Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 1265930, 12 pages
https://doi.org/10.1155/2019/1265930

Research Article

WFRFT Secure Communication Method Based on Chaotic Parameter Pool

Fang Liu

School of Information Science and Engineering, Shenyang Ligong University, Shenyang, China

Correspondence should be addressed to Fang Liu; zhqing1019@163.com

Received 12 May 2019; Revised 21 July 2019; Accepted 5 August 2019; Published 7 October 2019

Academic Editor: Paolo Manfredi

In this study, to solve the hidden limitation of conventional weighted fractional Fourier transform (WFRFT), a random modulation order parameter pool is established by applying chaos technology. Further, a WFRFT secure communication method based on the chaotic parameter pool (CPP) is proposed. Based on the effective characteristics of tent mapping and the sequence output range, the parameter pool constructor is established by parameter transformation. Furthermore, for each parameter selection period, the information can be processed by WFRFT using different modulation orders. The modeling and simulation demonstrate that this method can significantly increase the bit error rate and processing time of unauthorized receivers. This indicates that it can greatly increase the scanning difficulty of unauthorized users and improve the concealment and security of the original information transmission.

1. Introduction

Fourier transform [1] has an inherent defect: it provides signal processing and analysis in the frequency or time domain based on a single frequency or time domain signal, which restricts increases in system capacity and spectral efficiency. Fractional Fourier transform (FRFT) [2, 3] is a new signal processing and analysis method in the transform domain of wireless communication systems. As a special branch of traditional Fourier transform, FRFT not only exhibits the characteristic of time-frequency conversion analysis of the traditional Fourier transform but also develops a unique joint signal processing ability in the time-frequency domain. FRFT can transform signals into each other in the time domain, frequency domain, and any transform domain in the transition region. Therefore, compared to the traditional Fourier transform, FRFT has gradually gained widespread attention and recognition in the field of nonstationary signal processing. In general, FRFT includes Chirp FRFT (CFRFT) [4, 5] and weighted FRFT (WFRFT) [6, 7]. CFRFT has been used extensively in radar signal processing, optical image processing, quantum mechanics, ranging, and other fields. However, owing to its discrete algorithm implementation, the application of CFRFT in the communication field has been severely limited. Compared to CFRFT, the WFRFT theory appeared at a later stage. Its signal is a form of the time-frequency domain signal fusion. The weighted fraction domain is in the middle of the traditional time and frequency domains. According to the characteristics of WFRFT, new physical characteristics are derived based on retaining the respective advantages of the traditional time-frequency domain signal. Owing to its simple implementation, and the low complexity of the discrete algorithm, WFRFT has been widely used in information optics, image encryption, and other engineering fields. Moreover, it has gradually been extended to image encryption, signal fractional domain sampling and reconstruction, and communication signal processing.

Because of the unique physical characteristics of the WFRFT signal, its application in secure communication has also become a topic of interest. In [8], a novel combinatory strategy was presented to embed WFRFT precoding signals into a transform domain communication system. This system could achieve an improved anti-eavesdropping capacity while maintaining its own communication quality with regard to bit error rate (BER) performances. In [9], a

parallel-combinatory-spreading-based WFRFT system aimed at guaranteeing physical layer (PHY) security was proposed. In [10], a novel user cooperation scheme based on WFRFT was proposed to enhance the PHY security of wireless transmissions against eavesdropping. In [11], a novel transmission scheme based on constellation rotation and WFRFT was proposed to enhance the PHY security in polarization modulation-based dual-polarized satellite communications. In [12], a WFRFT-based cooperative overlay system, aiming at guaranteeing PHY security, was presented. In the proposed system, WFRFT was first performed on the secret data, such that the transmitted signal was distorted and could only be neutralized by inverse WFRFT with the same parameter. Thereafter, two streams of the transformed sequences bearing different messages were cooperatively and simultaneously transmitted to two legitimate receivers by means of a beamforming-like method.

In WFRFT communications, although demodulation parameters cannot be obtained for nonscanning methods, and the purpose of confidentiality can be achieved, demodulation parameters may be obtained by unauthorized receivers with scanning capability. As a result, the confidentiality performance of unauthorized receivers with a rapid scanning ability is also threatened. Although the modulation order can be extended, from one to many, for example, in multiple parameters WFRFT [13–15], or the state function can be extended from four to many, as in MWFRFT [16, 17], this will also increase the system complexity. Thus, to solve the hidden limitation of conventional WFRFT, chaos technology [18, 19] is introduced, following which a random modulation order parameter pool is established, so that a WFRFT secure communication method based on the chaotic parameter pool (CPP) is proposed.

2. CPP Method

Based on chaos and WFRFT, the innovation of the CPP method is the establishment of the association and control rules. Based on the effective characteristics of tent mapping and the sequence output range, the parameter pool constructor is established by parameter transformation. Furthermore, for each parameter selection period, the information can be processed by WFRFT using different modulation orders. The establishment of the association and control rules can greatly improve the security performance of the system.

Firstly, the generation trajectory of the chaotic signal is very complex and irregular resulting in superior concealment effect and high unpredictability. The generation of chaotic signals depends on the iteration equation, initial value, and the fractal parameters, which is conducive to the replication and regeneration of the signal. The specific form of chaos is reflected by bifurcation diagram, which reflects the traversal of chaotic sequence. The bifurcation diagram results of classical chaotic mappings are shown in Figure 1. It can be seen that the sequence has reached the best ergodicity state, and the range of fractal parameters can be obtained when each chaotic map reaches the state of full mapping. And tent mapping has the widest range of fractal parameters and the largest application space. As tent mapping presents the best chaotic state when α is greater than 0.4, the mapping can reach full mapping. And considering that the range of fractal parameter α is between 0 and 1, so the optimum range of α is between 0.4 and 1. In this paper, the parameter α is set to 0.4997.

Thus, chaotic technology based on tent mapping is imported, and the CPP method is established, whose principle is illustrated in Figure 2.

Then, following substantial preliminary research and analysis, we believe that the Lyapunov exponents of tent mapping are relatively high; that is, they are more sensitive to the initial values, and the fractal parameters of the full mappings of tent maps have a wider range and larger application space. For this reason, a parameter pool constructor based on tent mapping is established.

The tent sequence is generated by the following iterating formula:

$$x_m = \begin{cases} \dfrac{(1 - x_{m-1})}{(1 - \alpha)}, & \alpha < x_{m-1} < 1, \\ \dfrac{x_{m-1}}{\alpha}, & 0 < x_{m-1} \le \alpha. \end{cases} \tag{1}$$

The range of the tent mapping initial value is from 0 to 1, so the sequence value x_m ranges from 0 to 1.

Then, the parameters are transformed by using the sequence x_m of the tent mapping output, as indicated in formula (2), so that the range of the parameters following transformation is $[0, 4)$, which accords with the periodic characteristics of the modulation order 0–4. The parameter y_m is a floating-point value whose value is controlled by chaotic sequence x_m, which is approximately random. So y_m is much better than the integer parameter pool controlled by m/M sequence:

$$y_m = 4x_{m-1}. \tag{2}$$

The parameter pool is formed by the parameter y_m, and $m \in [1, N]$. The value range of m is determined by N, which is the number of switching times of the modulation order and also the number of times of information division to be transmitted. The calculation of N for a transmission cycle is carried out according to the following formula:

$$N = R_b \cdot T, \tag{3}$$

where R_b is the rate of information to be transmitted and T is the period of selecting parameters sequentially from the parameter pool.

