Multilayer WFRFT and chaotic encryption wireless communication system based on MIMO

Lei Zhuang¹, Jing Hu¹ and Jian Cheng¹*

¹Institute of Communications Engineering, Army Engineering University of PLA, Nanjing, Jiangsu, 210001, China
²Jian Cheng’s e-mail: chjatice@163.com

Abstract. In order to improve the concealment and anti interception performance of satellite and other wireless communication. Based on the characteristics of multilayer weighted fractional-order Fourier transform and chaotic mapping, a multilayer weighted fractional-order Fourier transform and chaotic mapping wireless communication system is designed. The number of modulation layers of multilayer WFRFT is consistent with the number of transmitting antennas, and different modulation orders are adopted in each layer, which makes it more difficult to crack the information by chaotic mapping scrambling codes on the modulated signals. The simulation results show that the designed system has better concealment performance by comparing the bit error rate of the receiver with that of the eavesdropper. The bit error rate of the eavesdropper is about 0.5 when the eavesdropper does not know the specific parameters.

1. Introduction

Satellite communication has the advantages of wide coverage, large data capacity and fast transmission rate[1-3]. However, with the development of social economy, high-speed and high-quality data transmission is more urgent, which requires more spectrum resources and increased transmission power for satellite communication. Research shows that in the mobile communication system, Multiple Input Multiple Output (MIMO) technology can improve the system capacity and spectrum utilization without additional transmission power and bandwidth[4]. Literature[5] applies mimo-ofdm to satellite communication, and the system has a stronger performance of resisting multi-path fading. Therefore, the spectrum utilization of MIMO satellite is higher, its reliability is stronger and its performance is better.

Wireless communication is characterized by openness and the broadcasting of electromagnetic signals, and it is vulnerable to theft and interference. The security and concealment of signal transmission are poor, so some measures are needed to ensure the security of communication information. Modulation encryption is a new physical layer security technology. By encrypting the modulation signal, the constellation symbol changes and aliases, and finally makes the eavesdropper unable to identify the modulation mode[6].

Fractional Fourier transform (FRFT) can rotate in the time-frequency domain, so that the signal is not easy to be intercepted and has good stealth performance. Since it was proposed, it has been widely concerned by researchers. In the Weighted Fractional Fourier Transform (WFRFT) defined by merlyn et al., it is found that the signals modulated by WFRFT have the characteristics of constellation rotation aliasing, uniform bit energy distribution and good anti-parameter scanning characteristics. Compared with the original signal, the modulated constellation diagram has become disordered. With different modulation orders, the modulated constellation diagram of WFRFT is quite different. According to literature, the possibility of using this feature to secure or resist interception communication was
proposed[7-9]. However, in the communication process, the eavesdropping party can obtain the modulation order through parameter scanning for a long time, so as to recover the original signal.

Based on the above analysis, the author proposes to establish Weighted Type Fractional Fourier transform (WFRFT) and chaos mapping for anti-interception wireless communication system based on Multiple Input Multiple Output (MIMO) technology. After multi-layer WFRFT modulation, the signal is encrypted with higher degree of chaos and higher security of the system.

2. Fundamentals

2.1. Weighted Fractional Fourier transform

According to the definition of weighted fractional Fourier transform (WFRFT) [10-11] proposed by C.C. Shih, the definition of 4-WFRFT is:

\[
F_{4w}^\alpha[g(x)] = \omega_0(\alpha)g(x) + \omega_1(\alpha)G(x) + \omega_2(\alpha)g(-x) + \omega_3(\alpha)G(-x)
\]

(1)

The calculation method of the weighting coefficient is shown in equation (2):

\[
\omega_l(\alpha) = \cos\left(\frac{(\alpha - l)\pi}{4}\right) \cos\left(\frac{2(\alpha - l)\pi}{4}\right) \exp\left[\frac{3(\alpha - l)\pi i}{4}\right] (l = 0, 1, 2, 3)
\]

