RF Steganography via LFM Chirp Radar Signals

ZHIPING ZHANG, Member, IEEE
YANG QU, Member, IEEE
ZHIQIANG WU, Senior Member, IEEE
Wright State University, Dayton, OH, USA

MICHAEL J. NOWAK, Member, IEEE
JOHN ELLINGER
Wright-Patterson Air Force Base, Dayton, OH, USA

MICHAEL C. WICKS, Fellow, IEEE
Air Force Research Laboratory, Dayton, OH, USA

A novel radio frequency (RF) steganography scheme is proposed to hide digital communication in linear frequency modulation (LFM) radar signals. This joint radar/communication waveform serves two purposes simultaneously: it performs as the original radar waveform, and it provides a covert communication to legitimate receivers. The proposed RF steganography scheme hides digitally modulated communication information inside an LFM radar signal to prevent enemy from detecting the existence of such hidden information via a new modulation and variable symbol duration design.

Manuscript received November 7, 2015; revised May 22, 2016 and December 14, 2016; released for publication January 3, 2017. Date of publication November 22, 2017; date of current version June 7, 2018.

DOI. No. 10.1109/TAES.2017.2776698

Refereeing of this contribution was handled by J. Wallace.

This work was supported in part by the National Science Foundation under Grant 1323240 and Grant 1748494 and in part by the Air Force Research Laboratory.

Authors' addresses: Z. Zhang, Y. Qu, and Z. Wu are with the Department of Electrical Engineering, Wright State University, Dayton, OH 45435 USA, E-mail: (Zhang.176@wright.edu; Qu.10@wright.edu; Zhiqiang.wu@wright.edu); M. J. Nowak and J. Ellinger are with the Sensors Directorate Air Force Research Laboratory, Wright-Patterson Air Force Base, Dayton, OH 45433 USA, E-mail: (Michael.nowak.2@us.af.mil; john.ellinger@us.af.mil); M. C. Wicks is with the Spectral Warfare Division of Sensors Directorate, Air Force Research Laboratory, Dayton, OH 45469 USA, Email: (Michael.Wicks@udri.udayton.edu). *(Corresponding author: Zhiqiang Wu.)*

I. INTRODUCTION

In military operations and other covert operations, it is highly desirable to prevent the enemy and other parties from detecting the existence of radio frequency (RF) communication. Many researchers have proposed to develop low probability of detection (LPD) RF waveforms by making the power spectral density (PSD) lower than the noise floor through spread spectrum technologies, such as direct-sequence spreading spectrum or frequency hopping [1], or by exploiting noise like signals, such as chaotic signals to carry information [2], or both [3].

However, existing LPD waveforms do not provide true LPD capability when new advanced detection schemes, such as cyclostationary analysis are exploited. Cyclostationary analysis has been accepted as an important tool to perform signal detection, signal parameter estimation, and modulation detection of RF signals [4]–[11]. Cyclostationary analysis is based on the fact that most man-made signals are not accurately described as stationary, but rather more appropriately modeled as cyclostationary. While stationary signals have statistics that remain constant in time, the statistics of cyclostationary signals vary periodically. These periodicities occur for signals of interest in well defined manners due to underlying periodicities, such as modulation. The resulting periodic nature of such signals can be exploited to detect the existence of the signal, estimate important parameters of the signal, and determine the modulation scheme of the unknown signal.

Employing a cyclostationary analysis based detection algorithm, all existing LPD waveform designs become vulnerable: First of all, noise has no cyclostationary features. Therefore, cyclostationary analysis such as spectral correlation function (SCF) and spectral coherence function are resistant to noise. As a direct result, even if the RF signal has minimal transmission power, cyclostationary analysis will exhibit clear features for the enemy's detector to exploit. More importantly, using noise-like signals to hide the existence of digital communication would not work either. As long as conventional digital modulation exists, a cyclostationary analysis will exhibit a strong feature at the symbol rate.

In this paper, we propose an interesting and underinvestigated approach to hide the communication. The idea is not to hide the waveform itself through conventional LPD designs, but to hide the communication in another form of RF transmission. We call this RF steganography. Recently, the United States has recognized the importance of spectrum sharing and coexistence of not only communication systems, but also other RF systems [12]–[14]. For example, defense advanced research projects agency (DARPA) launched its new shared spectrum access for radar and communications (SSPARC) program in 2015 to investigate spectrum sharing both between military radar and military communication systems ("military/military sharing") and between military radar and commercial communication systems ("military/commercial sharing") [15]. The SSPARC treats spectrum sharing as a cooperative problem and aims to enable spectrum sharing between radar and communication systems through collaboration and information exchange between such systems. At the same time, there has been a growing interest in the area of cooperative radar and communication where a joint waveform is designed to serve both the radar function and communication function (e.g., [16]–[18]) or joint sensing and communications (e.g., [19]) simultaneously. However, to the best of our knowledge, these jointly designed radar/communication systems are not aimed for information hiding or RF steganography purposes.

In this paper, we discuss a novel RF steganography scheme to hide communication in an LFM chirp radar signal [20]. The newly designed linear frequency modulation (LFM) chirp signal will serve two purposes simultaneously: it is still a radar signal providing radar functions for its original radar operators, however, it also carries secure digital communication information intended for designated receivers. We first provide a review of the LFM chirp signal and conventional LFM chirp based communications. Then, we discuss how to use a new modulation called reduced phase shift keying (RPSK) and system designs to make the LFM chirp signal with embedded communication information nearly identical to the original radar signal without any indication of the embedded digital modulation. This will enable the radar operator similar radar performances, and it will also ensure that it is very difficult for the enemy to detect the existence of the hidden communication signal embedded in the radar signal.

The rest of the paper is organized as follows: In Section II, we review the LFM chirp radar signal and conventional LFM chirp based communication schemes. Section III discusses the RF steganography scheme by using a novel RPSK modulation. In Section IV, we further enhance the security of the scheme by introducing variable symbol duration and modulation design. Most importantly, we demonstrate that the newly designed RF steganography scheme eliminates cyclostationary features that could be used by the enemy to detect the existence of the digital modulation. In Section V, we evaluate the ambiguity functions of unmodulated and modulated LFM chirp signals to evaluate the impact on radar performance. The conclusion follows.

II. LINEAR CHIRP FOR RADAR AND COMMUNICATION

A. LFM Chirp Waveform

The linear chirp signal, or LFM signal, is widely used in sonar and radar systems [20]. A linear chirp is a signal, in which the frequency linearly increases (up-chirp) or decreases (down-chirp) with time. Fig. 1 illustrates a typical LFM chirp signal and its corresponding autocorrelation function response.

As can be seen clearly from the figures, the instantaneous frequency $f(t)$ varies linearly with time: $f(t) = f_0 + kt$, where f_0 is the starting frequency, and k is the rate of frequency increase or chirp rate. When k is larger than 0, the signal is an up-chirp; when k is less than 0, the signal is a down-chirp. Mathematically, the LFM chirp signal corresponds to

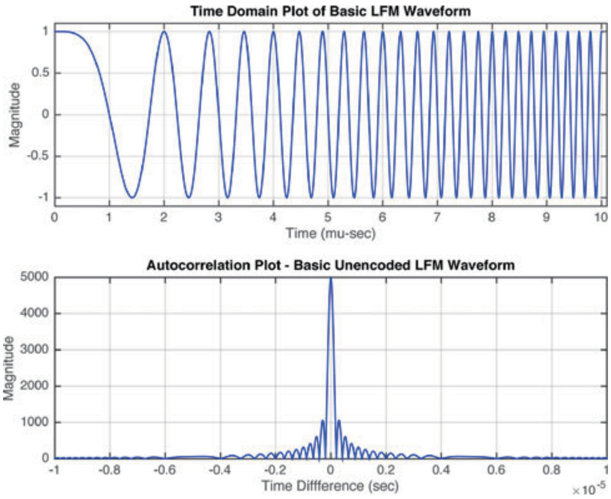


Fig. 1. LFM chirp signal and autocorrelation function.

$$x(t) = A_c \cos\left(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \phi_I\right), \qquad 0 \le t \le T \tag{1}$$

where A_c is the amplitude of the LFM chirp signal, ϕ_I is the initial phase of the chirp signal, and T is the duration of the LFM chirp pulse. At time T, the stopping frequency of the LFM chirp signal is simply $f_1 = f_0 + kT$.

B. LFM Based Communication Waveforms

The inherent capability of interference rejection makes the chirp signal very attractive to spread spectrum communication systems as well, where a significant advantage is the low Doppler sensitivity. So, it is no surprise that many researchers have conducted research in using chirp signals for communication purposes.

The first communication scheme employing chirp signals is called chirp modulation. Chirp modulation was patented by Sidney Darlington in 1954 [21] with significant later work performed by Winkler in 1962 [22]. The idea of chirp modulation is very simple: binary data is transmitted by mapping the bits into up-chirps and down-chirps. For instance, over one bit period "1" is assigned a chirp with positive rate k and "0" a chirp with negative rate $-k$.

