http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (1): 158-163, 2010
ISSN 1812-5638

Secure Communication System Based on Alterable-Parameter 4-Weighted Fractional Fourier Transform

Bo Ding, Lin Mei and Xuejun Sha
School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China

Abstract: By discussing the development of 4-WFRFT, a discrete sequence algorithm for 4-WFRFT based on DFT is introduced and this makes it possible to use 4-WFRFT in a discrete time system. On the basis of analyzing the rotating, squeezing effect to the digital signal constellation by 4-WFRFT process also the similarity of 4-WFRFT signal to Gaussian distribution and the anti-scanning competence of 4-WFRFT signal, an alterable-parameter secure communication system is introduced based on 4-WFRFT secure communication system. Moreover, in the light of frequency-hopping patterns, a dynamic alterable-parameter strategy for single parameter 4-WFRFT and three strategies for multi-parameters 4-WFRFT are designed to avoid a non-receiver's intercepting and decoding. "Tracking coefficient" is defined to judge the anti-scanning capacity. The results of simulation show that the alterable-parameter 4-WFRFT secure communication system has strong practical significance.

Key words: Secure communication, 4-weighted fractional fourier transform, alterable-parameter

INTRODUCTION

Recently years Fractional Fourier Transform (FRFT) has aroused extensive attention in optic and signal processing field (Ozaktas *et al*., 2000; Tao *et al*., 2006). Because it is the extension of traditional Fourier transform, it becomes one kind of powerful tools in scientific research and engineering. The FRFT combines the time and frequency field of the signal by introducing the time-frequency expression of signal. It makes the transformed signal containing both time and frequency information, then shows us a novel way to process signal. There are two kind of FRFT: traditional chirp-type FRFT and weighted-type FRFT. The main difference between these two kinds of FRFT results from the different forms of their transform functions (Cariolaro *et al*., 1998, 2000). In 1995, Weighted-type Fractional Fourier Transform (WFRFT) was originally proposed by Shih (1995), then researchers began to pay attention to the multiplicity of the definition of WFRFT and focus on the relationship between WFRFT and traditional chirp-type FRFT (Santhanam and McClellan, 1996; Liu *et al*., 1997; Ran *et al*., 2005; Lang *et al*., 2008). Liu *et al*. (1997) expended Shih's (1995) WFRFT from 4 weights to 4l (l is a natural number) and explained that WFRFT and traditional chirp-type FRFT were two special cases when l respectively equaled to positive infinity and zero. After that, Ran *et al*. (2005) expanded WFRFT coefficient to an arbitrary integer not less than 2 and introduced a new definition which covered all former ones for parameter, also the transform parameter was expanded to several ones from only one (Lang *et al*., 2008).

Mei *et al*. (2008) implemented 4-WFRFT into secure communication system for the first time. Based on it and cooperated with the alteration of parameter, a novel alterable-parameter 4-WFRFT secure communication system which could further increase the security of communication system and therefore protect the signal from being intersected and decoded is proposed in this study.

4-WEIGHTED FRACTIONAL FOURIER TRANSFORM

Denoting F as the Fourier Transform operator,, then the 1~4 times Fourier transformation of g(x)(its Fourier Transform is G(x)) will be G(x), g(-x), G(-x), g(x). F^{α} means a times Fourier Transform to a function. In the traditional Fourier Transform, α is an integer, while it can be an arbitrary real number in FRFT. The FRFT satisfies the law of conservation of energy and the following basic axiom:

- **Continuity axiom:** For all real number |A, the transform should be continuous, namely $\{F^{\alpha}: L^2(R)\rightarrow L^2(R)\}$
- **Boundary axiom:** Fα should reduce to an ordinary Fourier transform when α is an integer, $F^0[g(x)]=g(x)$ and $F^1[g(x)]=G(x)$

Corresponding Author: Bo Ding, School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China

