IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 9, 2019, accepted December 28, 2019, date of publication January 1, 2020, date of current version January 10, 2020.

*Digital Object Identifier 10.1109/ACCESS.2019.2963481*

# Antijamming Design and Analysis of a Novel Pulse Compression Radar Signal Based on Radar Identity and Chaotic Encryption

**JIAN DAI, XINHONG HAO, (Member, IEEE), PING LI, ZE LI, AND XIAOPENG YAN**
Science and Technology on Electromechanical Dynamic Control Laboratory, School of Mechatronical Engineering, Beijing Institute of Technology, Beijing 100081, China

Corresponding author: Xiaopeng Yan (yanxiaopeng@bit.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61973037 and Grant 61673066.

**ABSTRACT** As the use of radar and radar jammers increases, a radar device is likely to face interference from jammers or other radar devices. Traditional phase-coded pulse compression radar devices are widely used, but these tools struggle to overcome jamming and mutual interference. To solve this problem, we propose a novel chaotic-encrypted pulse compression radar signal based on radar identity (ID). Each radar has its own ID, which is encrypted with different chaotic binary sequences in every pulse period. The ambiguity function calculated for the coded radar signal is thumbtack-shaped, indicating that the signal has a good resolution. The received signal is used to range and decrypt in two channels: the range channel and the radar ID channel. The signals of the two channels are analyzed separately. Analyses of anti-barrage jamming and anti-mutual interference show that both channels perform well in terms of antijamming, while the antijamming ability is influenced by the processing gain, bit error rate (BER) and correlation function. In addition, the dual-channel antijamming method further improves the radar antijamming ability. The simulation result verifies the strong antijamming ability and high range resolution of the proposed radar signal, and the proposed antijamming method performs much better than the traditional phase-coded pulse compression radar signal in the antijamming scenario.

**INDEX TERMS** Pulse compression radar, radar ID, chaotic encryption, mutual interference, antijamming ability.

## I. INTRODUCTION

Phase-coded pulse compression radar has been widely applied due to its high range-Doppler resolution, large unambiguous range and low probability of intercept. Binary phase-coded pseudorandom codes, such as Barker codes, m sequences and Gold codes, are often used in phase-coded pulse compression radar for practical applications [1]–[3]. However, these codes are usually periodical and limited in quantity, which means that radar using these codes can easily be intercepted and interfered with by jammers. Jan *et al.* [4] proposed an integrated design based on digital channelized reconnaissance and jamming to achieve accurate and effective jamming against pulse compression radar. Liu *et al.* [5] reconstructed binary pseudorandom codes by using a third-order correlation function; the codes were used to construct a jamming signal, and the experimental result verified its high efficiency in jamming. Moreover, with the increasing use of radar technology and its frequency spectrum requirements, radar signals that coexist within the same bandwidth face the severe threat of the mutual interference [6]. References [7] and [8] studied antenna coupling problems, pointing out that the coupling of antennas for two radars could cause mutual interference. Thayaparan *et al.* [9] investigated the mechanisms of mutual interference and pointed out that mutual interference could lead to problems such as ghost targets and a reduced signal-to-noise ratio (SNR). Brooker [10] analyzed the mutual interference of radar systems, showing that the signal of one radar device could be reflected into another radar device and become a false target through a radar antenna, especially when the two radar devices are of the same type. Therefore, a design to enhance the antijamming performance of a pulse compression signal with low probability of intercept and to reduce the mutual interference between two radar signals is urgently needed to improve the radar antijamming ability.

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wang.

Aperiodic phase-coded codes provide a new way to achieve antijamming, with the chaotic signal being one example. The statistical characteristics of a chaotic signal are similar to those of real noise. Chaotic signals have strong antijamming ability and confidentiality since they are wideband and sensitive to initial conditions. In contrast to real noise and some pseudorandom sequences, chaotic signals are numerous and easy to generate [11], [12]. Hence, a chaotic signal has superiority in constructing a pulse compression radar signal. Therefore, chaotic signals are increasingly applied in secure communications and radar signal design. A previous study [13] optimized the chaotic-based random stepped frequency radar signal to achieve excellent performance in terms of both anti-single-frequency interference and target detection. Hambling [14] also used a chaotic radar signal to reduce the probability of interference. Yin *et al.* [15] designed a frequency-modulated radar waveform based on sampled chaotic series, and on the basis of frequency modulation, Zeng *et al.* [16] proposed a novel chaos-based stepped frequency synthesized wideband radar signal. This approach effectively overcame the range-Doppler coupling caused by linear frequency modulation and provided a thumbtack-shaped ambiguity function; however, the computational complexity limits the application of the method. To reduce the algorithm complexity for practical applications, Xin *et al.* [17] generated a simple chaotic phase code for radar pulse compression. However, due to the autocorrelation and cross-correlation performance of chaotic signals, their antijamming ability is still limited against increasing jamming power.

Several methods have been proposed for mutual interference mitigation. Choi *et al.* [18] proposed a mutual interference suppression method using clipping and weighted-envelope normalization for automotive radar, but it is hard to separate the interference coming within a short interval, and suppression is greatly influenced by the parameters of the algorithm. Reference [19] mitigated interference by zeroing or inverse windowing the interference-contaminated parts of the signal in the time domain, but the zeroing of the signal would cause signal phase discontinuity and result in worse range resolution. Neemat *et al.* [20] proposed an interference mitigation technique using beat frequency interpolation in the STFT domain, and the known beat signal model effectively suppresses interference. However, the proposed method is not applicable for phase-coded pulse compression radar. References [21]–[23] proposed a radar communication approach for combating mutual interference without reducing radar accuracy, and it works well when the two radars are collaborative and the communication is well established but could not work in a noncooperative scenario since the radar may not be able to communicate with an unknown radar system.

In addition, research on specific emitter identification (SEI) recently offered a new idea for anti-mutual interference and antijamming radar design. The signal generated by a radar device can be distinguished from that by other radar devices and jammers; thus, mutual interference and jamming can be reduced. Research on SEI can be divided into two areas. Some researchers [24]–[27] focused on nonlinear devices in radar systems; the radar signals generated by those devices were unique and thus could be specifically recognized, resulting in an improved antijamming ability. Other researchers mainly considered the time-frequency analysis of the intrapulse features of radar signals. Reference [28] used a feature extraction algorithm to characterize the radar such that the probability of interference by jamming decreased. Empirical mode decomposition was used to identify a specific radar emitter in [29], the result of which showed that this method was more accurate than wavelet transformation. To improve the recognition accuracy, Li *et al.* [30] proposed a quadratic time-frequency analysis method and updated the classifier online, which obviously improved the recognition accuracy of a specific radar device under barrage jamming. Wen *et al.* [31] utilized a time-space domain information fusion method for SEI, which had the ability to deal with uncertain information when processing a radar signal. Furthermore, some researchers [32] studied the classification algorithm in radar identification, with the pattern recognition method being used to improve the accuracy of radar identification. However, the methods mentioned above require a high sampling resolution and are computationally complex, and their recognition accuracy is severely influenced by the SNR, which limits their application.

Based on the analysis above, this paper presents a novel pulse compression radar signal based on radar identity (ID) and chaotic encryption. Different from the traditional pulse compression and radar antijamming methods mentioned above, in this paper, each radar device has its own ID, which is encrypted with different chaotic binary sequences in every pulse period. The received signal is used to perform the range and decrypt functions in the range channel and radar ID channel. Then, the outputs of the channels are combined to achieve radar antijamming. In this way, the proposed method significantly decreases the probability of interference from other radar devices or jammers. Radar using this method will possess high resolution and a strong antijamming ability.

## II. RADAR TRANSMITTED SIGNAL DESIGN

The proposed radar signal mainly consists of radar ID and chaotic binary sequences. Before transmission occurs, the radar ID is encrypted by a chaotic binary sequence.

### A. RADAR ID

The unique feature of a radar signal can be used to identify a specific radar target echo and jamming signal. However, the subtle features of a radar signal are unstable and difficult to extract, especially under a low SNR. Therefore, a unique identity must intentionally be added to the radar signal.

To ensure that each radar signal has a unique ID, $L \times 7$-bit ASCII codes are used to identify each radar signal, where the radar ID is $M$; thus, there are $2^{7L}$ different ID codes for a radar signal. Hence, at most $2^{7L}$ different radar signals can be specifically distinguished. The radar ID can be

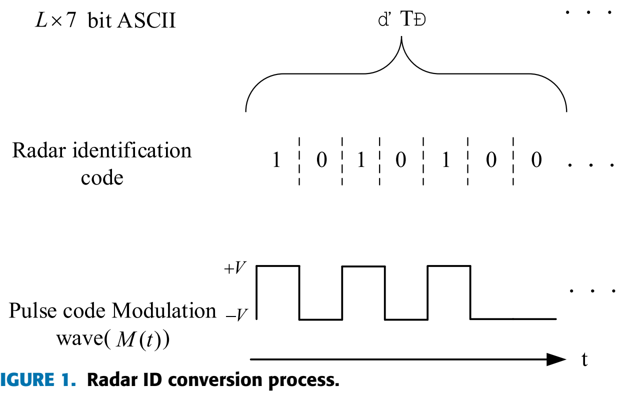

$L\times7$ bit ASCII
ď TĐ
. . .
Radar identification code
1 0 1 0 1 0 0 . . .
+V
−V
Pulse code Modulation wave( $M(t)$)
. . .
t

**FIGURE 1.** **Radar ID conversion process.**

converted into binary code by pulse-code modulation,

$$M(t)=\sum_{n=0}^{7L-1}P_{\tau_M}(t-n\tau_M)m_n \tag{1}$$

where $P_{\tau_M}$ is a pulse, $\tau_M$ is the pulse width of $P_{\tau_M}$, the amplitude of $P_{\tau_M}$ is 1, and $m_n\in\{0,1\}$. The radar ID conversion process is shown in Fig. 1, taking ASCII 'T' as an example.

