pass. So for a decoder it is very difficult to identify the start bit of each pass as length of each pass is dynamic and this length can be known by the decoder only after the pass is totally decoded. So in order to facilitate parallel execution of multiple passes in a decoder, the design of bit stream should be in such a way that it should look ahead for the length of the bit -stream for each pass.

Therefore before the start of RP the final bit of RP magnitude is identified which in turn facilitates the decoding of both SP sorting bits and RP magnitude bits in parallel. Alternatively,the sign bits in the RP can be identified only after the magnitude bits of equivalent RP are decoded. Hence the sign bits of RP are decoded with one cycle delay with equivalent to magnitude bit. The no of sorting bits for FRP by the SP is known only after SP is completed. Hence the FRP magnitude bits can be decoded only after one cycle of SP. The outcome of SP determines the no. of magnitude bits for FRP in the same bit-plane. Hence the length of FRP can be calculated in advance before FRP starts. This also shows that the first bit of RP of the next 4×4 bit block is identified before the start of FRP. Therefore both the SP and RP of the next 4×4 bit block is carried out in the same cycle of FRP. Hence SP and RP can be processed in parallel with the previous 4×4 bit blocks of the FRP.

Sign bits are stored from the right of bit stream. The length of sign bits transmitted by RP isn't known before the RP is finished. As it is distinguished by the RP dependent on the magnitude bit. Therefore the sign bits are processed by the decoder after one cycle of equivalent magnitude bit. The sign bit of FRP can start only after the magnitude bits of FRP are decoded. Therefore the decoding of FRP sign bits is done once cycle after the decoding of FRP magnitude bits. It is to be noted that FRP sign bits can be prepared in same cycle as the RP sign bits of the following 4×4 bit block.

3 Decompression

Decompression is the inverse of the compression technique. After doing SPIHT it is necessary to transform data to the original domain and for this Inverse Fractional Fourier Transform is applied first on columns and then on the rows.

3.1 Decryption using R-Prime RSA

Decryption is similar to the process of encryption and the most important point is need of secret key which is computed once again by the modular exponentiation to recover the original digital image.

4 Results

ISSN: 2005-4238 IJAST

The results are carried out in MATLAB 16. The proposed method is compared with image compression using Haar Transform.