At each time T, the parameters are selected sequentially from the parameter pool y_m, and the selected parameters are used as the modulation order. Thereafter, the information to be transmitted is processed by WFRFT using this modulation order. In the next time T, the above operation is repeated, the next parameter is selected as the modulation order from the parameter pool y_m sequentially, and the information to be transmitted by WFRFT is processed using the new modulation order. Thus, at the ith T time, the parameter y_i is selected from y_m and used as the modulation

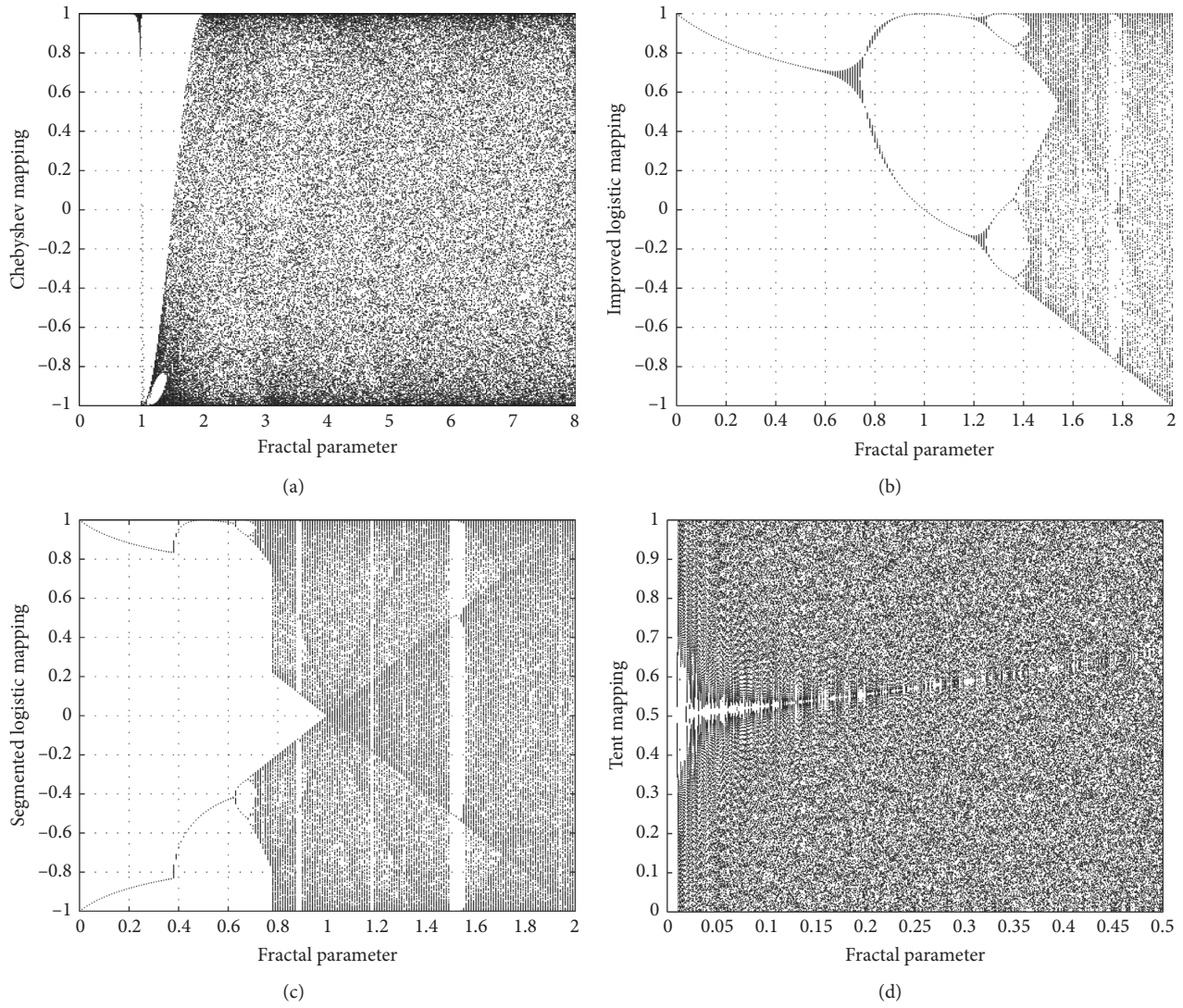

Figure 1: The bifurcation diagram of chaos mapping. (a) Chebyshev mapping. (b) Improved logistic mapping. (c) Segmented mapping. (d) Tent mapping.

order, while the transmission information $s(n)$ is processed by the y_i-order WFRFT and is expressed as

$$F^{y_i}(s(n)) = \omega_0(y_i)s(n) + \omega_1(y_i)S(n) + \omega_2(y_i)s(-n) + \omega_3(y_i)S(-n). \quad (4)$$

The y_i-order WFRFT processing is denoted by $F^{y_i}(\cdot)$. In formula (4), the four "state functions" $s(n)$, $S(n)$, $s(-n)$, and $S(-n)$ are the results of 0, 1, 2, and 3 times of Fourier transformation of $s(n)$, respectively. The weighting coefficient $\omega_l(y_i)$ is defined as

$$\omega_l(y_i) = \frac{1}{4}\sum_{k=0}^{3}\exp\left[\frac{2\pi j}{4}(l - y_i)k\right], \quad (l = 0, 1, 2, 3). \quad (5)$$

In receiving, the baseband signal $r(n)$ following the frequency downconversion, power amplifying, and bandpass filtering can be set to formula (6). Here, $\lambda_0(n)$ represents the mixed noise item caused by the transmission process and receiving pretreatment:

$$r(n) = F^{y_i}(s(n)) + \lambda_0(n). \quad (6)$$

The signal processing of WFRFT can be viewed as the process of rotating the input signal $s(n)$ in the time-frequency plane, thereby realizing the signal energy redistribution in the time-frequency plane. Therefore, only when the receiver rotates the communication signal $F^{y_i}(s(n))$ at the same angle in the opposite direction can the receiver achieve signal energy aggregation. When the demodulation order is selected incorrectly, the signal energy will be lost, which will result in a loss of reception performance and reduce the receiver reception performance.

To synchronize the demodulation order of the inverse process with the modulation order of the transmitter, the receiver generates the sequence according to the same tent chaotic mapping and generates the same parameter pool y_m according to formulas (1) and (2). Moreover, the parameters are selected sequentially from the parameter pool y_m every time T, and at the ith T time, the selected parameter is y_i'.