### B. CHAOTIC BINARY SEQUENCES

A logistic map is used to generate the chaotic sequence, defined as

$$x_{n+1}=ax_n(1-x_n) \tag{2}$$

where $a$ is a bifurcation parameter that can control the logistic map,$a\in[0,4]$, and $x_n$ is a real number, $x_n\in[0,1]$. The logistic map can be used to generate a chaotic sequence when $a$ is close to 4. To encrypt the radar ID, $x_n$ needs to be converted into an integer since the encryption is usually operated in integer fields. The method of extracting binary sequences from chaotic sequences is proposed in Reference [33]. The threshold function is defined as

$$\Theta_v(x)=\begin{cases}1, & x\geq v\\ 0, & x<v\end{cases} \tag{3}$$

where $v$ is the threshold, usually represented by the average of the sequences. The chaotic sequence can be converted into binary code by the threshold function

$$Z(t)=\sum_{i=0}^{N-1}P_{\tau_Z}(t-i\tau_Z)z_i \tag{4}$$

where $N$ is the length of the chaotic binary sequences and $\tau_Z$ is the width, $\tau_Z=7L\tau_M/N$; $z_i\in\{0,1\}$.

### C. CHAOTIC-ENCRYPTED RADAR TRANSMITTED SIGNAL

The chaotic-encrypted binary sequence $C(t)$ can be obtained by encrypting the radar ID with chaotic binary sequences as

$$\begin{aligned}C(t)&=E_k(M(t))\\&=\sum_{n=0}^{7L-1}P_{\tau_M}(t-n\tau_M)m_n\oplus\sum_{i=0}^{N-1}P_{\tau_Z}(t-i\tau_Z)z_i(k)\\&=\sum_{i=0}^{N-1}P_{\tau_Z}(t-i\tau_Z)C_i\end{aligned} \tag{5}$$

where $E_k$ is the encryption algorithm, $k$ is a key represented by $a$ and the initial value $x_0$, as in this paper, $\oplus$ means exclusive-OR (EOR), $Z_i(k)$ is a chaotic binary sequence generated under the control of $k$, and $C_i\in\{0,1\}$. The radar transmitted signal model is shown in Fig. 2.

Then, the chaotic-encrypted radar signal based on chaotic encryption can be expressed as

$$S_t(t)=A_t\exp(j(\omega_0t+\pi C(t)+\varphi_0))[P_{T_m}(t)\otimes\sum_{-\infty}^{\infty}\delta(t-KT_r)] \tag{6}$$

where $A_t$ is the amplitude of the transmitted pulse, $\omega_0$ is the carrier angular frequency, $\varphi_0$ is the initial phase and set to 0 for the sake of efficiency, $T_m$ is the transmitted pulse width, with $T_m=N\tau_Z$, and $\otimes$ means convolution. $\delta(*)$ is the unit-pulse function, and $T_r$ is the pulse repetition period. The chaotic-encrypted sequence is aperiodic because of the random key. The random key generates different chaotic binary sequences in different pulse repetition periods. During the pulse duration, the radar ID is encrypted by a chaotic binary sequence generated by the random key. The radio frequency carrier is directly modulated by the encrypted binary sequence using binary phase shift keying (BPSK); then, the modulated pulse radiates through the antenna.

## III. RADAR TRANSMITTED SIGNAL ANALYSIS

The complex envelope of the chaotic-encrypted radar signal is expressed as

$$\begin{aligned}u(t)&=\exp(j\pi tC(t))P_{T_m}(t)\otimes\sum_{-\infty}^{\infty}\delta(t-KT_r)\\&=\exp(j\pi t\sum_{i=0}^{N-1}P_{\tau_Z}(t-i\tau_Z)C_i)P_{T_m}(t)\otimes\sum_{K=-\infty}^{\infty}\delta(t-KT_r)\end{aligned} \tag{7}$$

Then, the single-period ambiguity function of the chaotic-encrypted radar signal can be deduced as

$$\begin{aligned}&|\chi(\tau,\xi)|\\&=\left|\frac{1}{T_m}\int_{-T_m}^{T_m}u(t)u^*(t+\tau)\exp(j2\pi\xi t)dt\right|\\&=\left|\begin{matrix}\frac{1}{N\tau_Z}\int_{-T_m}^{T_m}\exp[j\pi\sum\limits_{i=0}^{N-1}P_{\tau_Z}(t-i\tau_Z)C_i\\+j\pi\sum\limits_{l=0}^{N-1}P_{\tau_Z}(t-l\tau_Z+\tau)C_l+j2\pi\xi t]dt\end{matrix}\right|,-T_m\leq\tau\leq T_m\end{aligned} \tag{8}$$

where $\tau$ is the delay and $\xi$ is the frequency shift. With $L=1$, $N=70$, and $\tau_Z=1$ $\mu s$, the ambiguity function of the chaotic-encrypted radar signal can be obtained, as shown in Fig. 3.

Fig. 3 shows an obvious peak at the center of the ambiguity function with small side lobes scattered around, and the ambiguity function diagram is in the shape of a 'thumbtack'.

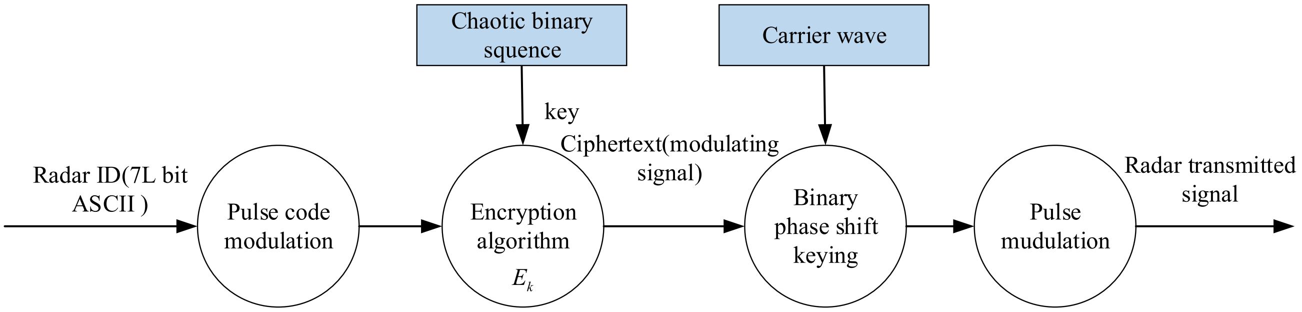
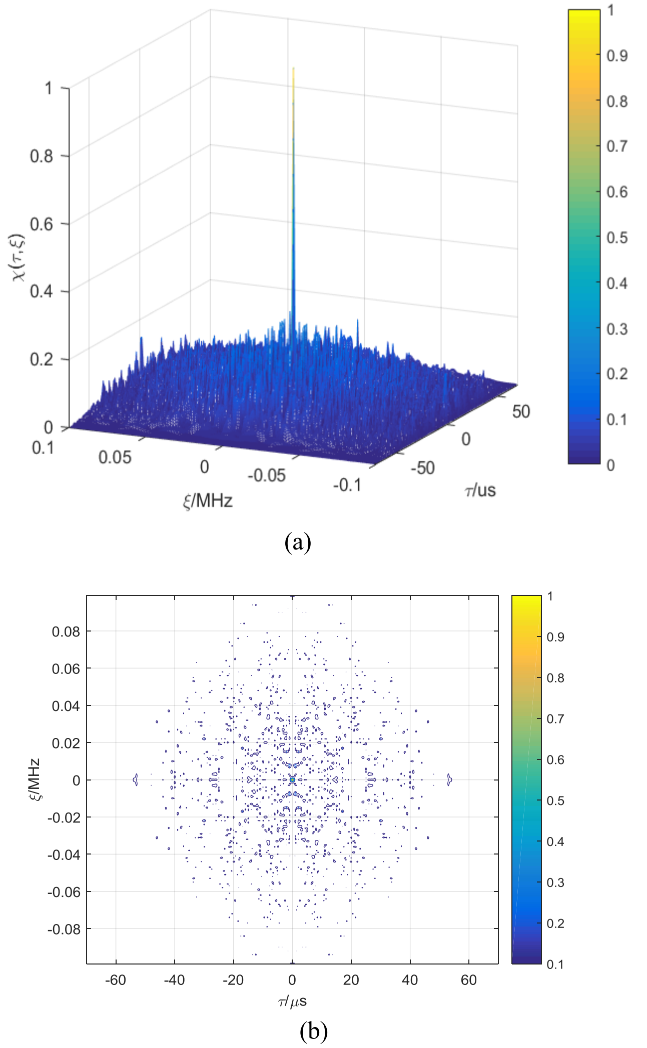


