Image Encryption Using Block Based Transformation With Fractional Fourier Transform

Delong Cui[1,2], Lei Shu[2], Yuanfang Chen[3], Xiaoling Wu[4]
[1]College of Computer and Electronic Information, Guangdong University of Petrochemical Technology, China
[2]Guangdong Provincial Key Lab of Fault Diagnosis of Petrochemical Equipment
Guangdong University of Petrochemical Technology, China
[3]Institute Mines-Telecom, Universite Pierre et Marie Curie, UPMC
[4]Guangzhou Institute of Advanced Technology,Chinese Academy of Sciences
Email: {delong.cui,lei.shu}@lab.gdupt.edu.cn, cyuanfang@acm.org, xl.wu@giat.ac.cn

***Abstract*—In order to transmit image data in open network, a novel image encryption algorithm based on fractional Fourier transform and block-based transformation is proposed in this paper. The image encryption process includes two steps: the original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the fractional Fourier transform (FRFT) algorithm. The security of the proposed algorithm depends on the transformation algorithm, sensitivity to the randomness of phase mask and the orders of FRFT. Theoretical analysis and experimental results demonstrate that the algorithm is favorable.**

***Index Terms*—Image encryption, fractional Fourier transform(FRFT), block-based transform, entropy**

I. Introduction

In the digital world today, how to protect the security of images is a serious problem, since special storage and transmission of digital images is needed in many applications, such as internet communication, multimedia systems, medical imaging, telemedicine, military communication, large-scale petrochemical industries, etc. Data encryption is widely used to ensure security. however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia streaming data [1-3]. The simplest way to encrypt an image is to consider the 2-D image stream as a 1-D data stream, and then encrypt this 1-D stream with any available cipher [4]. Although such a simple way is sufficient to protect digital images in some civil applications, encryption schemes considering special features of digital images, such as the bulky size and the large redundancy in uncompressed images, are still needed to provide better overall performance and make the adoption of the encryption scheme easier in the whole image processing system. A classification of the proposed schemes from the open literature is given in Table 1 [5-9].

The fractional Fourier transform (FRFT) is a generalization of the ordinary Fourier transform and has been applied in optics, quantum mechanics, signal processing areas, and image encryption. In the past decade, a number of new encryption approaches are proposed and demonstrated with optical implementations. Refregier [10] proposed a double random phase encoding method to encrypt images in Fourier domain. Unnikrishnan [11] placed the Fourier transform with the FRFT for the double random phase encoding method. Recently, Tao propose a method to encrypt an image by multiorders of FRFT [12]. In the image encryption, the encrypted image is obtained by the summation of different orders inverse discrete FRFT of the interpolated subimages. And the original image can be perfectly recovered using the linear system constructed by the fractional Fourier domain analysis of the interpolation. Applying the transform orders of the utilized FRFT as secret keys, the proposed method is with a larger key space than the existing security systems based on the FRFT. Additionally, the encryption scheme can be realized by the fast-Fourier-transform-based algorithm and the computation burden shows a linear increase with the extension of the key space. It is verified by the experimental results that the image decryption is highly sensitive to the deviations in the transform orders. Many encryption systems are based on Fourier transform (FT) or FRFT, these systems usually use pure random phase masks, such as double random phase encoding [13,14], to add noise information into the image. One of the main drawbacks of such image encryption schemes is that the encrypted images are complex and hence inconvenient in real applications.

It is well knows that most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). In order to dissipate the high correlation among pixels and increase the entropy value, a transformation algorithm that divides the image into blocks and then shuffles their positions before it passes them to the fractional Fourier transform base algorithm is proposed.

The security of the proposed algorithm depends on the transformation algorithm, sensitivity to the randomness of phase mask and the orders of FRFT. Theoretical analysis and experimental results demonstrate that the algorithm is favorable.