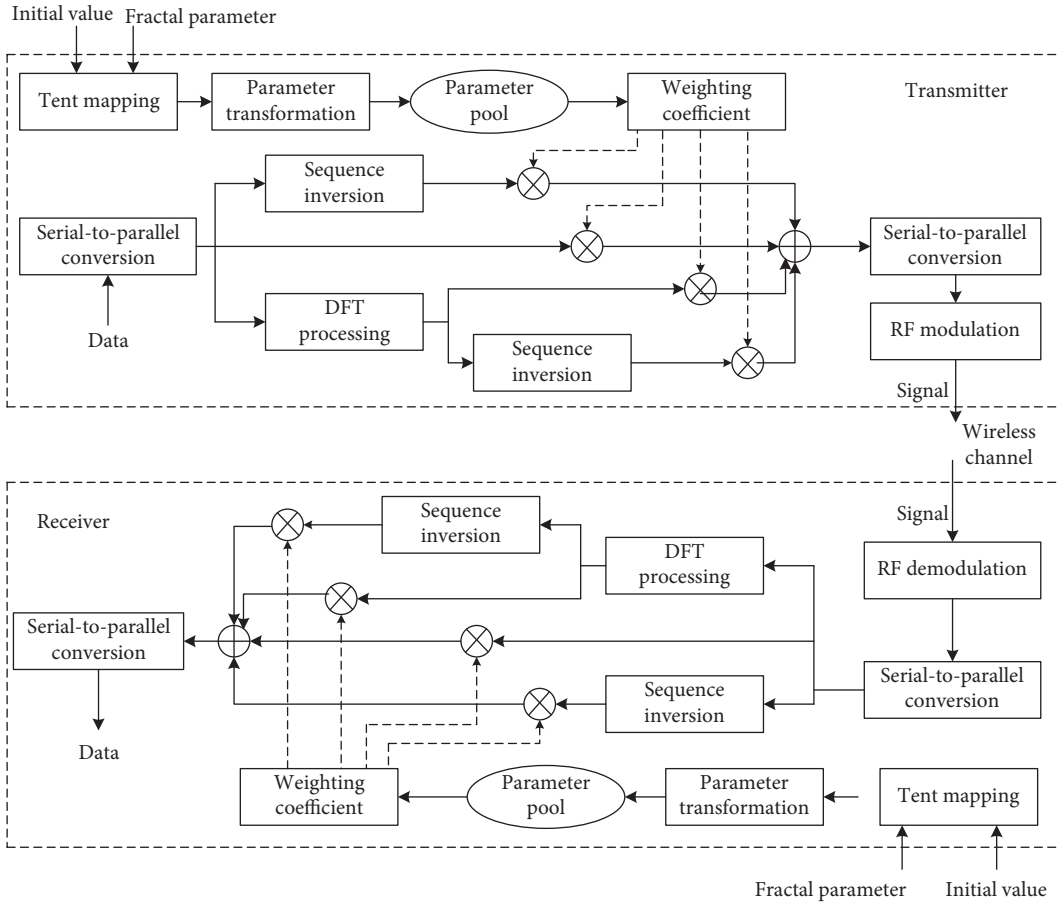

Figure 2: Schematic of the CPP method.

Furthermore, the received signal is processed by WFRFT using y_i' as the demodulation order, as follows:

$$\begin{aligned} r'(n) &= F^{-y_i'}(r(n)), \\ &= F^{-y_i'}\left(F^{y_i}(s(n)) + \lambda_0(n)\right), \\ &= F^{-y_i'}\left(F^{y_i}(s(n))\right) + F^{-y_i'}\left(\lambda_0(n)\right), \\ &= F^{y_i - y_i'}(s(n)) + \lambda_0'(n). \end{aligned} \tag{7}$$

Here, $\lambda_0'(n)$ represents the mixed noise in the receiving system, which is related to the channel environment and receiver processing technology. In the following tests, the channel noise is Gauss noise.

When the parameters selected in the parameter pool are in the same order, and the switching time can be synchronized, $y_i' = y_i$ can be obtained. Thereafter, it is introduced into formula (7) and the following formula (8) is obtained. It can be observed that, if the influence of noise is within a certain extent, the original information can be received and restored correctly:

$$\begin{aligned} r'(n) &= F^0(s(n)) + \lambda_0'(n), \\ &= \omega_0(0)s(n) + \omega_1(0)S(n) + \omega_2(0)s(-n) \\ &\quad + \omega_3(0)S(-n) + \lambda_0'(n), \\ &= 1 \cdot s(n) + 0 \cdot S(n) + 0 \cdot s(-n) + 0 \cdot S(-n) + \lambda_0'(n), \\ &= s(n) + \lambda_0'(n). \end{aligned} \tag{8}$$

For unauthorized users without scanning capabilities, the demodulation order y_Δ of the WFRFT inverse transform of the receiver and modulation order y_i of the transmitter cannot be exactly the same or synchronized, so the equivalent original information is processed by WFRFT with the modulation order $y_i - y_\Delta$. Thus, the correct information $s(n)$ cannot be received and restored correctly, which is expressed as

$$\begin{aligned} r'(n) &= F^{-y_\Delta}(r(n)), \\ &= F^{-y_\Delta}\left(F^{y_i}(s(n)) + \lambda_0(n)\right), \\ &= F^{-y_\Delta}\left(F^{y_i}(s(n))\right) + F^{-y_\Delta}\left(\lambda_0(n)\right), \\ &= F^{y_i - y_\Delta}(s(n)) + \lambda_0'(n), \\ &\neq s(n). \end{aligned} \tag{9}$$

However, for unauthorized receivers with scanning capabilities, when y_Δ is equal to y_i, the true transmission signal can be received and restored correctly. Therefore, to meet the requirements of the $y_\Delta = y_i$ equation under the condition that the switching rule is unknown, the aim of y_i scanning is achieved by means of y_Δ scanning in the main period of $[0, 4)$. The difference between the switching rule of the inverse transformation and positive transformation is $\Delta y = y_i - y_\Delta$. Combined with the relationship between the scanning interval and BER, a smaller Δy results in a smaller bit error rate of the signal after inverse transform; that is, the error between $r'(n)$ and the real signal is reduced. However, with a smaller Δy, more time is required for scanning in the 0–4 interval.

3. Performance Analysis

The BER performance of unauthorized receivers and that of authorized receivers is mainly affected by the E_b/N_0. For unauthorized receivers, the signal processed by CPP increases the noise energy superimposed on the signal and reduces the signal-to-noise ratio of unauthorized receivers. Thus, E_b/N_0 of the unauthorized receivers is also reduced due to the mathematical relationship between E_b/N_0 and the signal-to-noise ratio. Therefore, the CPP method can increase the BER of unauthorized receivers.

The average power of signal is defined as P_0 and the average power of noise is N_1. When the transformation order is known, the SNR of the receiver is written as

$$\mu = 10 \cdot \log\left(\frac{P_0}{N_1}\right). \tag{10}$$

Then, by using formula (5), $|\omega_0|^2$ is calculated as

$$\left|\omega_0\right|^2 = \omega_0 \cdot \omega_0^* = \cos^2\left(\frac{\Delta y\pi}{4}\right)\cos^2\left(\frac{\Delta y\pi}{2}\right). \tag{11}$$

For unauthorized receivers, the equivalent energy of the signal after WFRFT becomes P_0':

$$P_0' = \left|\omega_0\right|^2 \cos^2\left(\frac{-3\Delta y\pi}{4}\right) \cdot P_0 = \left|\omega_0 \cos\left(\frac{-3\Delta y\pi}{4}\right)\right|^2 \cdot P_0 = \left|\cos\left(\frac{\Delta y\pi}{4}\right)\cos\left(\frac{\Delta y\pi}{2}\right)\cos\left(\frac{-3\Delta y\pi}{4}\right)\right|^2 \cdot P_0. \tag{12}$$

Thus, the equivalent SNR of the unauthorized receivers is expressed as

$$\mu_1 = 10 \cdot \log\left[\frac{P_0'}{1 - P_0' + N_1}\right] = 10 \cdot \log\left[\frac{\left|\omega_0 \cos\left(-3\Delta y\pi/4\right)\right|^2}{1 - \left|\omega_0 \cos\left(-3\Delta y\pi/4\right)\right|^2 + 10^{-(\mu/10)}}\right]. \tag{13}$$

Further, consider the mathematical relationship between E_b/N_0 and P_0/N_1, which is shown in formula (14), then the logarithmic E_b/N_0results of the unauthorized receivers are calculated as shown in formula (15), where W is signal bandwidth, R_b is the number of bits transmitted per second, and it is also the transmission rate:

$$\frac{E_b}{N_0} = \frac{P_0}{N_1} \cdot \frac{W}{R_b}, \tag{14}$$

$$ebn0 = 10 \cdot \log\left[\frac{P_0'}{1 - P_0' + N_1} \cdot \frac{W}{R_b}\right] = 10 \cdot \log\left[\frac{\left|\omega_0 \cos\left(-3\Delta y\pi/4\right)\right|^2}{1 - \left|\omega_0 \cos\left(-3\Delta y\pi/4\right)\right|^2 + 10^{-(\mu/10)}}\right] + 10 \cdot \log\left[\frac{W}{R_b}\right]. \tag{15}$$

This formula shows that the E_b/N_0 decreases when the transformation order is unknown, which also shows that the BER increases for the unauthorized receivers. Thus, it shows that the theoretical antiscanning performance of the CPP method is superior.