**FIGURE 2.** Block diagram of radar transmitted signal.



(a)

(b)

**FIGURE 3.** (a) Ambiguity function; (b) contour of ambiguity function.

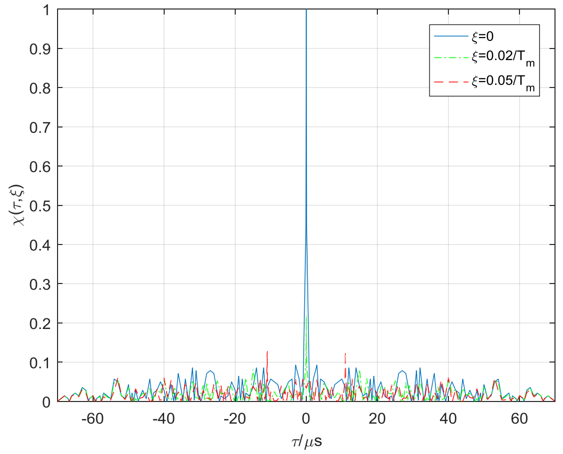


**FIGURE 4.** Range ambiguity function.

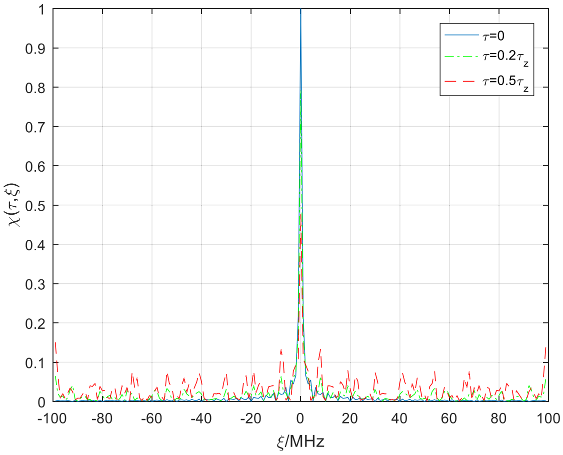


**FIGURE 5.** Doppler ambiguity function.

The single-period range ambiguity function at different $\xi$ values is shown in Fig. 4.

As shown in Fig. 4, the single-period range ambiguity function is equal to the range autocorrelation function when $\xi = 0$. The main lobe in the center of the range correlation indicates that the range resolution is high. The range resolution is $\Delta R = \frac{c\tau_Z}{2}$. However, when $\xi = 0.02/T_m$ and $\xi = 0.05/T_m$, the main lobe of the range ambiguity decreases and the side lobe obviously increases, which affect the ranging performance of the radar. Obviously, the existence of Doppler frequency affects the range performance of chaotic-encrypted radar, and the Doppler tolerance is $1/2T_r$. In practical applications, $\xi \ll 1/2T_r$ is required to ensure the reliability of a measurement. The single-period velocity ambiguity function at different $\tau$ values is shown in Fig. 5.

As shown in Fig. 5, the single-period velocity ambiguity function presents a sinc-shaped envelope. When $\tau = 0$, the single-period velocity ambiguity function has an obvious

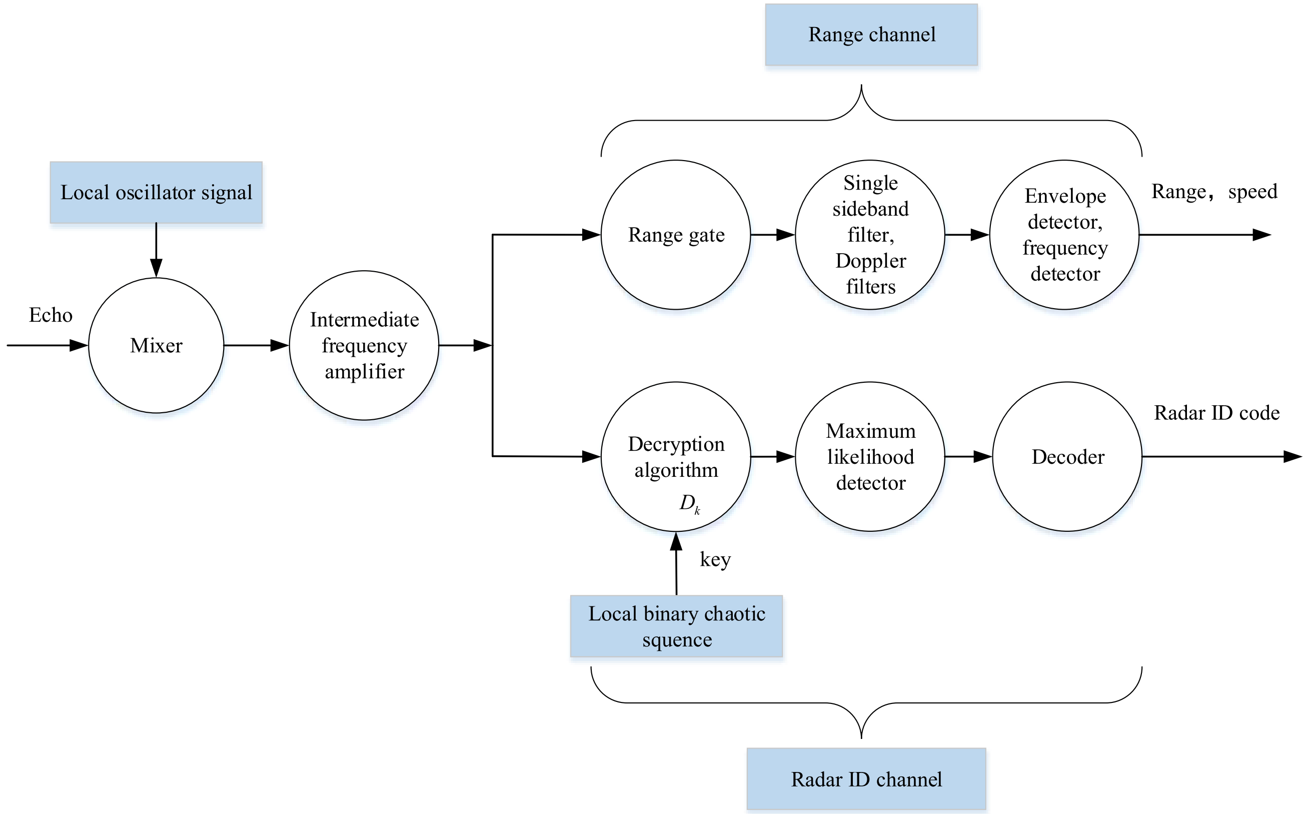

Range channel
Local oscillator signal
Echo
Mixer
Intermediate frequency amplifier
Range gate
Single sideband filter, Doppler filters
Envelope detector, frequency detector
Range，speed
Decryption algorithm
$D_k$
Maximum likelihood detector
Decoder
Radar ID code
key
Local binary chaotic squence
Radar ID channel

**FIGURE 6.** Block diagram of chaotic-encrypted radar signal processing.

main lobe of velocity autocorrelation, and its velocity resolution is $\frac{1}{T_m}$. However, when $\tau = 0.2\tau_Z$ and $\tau = 0.5\tau_Z$, the velocity main lobe decreases, and the velocity side lobe rapidly increases. Therefore, the speed extraction ability of chaotic-encrypted radar for long-range targets is weak. Above all, chaotic-encrypted radar is suitable for detecting low-speed targets.

## IV. CHAOTIC-ENCRYPTED RADAR SIGNAL PROCESSING

The signal received by the radar receiver is divided into two channels: the range channel and the radar ID channel. The signal processing flow chart is shown in Fig. 6.

The target echo can be expressed as

$$\begin{aligned} S_r(t) &= A_r \exp(j(\omega_0(t-\tau) + \pi C(t-\tau)) + \varphi_r) \\ &\quad \cdot [P_{T_m}(t-\tau) \otimes \sum_{-\infty}^{\infty} \delta(t-KT_r)] \\ &= A_r \exp(j((\omega_0 + 2\pi\omega_d)t + \pi C(t-\tau)) + \varphi_r) \\ &\quad \cdot [P_{T_m}(t-\tau) \otimes \sum_{-\infty}^{\infty} \delta(t-KT_r)] \end{aligned} \tag{9}$$

where $A_r$ is the amplitude of the target echo, $\omega_d$ is the Doppler angular frequency, and $\varphi_r$ is the initial phase of the echo.