(2)

As can be seen from the above formula, \(F^\alpha[g(x)]\) is the sum of the four basic functions \(g_0, g_1, g_2, g_3\) and the weighting coefficient \(\omega_0(\alpha), \omega_1(\alpha), \omega_2(\alpha), \omega_3(\alpha)\). The discrete form of 4-WFRFT is shown in equation (3):

\[
F^\alpha[g(n)] = \omega_0(\alpha)g(n) + \omega_1(\alpha)G(n) + \omega_2(\alpha)g(-n) + \omega_3(\alpha)G(-n)
\]

(3)

![Figure 1. Digital communication block diagram of WRTFT.](image)

The digital communication block diagram of 4-WFRFT is shown in figure 1. A set of data of length \(N\) is converted into four branches after serial parallel conversion. Among them, the data information of \(\omega_1\) and \(\omega_3\) two branches is weighted after passing through the DFT transformation module, corresponding to the frequency domain. While the other two branches \(\omega_0\) and \(\omega_2\) without passing through the DFT transformation module are corresponding to the time domain. The signal after WFRFT modulation belongs to the time-frequency domain signal, with more uniform energy distribution and better performance through fading.

The signal constellation diagram after WFRFT modulation is shown in figure 2. It can be seen from the figure that the signal constellation diagram after WFRFT modulation is disordered[12]. If the modulation order \(\alpha\) is different, the constellation diagram after WFRFT modulation is also different. If the modulation order \(\alpha\) can't be obtained, the eavesdropper can't recover the original signal. However, WFRFT has only one modulation order \(\alpha\), and the eavesdropper can intercept the original signal through ergodic scanning of the modulation order \(\alpha\) based on the cost of time. In view of the above shortcomings, the multi-layer weighted fractional-order Fourier transform and chaotic encryption technology are combined with MIMO.
2.2. MIMO technology

MIMO technology can improve the communication capacity and spectrum resource utilization of the system on the premise of not adding extra power and bandwidth by configuring multiple transceiver antenna units at the sending and receiving end of the signal and adopting space-time block coding at the same time [13].

![Block diagram of two transmitting and one receiving antennas.](image)

MIMO technology use space-time block coding to realize spatial and temporal diversity, taking two sending and one receiving antennas as an example to illustrate space-time block coding. The encoder divides the input signal into two groups $m_1, m_2$, and encodes according to the encoding matrix data shown in equation (4).

$$
\begin{bmatrix}
    m_1 - m_2^* \\
    m_2 - m_1^*
\end{bmatrix}
$$

(4)

After the signal is encoded, it is transmitted from the corresponding antenna at the corresponding moment. In two consecutive transmission periods $t_1, t_2$, the signal $m_1, m_2$ is transmitted from antenna one and two at the time $t_1$ respectively, and the signal $-m_2^*, m_1^*$ is transmitted from antenna one and antenna two at the time $t_2$ respectively. The receiver antenna performs channel estimation and space-time block decoding.

2.3. A new chaotic mapping scheme

The main characteristics of chaos are: non-periodicity, bounded but non-convergence, extreme sensitivity to initial conditions, etc. [14-15]. The noise-like characteristics of chaotic map track can help enhance the anti-interception characteristics of communication system. In addition, the characteristics of accurate regeneration can be accurately used for signal recovery, and chaotic map is increasingly applied in covert communication [16-17].

Logistic mapping system is the most widely used discrete chaotic mapping system. Logistic mapping is defined as:
\[ x_{n+1} = f(x_n) = kx_n(1 - x_n) \]  

(5)

Among which Initial rang \( x_0 \in (0,1) \) mapping parameters \( k \in (0,4) \). When \( k \in (3.56999 \ldots, 4) \), the system is in a chaotic state, and the correlation function of chaotic sequence is relatively ideal. Logistic mapping only reaches full mapping state when \( k=4 \), as shown in figure 4:

![Logistic mapping bifurcation diagram.](image)

Figure 4. Logistic mapping bifurcation diagram.