In chirp modulation, only one bit is transmitted on one chirp signal. To increase the data rate and transmit multiple bits on one chirp signal, it is natural to use a shorter symbol duration and modulate multiple information bits sequentially onto the chirp signal [23]. Fig. 2 illustrates an example of such a combination of digital binary phase shift keying (BPSK) and chirp modulation. Fig. 2(a) shows the unmodulated chirp signal with length 3, Fig. 2(b) shows the baseband 2PAM signal where three binary bits (1 0 1) are represented by antipodal amplitudes (+1 or −1), and Fig. 2(c) shows the modulated chirp signal.

This modulation can be done by simply multiplying the baseband binary pulse amplitude modulation (2PAM)

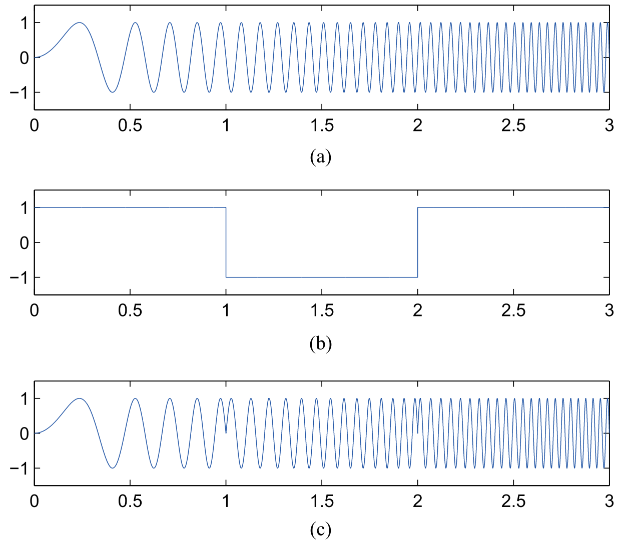


Fig. 2. BPSK Modulated chirp signal. (a) Unmodulated chirp signal. (b) Binary data. (c) Binary modulated chirp signal.

signal [see Fig. 2(b)] with the original chirp signal. Mathematically, the BPSK modulated chirp signal is

$$\begin{aligned} s(t) = a(t) \cdot x(t) &= \sum_{i=0}^{N-1} b_i p(t - iT_b) \cdot x(t) \\ &= \sum_{i=0}^{N-1} b_i p(t - iT_b) \cdot A_c \cos\left(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \phi_I\right) \end{aligned} \tag{2}$$

where $a(t)$ is the baseband 2PAM signal containing N bits, b_i is the ith information bit and $b_i \in \{+1, -1\}$, $p(t)$ is a rectangular pulse with unit height and duration T_b, and since we are transmitting N bits over one LFM chirp waveform, $T = NT_b$.

It is important to note that the multiplication of the baseband 2PAM signal with the LFM chirp signal is equivalent to introducing a 0 or π phase offset to the unmodulated chirp signal at different data symbols

$$s(t) = \sum_{i=0}^{N-1} p(t - iT_b) \cdot A_c \cos\left(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \theta_i + \phi_I\right) \tag{3}$$

where $\theta_i = 0$ if $b_i = 1$, and $\theta_i = \pi$ if $b_i = -1$.

As can be seen in Fig. 2(c), phase reversal occurs when two adjacent data bits are different. As a direct result, the BPSK modulated chirp signal is very different from the unmodulated chirp signal. Therefore, the enemy can easily recognize that there is digital modulation in the chirp signal.

To enhance the communication performance, pseudonoise spreading was proposed to be combined with the chirp modulated signal. This scheme was first proposed by Baier *et al.* [24] and Kowatsh *et al.* [25], [26] and termed pseudonoise-chirp (PN-chirp). The idea is also quite straightforward: A pseudonoise spreading code with M chips is used to represent one data symbol in a chirp modulated signal. This way, a processing gain M of the spread spectrum is exploited and offers a significant performance gain to the chirp modulated communication system. In the PN-chirp signal, the baseband signal is a direct-sequence spread spectrum signal

$$y(t) = \sum_{i=0}^{P-1} b_i c(t - iT_b) \tag{4}$$

where $c(t)$ is the pseudonoise spreading code with M chips with chip duration $T_c = \frac{T_b}{M}$

$$c(t) = \sum_{k=0}^{M-1} c_k p_c(t - kT_c) \tag{5}$$

c_k is the kth chip of the spreading code where $c_k \in \{+1, -1\}$, $p_c(t)$ is a rectangular pulse with unit height and duration T_c, and P is the number of bits carried by one LFM pulse.

The transmitted PN-chirp signal corresponds to

$$\begin{aligned} s(t) &= y(t) \cdot x(t) \\ &= \sum_{i=0}^{P-1} b_i \sum_{k=0}^{M-1} c_k p_c(t - iT_b - kT_c) \\ &\quad \cdot A_c \cos\left(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \phi_I\right) \\ &= \sum_{i=0}^{P-1} \sum_{k=0}^{M-1} p_c(t - iT_b - kT_c) \\ &\quad \cdot A_c \cos\left(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \theta_{i,k} + \phi_I\right) \end{aligned} \tag{6}$$

where $\theta_{i,k} = 0$ if $b_i c_k = 1$, and $\theta_{i,k} = \pi$ if $b_i c_k = -1$.

At the receiver side, a matched filter receiver can be exploited to obtain excellent bit error rate (BER) performance for these chirp modulated communication signals. However, all these chirp modulated communication signals were developed purely for communication purposes, not for radar function or information hiding. As can be seen from the different versions of modulated chirp signals, it is apparent that digital modulation has taken place and the signal is significantly different from the unmodulated chirp signal. Take chirp modulation as an example, a simple spectrogram analysis of the signal will reveal the up and down frequency change, indicating the signal is digitally modulated. The BPSK modulated chirp signal and the PN-chirp signal both exhibit a 180 degree phase change when two adjacent bits or adjacent chips are different, indicating the embedded digital modulation.

III. RF STEGANOGRAPHY VIA LINEAR CHIRP RADAR SIGNAL

We now propose a new RF steganography scheme exploiting an LFM chirp radar signal to hide communication through embedded digital modulation. The pulsed LFM chirp signal has been used widely in radar. Specifically, the same LFM chirp signal is transmitted from the radar periodically with a pulse repetition interval larger than the pulse

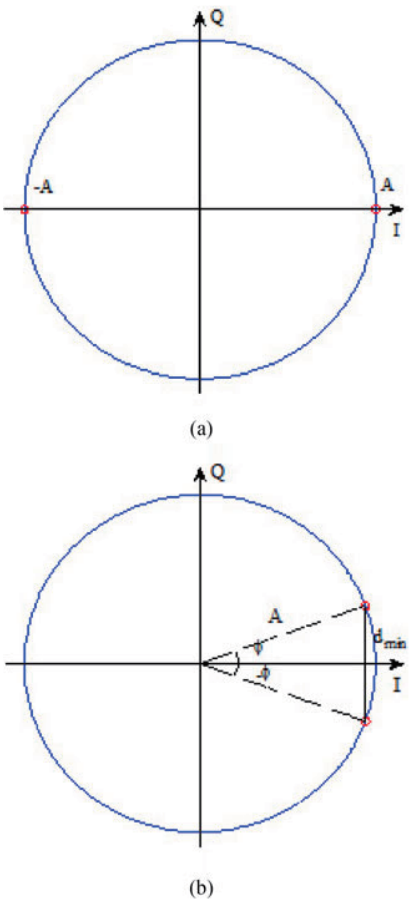


Fig. 3. Binary RPSK modulation. (a) BPSK. (b) BRPSK.

width of the chirp signal. In the silent period between two adjacent chirp signals, the radar receives the reflections of the chirp signal to perform radar functions, such as range detection of objects.

Now, instead of designing and transmitting an LPD communication waveform hoping to avoid detection from the enemy, we embed the communication signal inside the linear chirp radar signal. The joint radar/communication signal is transmitted from the radar transmitter and reaches the intended communication receiver and also reflects from objects the radar is trying to detect. The radar signal needs to complete a round-trip path to perform its function, and this creates a significant reduction in signal strength. Hence, most radar transmitters transmit signals at very high power compared to normal communication transmitters. On the other hand, the embedded communication signal only needs to reach its target through a one-way trip. Therefore, the received signal enjoys a very high signal-to-noise ratio (SNR).

This enables us to adopt a different phase shift keying modulation suitable for our purposes in this scenario. Instead of using phases 0 and π in the signal constellation to represent our binary data like a regular BPSK [see Fig. 3(a)], we use two constellation points with a much smaller phase difference [see Fig. 3(b)]. Specifically, we use phase ϕ and phase $-\phi$ to represent the binary data. We call this new modulation scheme binary reduced phase shift keying (binary RPSK, or BRPSK).