The output signal is obtained by mixing the echo signal with the local oscillator signal, and the output can be expressed as

$$\begin{aligned} S_{rm}(t) &= K_m A_r \exp(j(\omega_d t + \pi C(t-\tau) + \varphi_r)) \\ &\quad \cdot [P_{T_m}(t-\tau) \otimes \sum_{-\infty}^{\infty} \delta(t-KT_r)] \end{aligned} \tag{10}$$

where $K_m$ is the coefficient of the mixer.

Then, $S_{rm}(t)$ is divided into two channels. One is the range channel. $S_{rm}(t)$ is processed in the correlator with the reference signal. The reference signal is the transmitted signal $C(t)$ with a preset delay. The output signal of the correlator is

$$\begin{aligned} u_r(t) &= \frac{1}{T_m}\int_0^{T_m} S_{rm}(t) C(t-\tau_p) dt \\ &= \frac{A_{rm}}{T_m}\int_0^{T_m} \exp(j\pi(C(t-\tau) + C(t-\tau_p))) \\ &\quad \cdot \exp(j(\omega_d t + \varphi_r)) dt \end{aligned} \tag{11}$$

where $A_{rm} = K_m A_r A_m$, $A_m$ is the amplitude of the reference signal,$\tau_p$ is the preset delay time for the local reference signal, $p = 1, 2, \ldots, P$, and $P$ is the number of range gates. As shown in Eq. (11), the Doppler frequency could affect the output signal of the correlator. When $\omega_d \ll \frac{\pi}{T_m}$, Eq. (11) can be written as

$$\begin{aligned} u_r(t) &= \frac{A_{rm}}{T_m}\int_0^{T_m} \exp(j\pi(C(t-\tau) + C(t-\tau_p)))dt \\ &\quad \cdot \exp(j(\omega_d t + \varphi_r)) \end{aligned} \tag{12}$$

As shown in Eq. (12), the output signal of the correlator contains the range and velocity information, which can be obtained by processing the correlator output signal with a Doppler filter and envelope detector. The output of the envelope detector will exceed the preset threshold when its delay is $\tau_R$. Thus, the measurement range of the target is $R = \frac{c\tau_R}{2}$.

The other channel is the radar ID channel. Before decryption, $S_{rm}(t)$ is converted into a unipolar signal with an amplitude of 0 or 1. Then, $S_{rm}(t)$ is decrypted with the reference chaotic binary sequences. The reference chaotic binary sequences are the transmitted chaotic binary sequences controlled by a local key with a preset delay. The decrypted sequences can be written as

$$\begin{aligned} M_R(t) = D_k(S_{rm}(t)) = \Lambda_n(\int_{(n-1)\tau_M}^{n\tau_M} (S(A_{rm}\exp(j(\omega_d t+\varphi_r \\ +\pi \sum_{i=0}^{N-1} P_{\tau_Z}(t-\tau-i\tau_Z)C_i))) \\ \oplus \sum_{i=0}^{N-1} P_{\tau_Z}(t-\tau_p-i\tau_Z)z_i(k))dt) \qquad (13) \end{aligned}$$

where $D_k$ is the decryption algorithm under the control of $k$, $S_i(\cdot)$ is a unipolar conversion function, and $S_i(\cdot) \in \{0, 1\}$, $\Lambda_n$ is the binary maximum likelihood decision function, and $\Lambda_n(\cdot) = \begin{cases} 1, & if \cdot > 1/2 \\ 0, & if \cdot < 1/2 \end{cases}$. Since $\omega_d \ll \frac{\pi}{T_m}$, Eq. (13) can be simplified to Eq. (14).

$$\begin{aligned} M_R(t) &= D_k(S_{rm}(t)) \\ &= \Lambda_n(\int_{(n-1)\tau_Z}^{n\tau_Z} (S(A_{rm}\exp(j\pi\sum_{i=0}^{N-1}P_{\tau_Z}(t-\tau-i\tau_Z)C_i))\cdots \\ &\quad \oplus \sum_{i=0}^{N-1} P_{\tau_Z}(t-\tau_p-i\tau_Z)z_i(k))dt) \qquad (14) \end{aligned}$$

After $M_R(t)$ is converted to 7-bit ASCII codes $M_R$ by the decoder, the radar ID can be recognized by comparing $M_R$ with the local radar ID $M$. Each period of the pulse has a unique key and chaotic binary sequences. Furthermore, encryption and decryption must be accomplished with the same key. Therefore, obtaining the same decrypted ASCII codes $M_R$ in different pulse periods is technically impossible.

## V. ANALYSIS OF ANTIJAMMING ABILITY

### *A. ANTI-BARRAGE JAMMING ABILITY*

Barrage jamming refers to a kind of jamming that uses noise or noise-like signals to barrage or floor the echo of a target; thus, a radar device cannot detect the target. The SNR of the radar-received signal needs to meet the requirements of false alarm probability; in only this case can the radar device detect the target. The rest of this chapter discusses the anti-barrage jamming ability of the chaotic-encrypted radar signal. Consider wideband noise jamming as an example.

#### 1) RANGE CHANNEL

For the range channel, the SNR will decrease severely as the wideband noise jamming power increases, and if the output of the correlator exceeds the preset threshold of the radar device, then the device will yield a false alarm. Therefore, the SNR of the correlator output is discussed to evaluate the anti-barrage jamming ability of the chaotic-encrypted radar signal. Correlation can be realized in the frequency domain by a matched filter. Therefore, the signal is analyzed from the frequency domain for convenience. When the amplitude of $C(t)$ is set to $A_c$, the corresponding frequency spectrum can be expressed as

$$\begin{aligned} C(\omega) &= F(C(t)) = F(A_c\sum_{i=0}^{N-1} P_{\tau_Z}(t-i\tau_Z)C_i) \\ &= \tau_Z A_c \sin c(\frac{\omega\tau_Z}{2})\sum_{i=0}^{N-1} C_i\exp(-j\omega(i\tau_Z+\frac{\tau_Z}{2})) \qquad (15) \end{aligned}$$

The frequency response of the matched filter should be

$$\begin{aligned} H(\omega) &= C^*(\omega) \\ &= \tau_Z A_c \sin c(\frac{\omega\tau_Z}{2})\sum_{i=0}^{N-1} C_i\exp(j\omega(i\tau_Z+\frac{\tau_Z}{2})) \qquad (16) \end{aligned}$$

where $C^*(\omega)$ is the conjugate of $C(\omega)$. According to Eq. (16), the maximum SNR of the correlator output is

$$(\frac{S}{N_o})_{\max} = \frac{2E}{N_0} = \frac{NA_c^2\tau_Z}{N_0} \qquad (17)$$

where $N_o$ is the power spectral density of output noise, and $N_o = \frac{N_0}{4\pi}\int_{-\infty}^{\infty}|C^*(\omega)|^2 d\omega$, $N_0$ is the power spectral density of noise, and $E$ is the energy of $C(\omega)$. As shown in Eq. (17), when $A_c$ is fixed, the SNR of the correlator output is mainly controlled by the length of the encrypted binary sequence $C(t)$ and the width of each chaotic chip. The larger the values of $N$ and $\tau_Z$, the higher the SNR and the stronger the anti-barrage jamming ability of the radar.

#### 2) RADAR ID CHANNEL

For the radar ID channel, the wideband noise jamming is received by the radar antenna and becomes narrowband noise $n(t)$, and the decrypted sequence can be expressed as

$$\begin{aligned} M_n(t) &= D_k(n(t)) \\ &= \Lambda_n(\int_{(n-1)\tau_M}^{n\tau_M} n(t)\oplus\sum_{i=0}^{N-1}P_{\tau_Z}(t-\tau_p-i\tau_Z)z_i(k))dt) \qquad (18) \end{aligned}$$

From Eq. (18), $M_n(t) \neq M(t)$ because $n(t)\exp(j\omega_0 t)$ is not matched with the decryption sequence $\sum_{i=0}^{N-1} P_{\tau_Z}(t-\tau_p-i\tau_Z)z_i(k)$. Therefore, the radar will not be jammed by noise jamming as long as the decrypted sequence is not equal to radar ID, and the probability of being jammed is only $2^{7L}$. However, noise jamming will influence the decryption of the target echo by the bit error rate (BER), which can lead to an incorrect decrypted sequence. A high