The remaining of this paper is organized as follows: The concept of FRFT is briefly introduced in section 2. The chaotic key-based image encryption algorithm is also illustrated in section 3. The details of the proposed scheme and security analysis are described in section 4. A conclusion is drawn in

978-1-4799-1406-7

TABLE I
VARIOUS KERNELS AVAILABLE WITH FRFT

Type of data	Domain	Proposal	Encryption Algorithm	What is encrypted?
Image	Frequency Domain	Cheng & Li, 2000	No algorithm is specified	Pixel and set related significance information in the two highest pyramid levels of SPIHT
		Droogenbroeck & Benedett, 2002	DES, Triple DES and IDEA	Bits that indicate the sign and magnitude of the non-zero DCT coefficients
		Pommer & Uhl, 2003	AES	Subband decomposition structure
	Spatial Domain	Cheng & Li, 2000	No algorithm is specified	Quadtree structure
		Droogenbroeck & Benedett, 2002	Xor	Least significant bitplanes
		Podesser, Schmidt & Uhl, 2002	AES	Most significant bitplanes

section 5.

II. FRACTIONAL FOURIER TRANSFORM (FRFT): BACKGROUND AND THEORY

The Fourier transform (FT) is undoubtedly one of the most valuable and frequently used tools in signal processing and analysis [15]. The fractional Fourier transform (FRFT) is the generalization of the classical Fourier transform. It depends on a parameter $\alpha(= a\pi/2)$ and can be interpreted as a rotation by an angle in the time-frequency plane or decomposition of the signal in terms of chirps.

The idea of fractional powers of the Fourier transform operator appears in the mathematical literature as early as 1929 [16]. The FRFT was first introduced by Victor Namias in 1980 [17]. Mendlovic and Ozaktas[18,19] first introduced fractional Fourier transform (FRFT) for image analysis in optics. Furthermore, a general definition of FRFT for all classes of signals (one- and multidimensional, continuous and discrete, and periodic and nonperiodic) was given by Cariolario et al. Nowadays, FRFT has established itself as a powerful tool for the analysis of time-varying signals in a very short span of time. Therefore, applications of the transform include in solution of differential equations, optical beam propagation and spherical mirror resonators, optical diffraction theory, quantum mechanics, statistical optics, optical system design and optical signal processing, signal detectors, correlation and pattern recognition, space or time-variant filtering, multiplexing, signal and image recovery, restoration and enhancement[20], study of space or time-frequency distributions (TFDs), etc. However, in every area where FT and related concepts are used, there exists the potential for generalization and implementation by using FRFT.

The Definition of FRFT is

$$F^a[s(x_1)] = S(x) = \frac{\exp i(\frac{\pi}{4} - \frac{\pi}{2})}{\sqrt{2\pi \sin\alpha}} \exp(-\frac{i}{2}x^2 \cot\alpha) \cdot \int_{-\infty}^{\infty} \exp(-\frac{i}{2}x_1^2 \cot\alpha - \frac{ix_1 x}{\sin\alpha}) s(x_1) dx_1 \quad (1)$$

TABLE II
VARIOUS KERNELS AVAILABLE WITH FRFT

Value of parameter α	$\alpha = a\pi/2$	Kernel	Fractional operator	Operation on signal
0 or 4	0 or 2π	$\delta(x - x_1)$	$F^0 = F^4 = I$	Identity operator
1	$\pi/2$	$\exp(ixx_1)$	$F^1 = F$	Fourier operator
2	π	$\delta(x + x_1)$	$F^2 = FF = I$	Reflection operator
3	$3\pi/2$	$\exp(-ixx_1)$	$F^3 = FF^2 = F^{-1}$	Inverse Fourier operator

and the inverse FRFT can be given as

$$F^{-a}[s(x_1)] = \frac{\exp -i(\frac{\pi}{4} - \frac{\pi}{2})}{\sqrt{2\pi \sin\alpha}} \exp(+\frac{i}{2}x^2 \cot\alpha) \cdot \int_{-\infty}^{\infty} \exp(+\frac{i}{2}x_1^2 \cot\alpha - \frac{ix_1 x}{\sin\alpha}) s(x_1) dx_1 \quad (2)$$

where $\alpha = a\pi/2$

Some different cases are discussed in the following:

1) When $\alpha = \pi/2$

$$F^a[s(x_1)] = F^1[S(x)] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} s(x_1) \exp(-ixx_1) dx_1 \quad (3)$$

is the ordinary Fourier transform.