The transmitted LFM chirp signal with embedded BRPSK modulation corresponds to

$$\begin{aligned} s(t) &= Re\left[\sum_{i=0}^{N-1} p(t-iT_b)\tilde{x}(t)\cdot e^{j\theta_i}\right] \\ &= Re\left[\sum_{i=0}^{N-1} p(t-iT_b)A_c e^{j2\pi f_0 t}\cdot e^{j2\pi\frac{k}{2}t^2}\cdot e^{j\theta_i}\cdot e^{j\phi_I}\right] \\ &= \sum_{i=0}^{N-1} p(t-iT_b)\cdot A_c\cos\left(2\pi f_0 t+2\pi\frac{k}{2}t^2+\theta_i+\phi_I\right) \\ &= \sum_{i=0}^{N-1} p(t-iT_b)\cdot A_c\cos\left(2\pi f_0 t+2\pi\frac{k}{2}t^2+b_i\cdot\phi+\phi_I\right) \end{aligned} \tag{7}$$

where $\tilde{x}(t)=e^{j(2\pi f_0 t+2\pi\frac{k}{2}t^2+\phi_I)}$ is the complex envelope of the LFM chirp waveform.

Note that the phase offset being introduced to the ith data symbol now is $\theta_i=b_i\cdot\phi$, hence, if $b_i=1$, phase ϕ is introduced, and if $b_i=-1$, phase $-\phi$ is introduced. Clearly, the conventional BPSK can be considered as a special case of the BRPSK with $\phi=90^\circ$ (with a constant phase offset of $\frac{\pi}{2}$).

Fig. 4 illustrates the block diagram of the proposed BRPSK modulated LFM chirp signal transmitter.

Because the RPSK modulation uses a smaller phase difference, the constellation points have a much smaller distance ($d_{\min}$). As a direct result, this new modulation scheme has poorer BER performance compared with the original BPSK. The BER of original BPSK in the additive white gaussian noise (AWGN) channel is determined by

$$Q\left(\frac{d_{\min}/2}{\sigma}\right)=Q\left(\frac{A}{\sigma}\right)=Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{8}$$

where $A=\sqrt{E_b}=\sqrt{\frac{A_c^2}{2}T_b}$, $\sigma^2=N_0/2$ is the PSD of the additive white Gaussian noise, E_b is the bit energy, and $Q(x)$ is the Q function which corresponds to

$$Q\left(x\right)=\frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-\frac{u^2}{2}\right)du \tag{9}$$

On the other hand, the BER of BRPSK is

$$Q\left(\frac{d_{\min}/2}{\sigma}\right)=Q\left(\frac{A\sin(\phi)}{\sigma}\right)=Q\left(\sqrt{\frac{2E_b\sin^2(\phi)}{N_0}}\right) \tag{10}$$

Comparing (8) and (10), it is clear that the $\sin^2(\phi)$ term significantly reduces the BER performance of BRPSK. For example, when $\phi=15^\circ$, $\sin^2(\phi)=0.0670$ which corresponds to -11.74 dB. Hence, the BER performance of such a binary reduced PSK requires 11.74 dB in additional SNR to achieve the same BER performance of the original BPSK. However, because of the very high SNR of the LFM chirp radar signal, this performance loss can be tol-

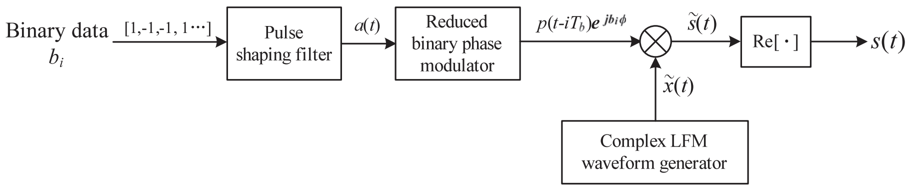


Fig. 4. Transmitter of BRPSK modulated chirp signal.

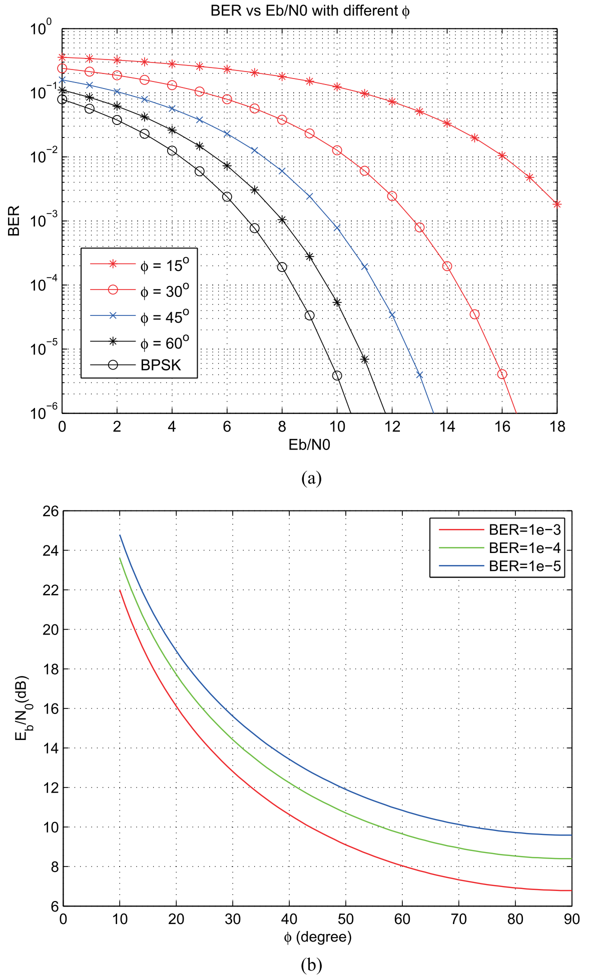


Fig. 5. BER of BRPSK modulation. (a) BER vs Eb/N0 of BRPSK. (b) Required Eb/N0 vs ϕ of BRPSK.

erated. Fig. 5(a) shows the BER versus E_b/N_o curves of BRPSK modulations with different phase ϕ, and Fig. 5(b) demonstrates the required E_b/N_0 versus the phase angle ϕ of BRPSK for different BERs. As shown in Fig. 5(a), there is an 11.74 dB difference in the BER performance of a BRPSK with $\phi = 15^{\mathrm{o}}$ versus that of a conventional BPSK (where $\phi = 90^{\mathrm{o}}$).

It is important and interesting to note that when we project the binary RPSK constellation to its in-phase component and quadrature component (see Fig. 6), it is evident that only the quadrature component contains the digital data. Hence, the optimum receiver can be implemented easily by a matched filter only considering the quadrature component of the received signal. Fig. 7 shows the block diagram of such a matched filter receiver for a BRPSK modulated LFM chirp signal. Specifically, the matched filter creates a decision variable for the ith data symbol

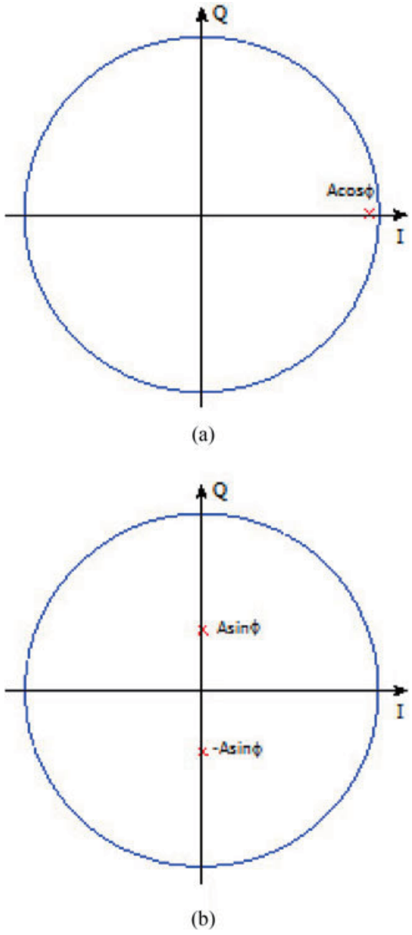


Fig. 6. In-phase and quadrature components of binary reduced phased shift keying. (a) In-phase. (b) Quadrature.

$$\begin{aligned} r_i &= \int_{iT_b}^{(i+1)T_b} r(t)x'(t)dt \\ &= \int_{iT_b}^{(i+1)T_b} r(t)\cdot A_c \cos\left(2\pi f_0 t + 2\pi\frac{k}{2}t^2 + \frac{\pi}{2} + \phi_I\right) dt \end{aligned} \tag{11}$$

where $r(t)$ is the received signal, and $x'(t)$ is a $\pi/2$ phase shifted original LFM chirp signal. Next, a hard decision device is used to make the decision on the estimate of the

