Invisible Encryption Communication Method based on WFRFT

Fang Liu, Lizhi Chen, Yongxin Feng

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

*Corresponding author: Fang Liu Email: zhqing1019@163.com

Abstract: Considering that the open signal transmission mode can lead to the potential risk of interception, identification, decoding, and interference, high confidentiality is imperative for wireless communication. The security of communication process is typically ensured by encrypting and concealing transmitted information. The weighted fractional Fourier transform (WFRFT) technology can substantially change the signal characteristics, and the statistical characteristics of the signal diversify to effectively hide the communication information. In this paper, considering a single parameter-WFRFT as the breakthrough point, the in-depth investigation of the mechanism of a single-parameter fractional domain and the analysis of its potential micro-features and dark features are presented; accordingly, an invisible encryption method with vector jumping is proposed. The relationship between modulation order and constellation diagram is utilized, the jumping matrix and vector are thereafter established, and the control rules are formulated accordingly; furthermore, the dynamic modulation order is obtained by the jumping vector control. The new method can improve the security performance of the system and provide a technical basis for securing communication with anti-jamming, anti-interception, and anti-deception capability.

Keywords: Communication; WFRFT; Signals; Encryption

1 Introduction

With the increasing complexity of the information environment, interference and anti-interference as well as control and anti-control is becoming increasingly more critical. In high-risk situations, such as rejection, interference, deception, and intrusion, it is important to maintain the reliability, confidentiality, and anti-interference in the communication process. Considering that the open signal transmission mode can also lead to the potential risk of interception, identification, decoding, and interference, wireless communication should have high confidentiality. The security of the communication process is typically ensured by encrypting and concealing transmitted information. Traditionally, the encryption system based on the cryptography theory is the most well-established and widely used security mechanism in the field of wireless communication. However, the design concept of encryption system is adopted from the traditional computer network, which ignores the physical layer characteristics (e.g., openness of wireless channels, time-varying network topology, and resource constraints of terminals) of wireless communication systems. This has also led to the present unprecedented problems in wireless communication. In recent years, a large number of secure communication technologies and methods have emerged. For example, some physical layer encryption methods were proposed in the orthogonal frequency division multiplexing system. Additionally, the following are proposed: two-dimensional encryption method, dynamic secret-based encryption scheme, digitally secure communication method using one-dimensional PWL map, and secret reconstruction with optimal communication efficiency.

Thereafter, the weighted fractional Fourier transform (WFRFT) technology emerged. Its characteristics include the simultaneous and co-frequency interference among signal sub-components. The superposition of each component leads to the essential change in signal characteristics; this makes the WFRFT a promising signal security technology. The WFRFT signals exhibits more diversified statistical
characteristics. Compared with traditional communication signals, the WFRFT signals can effectively hide communication information and resist detection and interception of non-purpose receivers. At present, the communication system based on the WFRFT mainly increases the complexity of the system from the perspective of multiple parameters [12-14]; consequently, security performance increases. For example, in [15], a WFRFT-based cooperation scheme is proposed to improve the physical layer security against eavesdropping in wireless communications. Rather than dissipating valuable transmission power to jam the eavesdropper, the information-bearing signal can create an “artificial noise” effect on the eavesdropper by leveraging the features of WFRFT while imposing no effect on the legitimate receiver. In [16], the WFRFT is employed to enhance the security performance of conventional directional modulation. The proposed method affords additional security to the physical layer communication by scrambling constellations in all directions; therefore, the information could not be demodulated albeit the eavesdropper knows the intended direction. In [17], a data-carrying artificial noise based on the WFRFT is introduced to achieve physical layer security in satellite transmission; this outperforms the traditional artificial noise method when the channel state information is not precise at the transmitter. The DM technique in [18], which has multiple-parameter weighted-type fractional Fourier transform and chaotic scrambling, is proposed to achieve power-efficient and security-enhanced wireless transmissions.