2) When $\alpha = 0$, the transform kernel reduces to identity operation. When α approaches 0, $\sin\alpha$ approaches α, $\cot\alpha$ approaches $\frac{1}{\alpha}$ and using the fact in the sense of generalized functions

$$\lim_{\varepsilon \to 0} \frac{1}{\sqrt{i\pi\varepsilon}} (-\frac{x^2}{i\varepsilon}) = \delta(x) \quad (4)$$

so that we have

$$F^0[s(x_1)] = \int_{-\infty}^{\infty} \delta(x - x_1) s(x_1) dx_1 = s(x_1) \quad (5)$$

TABLE III
IMPORTANT PROPERTIES OF FRFT

No	Properties	Calculus
1	Multiplication rule	$F_\alpha(gf) = g(x\cos\alpha + \frac{1}{i}\sin\alpha\frac{d}{dx})F_\alpha(f)$
2	The division rule	$F_\alpha(f/x) = (i/\sin\alpha)\exp(-\frac{ix^2}{2}\cot\alpha)\int_{-\infty}^{x}\exp(+\frac{ix^2}{2}\cot\alpha)F_\alpha(f)dx$
3	Mixed product rule	$F_\alpha(x\frac{d}{dx}) = -(\sin\alpha + ix^2\cos\alpha)\sin\alpha F_\alpha(f) + x\cos 2\alpha\frac{d}{dx}F_\alpha(f) - \frac{1}{2}\sin 2\alpha\frac{d^2}{dx^2}F_\alpha(f)$
4	Differentiation rule	$F_\alpha(\frac{df}{dx}) = (-ix\sin\alpha + \cos\alpha\frac{d}{dx})F_\alpha(f)$ $F_\alpha(\frac{d^m}{dx^m}) = (-ix\sin\alpha + \cos\alpha\frac{d}{dx})^m F_\alpha$
5	Integration rule	$F_\alpha\int_\alpha^x f(x)dx = \sec x\exp(-\frac{ix^2}{2}\tan\alpha)\int_\alpha^x\exp(+\frac{ix^2}{2}\tan\alpha)F_\alpha(f)dx$
6	Shift rule	$F_\alpha f(x+k) = \exp[-ik\sin\alpha(x+\frac{k}{2}\cos\alpha)]F_\alpha(f)_{[x+k\cos\alpha]}$
7	Similarity rule	$F_\alpha f(-x) = F_{\alpha-\pi}f(x)$
8	Convolution rule	$f *^\alpha g = \exp(-ibt^2)\int_{-\infty}^{\infty} f(\tau)e^{ibt^2}g(t-\tau)e^{ib(t-\tau)^2}d\tau$ where $b = 0.5\cot(0.5\pi\alpha)$

3)When $\alpha = \pi$, the result turns out to be

$$F^2[s(x_1)] = \int_{-\infty}^{\infty}\delta(x+x_1)s(x_1)dx_1 = s(-x_1) \qquad (6)$$

So, it can be drown that the transform kernel is periodic with α period 4 form the above several cases. Table II gives the various kernels of FRFT for various α from 0 to 4.

The FRFT kernel can be written as $\phi_\alpha(f,t)$

$$F^\alpha[s(t)] = \int_{-\infty}^{\infty}\phi_\alpha(f,t)s(t)dt = S_\alpha(f) \qquad (7)$$

The properties of FRFT are useful not only in deriving the direct and inverse transform of many time-varying functions but also in obtaining several valuable results in signal processing. Recalling some of the well-established properties of Fourier transform, the operational calculus for FRFT is described in Table III. When two functions multiply (or convolve) in time domain ($a = 0$) they get convolved (or multiplied) in frequency domain ($a = 1$). More generally, multiplication (or convolution) in the a^{th} domain is convolution (or multiplication) in $(a+1)^{\text{th}}$ domain. In $(a+2)^{\text{th}}$ domain convolution (or multiplication) operation in the a^{th} domain remains the same. The concept of fractional convolution and correlation has been developed differently by various authors [21-24].