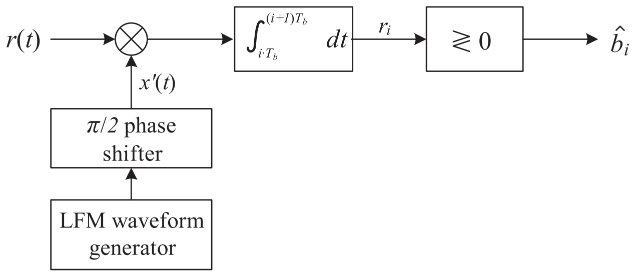
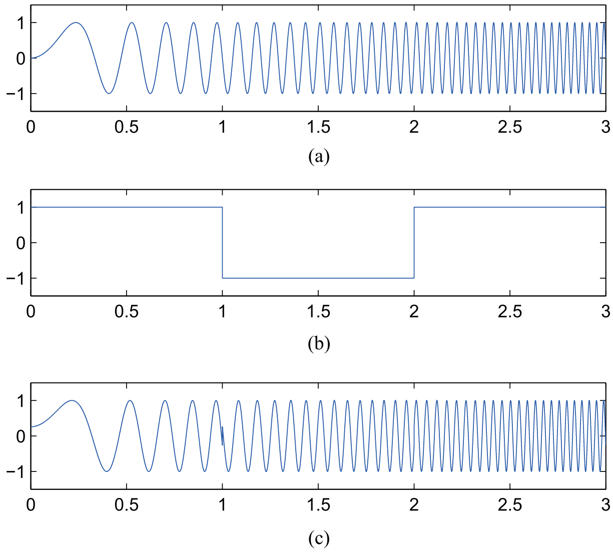


Fig. 7. Matched filter receiver of BRPSK modulated LFM chirp.



(a)

(b)

(c)

Fig. 8. Binary reduced PSK modulated chirp signal. (a) Unmodulated chirp signal. (b) Binary data. (c) Binary reduced PSK modulated chirp signal.

ith data symbol

$$\hat{b}_i = \begin{cases} 1 & \text{if} \quad r_i > 0 \\ -1 & \quad \text{else} \end{cases} \tag{12}$$

By exploiting the new reduced PSK modulation, the LFM chirp signal with embedded communication comes very close to the original unmodulated linear chirp signal. Fig. 8 shows the same example of a chirp modulated signal with three bits modulated using binary RPSK with $\phi = 15^{\circ}$. Compared with Fig. 2(c), it is clear that the phase reversal between adjacent symbols in the original BPSK modulated chirp signal is now replaced by a much smaller phase change, leading to a modulated chirp signal almost identical to the original unmodulated chirp signal. It is evident that the smaller the ϕ is, the less difference there is between the modulated chirp signal and the original chirp signal.

IV. ENHANCED RF STEGANOGRAPHY VIA VARIABLE SYMBOL DURATION

However, the chirp modulated signal with reduced PSK modulation itself is not enough to give us the RF steganography capability we desire. Although the signal does exhibit almost the identical time and frequency behavior as an unmodulated linear chirp, it has a cyclostationary feature that is exploitable by the enemy to find the existence of digital modulation embedded in the radar signal.

Cylostationary analysis has been recognized as an important tool to perform signal detection, RF parameter estimation, and signal classification [4]–[11]. A man-made signal such as communication signal often exhibits cyclostationarity due to the inherent modulation of the communication signal. The second-order spectral moment, also called the SCF, will reveal features of the inherent modulation and its parameters in the cyclic frequency domain. For example, the SCF of a BPSK signal will exhibit peaks in the cyclic frequency domain at twice the carrier frequency f_c, and at the symbol rate $1/T_b$.

Assume $x(t)$ is a cyclostationary signal, its correlation function is

$$R_x\left(t+\frac{\tau}{2}, t-\frac{\tau}{2}\right) = E\left[x\left(t+\frac{\tau}{2}\right)x^*\left(t-\frac{\tau}{2}\right)\right]. \tag{13}$$

Since the $R_x(t+\frac{\tau}{2}, t-\frac{\tau}{2})$ is a periodic function with period T, we can rewrite it as Fourier series

$$R_x\left(t+\frac{\tau}{2}, t-\frac{\tau}{2}\right) = \sum_{\alpha} R_x^{\alpha}(\tau)e^{j2\pi\alpha t}. \tag{14}$$

The Fourier coefficients are

$$\begin{aligned} R_x^{\alpha}(\tau) &= \frac{1}{T}\int_{-T/2}^{T/2} R_x\left(t+\frac{\tau}{2}, t-\frac{\tau}{2}\right)e^{-j2\pi\alpha t}dt \\ &= \lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2} x\left(t+\frac{\tau}{2}\right)x^*\left(t-\frac{\tau}{2}\right)e^{-j2\pi\alpha t}dt \end{aligned} \tag{15}$$

where α is the cyclic frequency, $R_x^{\alpha}(\tau)$ is the cyclic autocorrelation function, and the Fourier transformation of the cyclic autocorrelation function is

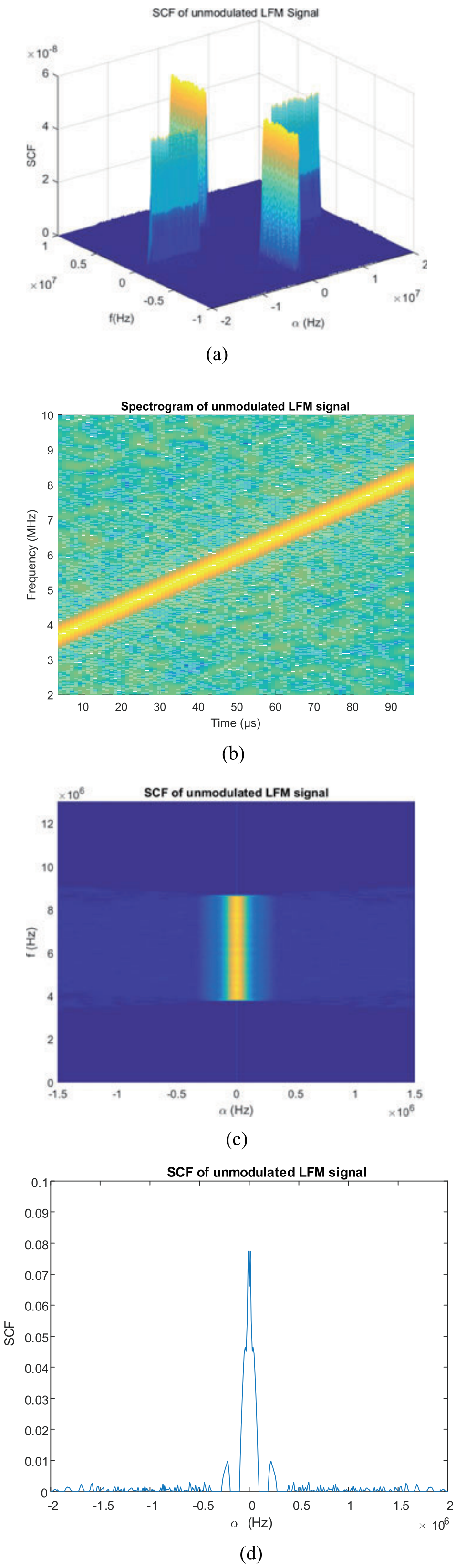
$$S_x^{\alpha}(f) = \int_{-\infty}^{\infty} R_x^{\alpha}(\tau)e^{-j2\pi f\tau}d\tau \tag{16}$$

where $S_x^{\alpha}(f)$ is the SCF.

Fig. 9(a) illustrates the SCF of an LFM radar chirp signal with 5 MHz bandwidth and 10 μs pulse width where the starting frequency is 3.5 MHz and the ending frequency is 8.5 MHz, Fig. 9(b) shows the spectrogram of the LFM chirp, Fig. 9(c) shows the zoomed-in top down view of this SCF, and Fig. 9(d) shows the projection of the SCF to the cyclic frequency (α) domain.

As soon as we embed digital modulation into the LFM chirp signal, cyclostationary analysis is capable of revealing the existence of the modulation. The linear chirp signal with embedded reduced PSK modulation that we have discussed so far uses a fixed symbol duration T_b to transmit one bit. Therefore, cyclostationary analysis of such a signal will exhibit peaks at the symbol rate $1/T_b$ in the cyclic frequency domain and at multiples of the symbol rate m/T_b, where m is an integer. Hence, although time domain analysis and frequency domain analysis do not give our enemy any indication of the existence of embedded digital modulation, a cyclostationary analysis will reveal this fact.