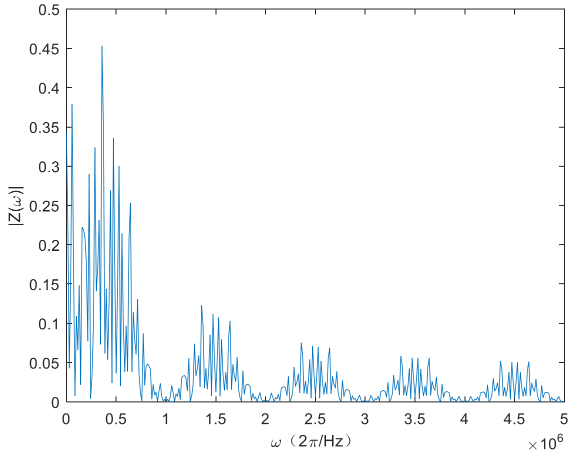


**FIGURE 7.** **Frequency spectrum of binary chaotic code.**

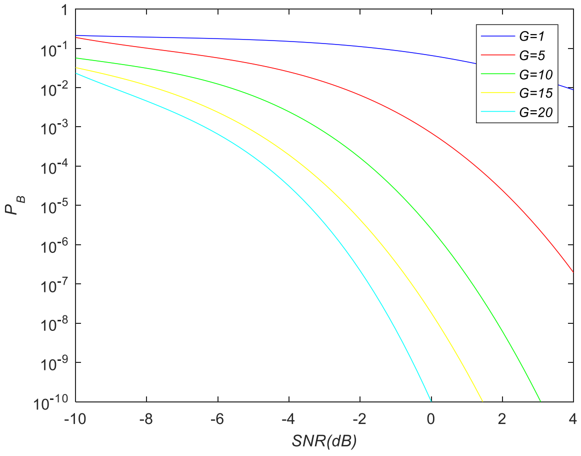


**FIGURE 8.** **Bit error rate at different processing gains.**

BER will result in a low probability of obtaining the correct radar ID through decryption. The BER is relative to the processing gain of the radar system. Therefore, the processing gain and BER are focused on here to evaluate the anti-barrage jamming ability of the chaotic-encrypted radar signal.

The chaotic binary sequences $Z(t)$ also spread the spectrum while encrypting the radar ID. The frequency spectrum of $Z(t)$ is

$$Z(\omega) = \tau_Z \sin c(\frac{\omega\tau_Z}{2}) \cdot \sum_{i=0}^{N-1} z_i \exp(-j\omega(i\tau_Z + \frac{\tau_Z}{2})) \tag{19}$$

For $\tau_Z = 1\mu s$ and $N = 70$, the corresponding frequency spectrum is as shown in Fig. 7.

As shown in Fig. 7, the chaotic binary sequences present a sinc-shaped envelope, and the power of $Z(t)$ is concentrated in the center of the spectrum. Thus, the main lobe width $\Delta f$ is defined as the bandwidth of $Z(t)$, where $\Delta f = \frac{1}{\tau_Z}$. Therefore, the processing gain can be expressed as

$$G = W_z/R_m = \frac{\tau_M}{\tau_Z} \tag{20}$$

where $W_z$ is the bandwidth of the spread spectrum, referring to the bandwidth of $Z(t)$, and $R_m$ is the transmission rate, referring to the transmission rate of the radar ID. Due to the processing gain of the chaotic binary sequences, the power spectral density of the radar signal decreases such that the radar signal has a low probability of intercept, which, for the enemy, increases the difficulty of detecting the radar signal. To make the power spectral density remain unchanged, the power of transmitted jamming must increase to G times the original power. Correspondingly, the cost of jamming will increase.

The modulation method used for the chaotic-encrypted radar signal is BPSK, and the BER is

$$\frac{E_b}{N_0} = G\frac{S}{N_j} \tag{21}$$

$$P_B = Q(\sqrt{\frac{2E_b}{N_0}}) = Q(\sqrt{\frac{2GS}{N_0}}) \tag{22}$$

where $E_b$ is the power of the received signal, $N_0$ is the power spectrum density of noise jamming, $S$ is the power of the received signal, $N_j$ is the power of noise jamming before it is received by the radar, $N_0 = \frac{N_j}{W_z}$, $Q(\cdot)$ is the complementary error function, and $Q(\cdot)$ can be expressed as

$$Q(x) \approx \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{u^2}{2})du \tag{23}$$

where $s = a_g + N_0,\ g = 1, 2\ , a_1 = \sqrt{E_b}, a_2 = -\sqrt{E_b}$, and $u = (s - a_2)/\sqrt{\frac{N_0}{2}}$. Fig. 8 shows that, at different processing gains, the BER is low at different SNRs; hence, the radar ID channel possesses a strong anti-barrage jamming ability. As the SNR increases, the BER decreases rapidly. At the same SNR, the higher the gain is, the lower the BER and the stronger the anti-barrage jamming ability.

### *B. ANTI-MUTUAL INTERFERENCE ABILITY*

With the widespread use of radar, the probability of mutual interference has increased rapidly because of signal overlap in time, space and frequency, especially when the radar devices are of the same type. When two radar signals have similar parameters, as shown in Fig. 9, the signal generated by one radar device may be mistaken for a true target by another, which is similar to deceptive jamming. Obviously, mutual interference is also a kind of jamming and has a negative effect on radar, although it is generated unintentionally. Therefore, the anti-mutual interference ability is analyzed in the remainder of this chapter based on the assumption that radar A and radar B are of the same type but have different radar IDs. The range channel and radar ID channel are both discussed.

#### 1) RANGE CHANNEL

A signal from the transmitter of radar B may be received by radar A through reflection of direct coupling. Radar A may mistake this signal as a target echo and be deceived in both range and velocity. For chaotic-encrypted radar, the mutual

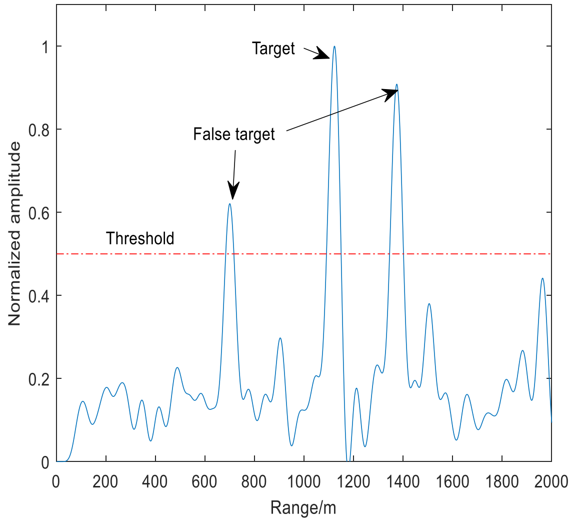


**FIGURE 9.** **False target caused by mutual interference.**

interference signal from radar B can be expressed as

$$S_j(t) = A_j \exp(j(\omega_j(t-\Delta\tau_j) + \pi C^B(t-\Delta\tau_j) + \varphi_j)) \\ \cdot[P_{T_m}(t-\Delta\tau_j) \otimes \sum_{-\infty}^{\infty} \delta(t-KT_r)] \tag{24}$$

where $A_j$ is the amplitude of mutual interference from B, $\omega_j$ is the angular frequency of the carrier wave of radar B, $\Delta\tau_j$ is the transmission delay, $C^B(t-\Delta\tau_j)$ is the chaotic-encrypted binary sequences of radar B, and $\varphi_j$ is the original phase of the mutual interference.

Then, the mutual interference from B is mixed with the local oscillator signal from radar A, and the output signal is

$$S_{jm}(t) = K_m A_j \exp(j((\omega_0-\omega_j)t + \omega_j\Delta\tau_j + \varphi_j \\ +\pi C^B(t-\Delta\tau_j))) \cdot [P_{T_m}(t-\Delta\tau_j) \otimes \sum_{-\infty}^{\infty} \delta(t-KT_r)] \tag{25}$$

Then, $S_{jm}(t)$ is processed in the radar correlator with the reference chaotic-encrypted binary sequences $C^A(t-\tau_p)$ of radar A, the output signal of which is

$$\begin{aligned} u_j(t) &= \frac{1}{T_m}\int_0^{T_m} S_{jm}(t)C^A(t-\tau_p)dt \\ &= K_j \int_0^{T_m} \exp(j(\Delta\omega t + \omega_0\Delta\tau_j + \varphi_j \\ &\quad +\pi(C^B(t-\Delta\tau_j) + C^A(t-\tau_p))))dt \end{aligned} \tag{26}$$

where $K_j = \frac{K_m A_j}{T_m}$, $\Delta\omega = \omega_0 - \omega_j$, and $R_{AB}(\cdot)$ is the cross-correlation function of the local reference signal from radar A and mutual interference from radar B. The cross-correlation function $R_{AB}(\cdot)$ can be expressed as

$$R_{AB}(b) = \frac{1}{N}\sum_{i=1}^{N-b} \exp(j\pi(C_i^A + C_{i+b}^B)), \\ b = 0, 1, \ldots N-1 \tag{27}$$

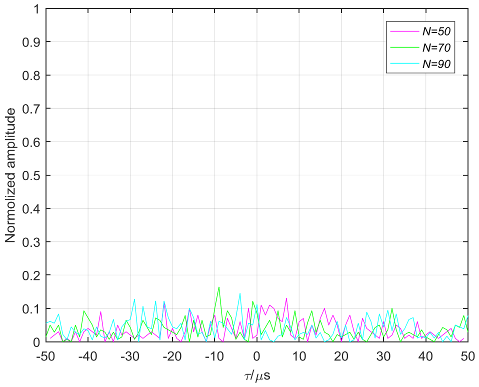


**FIGURE 10.** **Cross-correlations.**

When $\Delta\omega \ll \frac{\pi}{T_m}$, Eq. (26) can be simplified as

$$\begin{aligned} u_j(t) &= K_j \int_0^{T_m} \exp(j\pi C^B(t-\Delta\tau_j) + C^A(t-\tau_p))dt \\ &\quad \cdot \exp(j(\Delta\omega t + \omega_0\Delta\tau_j + \varphi_j)) \\ &= K_j R(\Delta\tau_j - \tau_p)\exp(j(\Delta\omega t + \omega_0\Delta\tau_j + \varphi_j)) \end{aligned} \tag{28}$$

As shown in Eq. (28), the amplitude of the output signal of the radar correlator is mainly influenced by $R_{AB}(\cdot)$ since $K_j$ is fixed.