III. PROPOSED ENCRYPTION ALGORITHMS

The image encryption process includes two steps: The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the fractional Fourier transform base algorithm. The detail of original image was divided into blocks and rearranged into a transformed image using a transformation algorithm was introduced by [24].

The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks.

The post-processed algorithm is encryption by FRFT. Every components of block image is encrypted by employing Fractional Fourier domain random phase and the cipher image is obtained. The fractional orders applied in the transforms are

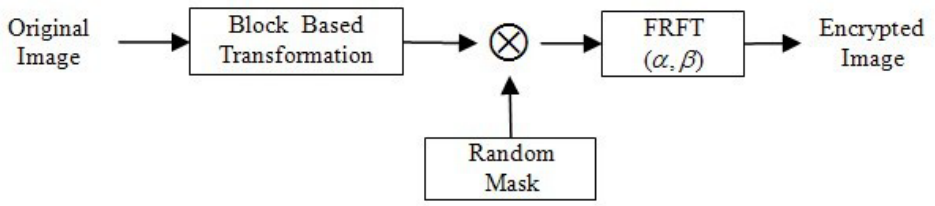

Fig. 1. General block diagram of the proposed method of image encryption

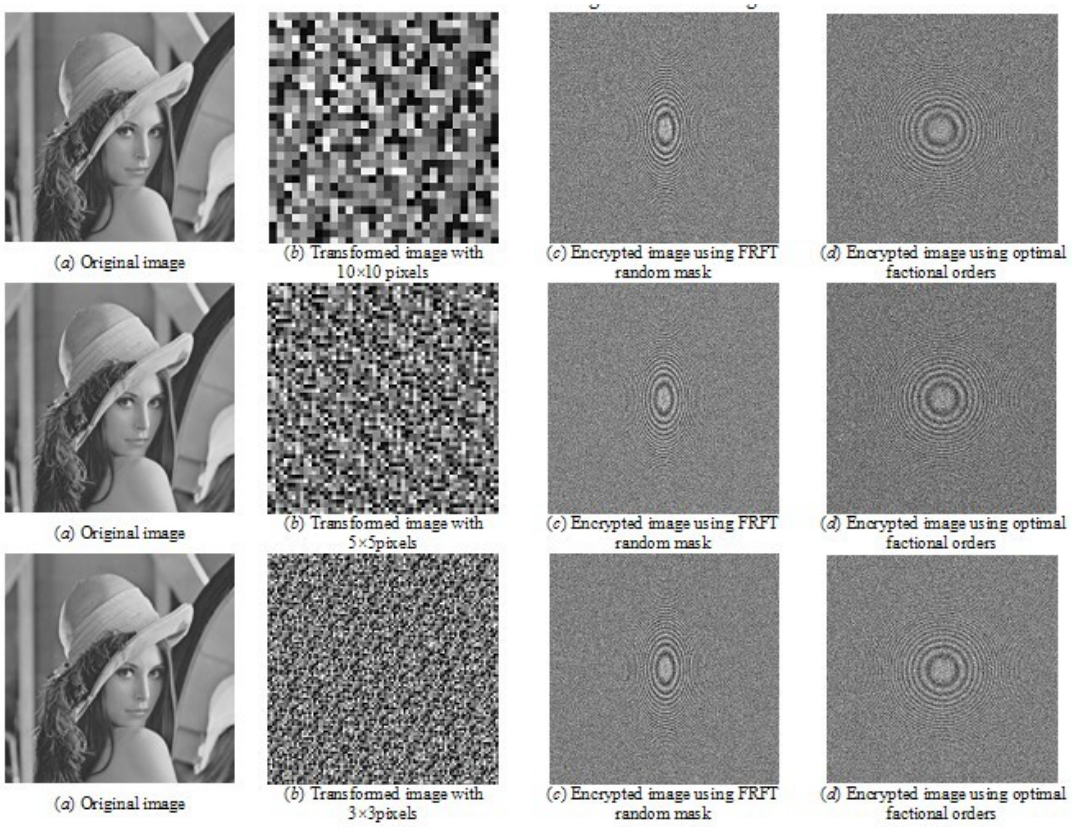

Fig. 2. Results of encryption by using proposed algorithm(The images in the first row are the original Lena, the second are the transformed images, the third are the encrypted images using FRFT random mask and the fourth are the encrypted image using optimal factional orders.)

decimal numbers between zero and four, generated from a key alphanumeric of six to ten characters. The framework of proposed image encryption algorithm is shown in Figure 1.