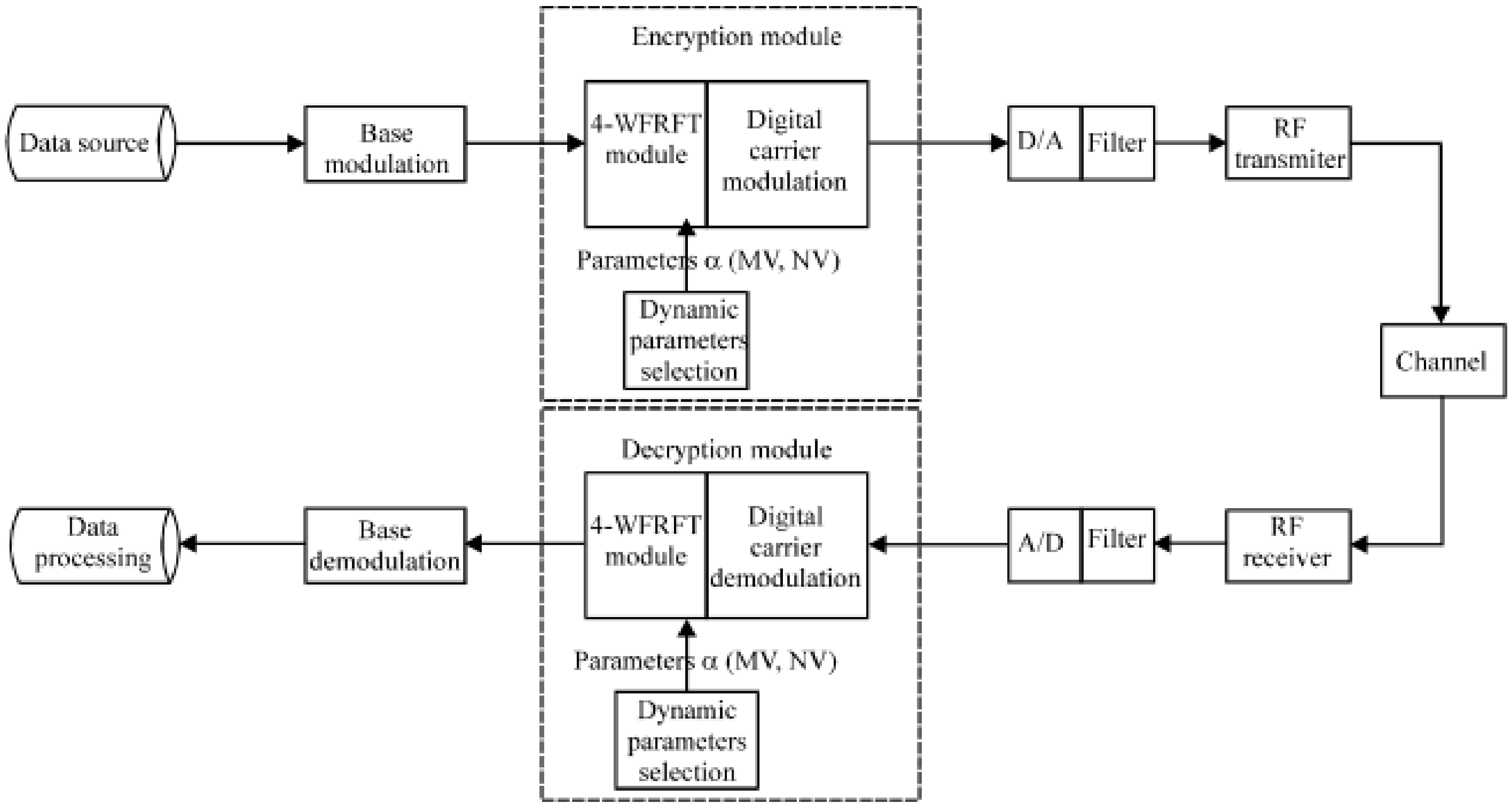

Fig. 1: Structure of the secure communication system based on 4-WFRFT

- **Additiveaxiom:**$F^{\alpha+\beta}[g(x)]=F^{\alpha}\{F^{\beta}[g(x)]\}=F^{\beta}\{F^{\alpha}[g(x)]\}$, for real number α and β