However, the multi-parameter WFRFT processing can significantly increase the complexity of the system, and the generation of multiple parameters and hardware implementation of the receiver can be extremely difficult. With the objective of resolving problems related to interception and eavesdropping of communication in the process of information transmission, the limitations and shortcomings in signal authenticity, integrity, and confidentiality are dealt with. Taking a single-parameter weighted-fractional Fourier transform as the breakthrough point, the in-depth investigation of the mechanism of a single-parameter fractional domain transformation and the analysis of its potential micro-features and dark features are presented; moreover, an invisible encryption method with vector jumping (IEVJ) is proposed.

2 IEVJ method

The modulation order of the WFRFT technology is typically fixed; however, considering the existence of an unauthorized receiver with a scanning ability, especially when the demodulation order error is less than 0.01, the interception bit error rate (BER) can basically achieve illegal reception ability. Therefore, an invisible encryption method with vector jumping is proposed.

In the process of WFRFT processing, considering that the relationship between modulation order and weighting coefficient periodically changes, the relationship between the modulation order (β) and constellation diagram of the WFRFT processing signal over a period is analyzed, as shown in Fig. 1; the basic period is [0.4]. It can be observed that regardless of the modulation order of β, the constellations of WFRFT processing signals under β, and βi+2 conditions are the closest, that is, the difference in signal characteristics between these two conditions is the smallest and is the most difficult to detect.

The number of available users in the system is set to M; a set of basic modulation orders is defined as β; m denotes the user ID, m∈[1 M]; the basic modulation order of the m th user is βm. Furthermore, the jumping matrix (C) is imported, and set C is composed of 0 and 1. Each user employs a row vector in C; hence, Cm is the jumping vector of the m th user and also the m th row vector in C.

The jump rate of each row vector is set to R; the dwell time of each jump is T, whose calculation process is shown in Eq. (1). For each user, there is a dynamic modulation order, which is converted every time T. In the t th time, T, the modulation order of user m is αmt, and its value is selected from βm to
\[ T = \frac{1}{R} \]

The control rules are expressed in Eq. (2), where \( i \in [1, R] \).

\[
\alpha_{mi} = \begin{cases} 
\beta_m, & (C_m(i) = 0) \\
\beta_m + 2, & (C_m(i) = 1) 
\end{cases}
\]

The selected \( \alpha_m \) is used to process the user data, \( d_m(n) \), with \( \alpha_{mi} \)-order WFRFT in each dwell time. The signal processing mechanism is illustrated in Fig. 2:

\[
s_m(n) = F^{\alpha_m}(d_m(n)) = \omega_0(\alpha_m)d_m(n) + \omega_1(\alpha_m)D_m(n) + \omega_2(\alpha_m)d_m(-n) + \omega_3(\alpha_m)D_m(-n)
\]

where \( F^{\alpha_m}(\cdot) \) is the processing function of \( \alpha_m \)-order WFRFT; the four state functions, \( d_m(n) \), \( D_m(n) \), \( d_m(-n) \), and \( D_m(-n) \) in Eq. (3) are the results of 0, 1, 2, and 3 Fourier transforms of \( d_m(n) \) in user \( m \), respectively; \( \omega_l(\alpha_m) \) is the weighted coefficient, which is defined in Eq. (4).

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

![Fig. 1 Processing mechanism of IEV method](image)

For authorized receivers, the hopping rate of each user is \( R \), and the hopping rate of user \( m \) is \( C_m \).