In this case, the anti-deceptive jamming ability mainly depends on the cross-correlation peak. The cross-correlation function at different code lengths is shown in Fig. 10.

As shown in Fig. 10, the cross-correlation peaks at different code lengths are all less than 0.2, indicating that the range channel has a good anti-mutual interference ability when the power of the mutual interference is limited because of the low cross-correlation peak. However, as the jamming power increases, the anti-mutual interference ability decreases, and the mutual interference is still able to form a false target, as shown in Fig. 9, because of the coefficients of the cross-correlation functions.

### 2) RADAR ID CHANNEL

To solve the problem that occurs when the mutual interference power is high, the radar ID is effectively applied. For the radar ID channel, $S_{jm}(t)$ is decrypted with the reference chaotic binary sequences of radar A, the decrypted sequences of which are

$$\begin{aligned} M_j(t) &= D_k(S_{jm}(t)) \\ &= \Lambda_n(\int_{(n-1)\tau_M}^{n\tau_M} (S(K_m A_j \exp(j\pi\sum_{i=0}^{N-1} P_{\tau_Z}(t-\Delta\tau_j-i\tau_Z)C_i^B))\cdots \\ &\quad \oplus \sum_{i=0}^{N-1} P_{\tau_Z}(t-\tau_p-i\tau_Z)z_i^A(k)\exp(j(\Delta\omega t+\omega_0\Delta\tau_j+\varphi_j)))dt) \\ &= \Lambda_n(\int_{(n-1)\tau_M}^{n\tau_M} M^B(t) \oplus \sum_{i=0}^{N-1} P_{\tau_Z}(t-\Delta\tau_j-i\tau_Z)z_i^B(k)\cdots \\ &\quad \oplus \sum_{i=0}^{N-1} P_{\tau_Z}(t-\tau_p-i\tau_Z)z_i^A(k)\exp(j(\Delta\omega t+\omega_0\Delta\tau_j+\varphi_j)))dt) \end{aligned} \tag{29}$$

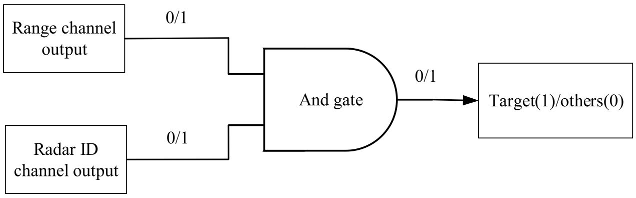


**FIGURE 11.** Block diagram of the dual-channel antijamming method.

where $M^B$ is the ID of radar B, $z_i^B$ is the chaotic binary sequences of radar B, and $z_i^A$ is the reference chaotic binary sequences of radar A. When $M_j(t)$ is converted to $L \times$ 7-bit ASCII code $M_j$ by the decoder, according to Eq. (29), when $\Delta\omega \ll \frac{\pi}{T_m}$, $M_j$ is related to only $\Delta\tau_j$ regardless of the jammer power. Thus, two cases exist. In one case, $\Delta\tau_j \neq \tau_p$ or $z_i^B \neq z_i^A$. In this case, the decryption chaotic binary sequences are inconsistent with the encryption sequences; thus, the decrypted ID $M_j \neq M^A$. In the other case, $\Delta\tau_j = \tau_p$ and $z_i^B = z_i^A$. In this case, $M_j \neq M^A$ because the ID $M^B$ of radar B is not equal to the ID $M^A$ of radar A, indicating that radar A can identify the true target and false target caused by mutual interference from radar B through the unique ID that radar A possesses. In the same way, the radar can also identify the mutual interference from radar A through the radar ID that radar B owns.

Furthermore, the decryption of $M_j(t)$ is unrelated to the mutual interference power, as shown in Eq. (26), indicating that the radar ID channel can effectively achieve anti-mutual interference regardless of the mutual interference power. Therefore, due to the unique ID possessed by each radar, the radar ID channel has a strong anti-mutual interference ability even if the jamming-to-signal ratio is high, which is difficult to attain by a traditional phase-coded pulse compression radar.

### C. DUAL-CHANNEL ANTIJAMMING METHOD

Although both channels perform well in terms of antijamming ability, the combination of the two channels to further improve the antijamming ability is still useful. Therefore, a dual-channel method is proposed, which means that the outputs of two channels are combined for the final antijamming decision. The block diagram of the dual-channel antijamming method is shown in Fig. 11.

When the output of the range channel exceeds a preset threshold, the output is set to 1; otherwise, the output is set to 0. When $M_j = M$, the output is set to 1; otherwise, the output is set to 0. Then, the two channels are combined to achieve further antijamming. If the probability of interference is $p_1$ in the range channel, and if the probability of interference is $p_2$ in the radar ID channel, then the probability of interference with the dual-channel antijamming method will be

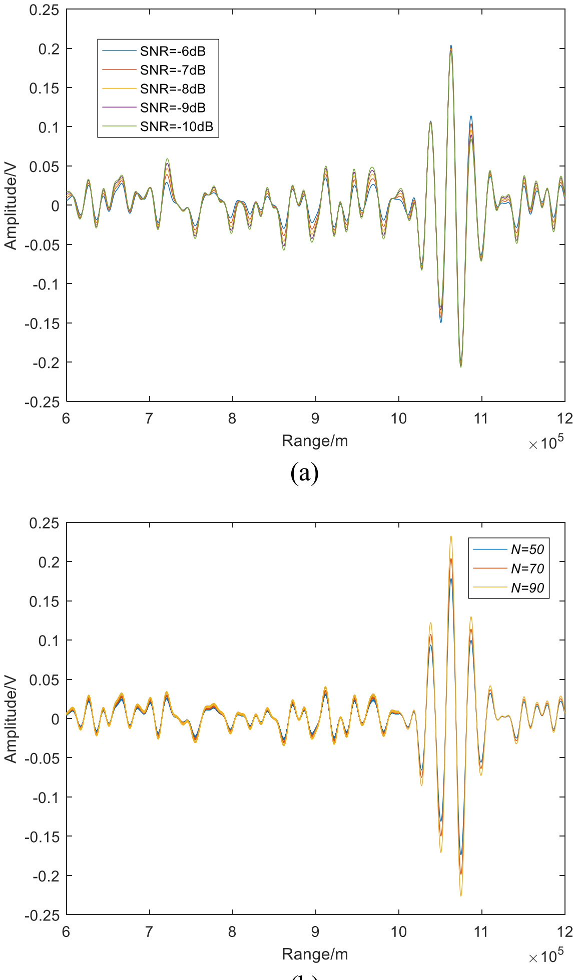
$$P_{12} = p_1 p_2 \tag{30}$$

As shown in Eq. (30), the probability of interference reduces to $p_1 p_2$ from $p_1$ because of the dual-channel antijamming method. Combining two channels can significantly improve the antijamming ability of chaotic-encrypted radar.

**TABLE 1.** Simulation parameters.

| Parameter | Value |
|---|---|
| $a$ | 3.8~4.0 |
| $x_0$ | 0.4~0.6 |
| $L$ | 1 |
| $\tau_M$ /μs | 0.2 |
| $A_t$ /V | 1 |
| $A_r$ /V | 0.5 |
| $\varphi_0$ /rad | $0 \sim \pi/2$ |
| $\tau_Z$ /ns | 20 |
| $N$ | 50~90 |
| $T_m$ /μs | 1.0~1.8 |
| $T_r$ /μs | 2.0~3.6 |
| $K_m$ | 1 |
| $\varphi_r$ /rad | $0 \sim \pi/2$ |
| $A_j$ /V | 1 |
| $\omega_0/2\pi$ /MHz | 100 |
| $\omega_j/2\pi$ /MHz | 100 |
| $\omega_d/2\pi$ /kHz | 10 ~80 |
| $\varphi_j$ /rad | $0 \sim \pi/2$ |
| $SNR$ /dB | -10~-6 |
| $JSR$ | -5~4 |
| ID of radar A ($M^A$) | 'T' |
| ID of radar B ($M^B$) | 'F' |
| ID of radar C ($M^C$) | 'N' |