To avoid the problems resulted from sampling and discreteness of signal (Candan *et al*., 2000; Candan and Ozaktas, 2003; Tao *et al*., 2007, 2008a, b) and based on Shih and Ran's continual definition of WFRFT, we introduce the sequence definition of WFRFT. $X_0(n)$ is an arbitrary complex sequence and $\{X_0(n), X_1(n), X_2(n), X_3(n)\}$ are the 0~3 times DFT of $X_0(n)$ separately and the definition of DFT is shown below:

$$\begin{cases} X(k)=\dfrac{1}{\sqrt{N}}\sum_{n=0}^{N-1}x(n)e^{-j\frac{2\pi}{N}kn} \\ x(n)=\dfrac{1}{\sqrt{N}}\sum_{k=0}^{N-1}X(k)e^{j\frac{2\pi}{N}kn} \end{cases} \tag{1}$$

Then the 4-WFRFT of $X_0(n)$ is:

$$F^{\alpha}[X_0(n)]=w_0X_0(n)+w_1X_1(n)+w_2X_2(-n)+w_3X_3(-n) \tag{2}$$

$$w_l=\cos\left(\frac{(\alpha-1)\pi}{4}\right)\cos\left(\frac{2(\alpha-1)\pi}{4}\right)\exp\left(-\frac{3(\alpha-1)\pi i}{4}\right),\quad (l=0,1,2,3) \tag{3}$$

$$w_l=\frac{1}{4}\sum_{k=0}^{3}\exp\left\{\pm\frac{2\pi i}{4}\left[(4m_k+1)\alpha(k+4n_k)-lk\right]\right\},\quad (l=0,1,2,3) \tag{4}$$

When w_l conforms to Eq. 3, it is the single parameter form of 4-WFRFT brought by Shih (1995). While, it is the multi-parameter form of 4-WFRFT by Ran when w_l conforms to Eq. 4, then w_l is decided by a, $MV = [m_0, m_1, m_2, m_3]$ and $NV = [n_0, n_1, n_2, n_3]$ 9 parameters. Figure 1 shows the structure of the secure communication system based on 4-WFRFT and several strategies focusing on the dynamic parameters selection part would be presented in this paper to enhance the security of coded signal from being intercepted or decoded.

SECURE COMMUNICATION SYSTEM BASED ON 4-WFRFT

Anti-scanning features of 4-WFRFT signal: By analyzing the single parameter 4-WFRFT signal, Mei *et al*. (2008) revealed that the signal constellations would be rotated, expanded and therefore changes the original uniform shape into a mess one. Along with the increase of transformation parameter α from 0 to 1, the area of each constellation point becomes larger and the distance between each constellation point becomes shorter, at the same time the whole constellation rotates in a clockwise direction. When the transformation parameter satisfies certain conditions, the constellation on the complex plane appears a quasi Gaussian probability density, which makes it more difficult for the un-destination receivers to detect and recognize. The receivers must do an inverse transformation with certain parameters. Otherwise, it is unable to demodulate with a confusing constellation (Mei *et al*., 2008).

Figure 2 shows the detection sensitivity (described as bit error rate (BER)) of parameter α of 4-WFRFT QPSK signals, where α = 0.7 and the detection step is 0.1, 0.05 and 0.01 separately. In the condition of high SNR, parameter difference Δα being less than 0.05 is necessary for the detection step to gain the ideal BER performance. The reasonable detection step should be between 0.01~0.05. Taking 0.05 as an example, at least 80 times attempts in a whole period have to be made in order to achieve the ideal BER. Besides this, when Δα = 2, due to the periodicity of Fourier transform, the constellation could be correctly identified, however, the signal sequence is reversed and cannot be decoded properly. However, in this case, when the non-destination receiver implemented a strategy that identifying the modulation type at first, then demodulation, after demodulation the parameter is determined as α or α+2 by the demodulated data, it would reduce the reliability of nonvariable parameter secure communication system greatly. It is true that there are still many times scanning for obtaining the parameter α, however, it is a possible mission for the extremely high performance CPU nowadays. To make the secure communication system more reliable, secure communication system based on 4-WFRFT is introduced to resist scanning decoding.

Secure communication system based on alterable-parameter 4-WFRFT: In single parameter 4-WFRFT secure system (MV=NV=0), α is the only parameter controlled, so it is very important to secrete α. In order to improve the anti-interception performance of 4-WFRFT signals, the scheme of alterable-parameter 4-WFRFT could be adopted.