Logistic mapping only reaches the maximum complexity when \( k=4 \), and the iterative results will be mapped to the whole interval, that is, the full mapping state. As a result, in the case of parameters in a large range, the iterative range of data is small, and the data may be distributed in a concentrated way, which is not conducive to the randomness and confidentiality of the sequence coding of wireless communication. In view of this shortcoming, a polynomial chaotic map designed can generate a larger range of full mapping parameters, and its mapping equation is as follows:

\[ x_{n+1} = f(x_n) = \frac{k^2}{2}x_n^2 + (k^2 - 2k)x_n + \frac{k^2}{2} - 2k + 1 \]

(6)

The improved quadratic polynomial chaotic map is full mapping in a large range of parameters \( k \in (1.53, 2) \). Among which Initial rang \( x_0 \in (-1,1) \), the chaos mapping bifurcation diagram is as figure 5.

![Bifurcation diagram of a new Polynomial chaotic map.](image)

Figure 5. Bifurcation diagram of a new Polynomial chaotic map.

3. Chaotic encryption WFRFT-MIMO system

3.1. New chaotic key encryption method

In this paper, the new chaotic sequence is used to generate the corresponding chaotic key \( x_n \) to further enhance the secrecy of system communication. The phase rotation factor generated by chaotic sequence can be expressed as:

\[ r_n = \exp(-j2\pi x_n) \]

(7)

\( x_n \in (-1,1) \), \( n = 1, 2, 3 \ldots N \), \( N \) is the number of iterations of chaos. Define Logistic phase rotation matrix \( E \):
3.2. Chaotic encryption communication system

The number of layers of multi-layer WFRFT is determined by the number of transmitting antennas. Taking two transmitting antennas as an example, two-layer WFRFT modulation has two different modulation orders, which effectively enhances the system’s safe communication. The structure block diagram of two-layer WFRFT is shown in figure 6:

![Figure 6. Schematic diagram of two-layer WFRFT modulation and demodulation.](image)

The block diagram of the new chaotic encryption communication system based on multi-layer WFRFT-MIMO is shown in figure 7:

![Figure 7. A new chaotic encryption multilayer WFRFT-MIMO communication system.](image)

The working principle of multi-layer wfrft-mimo system based on chaotic encryption is as follows: a new Logistic phase scrambler module of chaotic encryption is added on the basis of multi-layer WFRFT. The input signal constellation diagram is confused and disturbed by multilayer modulation order and chaotic encryption key to enhance the concealment of system communication.

We take two sending and one receiving antennas as an example to illustrate that the input data is mapped to a sequence of 2N points through the baseband, and the sequence of N points is regarded as a data block \( m_1(n), n = 0, 1, \ldots, N - 1 \) and the other continuous N points as a data block \( m_2(n), n = 0, 1, \ldots, N - 1 \).

The definition of WFRFT in equation (3) is written as a matrix:

\[
M = F_{\omega_{1}}(m(n)) = \omega_{1}m(n) + \omega_{2}Fm(n) + \omega_{3}F^{2}m(n) + \omega_{4}F^{3}m(n) = \omega_{1}I + \omega_{2}F + \omega_{3}F^{2} + \omega_{4}F^{3}m(n)
\]

\[
= F_{\omega_{1}}(\alpha)m(n)
\]

\( m(n) \) is the input signal sequence, \( F \) is the DFT matrix, \( \omega_{l} \) \((l = 0, 1, 2, 3)\) is the weighting coefficient, and \( F_{\omega_{1}}(\alpha) \) is the WTFRT matrix. \( m_1(n) \) and \( m_2(n) \) are respectively modulated by WFRFT of order \( \alpha_1 \) and \( \alpha_2 \).
and $\alpha_2$ to obtain data blocks $\mathbf{M}_1(n)$ and $\mathbf{M}_2(n)$, which are multiplied by chaotic phase rotation matrix $E$ to obtain the encrypted signal at the sending end:

$$S = \mathbf{M} \cdot E = \mathbf{F}_{4w}(\alpha_m(n))E$$

(10)

then

$$S_1(n) = \mathbf{M}_1(n) \cdot E = \mathbf{F}_{4w}(\alpha_1_m(n))E$$
$$S_2(n) = \mathbf{M}_2(n) \cdot E = \mathbf{F}_{4w}(\alpha_2_m(n))E$$