Figure 2 Original Image

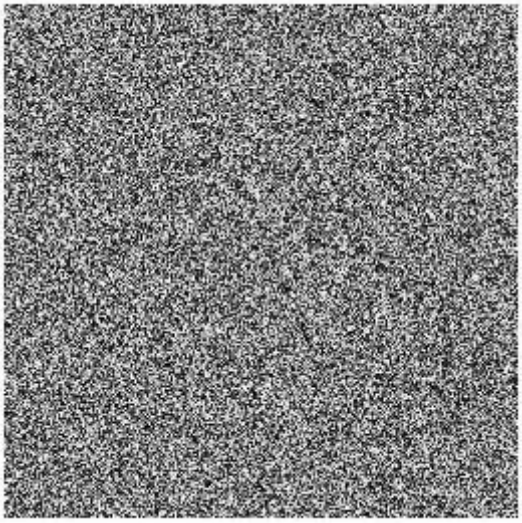

Figure 3 RSA Encrypted Image

ISSN: 2005-4238 IJAST

Figure 4 FRFT Transformed Image

Figure 5 SPIHT Transformed Image

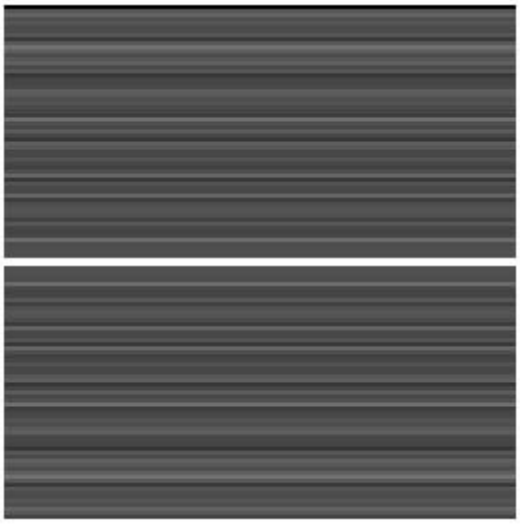

Figure 6 Inverse FRFT and SPIHT Transformed image

ISSN: 2005-4238 IJAST

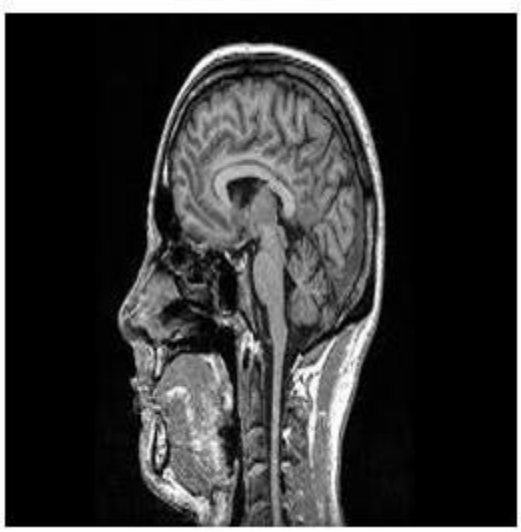

Figure 7 Decrypted Image

5 Conclusion

In this paper image is encrypted and decrypted using RSA. For providing the better image compression efficiency Fractional Fourier Transform is used. Block based parallel SPIHT is used for faster execution time

References

1. Sandeep Kumar, 2011. “Image Compression Based on Improved Spiht and Region of Interests”, 2011.
2. 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.
3. 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).
4. Cesar Alison Monteiro Paixao and Decio Luiz GazzoniFilho, 2003. “An efficient variant of the RSA cryptosystem.
5. Collins, T., Hopkins, D., Langford, S., and Sabin, M. (1997). Public key cryptographic apparatus and method. US Patent #5,848,159.
6. Pei, S.C. and Yeh, M. H. 1996. "Discrete fractional Fourier transform" IEEE International Symposium on Circuits and Systems,vol. 2, 536 – 539.
7. Pei, S.C.andYeh, M. H. 1998."Two dimensional discrete fractional Fourier transform", Signal Processing, vol. 67, 99-108.
8. 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.
9. V. Sanchez, R. Abugharbiieh, and P. Nasiopouos, 2009. “Symmetry-BasedScalableLossless Compression of 3D Medical Image Data”, IEEE Transactions on Medical Imaging, Vol. 28,No.7.
10. Andrew B. Watson, 1994. “Image Compression Using the Discrete Cosine Transform”, Mathematics journal, 4(1), 1994,p.81-88 .
11. 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 Pages:547-556.
12. 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).
13. Quisquater, J.-J. andCouvreur, C. (1982). Fast decipherment algorithm for RSA publickey cryptosystem. Eletronic Letters, 18:905–907.
14. 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.
15. 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).
16. Hualiang Zhu, ChundiXiu and Dongkai Yang, 2010."An improved SPIHT algorithm based on wavelet coefficient blocks for image coding", InternationalConference on Computer Application and System Modeling (ICCASM).
17. 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
18. Rajinder Kumar, Kulbir Singh and Rajesh Khanna, 2012. "Satellite Image Compression using Fractional Fourier Transform", International Journal ofComputer Applications (0975 – 8887) Volume 50 – No.3, 2012.
19. GaochangZhao ;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).
20. Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on InformationTheory, 36(3):553–558.
21. Boneh, D. and Shacham, H. (2002). Fast variants of RSA. RSA Laboratories.
22. Victor Namias, "The Fractional Order Fourier Transform and its Applications to Quantum Mechanics", J. Inst. Math Applications, vol 25, pp 241-265, 1980