The demodulation order of the \( i \)th time, \( T \), is \( \alpha'_m \), whose value is selected by the control from \(-\beta_m\) to \(-\beta_m - 2\). The control rules are shown in Eq. (5), where \( i \in [1, R] \).

\[
\alpha_{mi} = \begin{cases} 
-\beta_m, & (C_m(i) = 0) \\
-\beta_m - 2, & (C_m(i) = 1) 
\end{cases}
\]

Furthermore, the received signal, \( s_m(n) \), is processed by the WFRFT using \( \alpha'_m \) as the demodulation order in authorized receivers, as expressed in Eq. (6). Because the demodulation order of the inverse transform satisfies \( \alpha_m - \alpha_m \) (i.e., \( \Delta \alpha = \alpha_m + \alpha_m = 0 \)), and the hopping rule is synchronized with the sender in each hop dwell time, \( T \), the reverse transform result of the authorized receiver is equal to \( d_m(n) \) by using the rotational additivity of WFRFT. Thus, authorized receivers can achieve the correct reception.
\[ F^{\mu m}(s_m(n)) = F^{\mu m}(F^{\mu m}(d_m(n))) \]
\[ = F^{\mu m + \beta m}(d_m(n)) \]
\[ = F^0(d_m(n)) \]
\[ = d_m(n) \]  \hspace{1cm} (6)

However, for an unauthorized receiver, if its demodulation order of the inverse transform is \( \mu \), then it can be estimated that the relationship between \( \mu \) and modulation order \( -\alpha \) within a dwell time, \( T \), approximately satisfies Eq. (7) after a considerable number of scanning processes.
\[ \mu = -\alpha + \Delta \alpha \]  \hspace{1cm} (7)

If \( \alpha \) tends to be equal to the basic modulation order of a user (i.e., \( \alpha = \beta_n \), then \( C_n(i) \) jumps to 0; the successful symbol bit of \( C_n(i) \) jump is 0, and the failure symbol bit is 1. For this reason, every time \( C_n(i) \) jumps to 0, \( \alpha_m = \beta_n \), and the unauthorized receiver successfully scans illegally; scanning results are shown in Eq. (8). When \( C_n(i) \) jumps to 1, \( \alpha_m = \beta_n + 2 \), and the unauthorized receiver fails to scan, in Eq. (9).
\[ F^{\mu}(s_m(n)) = F^{\mu}(F^{\mu}(d_m(n))) \]
\[ = F^{\mu + \beta_n}(d_m(n)) \]
\[ = F^{\beta_n}(d_m(n)) \]
\[ \approx d_m(n) \]  \hspace{1cm} (8)
\[ F^{\mu}(s_m(n)) = F^{\mu}(F^{\mu}(d_m(n))) \]
\[ = F^{\mu - \beta_n + \Delta \alpha + \beta_n}(d_m(n)) \]
\[ = F^{\Delta \alpha}(d_m(n)) \]
\[ \approx d_m(n) \]  \hspace{1cm} (9)

Similarly, if \( \alpha = \beta_n + 2 \) is satisfied at this time, then it means that \( C_n(i) \) jumps to 1 at this time; hence, the successful symbol bit of \( C_n(i) \) jump is 1, and the failure symbol bit is 0. For this reason, every time \( C_n(i) \) jumps to 1, \( \alpha_m = \beta_n + 2 \) and the unauthorized receiver successfully scans illegally; the scan result is shown in Eq. (10). When \( C_n(i) \) jumps to 0, \( \alpha_m = \beta_n \), and the unauthorized receiver fails to scan; the scan result is expressed as Eq. (11).
\[ F^{\mu}(s_m(n)) = F^{\mu}(F^{\mu}(d_m(n))) \]
\[ = F^{\mu - \beta_n - 2 + \Delta \alpha + \beta_n + 2}(d_m(n)) \]
\[ = F^{\Delta \alpha}(d_m(n)) \]
\[ \approx d_m(n) \]  \hspace{1cm} (10)
\[ F^{\mu}(s_m(n)) = F^{\mu}(F^{\mu}(d_m(n))) \]
\[ = F^{\mu - \beta_n - 2 + \Delta \alpha + \beta_n}(d_m(n)) \]
\[ = F^{\Delta \alpha - 2}(d_m(n)) \]
\[ \approx d_m(n) \]  \hspace{1cm} (11)