(11)

Space-time grouping coding for $S_1(n)$ and $S_2(n)$ is obtained from equation (4):

$$\begin{bmatrix}
S_1(n) - S_2(n) \\
S_1(n) + S_2(n)
\end{bmatrix}$$

(12)

The first way represents antenna 1, the second way represents antenna 2, the first column represents period 1, the second column represents period 2, and the encoded IFFT transformation is:

$$\begin{align*}
v_{1,1}(n) &= F^{-1}(S_1(n)) \\
v_{1,2}(n) &= F^{-1}(-S_2(n)) \\
v_{2,1}(n) &= F^{-1}(S_2(n)) \\
v_{2,2}(n) &= F^{-1}(S_1(n))
\end{align*}$$

(13)

After IFFT transformation, the data is prefixed with a cycle and then transmitted through the corresponding antenna. Cyclic prefix: can avoid intercarrier interference; The series of receiving end can be equivalent to the cyclic convolution process of sending end sequence and channel impulse response. We assume that the channel is a slow channel, that is, the impact response of adjacent periodic channels is unchanged. The received signals are prefixed by decycling, and the signals received after processing are as follows:

$$\begin{align*}
y_1(n) &= v_{1,1}(n) * h_1(n) + v_{1,2}(n) * h_2(n) + z_1(n) \\
y_2(n) &= v_{2,1}(n) * h_1(n) + v_{2,2}(n) * h_2(n) + z_2(n)
\end{align*}$$

(14)

Where $z_1(n)$ and $z_2(n)$ respectively represent the white gaussian noise of the channel. FFT transformation is carried out on equation (14) and substituted into equation (13) to obtain:

$$\begin{align*}
Y_1(n) &= S_1(n)H_1(n) - S_2(n)H_z(n) + Z_1(n) \\
Y_2(n) &= S_1(n)H_1(n) + S_2(n)H_z(n) + Z_2(n)
\end{align*}$$

(15)

Equation (15) is transformed as follows[18]:

$$\begin{align*}
\tilde{Y}_1(n) &= \frac{H_1^*(n)Y_1(n) + H_z(n)Y_z(n)}{|H_1(n)|^2 + |H_z(n)|^2} \\
\tilde{Y}_2(n) &= \frac{H_1^*(n)Y_2(n) - H_z(n)Y_z(n)}{|H_1(n)|^2 + |H_z(n)|^2}
\end{align*}$$

(16)

Substitute equation (15) into equation (16) to get:

$$\begin{align*}
\tilde{Y}_1(n) &= S_1(n) + \frac{H_1^*(n)Z_1(n) + H_z(n)Z_z(n)}{|H_1(n)|^2 + |H_z(n)|^2} \\
\tilde{Y}_2(n) &= S_1(n) + \frac{H_1^*(n)Z_2(n) - H_z(n)Z_z(n)}{|H_1(n)|^2 + |H_z(n)|^2}
\end{align*}$$

(17)

$\tilde{Y}_1(n), \tilde{Y}_2(n)$ is the sequence obtained by space-time block decoding, and the obtained sequence is restored by chaotic decryption:
\[ M' = \bar{Y} \cdot E^{-1} \] (18)

then

\[
\begin{align*}
M'_1(n) &= \bar{Y}_1(n) \cdot E^{-1} \\
M'_2(n) &= \bar{Y}_2(n) \cdot E^{-1}
\end{align*}
\] (19)