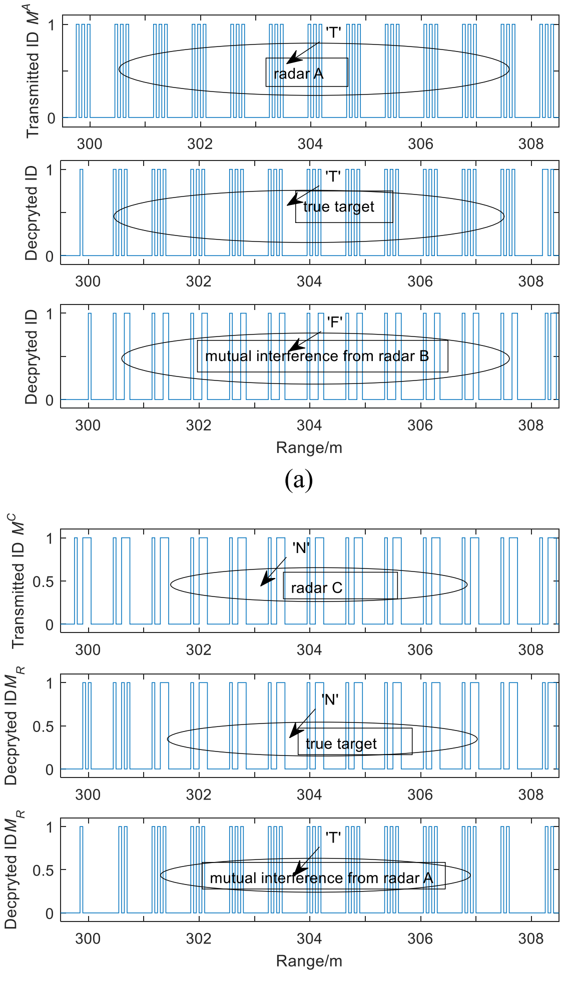
Above all, chaotic-encrypted radar performs well in terms of antijamming ability. The antijamming ability is mainly influenced by the length of the chaotic binary sequences, processing gain, BER, autocorrelation function, cross-correlation function and length of the radar ID.



(a)

(b)

**FIGURE 12. (a) Output of chaotic-encrypted radar correlator in the range channel at different SNRs; (b) Output of chaotic-encrypted radar correlator in the range channel at different code lengths.**



(a)

(b)

**FIGURE 13. (a) Output of chaotic-encrypted radar in radar ID channel at −10 dB SNR, 10 KHz Doppler frequency; (b) Output of chaotic-encrypted radar in radar ID channel at −10 dB SNR, 80 KHz Doppler frequency.**

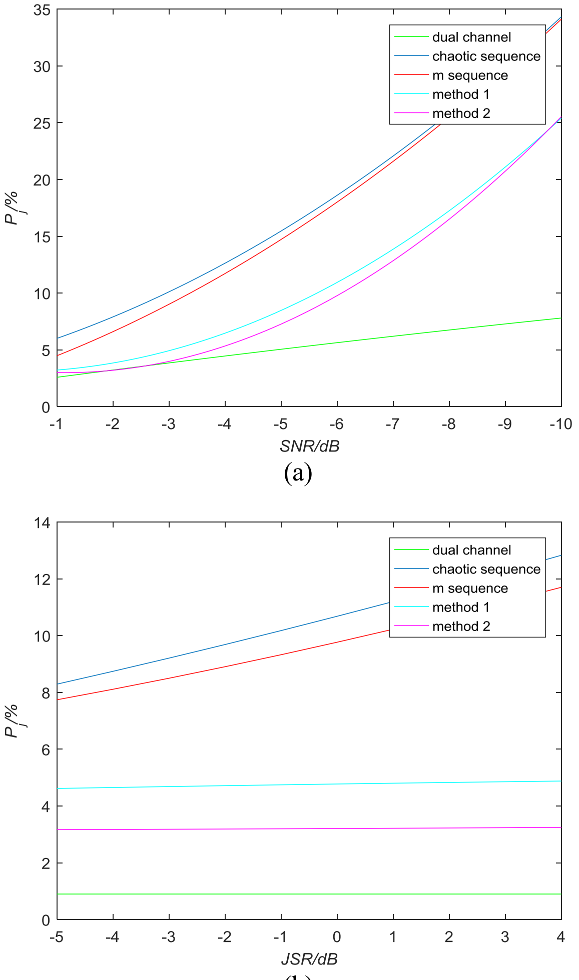
## VI. SIMULATION AND DISCUSSION

The simulation parameters of the chaotic-encrypted radar signal are shown in Table 1.

To verify the anti-barrage jamming ability of the proposed chaotic-encrypted radar, additive wideband noise jamming is added to the simulation, and the SNR is set to −10 dB. Then, the range channel output of the chaotic-encrypted radar is as shown in Fig. 12.

As shown in Fig. 12 (a), due to the processing gain of chaotic binary sequences, the range envelopes are obvious and stable at different SNRs. In Fig. 12 (b), the range envelopes are different because of the different processing gains caused by the different code lengths. This observation indicates that chaotic-encrypted radar can clearly recognize the target echo under noise jamming. The range envelope width of the correlator is approximately 3 m, which is consistent with the theoretical resolution $\frac{\tau_Z c}{2}$.

Regarding the mutual interference, radar devices A, B, and C are used to test the anti-mutual interference ability of chaotic-encrypted radar. The ID of radar A is 'T', the ID of B is 'F', and that of radar C is 'N'. Assume that the decryption chaotic sequences and time delay of A are the same as those of B and C. As shown in Fig. 13 (a), the Doppler frequency is 10 KHz, and radar A receives a signal, which may be the true target echo transmitted by radar A or a false target caused by mutual interference from radar B. Then, the received signal is decrypted by radar A, which can efficiently recognize the true target and the false target by comparing the decrypted ID with its own ID $M^A$. The decrypted ID of the true target is 'T', which is identical to the ID of radar A. However, the decrypted ID of mutual interference is 'F', which is inconsistent with the ID of radar A; hence, radar A recognizes this signal as mutual interference. In Fig. 13 (b), the Doppler frequency is 80 KHz; radar C identifies the target echo and mutual interference from radar A as well, but the high Doppler frequency has already slightly influenced the decryption of the radar ID. Thus, the proposed radar signal is more suitable for targets at low speed. The simulation results show that the chaotic-encrypted radar has a strong anti-mutual interference ability because of the use of unique radar IDs.



(a)

(b)

**FIGURE 14. (a) Probability of interference at different powers of barrage jamming; (b) Probability of interference at different powers of mutual interference.**

Meanwhile, to further evaluate the ability of anti-barrage jamming and mutual interference of the dual-channel antijamming method under different amounts of jamming power, the simulation compares the dual-channel antijamming method proposed in this paper with a traditional pulse compression signal using m sequences and a chaotic sequence. Empirical mode decomposition (method 1) and the quadratic time-frequency analysis method (method 2) for SEI in references [29] and [30] are also compared. The results are shown in Fig. 14.

$P_j$ is the probability of interference. As shown in Fig. 14 (a), as the barrage noise power increases, the SNR decreases from $-1$ dB to $-10$ dB, the $P_j$ values of the chaotic sequence, m sequence and method 1, and method 2 increase to more than 25%. but the $P_j$ value of the dual-channel method is still lower than 10%, The reason is that the processing gains of the m sequence and chaotic sequence are limited, and the specific features of the radar signal are hard to extract at low SNR. When the jamming power is high, the radar correlator cannot restrain the jamming or mutual interference effectively, and the specific features of radar signals are influenced by noise; thus, the probability of interference increases rapidly. In Fig. 14 (b), with the increasing power of mutual interference, the jamming-to-signal ratio (JSR) increases from $-5$ dB to 4 dB, the $P_j$ values of the chaotic sequence and m sequence increase to more than 10%, but the $P_j$ values of dual channels, method 1 and method 2 remain low, especially for the dual channels method, for which it is less than 1% and remains stable. Therefore, the dual channel method performs much better than the method mentioned above due to the unique radar ID and chaotic encryption sequences.

## VII. CONCLUSION

This paper proposes a novel antijamming method for pulse compression radar based on radar ID and chaotic encryption. The thumbtack-shaped ambiguity function shows the high resolution of the radar signal. The received signal is divided into a range channel and a radar ID channel. The signal processing methods and antijamming ability of the two channels are analyzed separately, and both channels perform well in terms of antijamming and mutual interference. Moreover, the antijamming ability can be further improved by combining the outputs of the channels. The simulation result verifies the theoretical analyses. The proposed radar signal and antijamming method perform much better than the traditional pseudorandom pulse compression signal.

## REFERENCES

[1] O. Akay and E. Erözden, "Employing fractional autocorrelation for fast detection and sweep rate estimation of pulse compression radar waveforms," *Signal Process.*, vol. 89, no. 12, pp. 2479–2489, Dec. 2009.

[2] X. Fan, T. Li, and S. Su, "Intrapulse modulation type recognition for pulse compression radar signal," *J. Appl. Remote Sens.*, vol. 11, no. 3, p. 1, Sep. 2017.