The secure communication system based on alterable-parameter 4-WFRFT is an evolution scheme to enhance the anti-interception performance of single-parameter scheme. It can be also employed with multi-parameter scheme, which makes the communication system more complicated but secret. In this scheme, the parameter α (or MV, NV) vary ceaselessly based on the designed pattern and the PN sequence in order to resist the detection of parameter, which is just like PN controlling the variation of frequency in FHSS (Tian, 2007). For the whole system, this scheme actualizes the function of dynamic parameter selection module in Fig. 3.

Figure 3 is an example of alterable-parameter α pattern. The whole period of parameter α B_α=4 is divided into 8 groups $\alpha_1(\alpha_1+2)$~$\alpha_8(\alpha_8+2)$. And each group is

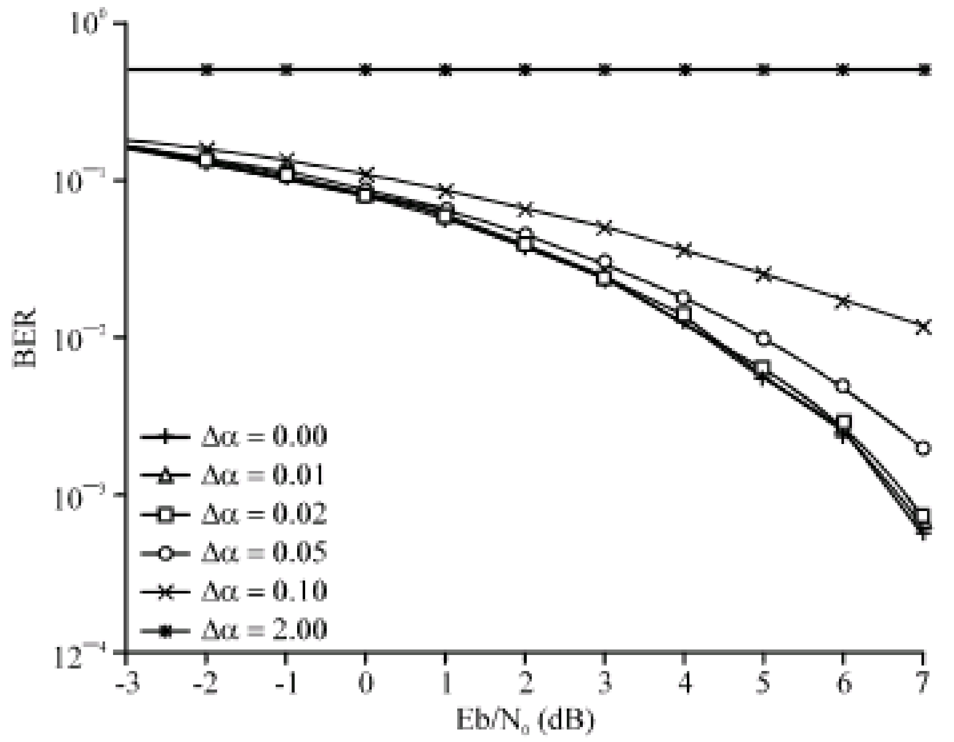

Fig. 2: The detection sensitivity of parameter α of 4-WFRFT QPSK signals

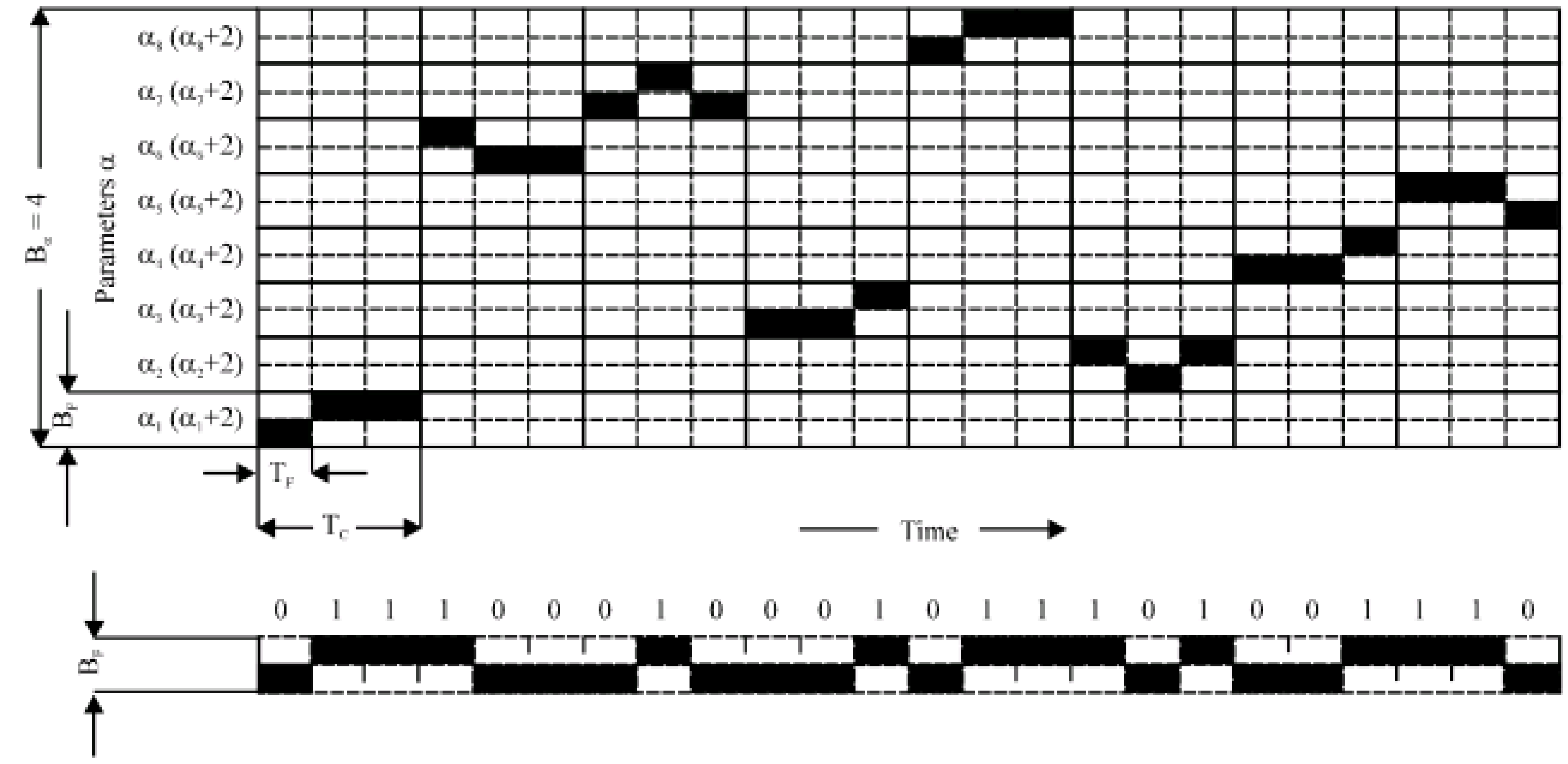

Fig. 3: An example of alterable-parameter α pattern

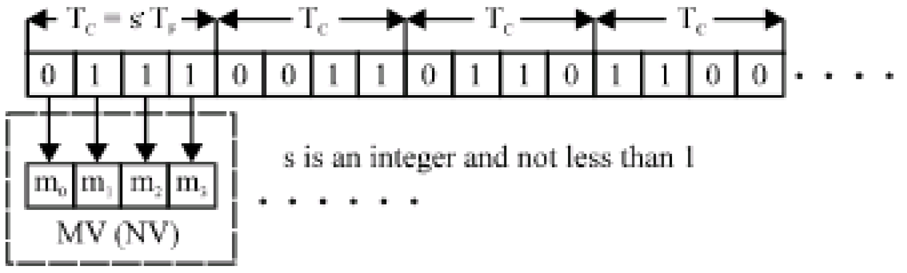

Fig. 4: Strategy A of the variation of alterable-parameter MV and NV

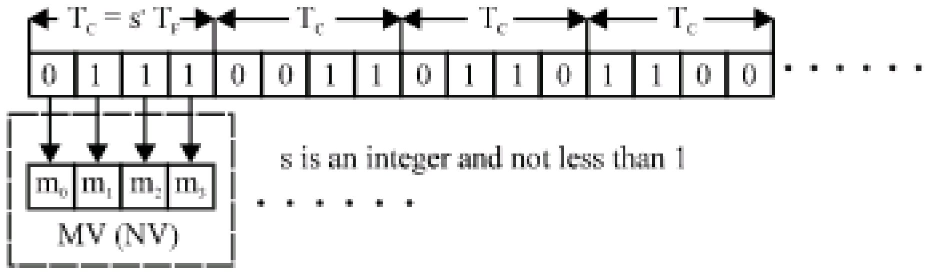

Fig. 5: Strategy B of the variation of alterable-parameter MV and NV