Fig. 10 illustrates the SCF of a BPSK modulated LFM chirp radar signal where a random binary data stream of



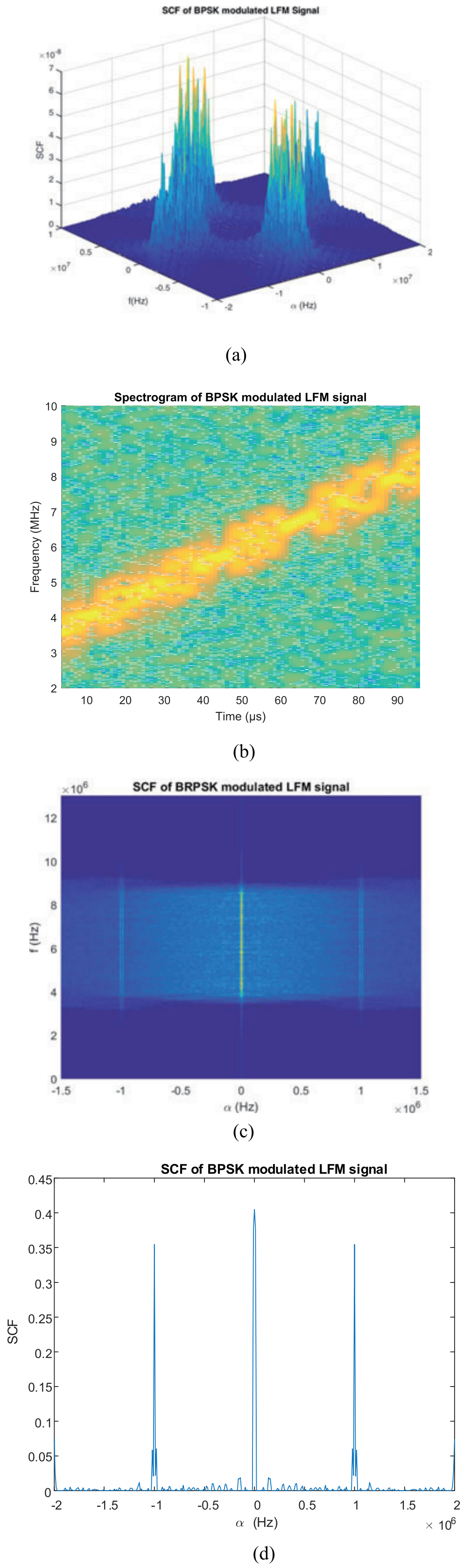
(a)

(b)

(c)

(d)

Fig. 9. SCF of unmodulated LFM radar chirp signal. (a) SCF of LFM. (b) Spectrogram of LFM. (c) Top view of SCF. (d) Cyclic frequency projection.



(a)

(b)

(c)

(d)

Fig. 10. SCF of BPSK modulated LFM radar chirp signal. (a) SCF of BPSK modulated LFM. (b) Spectrogram of BPSK modulated LFM. (c) Top view of SCF. (d) Cyclic frequency projection.

rate 1 MHz is modulated onto an LFM chirp signal with the same parameters as in Fig. 9. Similarly, Fig. 10(a) shows the three-dimensional SCF, Fig. 10(b) shows the spectrogram, Fig. 10(c) shows the top-down view and Fig. 10(d) is the projection of the SCF to the α domain. It is evident from Fig. 10(c) that at $\alpha = \pm 1/T_b = \pm 1$ MHz there is a clear feature spanning in the frequency domain from the starting frequency to the ending frequency of the LFM chirp. It can also be seen from Fig. 10(b) that the bandwidth of the LFM chirp is expanded due to the embedded BPSK modulation.

Next, we show that by exploiting the BRPSK modulation, this cyclic feature becomes less strong but still exploitable. Fig. 11 shows the case of a BRPSK modulated LFM chirp radar signal with $\phi = 30^{\text{o}}$ and Fig. 12 shows the case of $\phi = 15^{\text{o}}$. As shown in both figures, when reduced PSK modulation is employed, the cyclic feature at the symbol rate becomes less strong as the phase ϕ decreases. It can also be observed that the bandwidth expansion becomes smaller as the phase ϕ decreases. This is understandable, since if we decrease ϕ all the way to zero, the signal becomes an unmodulated LFM chirp, and the cyclic feature will entirely disappear. However, we cannot make ϕ too small because that would lead to too much SNR degradation and eventually the BER performance would become unacceptable. With a reasonable ϕ of 15^{o}, as Fig. 12(d) demonstrates, the cyclic feature of the embedded modulation is still very much exploitable.

Now, we propose to use a variable symbol duration scheme for our modulated LFM chip transmission. Specifically, we intentionally assign a unique symbol duration T_{b_i} for the ith data symbol. Different symbol durations are different, and one symbol duration is not the multiple of another symbol duration. This way, we no longer have a fixed symbol rate, and we eliminate the cyclostationarity associated with the symbol rate. Therefore, there will be no SCF feature exploitable by the enemy to find out the existence of our hidden digital modulation. At our intended receiver, on the other hand, because the unique symbol durations are known, there is no difficulty for the legitimate receiver to demodulate the data.

Mathematically, the modulated LFM chirp signal corresponds to

$$s(t) = \sum_{i=0}^{N-1} p_i(t) \cdot A_c \cos\left(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \theta_i + \phi_I\right) \tag{17}$$

where $p_i(t)$ is the ith data symbol's pulse with a pulse width T_{b_i}

$$p_i(t) = \begin{cases} 1 & \text{if } \sum_{l=0}^{i-1} T_{b_l} \le t < \sum_{l=0}^{i-1} T_{b_l} + T_{b_i} \\ 0 & \text{elsewhere} \end{cases} \tag{18}$$

However, the variable symbol duration leads to variable symbol energy (E_b) for different data symbols. Since the LFM chirp signal is a constant envelope signal, the symbol energy for the ith symbol is simply $\frac{A_c^2}{2} \cdot T_{b_i}$, where A_c is the amplitude of the chirp signal. Therefore, the data symbols with longer symbol duration will have higher symbol

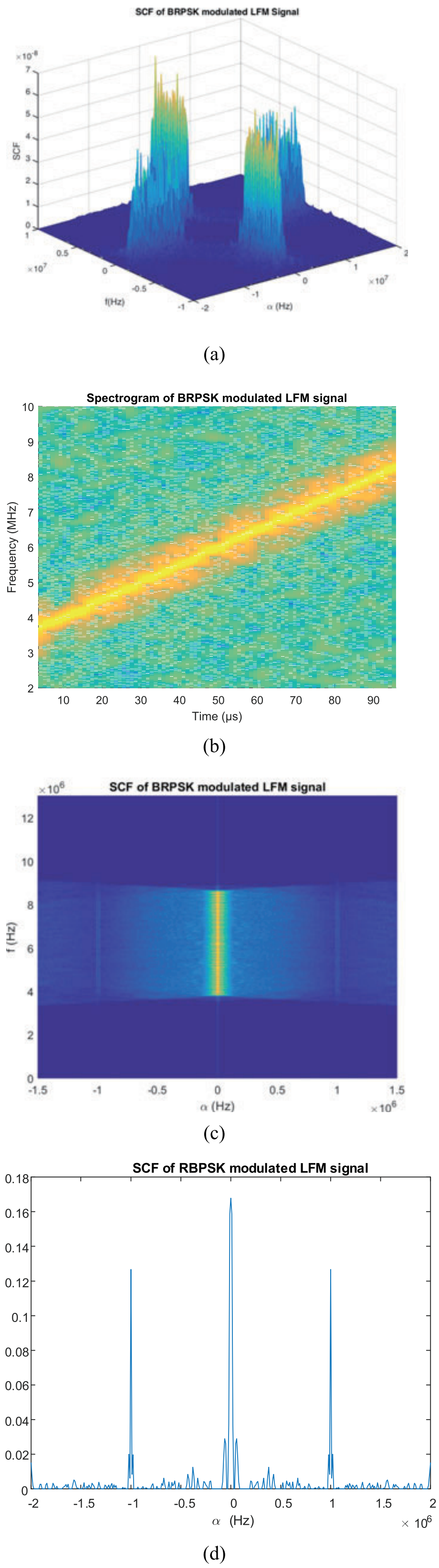
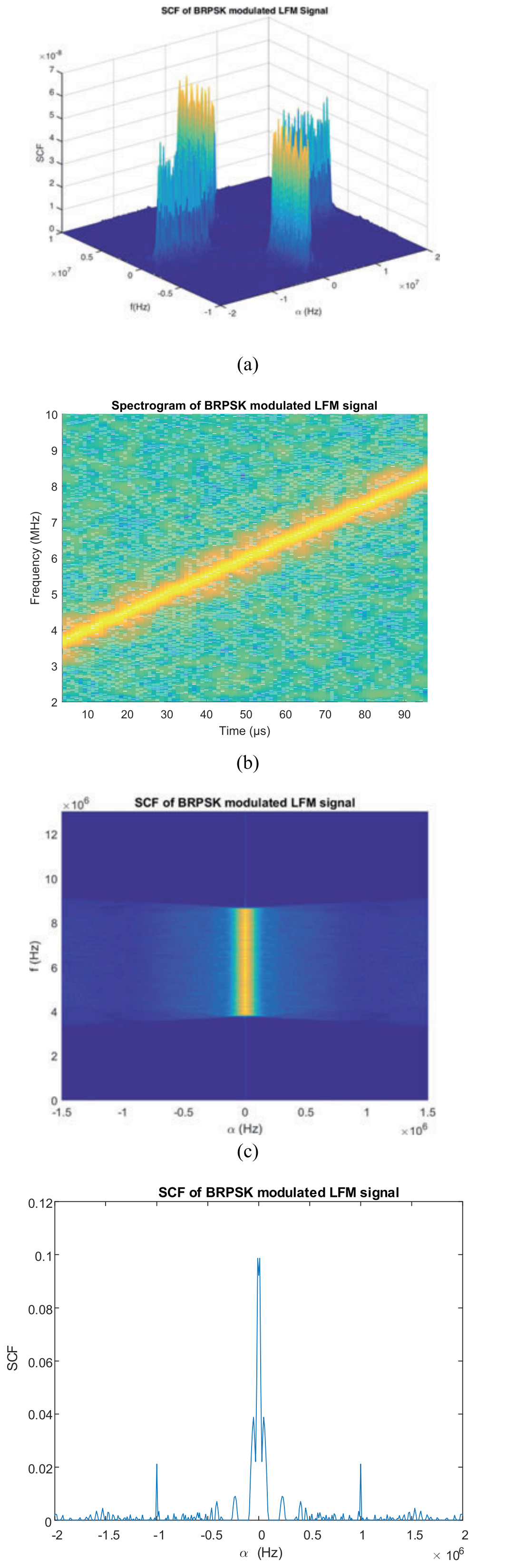