In addition, if the modulation order is fixed, the unauthorized receiver can scan at a step less than 0.01 and illegally receive signals. The number of scans is shown in formula (16). It can be seen that when the number of scans reaches 400, the security of the system is threatened. However, the CPP method also solves this problem. Under the same condition of less than 0.01 step, the number of scans is shown in formula (17). The number of scans is increased by N times, and when the value of N is larger, the degree of improvement of the number of scans will be very large. Thus, CPP method greatly improves the scanning complexity of unauthorized users and the security performance of communication system:

$$\chi = \frac{4}{0.01} = 400, \tag{16}$$

$$\chi' = N\frac{4}{0.01} = 400N. \tag{17}$$

4. Test and Analysis

Considering that the CPP method is a transmission technique for authorized users, the CPP method is compared to the scanning and nonscanning methods for unauthorized users. For the scanning method, conditions 1 and 2 are the cases in which different modulation orders are scanned. Condition 1 is to lock a parameter in the parameter pool with the smallest error. Condition 2 is to lock a random parameter in the parameter pool.

4.1. BER Analysis. Firstly, when $L = 102300$, the BER is tested under different modulation modes, which are illustrated in Figures 3.

It can be observed that with the increase in E_b/N_0, the BER of the nonscanning method is always very high; hence, it cannot recover data in any environment. Then, the CPP method has the lowest BER and the best performance. And the BER of the scanning method is also very high, and it

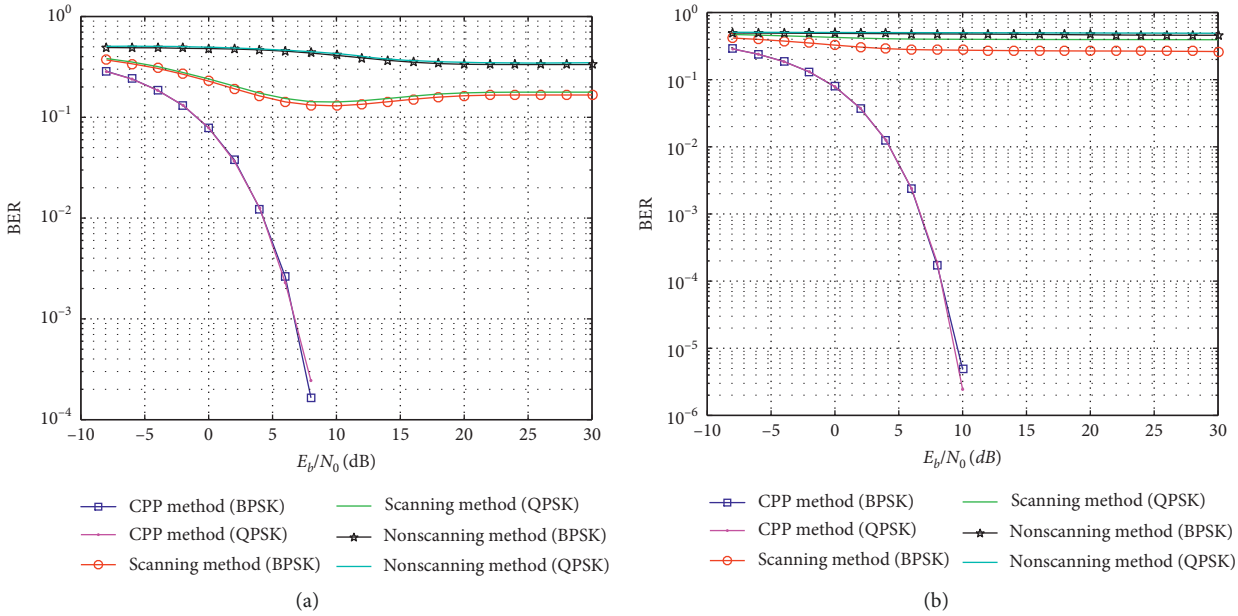

Figure 3: BER results under different modulation modes: (a) $N = 3$ and (b) $N = 12$.

cannot recover data. In traditional scanning methods, the demodulation parameters are first estimated, then fixed, and then the demodulation parameters are not re-estimated. Thus, the usual scanning method can only lock the demodulation order at one time, not all the demodulation orders. And the scanning method cannot synchronize the demodulation order switching frequency. Therefore, the BER of the scanning method is higher than that of the CPP method. This also demonstrates that the CPP method can resist the illegal acceptance of unauthorized users under the premise of effective transmission performance.

In addition, under the same methods, the BER performance of BPSK modulation is slightly better than that of QPSK modulation, but the performance difference is not obvious. Therefore, the following tests are performed with BPSK modulation.

Then, the influence of the amount of data L on the BER is tested. When E_b/N_0 is fixed at -8 dB, the lengths of the parameter pool N are 3 and 12. With the increase in L, the BER results are illustrated in Figures 4(a) and 4(b), respectively. Obviously, with the increase in L, the BER of each method is relatively stable. However, under the same L condition, the BER of the CPP method is the lowest, followed by the scanning method, while that of the nonscanning method is the highest. Furthermore, when the E_b/N_0 is fixed at 6 dB, the lengths of the parameter pool N are 3 and 12. With the increase in the amount of data L, the BER results are presented in Figures 4(c) and 4(d), respectively, and the same conclusion can be obtained. It can be observed that L has little effect on the BER of all methods.

Because L has very little influence on the BER of all methods, the following tests are carried out under the condition of a fixed L of 102300. Next, we test the influence of the number of the parameter pool length N on the BER. Then, when the E_b/N_0 is -8 and 6 dB, with the increase in N, the BER results are illustrated in Figure 5. It can be observed that, with the increase in N, the BER of the CPP method is the smallest and relatively stable, while the BER of the scanning method increases gradually. However, after $N > 10$, the BER reaches a high level and the change is not obvious. The BER of the nonscanning method is always very high and is not affected by the change in N. Comparatively, the BER of the CPP method is the lowest, and the scanning method is also lower when N is small, although it is still substantially higher than that of the CPP method. The nonscanning method has the highest BER and cannot achieve the correct reception conditions.

Thereafter, the influence of the transmission environment on the BER is tested. When N is 2, 3, 6, and 12, with the increase in E_b/N_0, the BER results are illustrated in Figure 6, respectively. It can be observed that, with the increase in E_b/N_0, the BER of the nonscanning method is always very high; hence, it cannot recover data in any environment.