divided into 2 slots, between which the distance on the scale of α is 2. Each of the parameter slots in a group, with which the orders of the output sequences after 4-WFRFT are just opposite, is the legal area corresponding to the values (either 0 or 1) of PN sequence respectively. B_F is the width of each parameter group, that is, the guardian area of parameter α for each frame of data when transformed. T_F is the interval scale of frame and T_C is the period of parameter hopping. In Fig. 3, T_C is 3 times of T_F and the rate could be altered to meet the actual demand. The designed order of parameter's alteration in the example is: $\alpha_1(\alpha_1+2)$, $\alpha_6(\alpha_6+2)$, $\alpha_7(\alpha_7+2)$,......, that is so called alter-parameter pattern.

Such method is also suitable to MV and NV. Figure 4-6 are the strategies of the variation of alterable-parameter MV and NV. In Strategy A, the PN sequence is divided into groups every 4 symbols. Each symbol in a group is corresponding to each element of vector MV or NV (m_l or n_l, $l = 0,1,2,3$), so the elements are either 0 or 1. Each group can be used for the period of parameter hopping $T_C = s\bullet T_F$, where s is an integer and not less than 1. If PN sequence is not the integer multiple of 4, reusing PN sequence in circle is also acceptable (Fig. 3).

In strategy B, the PN sequence is divided into groups every 16 symbols and each group is divided again into slices every 4 symbols. Each slice with 4 binary symbols is corresponding to each element of vector MV or NV, so the elements are decimal integers that not less than 0 and not larger than 15. Each group can be used for $T_C = s\bullet T_F$, where s is an integer and not less than 1. If PN sequence is not the integer multiple of 16, reusing PN sequence in circle is also acceptable. The size of slice can be also adjusted based on demand.

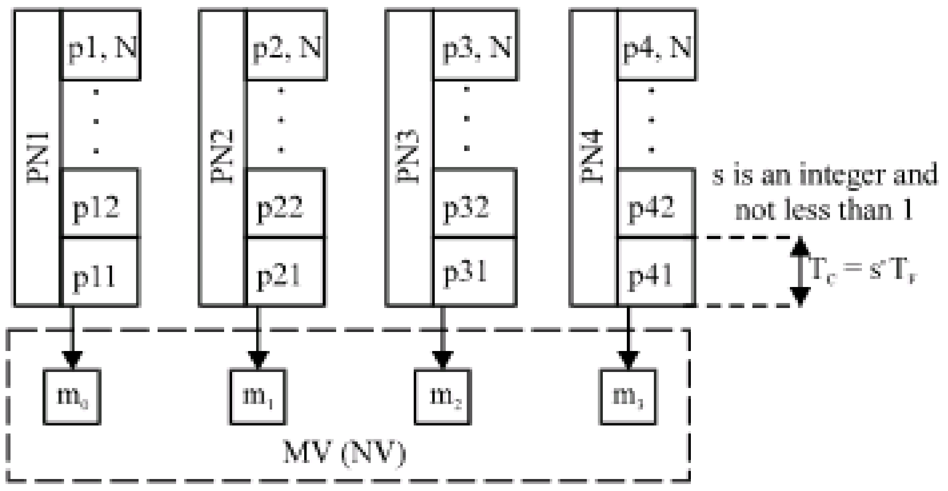

Fig. 6: Strategy C of the variation of alterable-parameter MV and NV

In strategy A and strategy B, all the elements of vector MV or NV are controlled by the same PN sequence, while strategy C is more generalized. In strategy C, each element of vector MV or NV is substituted by independent PN sequences or the same PN sequence with different original phases. So, the strategy is not restricted to the period of PN sequence and can be better combined with variation of parameter α. It is more flexible indubitably, whereas the complexity of system, for example, the synchronization of different PN sequences, should not be ignored.