Fig. 11. SCF of BRPSK modulated LFM radar chirp signal with $\phi = 30^{\text{o}}$. (a) SCF of BRPSK modulated LFM with $\phi = 30^{\text{o}}$. (b) Spectrogram of BPSK modulated LFM. (c) Top view of SCF. (d) Cyclic frequency projection.



(a)

(b)

(c)

(d)

Fig. 12. SCF of BRPSK modulated LFM radar chirp signal with $\phi = 15^o$. (a) SCF of BRPSK modulated LFM with $\phi = 15^o$. (b) Spectrogram of BRPSK modulated LFM. (c) Top view of SCF. (d) Cyclic frequency projection.

energy and correspondingly better BER performance. This is obviously not desirable.

Fortunately, we have an elegant and simple solution for this problem. By adjusting the phase difference parameter ϕ in the reduced PSK modulation, we can compensate for the shorter symbol duration with larger ϕ and ensure that the BER stays the same. For example, since the first data symbol has a symbol duration T_{b_1} and binary reduced PSK with ϕ_1, the second data symbol has a symbol duration T_{b_2} and ϕ_2, as long as we make sure that

$$T_{b_1}\sin^2(\phi_1) = T_{b_2}\sin^2(\phi_2) \tag{19}$$

the BER performance does not change.

Mathematically, the transmitted BRPSK modulated LFM chirp signal with variable symbol duration is

$$s(t) = \sum_{i=0}^{N-1} p_i(t)\cdot A_c\cos\left(2\pi f_0 t + 2\pi\frac{k}{2}t^2 + b_i\cdot\phi_i + \phi_I\right). \tag{20}$$

In (20), it is clear that both the symbol duration T_{b_i} and associated phase ϕ_i are now varying for different symbols.

Fig. 13 illustrates the block diagram of the transmitter of the proposed RF steganography scheme with BRPSK modulation and variable symbol duration. It is interesting to note that we have employed an elegant way to generate the variable symbol durations. We first generate the ϕ_i as a pseudorandom phase sequence. In practice, the phase ϕ_i can simply be chosen as a random variable with discrete uniform distribution between ϕ_L and ϕ_H with step size $\Delta\phi$, where ϕ_L is the smallest phase angle and ϕ_H is the largest phase angle. The cumulative distribution function of ϕ_i is simply

$$F(\phi_i;\phi_L,\phi_H) = \frac{\phi_i - \phi_L + \Delta\phi}{\phi_H - \phi_L + \Delta\phi}. \tag{21}$$

For example, if we choose ϕ_L as 12.5° and ϕ_H as 17.5° with step size $\Delta\phi = 0.1^o$, ϕ_i is equally distributed among $\frac{\phi_H-\phi_L}{\Delta\phi} + 1 = 51$ discrete phases. The associated symbol duration T_{b_i} can then be derived as

$$T_{b_i} = T_b\frac{\sin^2(\frac{\phi_L+\phi_H}{2})}{\sin^2(\phi_i)} \tag{22}$$

where T_b is now defined as the symbol duration associated with the mean of phase $E[\phi_i] = \frac{\phi_L+\phi_H}{2}$ which in our example is 15°. Fig. 14 illustrates the relationship between the variable symbol duration T_{b_i} and associated phase angle ϕ_i. The symbol duration is normalized to be 1 when $\phi = 15^o$. It is clear from the figure that because of the nonlinear relationship between the associated symbol duration T_{b_i} and the phase angle ϕ_i, such a uniformly distributed pseudorandom phase sequence will generate a series of symbol durations with no linear relationship among them.

Fig. 15 illustrates the SCF and spectrogram of the proposed BRPSK modulated LFM chirp signal with variable symbol duration where the ϕ_i uniformly varies between 12.5° to 17.5° with step size 0.1°. It is evident that the cyclic frequency feature is entirely eliminated. Compared with the SCF of an unmodulated LFM chirp shown in Fig. 9,

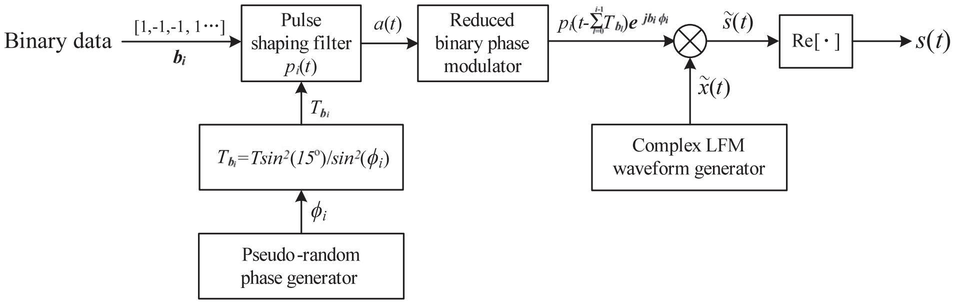

Binary data
[1,-1,-1, 1⋯]
b_i
Pulse shaping filter $p_i(t)$
$a(t)$
Reduced binary phase modulator
$p_i(t-\sum_{l=0}^{i-1} T_{b_l})e^{jb_i\phi_i}$
$\tilde{s}(t)$
Re[·]
$s(t)$
T_{b_i}
$T_{b_i}=Tsin^2(15^o)/sin^2(\phi_i)$
ϕ_i
Pseudo-random phase generator
$\tilde{x}(t)$
Complex LFM waveform generator

Fig. 13. Transmitter of BRPSK modulated LFM chirp signal with variable symbol duration.

TABLE I
LFM Pulse Parameters

Pulse Width	10 μs
Bandwidth	5 MHz
Sampling Frequency (f_s)	5×10^8 Hz
Signal Gain, A	1

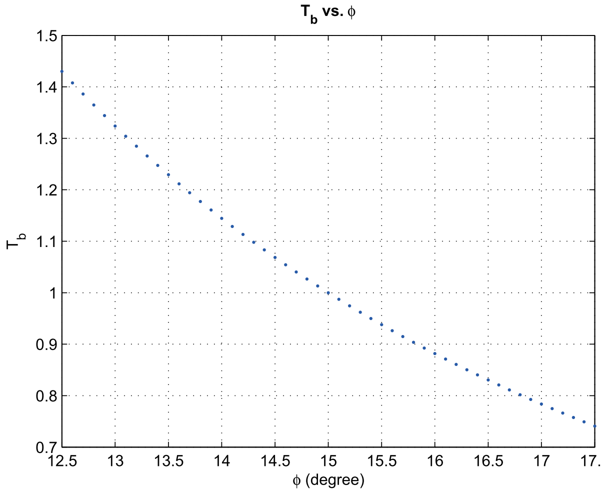


Fig. 14. Symbol duration versus ϕ.

the RF steganography transmissions exhibit an almost identical SCF as the unmodulated LFM chirp.