When $N = 2$, the parameter pool of the CPP method is equivalent to that of m/M sequence, and m/M sequence parameter pool is no longer affected by N. No matter how much N is taken, the result is the same as that of $N = 2$. The m/M sequence is a binary sequence, whose values are 0 and 1, and it is easy to be measured. Therefore, the parameter pool formed by m/M sequence will only consist of 0 and 1. The antiscanning ability of the method based on m/M sequence parameter pool is the same as that of Figure 6(a). It can be seen that the BER always keeps the trend of Figure 6(a), and the antiscanning ability is greatly reduced.

However, Chaos sequence parameter pool is greatly affected by N, and the larger the N, the better the antiscanning ability, which is illustrated in Figures 6(a) to 6(d). When N is large, the BER of the scanning method is also very high, and it cannot recover data. When N is small, the BER of the scanning method decreases, but it is still higher

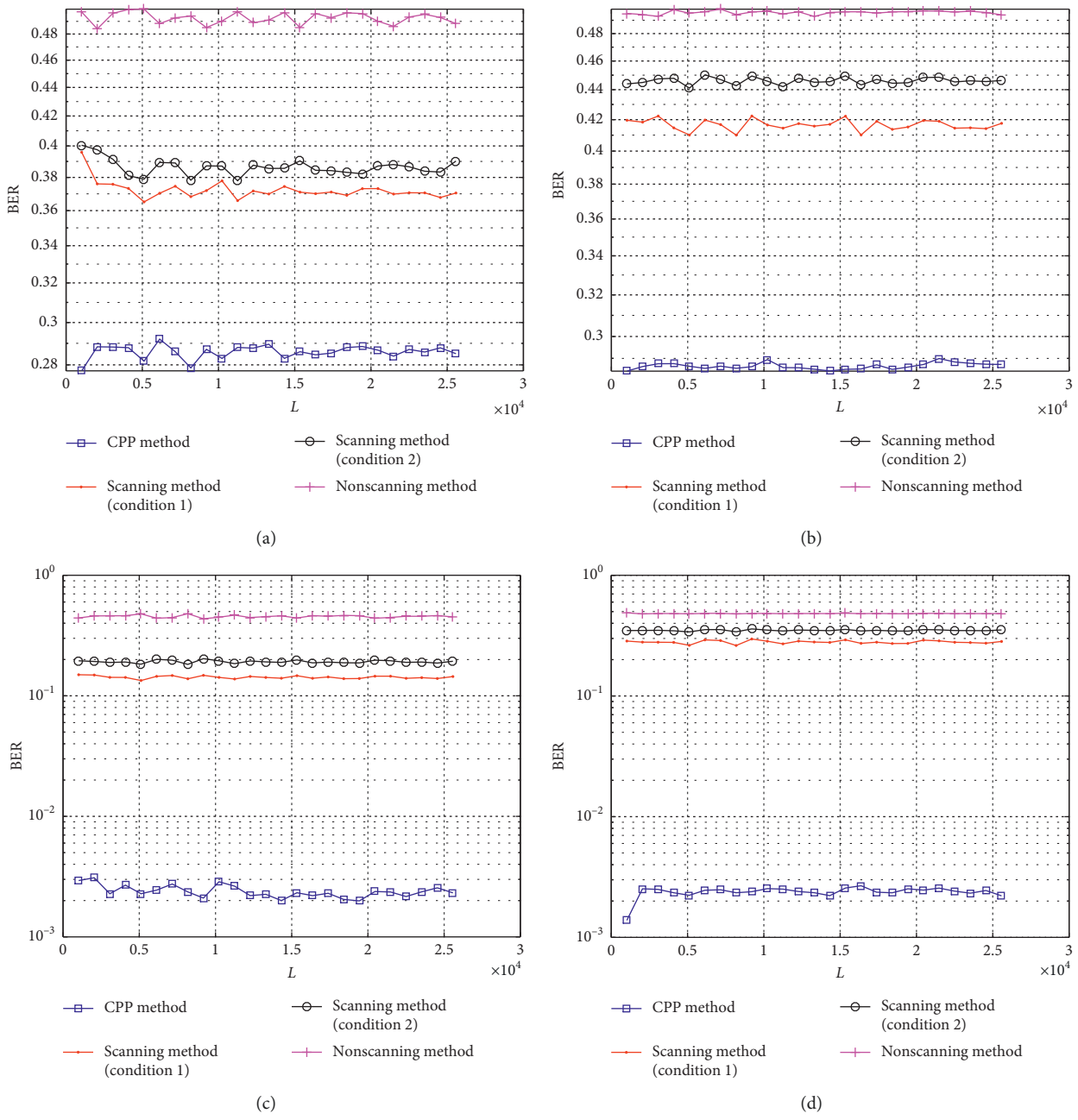

FIGURE 4: BER results with the change of L. (a) $E_b/N_0 = -8$ dB and $N = 3$. (b) $E_b/N_0 = -8$ dB and $N = 12$. (c) $E_b/N_0 = 6$ dB and $N = 3$. (d) $E_b/N_0 = 6$ dB and $N = 12$.

than that of the CPP method. Because the scanning method can only lock one of the N parameters, the larger the N, the smaller the proportion of locked parameters. Therefore, the smaller the proportion of correct demodulation, the larger the BER. In particular, when $N = 1$, that is, when the modulation order is not switched, the BER of the scanning method is the same as that of the CPP method. Therefore, apart from the special condition of $N = 1$, the BER of the CPP method is the lowest, and it is substantially lower than that of the other methods. To sum up, the bigger the N, the better the antiscanning ability of the CPP method, and the antiscanning ability of chaotic sequence parameter pool is much higher than that of m/M sequence parameter pool.

4.2. Detection Probability Analysis. For a secure transmission system, the effective detection probability analysis is also the main index. The detection probability results are shown in Figure 7. It can be seen that the detection probability of the CPP method is the best, followed by the scanning method, and that of the nonscanning method is the worst. These demonstrate that the CPP method can resist the illegal acceptance of unauthorized users under the premise of effective transmission performance.