It can be observed that regardless of whether \( \alpha = \beta_n \) or \( \alpha = \beta_n + 2 \) is satisfied by the condition of the successful scan of unauthorized receiver, \( \alpha \) is a fixed value; however, \( \alpha_m \) is changed every time \( T \) when the signal is transmitted. Whenever \( C_n(i) \) jumps to the corresponding successful symbol bits, it can
approximately receive transmission data; whenever \( C_m(i) \) jumps to the corresponding failed symbol bits, it cannot receive transmission data. Therefore, the jump rate \( (\gamma) \) is defined in Eq. (12), where \( \varepsilon \) is the number of successful symbol bits scanned by an unauthorized receiver, and \( N \) is the total length of jump vector \( C_m \).

\[
\gamma = \frac{\varepsilon}{N} \tag{12}
\]

Therefore, \( \gamma \) determines the anti-scanning ability of receiving data. The larger the \( \gamma \) value, the greater the probability of successful scanning of unauthorized receivers; that is, the anti-scanning ability of the system is weaker. The smaller the \( \gamma \) value, the smaller the probability of successful scanning of unauthorized receivers; that is, the anti-scanning ability is stronger.

3 Test and analysis

3.1 Basic test

Firstly, the similarity between the received data and transmitted real data is defined as \( P \). The bit error rate (BER) between the received data and transmitted real data is \( P_e \). The larger the \( P \) value or the smaller the \( P_e \) value, the better the reception performance. When the basic modulation order, \( \beta_m \), is fixed and \( \gamma = 50\% \), both the IEVJ and traditional scanning (TS) methods are compared and analyzed. Under the first experimental condition, the demodulation order errors, \( \Delta\alpha \), are 0.01, 0.1, and 0.2. The similarity results of inverse transform and the BER are shown in Figs. 2(a) and 2(b), respectively. The test results show that the similarity of both methods slightly decreases with the increase in \( \Delta\alpha \). Relatively, the similarity between the received data and real data of the IEVJ method is significantly higher than that of the TS method. Furthermore, the bit error rate of received data increases with the increase in \( \Delta\alpha \). The BER of the IEVJ method is significantly lower than that of the TS method, which exhibits the inability of correctly receiving data, thus achieving the anti-scanning objective.

In the second experimental condition, the demodulation order errors (\( \Delta\alpha \)) are 0.3, 0.4, and 0.5. The similarity results of inverse transform and the BER are shown in Figs. 3(a) and 3(b), respectively.
The test results show that the similarity of both methods decrease slightly with the increase in $\Delta \alpha$. Relatively, the similarity of the IEVJ method is significantly higher than that of the TS method, and the BER of received data increases with the increase in $\Delta \alpha$. The BER of IEVJ method is significantly lower than that of the TS method. However, when the demodulation order error is 0.5, the IEVJ method cannot effectively receive data.

3.2 Modulation order influence test

When $\gamma = 50\%$, and the demodulation order errors of inverse transform are fixed at 0.01, 0.32, and 0.43, and the basic modulation orders ($\beta_m$) are 0.01, 1.274, 2, and 3.021, similarity results are shown in Fig. 4.

It can be observed that with the increase in $E_s/N_0$, the similarity gradually increases; in the TS method, it becomes relatively stable and extremely low. The larger the modulation order error, the lower the similarity of the IEVJ method. Relatively, the similarity of the IEVJ method is significantly higher than that of the TS method. Statistical analysis shows that when $\beta_m$ extremely approaches 0 and 2, the similarity of the IEVJ method is considerably affected by the modulation order error. The similarity can be higher only when the demodulation order error is less than 0.01.
The BER results are illustrated in Fig. 5. It can be observed that the TS method has a considerably high BER and is unable to scan the received data correctly. The BER of the IEVJ method increases with the increase in demodulation order error. The BER of the IEVJ method is relatively lower than that of the TS method. Similarly, the statistical analysis shows that when $\beta_m$ is extremely close to 0 and 2, the BER of the IEVJ method is considerably affected by the modulation order error. The BER can satisfy the requirement of correct reception only when the demodulation order error is less than 0.01. Therefore, it is suggested that the fundamental modulation order, $\beta_m$, avoids 0 and 2.
3.3 Jump rate influence test