[3] P. Ghelfi, F. Scotti, F. Laghezza, and A. Bogoni, "Photonic generation of phase–modulated RF signals for pulse compression techniques in coherent radars," *J. Lightw. Technol.*, vol. 30, no. 11, pp. 1638–1644, Jun. 1, 2012.

[4] S. Libing, C. Xinnian, and G. Bo, "Integrated design on digital channelized reconnaissance and jamming," in *Proc. IEEE CIE Int. Conf. Radar*, Oct. 2011, pp. 238–241.

[5] S. K. Liu, X. P. Yan, and L. I. Ping, "Design of jamming signal on pseudo-random code phase-modulation and pulse Doppler combined fuze based on code reconstruction," *Acta Armamentarii*, vol. 39, no. 6, pp. 1088–1094, 2018.

[6] T. W. Tedesso and R. Romero, "Code shift keying based joint radar and communications for EMCON applications," *Digit. Signal Process.*, vol. 80, pp. 48–56, Sep. 2018.

[7] S. Zhang and G. F. Pedersen, "Mutual coupling reduction for UWB MIMO antennas with a wideband neutralization line," *IEEE Antennas Wireless Propag. Lett.*, vol. 15, pp. 166–169, 2016.

[8] J. Malmstrom, H. Holter, and B. L. G. Jonsson, "On mutual coupling and coupling paths between antennas using the reaction theorem," *IEEE Trans. Electromagn. Compat.*, vol. 60, no. 6, pp. 2037–2040, Dec. 2018.

[9] T. Thayaparan, M. Daković, and L. Stanković, "Mutual interference and low probability of interception capabilities of noise radar," *IET Radar, Sonar Navigat.*, vol. 2, no. 4, pp. 294–305, Aug. 2008.

[10] G. Brooker, "Mutual interference of millimeter–wave radar systems," *IEEE Trans. Electromagn. Compat.*, vol. 49, no. 1, pp. 170–181, Feb. 2007.

[11] B. Chen, "Foundational research on applications of Chaos to time-varying parameter secure communication and radar signal design," Ph.D. dissertation, Univ. Electron. Sci. Technol., Chengdu, China, 2007, pp. 1–13.

[12] J.-C. Gan, "Chaotic signal processing with application to radar and communication countermeasures," Ph.D. dissertation, Univ. Electron. Sci. Technol., Chengdu, China, 2004, pp. 1–19.

[13] Y. Quan, Y. Li, W. Hu, Y. Zhai, and M. Xing, "FM sequence optimisation of chaotic-based random stepped frequency signal in through-the-wall radar," *IET Signal Process.*, vol. 11, no. 7, pp. 830–837, Sep. 2017.

[14] D. Hambling, "Chaos radar uses messy signals to see through walls," *New Scientist*, vol. 211, no. 2822, pp. 16–17, Jul. 2011.

[15] Y. Jin, N. Lei, and Q. Zhaokun, "Frequency modulated radar waveform based on sampled chaotic series," *Chin. J. Electron.*, vol. 22, no. 2, pp. 426–432, 2013.

[16] T. Zeng, S. Chang, H. Fan, and Q. Liu, "Design and processing of a novel chaos–based stepped frequency synthesized wideband radar signal," *Sensors*, vol. 18, no. 4, p. 985, Mar. 2018.

[17] X. Wu, W. Liu, L. Zhao, and J. S. Fu, "Chaotic phase code for radar pulse compression," in *Proc. IEEE Radar Conf.*, May 2001, pp. 279–283.

[18] J.-H. Choi, H.-B. Lee, J.-W. Choi, and S.-C. Kim, "Mutual interference suppression using clipping and weighted–envelope normalization for automotive FMCW radar systems," *IEICE Trans. Commun.*, vol. E99.B, no. 1, pp. 280–287, 2016.

[19] M. Barjenbruch, D. Kellner, K. Dietmayer, J. Klappstein, and J. Dickmann, "A method for interference cancellation in automotive radar," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Apr. 2015, pp. 1–4.

[20] S. Neemat, O. Krasnov, and A. Yarovoy, "An interference mitigation technique for FMCW radar using beat-frequencies interpolation in the STFT domain," *IEEE Trans. Microw. Theory Techn.*, vol. 67, no. 3, pp. 1207–1220, Mar. 2019.

[21] Y. L. Sit, B. Nuss, and T. Zwick, "On mutual interference cancellation in a MIMO OFDM multiuser radar–communication network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3339–3348, Apr. 2018.

[22] Z. Yifan, Z. Huilin, and Z. Fuhui, "Resource allocation for a wireless powered integrated radar and communication system," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 253–256, Feb. 2019.

[23] C. Aydogdu, N. Garcia, L. Hammarstrand, and H. Wymeersch, "Radar communications for combating mutual interference of FMCW radars," in *Proc. IEEE Radar Conf. (RadarConf)*, Boston, MA, USA, Apr. 2019, pp. 1–6.

[24] T. L. Carroll, "A nonlinear dynamics method for signal identification," *Chaos*, vol. 17, no. 2, Jun. 2007, Art. no. 023109.

[25] X. Dan, "Research on mechanism and methodology of specific emitter identification," Ph.D. dissertation, Nat. Univ. Defense Technol., Hunan, China, 2008, pp. 13–31.

[26] H. Tao, "Research on radar emitter identification," Ph.D. dissertation, Nat. Univ. Defense Technol., Hunan, China, 2013, pp. 14–31.

[27] W. U. Bajwa, K. Gedalyahu, and Y. C. Eldar, "Identification of parametric underspread linear systems and super–resolution radar," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2548–2561, Jun. 2011.

[28] S. D'Agostino, G. Foglia, and D. Pistoia, "Specific emitter identification: Analysis on real radar signal data," in *Proc. Eur. Radar Conf.*, Oct. 2009, pp. 242–245.

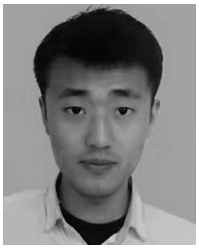
[29] C. Song, J. Xu, and Y. Zhan, "A method for specific emitter identification based on empirical mode decomposition," in *Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Secur.*, Beijing, China, Jun. 2010, pp. 25–27.

[30] L. Li, H. B. Ji, and L. Jiang, "Quadratic time-frequency analysis and sequential recognition for specific emitter identification," *IET Signal Processing*, vol. 5, no. 6, p. 1, 2011.

[31] J. Wen, C. Ying, and Y. Lin, "A time-space domain information fusion method for specific emitter identification based on dempster-Shafer evidence theory," *Sensors*, vol. 17, no. 9, p. 1972, 2017.

[32] S. Hassan, A. Bhatti, and A. Latif, "Emitter recognition using fuzzy inference system," in *Proc. IEEE Symp. Emerg. Technol.*, Dec. 2005, pp. 204–208.

[33] T. Kohda and A. Tsuneda, "Statistics of chaotic binary sequences," *IEEE Trans. Inf. Theory*, vol. 43, no. 1, pp. 104–112, Jan. 1997.



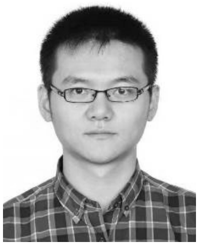
**JIAN DAI** was born in Anhui, China, in 1994. He received the B.S. degree in mechatronic engineering from the Beijing Institute of Technology, China, in 2015, where he is currently pursuing the Ph.D. degree in intelligent detection and control. His research interests include signal processing, proximity radar detection theory, and ECM.

**XINHONG HAO** was born in Henan, China, in 1974. She received the Ph.D. degree in mechatronic engineering from the Beijing Institute of Technology, in 2007.

She is currently an Associate Professor with the Beijing Institute of Technology. Her main research interests include target detection theory of radio sensor signal processing, real-time signal processing, and time-frequency analysis.

**PING LI** received the B.S. and M.S. degrees in mechantronical engineering from Dalian Jiaotong University, Dalian, China, in 1985 and 1987, respectively, and the Ph.D. degree from the Beijing Institute of Technology, China, in 1995.

In September 1996, she joined the School of Mechatronical Engineering, Beijing Institute of Technology, China. Her research interests include radio detection, proximity sensor signal processing, and information countermeasures in wireless systems.



**ZE LI** was born in Hebei, China, in 1989. He received the Ph.D. degree in armament science and technology from the Beijing Institute of Technology, in 2018.

He is currently an Electronic Engineer with the Beijing Institute of Technology. His main research interests include electronic countermeasures, radio sensor target detection theory, radar signal processing, and time-frequency analysis.

**XIAOPENG YAN** received the B.E. degree in mechanical and electronic engineering, the M.E. degree in pattern recognition and intelligent systems, and the Ph.D. degree in mechanical and electronic engineering from the Beijing Institute of Technology, Beijing, China, in 1999, 2003, and 2009, respectively.

He is a Professor with the School of Mechatronical Engineering, Beijing Institute of Technology, where he has been a Faculty Member, since 2003. His research interests include radio detection and signal processing of proximity sensors.