4.3. Speed Analysis. In addition, the processing time of various methods is tested. However, based on the previous

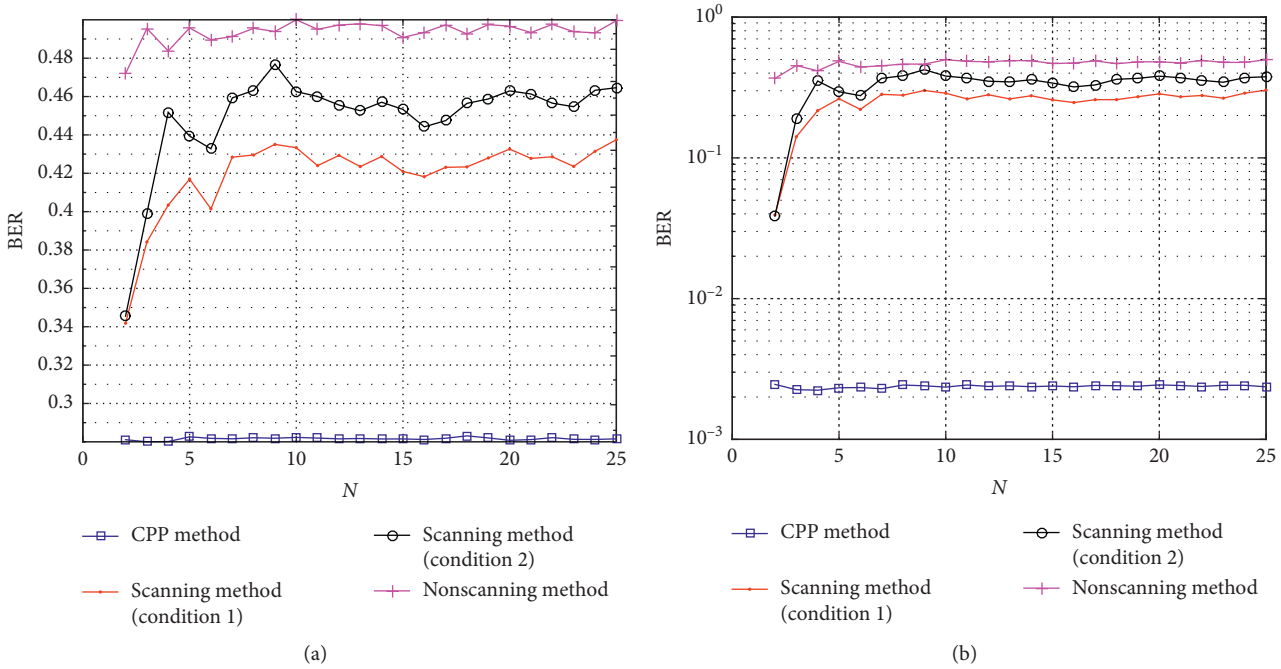

Figure 5: BER results with the change of N. (a) $E_b/N_0 = -8$ dB. (b) $E_b/N_0 = 6$ dB.

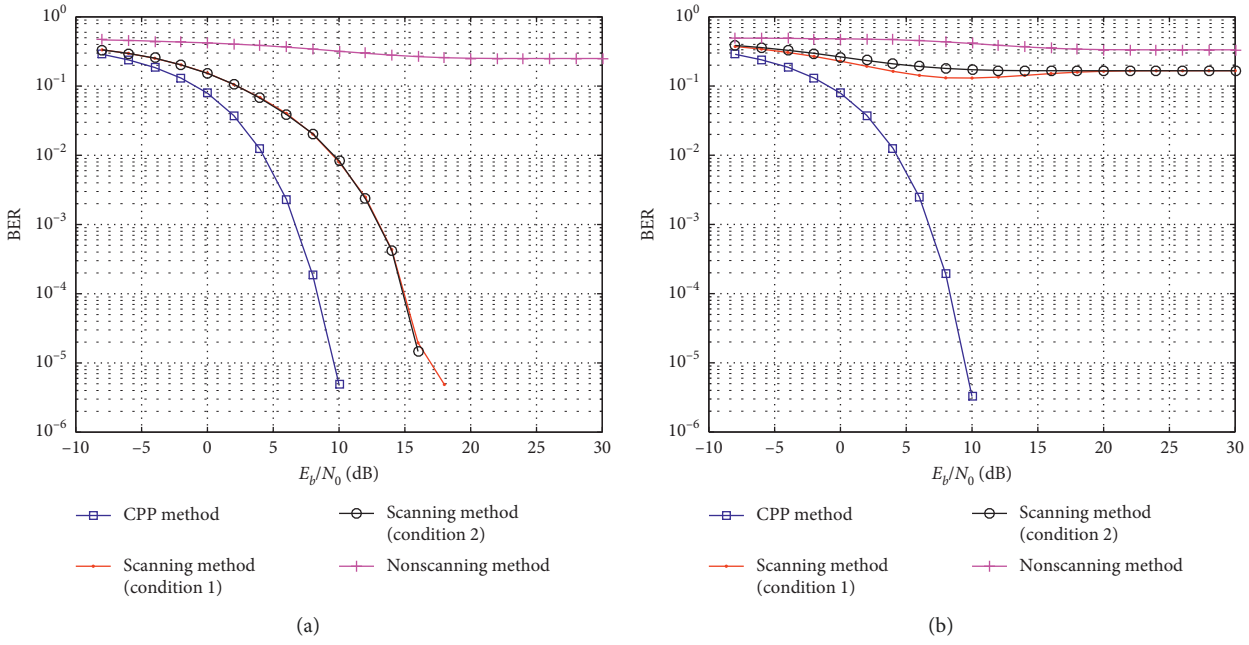

Figure 6: Continued.

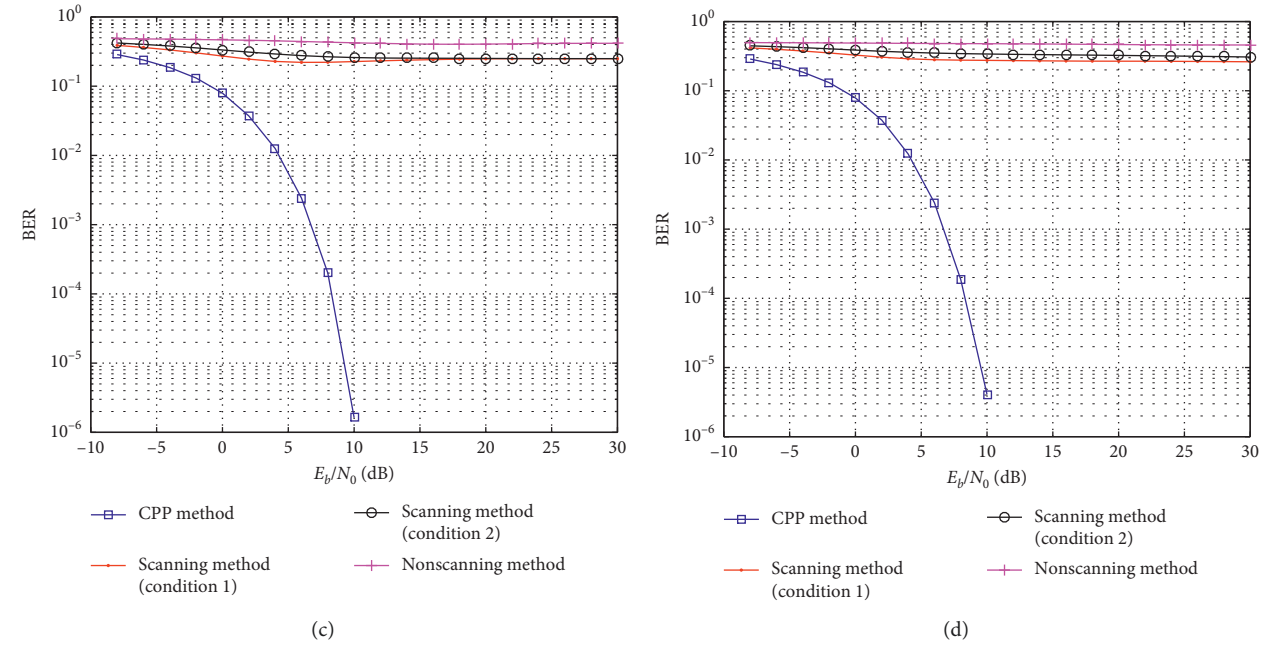

Figure 6: BER results with the change of E_b/N_0. (a) $N = 2$. (b) $N = 3$. (c) $N = 6$. (d) $N = 12$.