When the demodulation order errors of inverse transform are fixed at 0.01, 0.32, and 0.43, and the basic modulation order $\beta_\nu$ is 3.021, and $\gamma$ values are 0%, 40%, 80%, and 100%, the BER and similarity results are shown in Figs. 6 and 7.

It can be observed that the similarity and BER of the TS method are considerably affected by $\gamma$. The greater the $\gamma$ value, the greater the similarity and the smaller the BER. When $\gamma = 100\%$, the similarity and BER of the TS method are equal to those of the IEVJ method. The similarity and BER of the IEVJ method are not affected by $\gamma$. As long as $\beta_\nu$ avoids 0 and 2, it is only affected by the demodulation order error. The smaller the error, the greater the similarity and the smaller the bit error rate. Therefore, in order to avoid illegal scanning and receiving of unauthorized users, it is recommended that $\gamma = 50\%$; that is, the number of 0 s and 1s in each user’s $C_\nu$ should be as equal as possible.

Fig. 6 BER results at different $\gamma$ values
Fig. 7 Similarity results at different $\gamma$ values

**Conclusions**

An invisible encryption method with vector jumping (IEVJ) is proposed. The IEVJ method and traditional scanning (TS) method are tested and analyzed in a simulation environment. The test results show that the similarity of the IEVJ method is significantly higher than that of the TS method; the BER of the IEVJ method is significantly lower than that of TS method. Thus, it can be concluded that the IEVJ has a good anti-scanning ability. In addition, it is suggested that the fundamental modulation order, $\beta_m$, avoids the values 0 and 2. To avoid illegal scanning and receiving of unauthorized users, it is recommended that $\gamma = 50\%$; that is, the number of 0s and 1s in each user’s $C_m$ should be as equal as possible.

**Declaration statements**

*Funding*

This work is supported in part by the National Natural Science Foundation of China (Grant No. 61501309, 61971291), the Liaoning Natural Science Foundation of China (Grant No. 2020-MS-215), the Liaoning Provincial Colleges and Universities Innovative Talents Support Program, and the Liaoning BaiQianWan Talents Program(Grant No. 2020921087).

*Conflicts of interest*

The authors declare that they have no competing interests.

*Availability of data and material*

The data used to support the findings of this study are currently under protected. Requests for data, [6/12 months] after publication of this article, will be considered by the corresponding author.
*Code availability*

The Data is generated by using the formula principle. The type of data is floating-point.

*Authors' contributions*

Liu F and Chen L Z participated in the design of this study, and they both performed the statistical analysis. Feng Y X carried out the study and collected important background information. Liu F drafted the manuscript. All authors read and approved the final manuscript.

References

[1] Haitao Li, Yiming Qian. Effects of IQ imbalance for simultaneous transmit and receive based cognitive anti-jamming receiver[J]. AEU - International Journal of Electronics and Communications, 2017, 2(72):26-32.

[2] Prachin Bhoyer, Parul Sahare, S. B. Dhok, R. B. Deshmukh. Communication technologies and security challenges for internet of things: A comprehensive review [J]. AEU - International Journal of Electronics and Communications, 2019, 2(99):81-99.

[3] Xijin Lu ; Yuxin Shi ; Wei Li ; Jing Lei ; Zhipeng Pan. A Joint Physical Layer Encryption and PAPR Reduction Scheme Based on Polar Codes and Chaotic Sequences in OFDM System[J]. IEEE Access, 2019,7:73036-73045.