Fig. 16 illustrates an example of such a reduced PSK modulated chirp signal with variable symbol duration. As shown in Fig. 16(b), three different symbol durations are used to carry three binary bits. The first symbol duration $T_{b_1} = 1$, and the associated phase difference $\phi = 15^o$. The second $\phi_2 = 16.5^o$ and the associated symbol duration T_{b_2} is

$$T_{b_2} = T_{b_1} \frac{\sin^2(15^o)}{\sin^2(16.5^o)} \tag{23}$$

which leads to $T_{b_2} = 0.83$. The third symbol's phase $\phi_3 = 12.8^o$ and its associated symbol duration $T_{b_3} = 1.37$. It is evident that the longer the symbol duration is, the smaller the associated ϕ_i is.

As shown in Figs. 15 and 16, the newly designed LFM chirp signal with embedded digital modulation serves as an excellent example of RF steganography carrying covert communication for a designated communication receiver. The signal behaves almost identically to an unmodulated LFM chirp signal in the time domain, frequency domain, and cyclostationary domain; preventing the enemy from detecting the existence of the embedded modulation. It is worth noting that the difference between the SCF of unmodulated LFM chirp signal and that of the newly designed LFM chirp signal is very small even when there is no noise. Therefore, it is more difficult for the enemy's receiver to distinguish them when there is fading, noise, and other distortions.

V. EFFECT ON RADAR WAVEFORM

The proposed RF steganography scheme makes slight modifications to the LFM chirp signal. Hence, it is important to evaluate how much effect these modifications have on the radar waveform and if it deteriorates the radar performance significantly.

A commonly used metric to evaluate the performance of a radar waveform is the ambiguity function. This function provides a measure of the response of a matched filter to a finite energy signal in the presence of a time delay, τ, and Doppler frequency shift, ν. The periodic ambiguity function can be expressed as [20]

$$|\chi(\tau, \nu)| = \left| \int_0^T u(t)u^*(t-\tau)e^{2\pi j\nu t}dt \right| \tag{24}$$

where $u(t)$ is one LFM chirp, and the variables τ and ν represent the time delay and Doppler-shifted frequency of the returned signal, respectively.

The ambiguity function provides a means to determine radar performance in the face of time and Doppler shifts. The ideal (and hypothetical) ambiguity function has a "thumbtack" appearance at the origin (e.g., $\tau = 0$ and $\nu = 0$) for a Dirac delta impulse signal. In this situation, the radar can provide an accurate target position as long as there is no delay or Doppler frequency shift. More realistically, radars need to have some tolerance to time delays and Doppler shifts so the ideal "thumbtack" response is not necessarily a desired matched filter response.

To illustrate the ambiguity function, we use numerical simulations of an LFM pulse with the following parameters. For the modulated LFM chirp pulse, the carrier is assumed to be a C-band radar with a 10 KW peak power operating

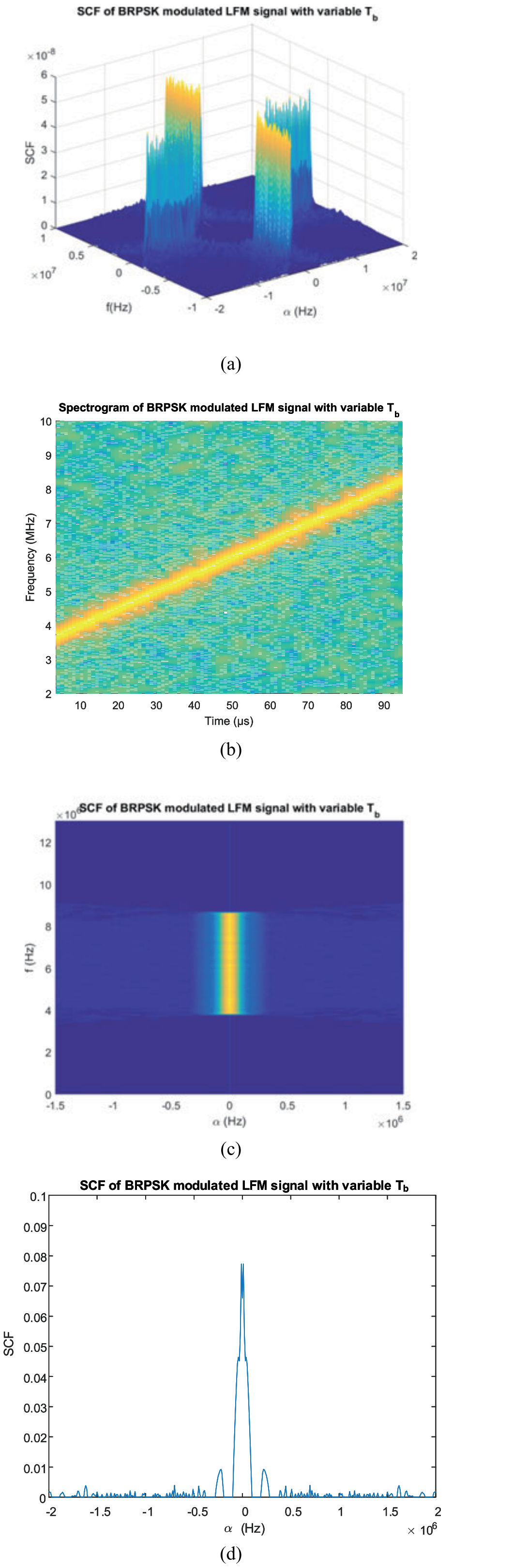


Fig. 15. SCF of BRPSK modulated LFM radar chirp signal with variable symbol duration. (a) SCF of BRPSK modulated LFM with variable symbol duration. (b) Spectrogram of BRPSK modulated LFM with variable symbol duration. (c) Top view of SCF. (d) Cyclic frequency projection.

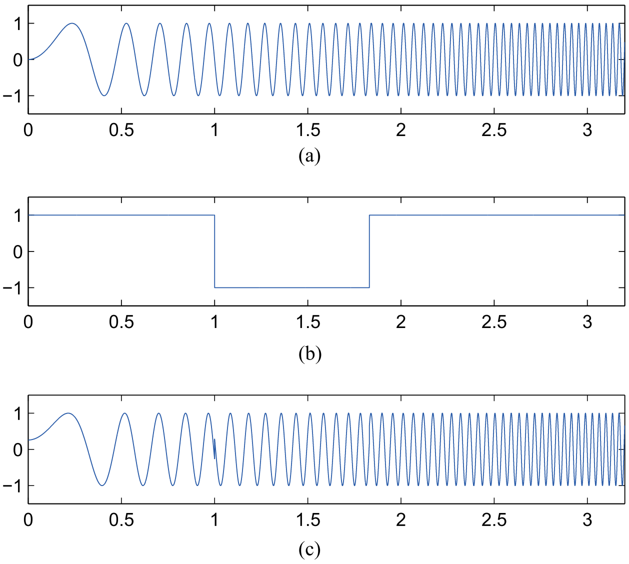


Fig. 16. Binary reduced PSK modulated chirp signal with variable symbol duration. (a) Unmodulated Chirp Signal. (b) Binary Data. (c) Binary Modulated Chirp Signal.

at 5 GHz. The overall gain of the transmitter antenna and receiver is assumed to be 2000 with 50 dB of attenuation due to transmitter, receiver, measurement, and processing losses.

Fig. 17 plots the ambiguity function for the unmodulated LFM signal. This provides a baseline for comparison with the LFM pulses that have embedded communication. The plot illustrates accuracy for determining target position in time but allows some flexibility for frequency error due to Doppler effects. As a comparison, Fig. 18 shows the ambiguity function of an LFM signal with an embedded BPSK modulated communication message (using phase changes of ± 90°). As Fig. 18 clearly shows, while time delay remains the same, Doppler tolerance has greatly diminished.

Fig. 19 depicts the PSD and autocorrelation of the BPSK modulated LFM chirp signal ($\phi = \pm 90^o$). The PSD plot clearly shows the increased bandwidth caused by the use of large phase angle changes. Further, the autocorrelation plot exhibits fairly high sidelobes beyond the first sidelobe.

The combination of the poor ambiguity function performance (when compared to the baseline LFM ambiguity plot) and the wider bandwidth of the PSD may not be acceptable for radar performance. For these reasons, we have explored the use of new reduced PSK modulated LFM chirp waveforms.

The following plots show the case of our proposed BRPSK modulated LFM chirp waveform with $\phi = 15^o$. The effect of using BRPSK modulation can be clearly seen in the radar ambiguity plots for the BRPSK modulated LFM chirp signal shown in Fig. 20. In the plot, the use of smaller phase differences preserves the Doppler tolerance of the LFM radar pulse.