PERFORMANCE OF SINGLE ALTERABLE-PARAMETER 4-WFRFT SCHEME

Because alterable-parameter 4-WFRFT secure communication system is analogous to a FHSS system (Tian, 2007), if the non-destination receiver intends to intercept the information carried by the signal, it has to follow the value of parameter α then decode. Assuming that the period system resting on a fixed α is T_F, the non-destination receiver spends T_D time to adjust the decoding α to current system α. Defining the trace coefficient $\eta = (1-T_D/T_F)\times 100\%$. When $\eta = 100\%$, it means the non-destination receiver follows the altering pattern to adjust the value of α precisely without difference; when $\eta = 50\%$, it means the non-destination receiver spends 0.5 T_F to adjust former α into current α. Figure 7 shows in AWGN channel, the non-destination receiver BER of QPSK signal encrypted by the alter-parameter scheme showed in Fig. 3 when η varies.

From Fig. 7, it is obtained that when the tracing coefficient is lower than 85%, the performance of whole system decreases sharply. It is almost impossible to maintain the tracing coefficient on a 90% level considering the complexity of tracing altering parameter and consequently, it is a very reliable scheme to avoid non-destination receiver's parameter scanning and information intercepting.

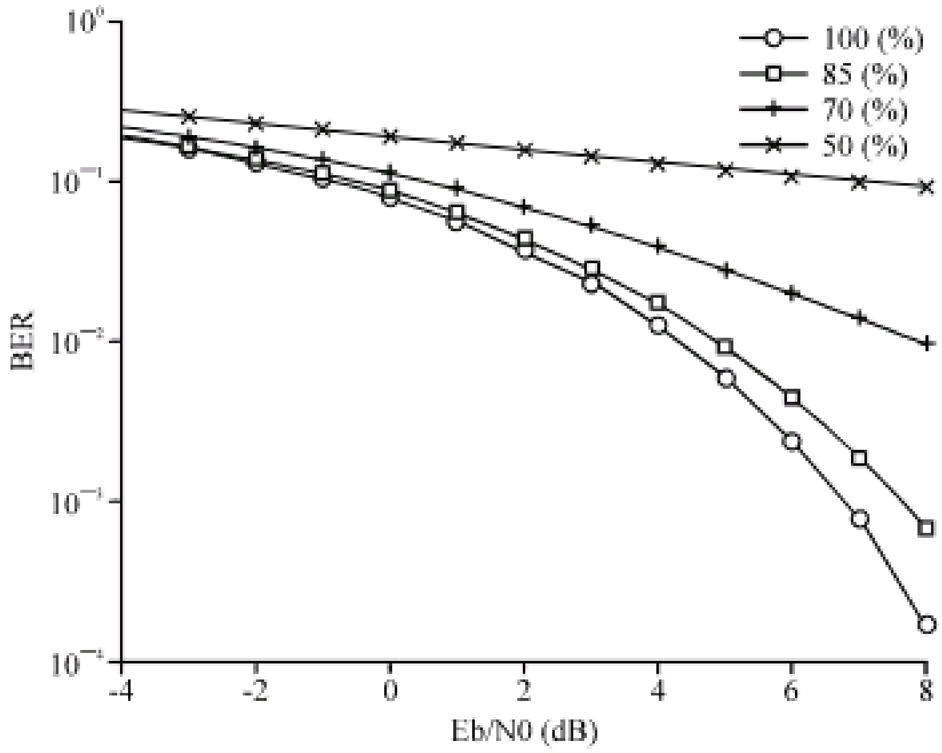

Fig. 7: Relationship between tracing coefficient and BER

CONCLUSIONS

By introducing the normalized DFT, the paper redefines 4-WFRFT to apply it into discrete sequence to avoid the intricate theoretical problems of sampling and discretization of Fractional Fourier Transform and then makes it possible to be applied into digital communication system. Meanwhile, the algorithm complexity is similar to FFT, which means a lower complexity compared with other FRFT system.