IV. EXPERIMENTS

Several benchmark images (such as Lena, Baboon, Peppers, F16, Cameraman, etc) are used to test the performance of the proposed scheme. In order to evaluate the impact of the number of blocks on the correlation and entropy, three different cases were tested. The number of blocks and the block sizes for each case are shown in Table 3, the block-based image encryption and finally encryption image are shown in Fig.2.

For comparison, an existing image encryption schemes by Kamlesh Gupta et al. [25] and several commercially available algorithms are chosen. The comparison of different algorithm based on correlation and entropy are shown in Table 4.

TABLE IV
DIFFERENT CASES TO TEST THE IMPACT OF THE NUMBER OF BLOCKS ON THE CORRELATION AND ENTROPY

Case Number	Number of blocks	Block size
1	30×30	10pixels×10pixels
2	60×60	5pixels×5pixels
3	100×100	3pixels×3pixels

TABLE V
THE COMPARISON OF DIFFERENT ALGORITHM BASED ON CORRELATION AND ENTROPY

Schemes	Number of blocks	Correlation	Entropy
Kamlesh Gupta's scheme	30×30	0.0049	5.5286
	60×60	0.0040	5.5439
	100×100	0.0034	5.5440
	300×300	0.0026	5.5437
Blowfish(448)	30×30	0.0063	5.4402
	60×60	0.0049	5.5286
	100×100	0.0044	5.5407
	300×300	0.0028	5.5438
Twofish(256)	30×30	0.0026	5.5437
	60×60	0.0040	5.5439
	100×100	0.0041	5.5438
	300×300	0.0029	5.5438
RijnDael(AES256)	30×30	0.0034	5.5440
	60×60	0.0024	5.5439
	100×100	0.0049	5.5438
	300×300	0.0016	5.5439
RC4(2048)	30×30	0.0024	5.5438
	60×60	0.0026	5.5437
	100×100	0.0034	5.5439
	300×300	0.0034	5.5438
Encrypted image using FRFT random mask	30×30	0.0027	6.8863
	60×60	0.0035	6.8783
	100×100	0.0026	6.8934
	300×300	0.0046	6.8830
Encrypted image using optimal factional orders	30×30	0.0019	6.9623
	60×60	0.0007	6.9720
	100×100	0.0039	6.9624
	300×300	0.0009	6.9176

V. CONCLUSION

In this paper a novel method has been proposed for image security using a combination of block based image transformation and FRFT based image encryption techniques. Compare with tradition image encryption algorithm, using fractional Fourier transform greatly increases safety parameters in the encrypted fingerprint, due to the sensitivity of the fractional orders used and random phase masks. Meanwhile, the relationship of block size and correlation, block size and entropy are also being proved. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy.

ACKNOWLEDGMENT

The work presented in this paper was supported by Maoming Municipal Science & Technology Program (No.203624) and the fund of Guangdong Provincial Key Lab of Fault Diagnosis of Petrochemical Equipment (No. 512013). Lei Shu's work is supported by the Guangdong University of Petrochemical Technologys Internal Project No. 2012RC0106. Lei Shu is Corresponding author.