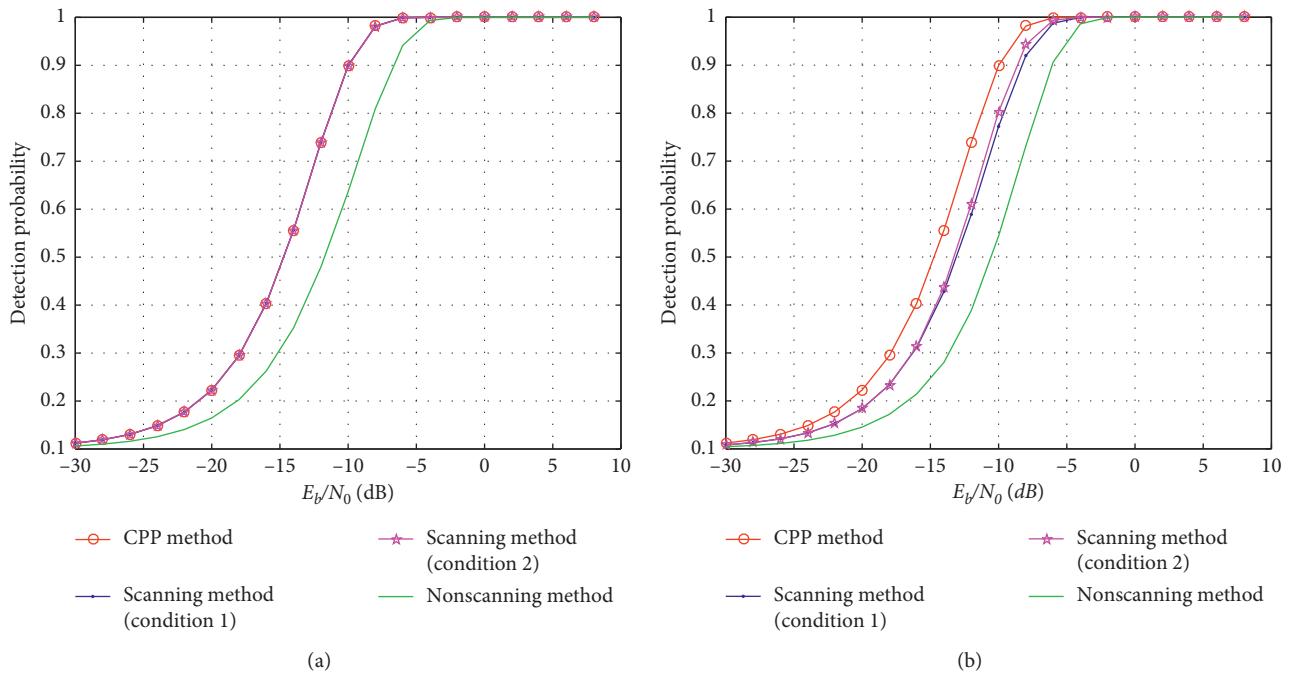

Figure 7: Continued.

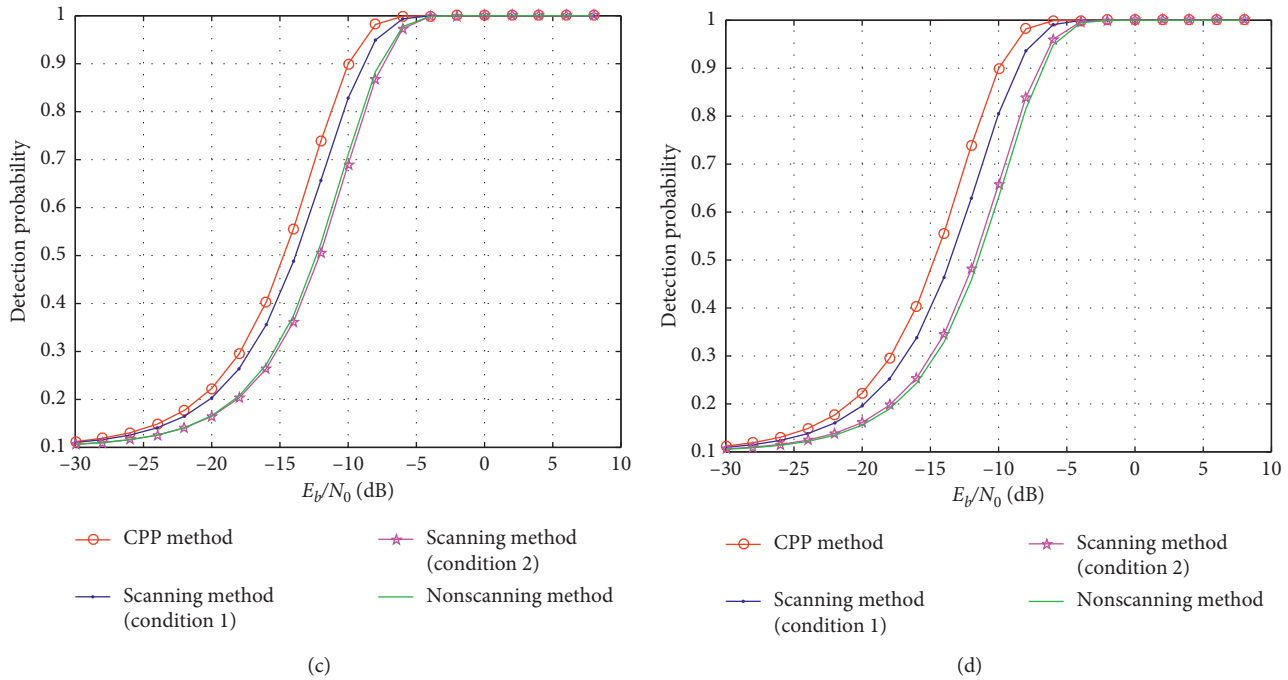

Figure 7: The detection probability results with the change of E_b/N_0. (a) $N=2$. (b) $N=3$. (c) $N=6$. (d) $N=12$.

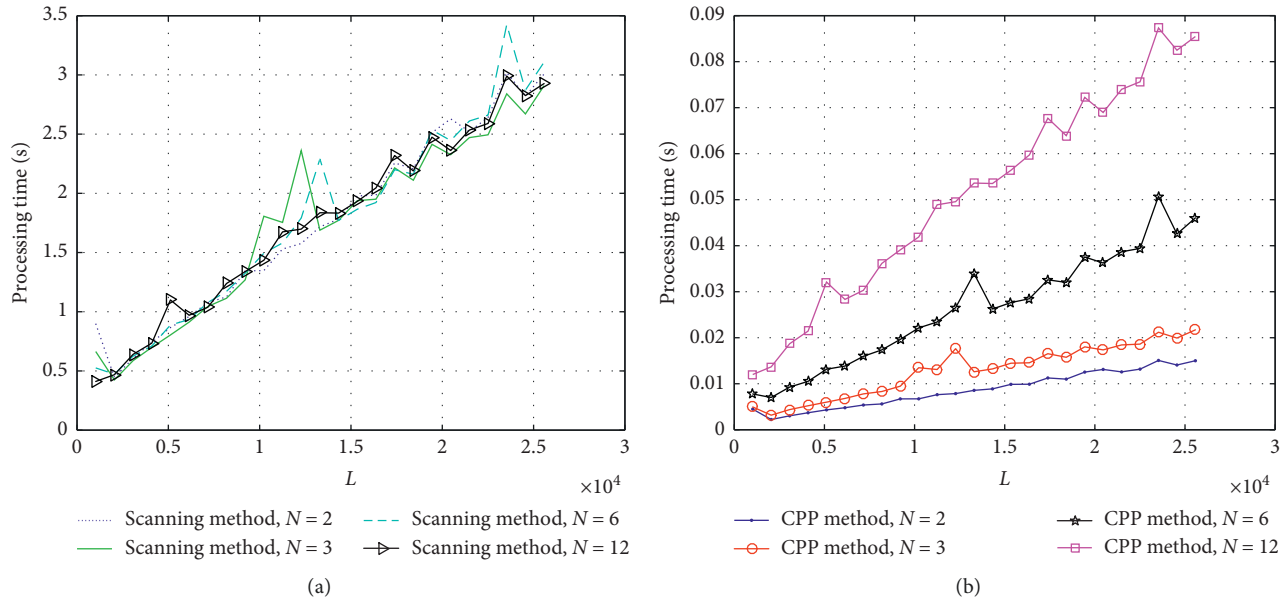

Figure 8: The processing time results with the change of L. (a) The scanning method. (b) The CPP method.