Signal processed by 4-WFRFT displays a quasi Gaussian distribution in time-frequency domain and the signal shows some secure characteristics as a result. However, by scanning the stationary 4-WFRFT parameter, especially for the single parameter 4-WFRFT system, it is probable to weaken the randomness of the signal then it could be intercepted and decoded by the non-destination receiver. To solve this possible problem, 4 different parameter altering strategies which could be implemented into secure communication system for single parameter and multi parameter 4-WFRFT are designed in this paper in order to achieve higher security.

By defining the tracing coefficient, the anti-scanning capacity of the secure system is measured. The simulation result shows that only by keeping the tracing coefficient in an extremely high accuracy to follow the altering pattern and the strategy the non-destination receiver could maintain the BER in a reasonable level, which makes it impossible to detect and decode the signal encrypted by the strategies mentioned above. In sum, the secure communication system based on alterable-parameter 4-WFRFT possess a much higher capacity of prevent from being intercepted and decoded.

ACKNOWLEDGMENT

Special thanks to professor Ran Qiwen, Department of Mathematics, Harbin Institute of Technology, who has helped a lot with this study. This work is supported by the National Basic Research Program (also called 973 Program) of P.R. China under Grant No. 2007CB310606.

REFERENCES

Candan, C., M.A. Kutay and H.M. Ozaktas, 2000. The discrete fractional fourier transform. IEEE Trans. Signal Proc., 48: 1329-1337.

Candan, C. and H.M. Ozaktas, 2003. Sampling and series expansion theorems for fractional fourier and other transforms. Signal Proc., 83: 2455-2457.

Cariolaro, G., T. Erseghe and P. Kraniauskas, 1998. A unified framework for the fractional fourier transforms. IEEE Trans. Signal Proc., 46: 3206-3219.

Cariolaro, G., T. Erseghe, P. Kraniauskas and N. Laurenti, 2000. Multiplicity of fractional fourier transforms and their relationships. IEEE Trans. Signal Proc., 48: 227-241.

Lang, J., R. Tao and Q.W. Ran, 2008. The multiple-parameter fractional fourier transform. Sci. China (Ser. F, Inf. Sci.), 51: 1010-1024.

Liu, S., J. Zhang and Y. Zhang, 1997. Properties of the fractionalization of a fourier transform. Optics Commun., 133: 50-54.

Mei, L., X.J. Sha and Q.W. Ran, 2008. The research on the application of 4-weighted fractional fourier transform in communication system. Sci. China (Ser. F, Inf. Sci.).

Ozaktas, H.M., Z. Zalevsky and M.A. Kutay, 2000. The Fractional Fourier Transform with Applications in Optics and Signal Processing. 1st Edn., Wiley, New York.

Ran, Q.W., D.S. Yeung, C.C.E. Tsang and Q. Wang, 2005. General multifractional fourier transform method based on the generalized permutation matrix group. IEEE Trans. Signal Proc., 53: 83-98.

Santhanam, B and J.H. McClellan, 1996. The discrete rotational fourier transform. IEEE Trans. Signal Proc., 44: 994-998.

Shih, C.C., 1995. Fractionalization of fourier transform. Optics Commun., 118: 495-498.

Tao, R., B. Deng and Y. Wang, 2006. Research progress of the fractional fourier transform in signal processing. Sci. China (Ser. F, Inf. Sci.), 49: 1-25.

Tao, R., B.Z. Li and Y. Wang, 2007. Spectral analysis and reconstruction for periodic nonuniformly sampled signals in fractional fourier domain. IEEE Trans. Signal Proc., 55: 3541-3547.

Tao, R., B.Z. Li and Y. Wang, 2008a. On sampling of band-limited signals associated with the linear canonical transform. IEEE Trans. Signal Proc., 56: 5454-5464.

Tao, R., F. Zhang and Y. Wang, 2008b. Research progress on discretization of fractional fourier transform. Sci. China (Ser. F, Inf. Sci.), 51: 859-880.

Tian, R.C., 2007. Spectrum Communication. 1st Edn., Tsinghua University, Beijing, ISBN: 9787302145790.