For the n-th of the restoration sequence \( M' \) is \( M'_n \):

\[ M'_n = M_n \cdot r_n \cdot r'_n + n \cdot r'_n = M_n \exp(-2\pi j \cdot (x_n - x'_n)) + n \cdot r'_n = M_n \exp(-2\pi j \cdot \Delta x_n) + n \cdot r'_n \] (20)

Therefore, at the legal receiving end \( \Delta x_n = 0 \), that is, \( M'_n = M_n + n \cdot r'_n \), and the influence of \( r'_n \) on the noise can be filtered out. The legal receiver can receive the correct encrypted recovery signal, and the output sequence can be obtained by \( \alpha_1 \) and \( \alpha_2 \) order WFRFT demodulation and baseband inverse mapping of \( M'_1(n) \) and \( M'_2(n) \). For illegal users, the number of antennas is increasing and the modulation order \( \alpha \) is also increasing. Since it is impossible to know the specific modulation order \( \alpha \) of multiple layers and the type of chaotic map and its initial value \( x_0 \), it is impossible to recover the correct WFRFT signal, and the hidden performance of the system is guaranteed.

4. System performance simulation and analysis

4.1. Characteristics of system signal constellation

In this paper, a two-layer WFRFT-MIMO and chaotic covert communication system is simulated under stationary channel. We take two sending and one receiving antennas as an example, and the parameters are set as follows: the size of the data block is 256 symbols. At this time, two consecutive data blocks (512 symbols are seen as a group) will be processed. In order to facilitate baseband mapping, taking the commonly used QPSK as an example. In the new chaotic mapping system, \( k = 3.6 \), initial value \( x_0 = 0.8 \), and the number of iterations is 200. Multipath delay is \([0, 1, 2, 4, 6]\), relative average power gain is \([0-2-4-8-10]\), and the channel is assumed to be a rational channel. The transmitter adopts multi-layer WFRFT to modulate the signal through WFRFT-MIMO technology. Due to the effect of phase rotation, diffusion of modulation order and chaotic mapping scrambling code, QPSK signal becomes difficult to recognize and intercept, which greatly increases the security of the system.

Figure 8 shows QPSK modulated signal, double-layer WFRFT modulated signal, chaos encryption after double-layer modulation and signal decrypted and demodulated by the destination receiver, respectively. Figure a shows the standard four points of the original QPSK signal constellation. In figure b, after two-layer WFRFT modulation, the signal constellation diagram has become disordered and has anti-interception property. In figure c, after chaotic encryption of the signal modulated by two-layer WFRFT, it can be seen that, its anti-interception is stronger. After receiving the signal, the target receiver carries out corresponding inverse transformation, and its constellation diagram is standard four points, that is, the target receiver can demodulate the original signal.

Figure 8. Signal constellation diagram.
4.2. Bit error rate analysis

Figure 9 shows the bit error rate of a double-layer WFRFT signal encrypted by chaotic phase scrambler. When the modulation order, $\alpha_1$, $\alpha_2$ chaotic map type and initial iteration value of the legitimate user are known, when the SNR is 25dB, the bit error rate of the demodulation signal is $1.32 \times 10^{-8}$, which meets the communication requirements. When illegal users modulation don’t know order $\alpha_1$, $\alpha_2$ chaotic map type and iterative initial value when the bit error rate is about 0.5, when modulation order $\alpha_1$, $\alpha_2$ chaotic mapping type and iterative initial is known by the illegal users. when $\Delta x_0 = 10^{-30}$ the bit error rate is still around 0.5. Firstly the illegal users get two modulation order and chaos mapping type is almost impossible, and deviation from the initial value of the mapping system by less than $10^{-10}$ orders of magnitude is less likely, so cracking by an illegal user is extremely costly. Modulation order, chaotic map type and parameters of Logistic guarantee the confidentiality of the system.