REFERENCES

[1] M. V. Droogenbroech and R. Benedett, "Techniques for A Selective Encryption of Uncompressed and Compressed Images", In ACIVS02, Ghent, Belgium, Proc. of Adv. Concepts for Intel. Vision Systems, 2002, pp. 90-97.
[2] S. Changgui and B. Bharat, "An Efficient MPEG Video Encryption Algorithm", Proc. of the Symposium on Reliable Distributed Systems, IEEE Comp. Society Press, 1998, pp. 381-386.
[3] S. Fong, P. B. Ray and S. Singh, "Improving The Lightweight Video Encryption Algorithm", Proc. of Iasted Intern. Conf., single proc., pattern recog. and appl., 2002, pp. 25-28.
[4] P.P. Dang, P.M. Chau, "Robust Image Transmission over CDMA Channels", IEEE Trans. on Cons. Elec., vol. 46, 2000, pp. 664C672.
[5] X. Liu, A.M. Eskicioglu, "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions", IASTED Commu., Inter. & Inform. Tech.(CIIT), USA, 2003.
[6] Ma. K., W. M. Zhang, X. F. Zhao, N. H. Yu, F. H. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE Trans. Inform. Forensics and Security, vol.8, 2013, pp. 553-562.
[7] T. Mehrdad, K. Reza, A. K. Sohrab, "Gray-Scale and Color Optical Encryption Based on Computational Ghost Imaging", Applied Physics Letters, vol. 100, 2012, pp. 101108-101108.
[8] X. P. Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE Trans. Inform. Forensics and Security, vol.7, 2012, pp. 826-832.
[9] X. P. Zhang, G. R. Feng, Y. L. Ren, "Scalable Coding of Encrypted Images", IEEE Trans. Image Proc., vol.21, 2012, pp. 3108 - 3114.
[10] P. Refregier, B. Javidi, "Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding", Opt. Lett., vol. 20, 1995, pp. 767-769.
[11] G. Unnikrishnan, K. Singh, "Double Random Fractional Fourier Domain Encoding for Optical Security", Opt. Eng., vol. 39, 2000, pp. 2853-2859.
[12] R. Tao, X.Y. Meng, Y. Wang, "Image Encryption with Multi-Orders Fractional Fourier Transforms", IEEE Trans. on Inform. Foren. and Secur., vol. 5, 2010, pp. 734-738.
[13] P. Refregier, B. Javidi, "Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding", Opt. Lett . vol. 20, 1995, pp.767-769.
[14] G. Unnikrishnan, J. Joseph, K. Singh, "Optical Encryption by Double-Random Phase Encoding in The Fractional Fourier Domain" , Opt. Lett. 25, 2000, pp. 887-889.
[15] R. N. Bracewell: The Fourier Transforms and Its Applications, McGraw-Hill 1986.
[16] E.U. Condon, National Academy Sciences, vol. 23, 1937, pp. 158.
[17] V. Namias, J. Inst. Math Appl, vol. 25, 1980, pp.241
[18] D.Mendlovic and H.M.Ozaktas, "Fractional Fourier Transforms and Their Optical Implementation: I", J. Opt. Soc. Am. A 10, 1993, pp. 1875-1880.
[19] H. M. Ozaktas and D. Mendlovic, "Fractional Fourier Transforms and Their Optical Implementation: II", J. Opt. Soc. Am. A 10, 1993, pp. 2522-2531.
[20] L. Yu, K. Q. Wang, C. F. Wang and D. Zhang, "Iris Verification Based on Fractional Fourier Transform", Proc. First Int. Conf. on Machine Learning and Cybernetics, Beijing, 2002, pp. 1470-1473.
[21] H. M. Ozaktas, B. Barshan, D. Mendlovic and L. Onural, "Convolution, Filtering and Multiplexing in Fractional Domains and Their Relation to Chirp and Wavelet Transforms", J. Opt. Soc. Am. A, 11, 1994, pp. 547-559.
[22] G. Cariolaro, T. Erseghe, P. Kraniauskas and N. Laurenti, "Multiplicity of Fractional Fourier Transforms and Their Relationships", IEEE Trans. Signal Proc., vol. 48, 2002, pp.227-241.
[23] O. Akay, G. F. Boudreaux-Bastel, "Fractional Convolution and Correlation via Operator Methods and An Application to Detection of Linear FM Signals", IEEE Trans. Signal Proc., vol.49, 2001, pp. 979-993.
[24] R. Yu, Y. Zhang, C. Huang and R. Gao, "Joint Admission and Rate Control for Multimedia Sharing in Wireless Home Networks", Elsevier Compu. Commu., special issue on "Multimedia Networking and Security in Convergent Networks", vol.33, 2010, pp.1632-1644.
[25] K. Gupta, S. Silakari, "Choase Based Image Encryption Using Block-Based Transformation Algorithm", Inter. J. of Comp. and Network Security, vol.1, 2009, pp. 19-23.