[4] Pan Cao ; Xiaofeng Hu ; Jiayang Wu ; Liang Zhang ; Xinhong Jiang ; Yikai Su. Physical Layer Encryption in OFDM-PON Employing Time-Variable Keys From ONUs[J]. IEEE Photonics Journal, 2014, 6(2):1-11.

[5] Yaoqiang Xiao ; Zhiyi Wang ; Jun Cao ; Rui Deng ; Yi Liu ; Jing He ; Lin Chen. Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system[J]. IEEE/OSA Journal of Optical Communications and Networking, 2018,10(1): 46-51.

[6] K. Ikeda ; Y. Sato ; O. Koyama ; M. Yamada. Two-dimensional encryption system for secure free-space optical communication of time-series data streams[J]. Electronics Letters, 2019,55(13): 752-754.

[7] Ting Liu ; Yang Liu ; Yashan Mao ; Yao Sun ; Xiaohong Guan ; Weibo Gong ; Sheng Xiao. A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication[J]. IEEE Transactions on Smart Grid, 2014,5(3):1175-1182.

[8] Li-Hai Zhou ; Zheng-Jin Feng. A new idea of using one-dimensional PWL map in digital secure communications-dual-resolution approach[J]. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 2000,47(10):1107-1111.

[9] Xingfu Yan ; Changlu Lin ; Rongxing Lu ; Chunming Tang. Design of Secret Reconstruction With Optimal Communication Efficiency[J]. IEEE Communications Letters, 2018,22(8): 1556-1559.

[10] Yuan Liang ; Xin Xiang ; Ye Sun ; Xinyu Da ; Cong Li ; Liyan Yin. Novel Modulation Recognition for WFRFT-Based System Using 4th-Order Cumulants[J]. IEEE Access, 2019,7: 86018 – 86025.

[11] Zhenduo Wang ; Lin Mei ; Xiaolu Wang ; Xuejun Sha ; Victor C. M. Leung. On the Performance of Hybrid Carrier System Based on WFRFT With Power Allocation[J]. IEEE Access, 2018,6: 29231 – 29240.

[12] Yuan Liang ; Xinyu Da ; Ruixiang Xu ; Lei Ni ; Dong Zhai ; Yu Pan. Research on Constellation-Splitting Criterion in Multiple Parameters WFRFT Modulations[J]. IEEE Access, 2018, 6: 34354 -34364.

[13] 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[J]. IEEE Transactions on Signal Processing, 2005, 53(1), pp.83–98.

[14] Jing Li ; Xuejun Sha ; Xiaojie Fang ; Lin Mei. 8-Weighted-type fractional Fourier transform based three-branch transmission method[J]. China Communications, 2018, 15(9): 147 – 159.

[15] Xiaojie Fang ; Ning Zhang ; Xuejun Sha ; Dajiang Chen ; Xuanli Wu ; Xuemin Sherman Shen. Physical layer security: A WFRFT-basec cooperation approach[C]. 2017 IEEE International Conference on
Communications (ICC), 2017,5,21-25.
[16] Feng Liu ; Ling Wang ; Jian Xie. Directional modulation via weighted fractional fourier transform — A way to enhance security[J]. 12th European Conference on Antennas and Propagation (EuCAP 2018), 2018,4,9-13.
[17] Ruiyang Xu ; Xinyu Da ; Hang Hu ; Yuan Liang ; Lei Ni. Power and Time Slot Allocation Method for Secured Satellite Transmission Based on Weighted Fractional Data Carrying Artificial Noise [J]. IEEE Access, 2018,6: 65043 – 65054.
[18] Feng Liu ; Ling Wang ; Jian Xie ; Yuexian Wang ; Zhaolin Zhang. MP-WFRFT and Chaotic Scrambling Aided Directional Modulation Technique for Physical Layer Security Enhancement[J]. IEEE Access, 2019,7: 74459 – 74470.