test and analysis because the nonscanning method cannot recover data or cannot receive correctly, the speed analysis of the nonscanning method is meaningless. Therefore, speed tests are carried out on the CPP and scanning methods, and the processing time of the scanning method is illustrated in Figure 8(a), and the processing time of the CPP method is illustrated in Figure 8(b). The results indicate that the processing time of the two methods increases with an increase of the data amount L. Moreover, the processing time of the scanning method is not affected by the parameter N, and it is very long. The processing time of the CPP method is affected by N. With the increase of N, the processing time increases, that is, the processing speed decreases. The processing time of the CPP method is obviously lower than that of the scanning method, that is, the processing speed of the CPP method is higher than that of the scanning method, demonstrating that the CPP method exhibits superior time performance. This is also consistent with the theoretical speed performance. For the transmitters and receivers of the authorized user, the chaotic type, the initial chaotic value,

Table 1: The scanning complexity results.

Number of scans	Number of N							
	$N=1$	$N=2$	$N=3$	$N=5$	$N=8$	$N=10$	$N=16$	$N=20$
Nonscanning method	1	1	1	1	1	1	1	1
Scanning method	400	800	2400	2000	3200	4000	6400	8000
CPP method	1	1	1	1	1	1	1	1

and the discarding and switching frequency are known. The CPP method can receive the signal without a large number of scans, so the speed is faster. These parameters are unknown to unauthorized users, they still need to scan, so the speed performance of CPP methods is better than the traditional methods.

Finally, because the scanning complexity is also one of the indicators to evaluate the processing speed, and the complexity is mainly affected by the number of scans, so the scanning complexity is analyzed from the angle of the number of scans. The test results are shown in Table 1. Although the complexity of the nonscanning method is very low, it cannot receive data successfully. Comparatively speaking, the scanning complexity of the scanning method is very large, especially when N is large. The scanning complexity of the CPP method is very low, and it can receive data successfully, which shows that its performance is the best.

5. Conclusions

The WFRFT secure communication method based on the chaotic parameter pool has been proposed to improve information transmission security. Compared to the scanning and nonscanning methods, the CPP method exhibits superior performance. Although the BER of the scanning method is lower when N is smaller, it is still much higher than that of the CPP method. The nonscanning method has the highest BER and cannot achieve the correct reception conditions. The BER of the CPP method is the lowest, and detection probability is the best, which also indicates that the CPP method can resist the illegal acceptance of unauthorized users under the premise of effective transmission performance. Moreover, the processing speed of the CPP method is obviously faster than that of the other methods, demonstrating that the CPP method exhibits superior time performance.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant no. 61501309), the China Postdoctoral Science Foundation (Grant no. 2017T100185), the Liaoning Natural Science Foundation of China (Grant no. 2017011002-301), and the Liaoning Provincial Colleges and Universities Innovative Talents Support Program.

References

[1] Y. Liu, Z. Nie, and Q. H. Liu, "DIFFT: a fast and accurate algorithm for fourier transform integrals of discontinuous functions," *IEEE Microwave and Wireless Components Letters*, vol. 18, no. 11, pp. 716–718, 2008.

[2] T. Wang, H. Huan, R. Tao, and Y. Wang, "Anti-eavesdropping FrFT-OFDM system exploiting multipath channel characteristics," *IET Communications*, vol. 11, no. 9, pp. 1371–1378, 2017.

[3] Y. Luo, C. Yu, S. Chen, J. Li, H. Ruan, and N. El-Sheimy, "A novel doppler rate estimator based on fractional fourier transform for high-dynamic GNSS signal," *IEEE Access*, vol. 7, pp. 29575–29596, 2019.

[4] R. Chen and Y. Wang, "Universal FRFT-based algorithm for parameter estimation of chirp signals," *Journal of Systems Engineering and Electronics*, vol. 23, no. 4, pp. 495–501, 2012.

[5] H. Wang and Y. Jiang, "Real-time parameter estimation for SAR moving target based on WVD slice and FrFT," *Electronics Letters*, vol. 54, no. 1, pp. 47–49, 2018.

[6] L. Yuan, X. Da, J. Wu, R. Xu, Z. Zhang, and H. Liu, "WFRFT modulation recognition based on HOC and optimal order searching algorithm," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 462–470, 2018.

[7] Z. Wang, L. Mei, X. Sha, and V. C. M. Leung, "BER analysis of WFRFT precoded OFDM and GFDM waveforms with an integer time offset," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9097–9111, 2018.

[8] X. Da, Y. Liang, H. Hu et al., "Embedding WFRFT signals into TDCS for secure communications," *IEEE Access*, vol. 6, pp. 54938–54951, 2018.

[9] X. Fang, X. Sha, and Y. Li, "Secret communication using parallel combinatory spreading WFRFT," *IEEE Communications Letters*, vol. 19, no. 1, pp. 62–65, 2015.

[10] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On physical layer security: weighted fractional fourier transform based user cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5498–5510, 2017.

[11] Z. Luo, H. Wang, K. Zhou, and W. Lv, "Combined constellation rotation with weighted FRFT for secure transmission in polarization modulation based dual-polarized satellite communications," *IEEE Access*, vol. 5, pp. 27061–27073, 2017.

[12] X. Fang, X. Sha, and L. Mei, "Guaranteeing wireless communication secrecy via a WFRFT-based cooperative system," *China Communications*, vol. 12, no. 9, pp. 76–82, 2015.

[13] Z. Zhang, X. Da, and H. Liu, "A study of the covered characteristics of MAP-WFRFT satellite signals," *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, vol. 29, no. 4, pp. 460–467, 2017.

[14] X. Fang, X. Sha, and Y. Li, "MP-WFRFT and constellation scrambling based physical layer security system," *China Communications*, vol. 13, no. 2, pp. 138–145, 2016.
[15] Y. Liang, X. Da, R. Xu, D. L. Ni, Z. Zhai, and Y. Pan, "Research on constellation-splitting criterion in multiple parameters WFRFT modulations," *IEEE Access*, vol. 6, pp. 34354–34364, 2018.
[16] Q. Ran, D. S. Yeung, E. C. C. Tsang et al., "General multi fractional fourier trans-form method based on the generalized permutation matrix group," *IEEE Transactions on Signal Processing*, vol. 53, no. 1, pp. 83–98, 2005.
[17] J. Li, X. Sha, X. Fang, and L. Mei, "8-Weighted-type fractional Fourier transform based three-branch transmission method," *China Communications*, vol. 15, no. 9, pp. 147–159, 2018.
[18] P. Manfredi, D. V. Ginste, D. D. Zutter, and F. G. Canavero, "Generalized decoupled polynomial chaos for nonlinear circuits with many random parameters," *IEEE Microwave and Wireless Components Letters*, vol. 25, no. 8, pp. 505–507, 2015.
[19] Y. Xu, L. Mili, A. Sandu, M. R. von Spakovsky, and J. Zhao, "Propagating uncertainty in power system dynamic simulations using polynomial chaos," *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 338–348, 2019.