![Figure 9. System bit error rate curve.](image)

5. Conclusion

In this paper, we propose a wireless covert communication system based on WFRFT-MIMO and chaotic mapping encryption. The confusion characteristic of WFRFT modulation and the chaotic encryption process of chaotic map enhance the concealment of the system. Multi-layer WFRFT modulation based on MIMO technology at the transmitting end not only increases the system capacity and improves the spectrum utilization, but also encrypts the system in the first step. Even if the modulation order is known, the original signal cannot be cracked due to the role of chaotic mapping encryption. The receiver can recover the original signal effectively through relevant demodulation. Because of the encryption of multilayer WFRFT and chaotic map, the concealment and anti-interception of the system are greatly improved.

References

[1] MARAL,G., BOUSQUET,M.(1998) Satellite Communications Systems. John Wiley & Sons Publishing, New York.

[2] Kato, S., Morikura, M., Kubota, S. et al. (2015) A TDMA satellite communication system for ISDN services. Selected Areas in Communications., 10(2):456-464.

[3] UTZ,E., WERNER,J., JAHN,A.(2000) Satellite Systems for Personal and Broad Communications. Springer Publishing, Berlin.
[4] Xie, H., Wang, B., Gao, F., et al. (2016) A Full-Space Spectrum-Sharing Strategy for Massive MIMO Cognitive Radio Systems. Selected Areas in Communications., 34(10): 2537-2549.

[5] Hasan, M., Sagar, S. M., (2014) Wireless communication through Long Term Evolution (LTE) over satellite channel by using MIMO-OFDM model. In: International Conference on Advances in Electrical Engineering. Tokyo. 170-175.

[6] Mei, L., Sha, X., J., Ran, Q. W., et al. (2010) Research on the application of 4-weighted fractional Fourier transform in communication system. Science China Information Sciences., 53(6): 1251-1260.

[7] Hui, Y. T., Li, B. B., Tong, Z., (2015) 4-weighted fractional Fourier transform over doubly selective channels and optimal order selecting algorithm. Electronics Letters., 51(2): 177-179.

[8] Wang, Z. D., Mei, L., Wang, X. L., Sha, X. J., (2015) BER analysis of hybrid carrier system based on WFRFT with carrier frequency offset. Electronics Letters., 51(21): 1708-1709.

[9] Fang, X. J., Sha X. J., Li, Y., (2015) Secret communication using parallel combinatorial spreading WFRFT. IEEE Communications Letters., 19(1): 62-65.

[10] Mer, L., Sha, X. J., Ran, Q. W., et al. (2010) Application of Fourier transform on four weighted scores in communication system. Science in China: information science., 40(5): 732-741.

[11] Shih, C. C., (1995) Fractionalization of Fourier transform. Optics Communications., 118(118): 495-498.

[12] Da, X. Y., Lian, C., (2015) A method of weighted Fourier transform domain communication. Systems engineering and electronics., 37(12): 2853-2859.

[13] Hofmann, C., Storek, K. U., Schwarz, R. T., et al. (2016) Spatial MIMO over satellite: A proof of concept. In: IEEE International Conference on Communications. Paris. 1-6.

[14] Wang, Y., Wong, K. W., Liao, X. F., et al. (2011) A new chaos-based fast image encryption algorithm. Applied Soft Computing., 11(1): 514-522.

[15] Wu, G. C., Baleaun, D., (2014) Chaos synchronization of the discrete fractional logistic map. Signal Processing., 102(9): 96-99.

[16] Lang, J., Tao, R., Wang, Y., (2010) Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function. Optics Communications., 283(10): 2092-2096.

[17] Liu, L. Z., Zhang, L. Q., Xu, G. X., et al. (2014) A chaotic secure communication method based on partial sequence parameter identification of chaotic system. Acta phys. Sin., 63(1): 32-37.

[18] Qiu, X., Sha, X. J., Mei, L., (2013) Hybrid carrier code division multiple access multi-antenna system based on weighted fractional Fourier transform. Journal of jilin university (engineering)., 43(1): 218-222.