Fig. 21 provides a view of the PSD and autocorrelation (i.e., zero-Doppler cut of the ambiguity function). In the followingfigure, the PSD of the BRPSK modulated LFM

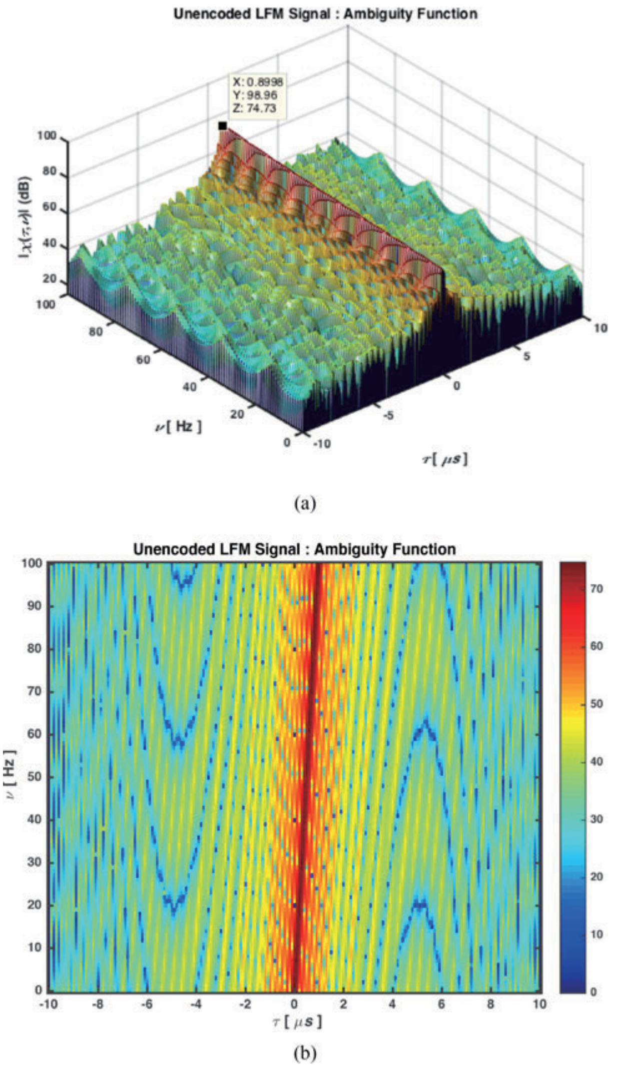


Fig. 17. Ambiguity function of unmodulated LFM chirp signal. (a) LFM ambiguity function (AF) plot. (b) LFM AF plot—top view.

chirp is in blue while the PSD of the unmodulated LFM pulse is shown in red. As can be seen, while additional energy is distributed in the sidelobes, the autocorrelation of the communication pulse is consistent with what one would expect for an LFM matched filter with a high in-band ($\tau = 0$) autocorrelation value and low out of band correlation.

Fig. 22(a) shows the receiver operator characteristic (ROC) curves of the newly designed LFM chirp signal with BRPSK modulation and variable symbol duration, and the unmodulated LFM chirp signal. In Fig. 22(a), the x-axis represents the probability of false alarm and the y-axis represents the probability of detection. In the numerical simulation, the receiver is designed as a coherent detector which is used to detect the LFM radar signal under -8 dB SNR. The detection is determined by the output of the matched filter through thresholding. Up to 500 000 trials have been conducted on the proposed BRPSK-LFM chirp signal with variable ϕ between 12.5$^{\text{o}}$ and 17.5$^{\text{o}}$, and the unmodulated LFM chirp signal, to obtain two ROC curves, respectively.

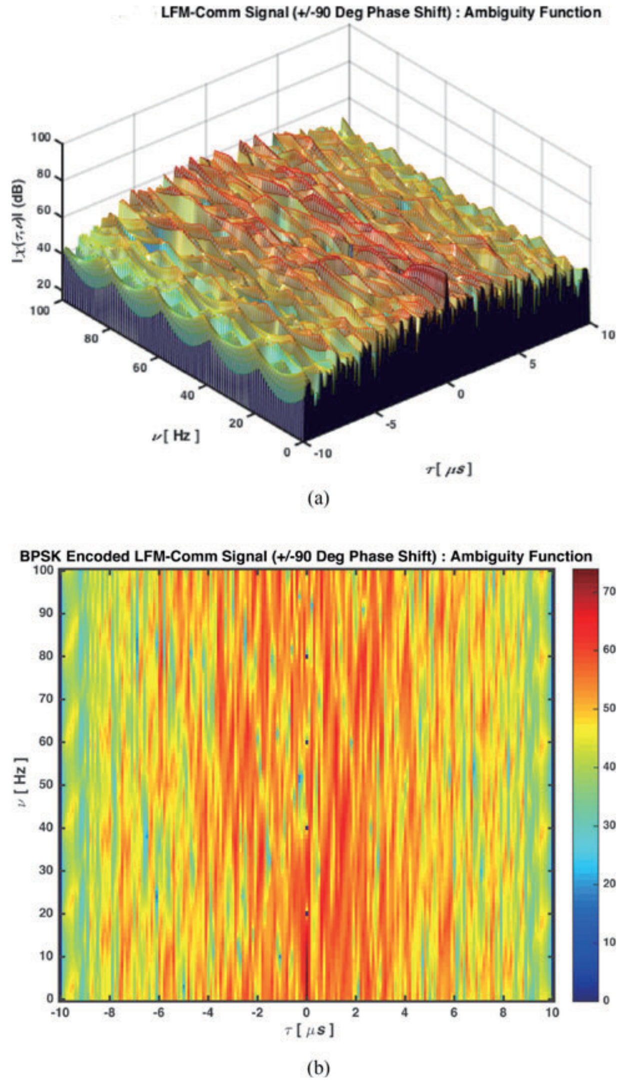


Fig. 18. Ambiguity function of BPSK modulated LFM chirp signal. (a) BPSK modulated LFM AF plot. (b) BPSK modulated LFM AF plot—top view.

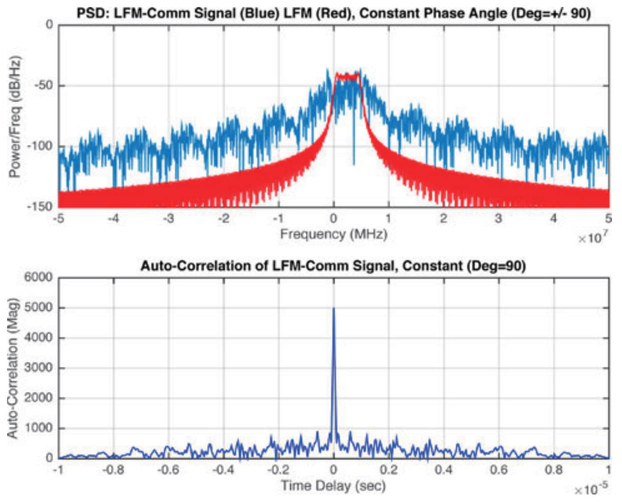
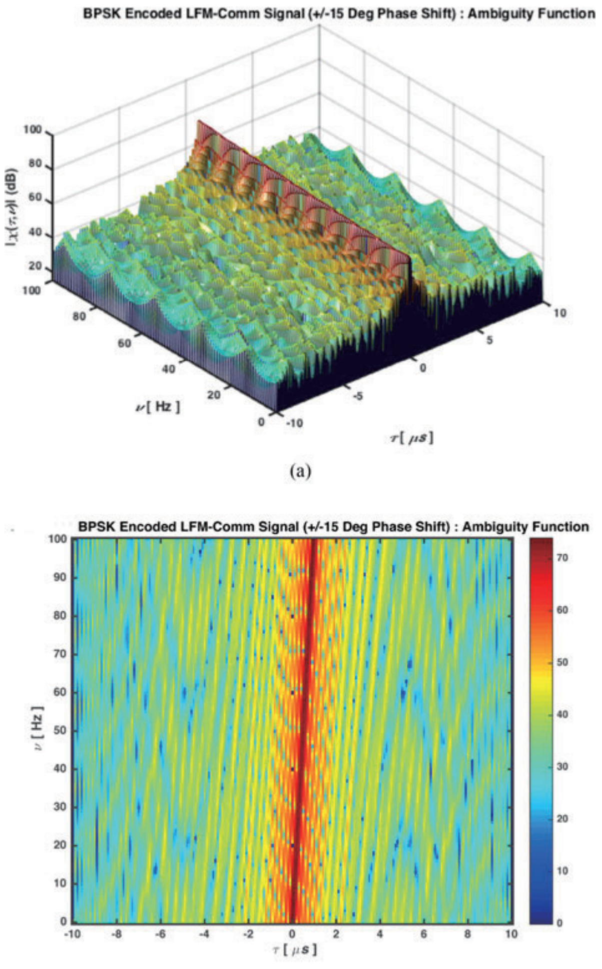


Fig. 19. PSD/autocorrelation of LFM chirp and BPSK modulated LFM chirp.



(a)

(b)

Fig. 20. Ambiguity function of reduced BPSK modulated LFM chirp signal. (a) BRPSK modulated LFM AF plot. (b) BRPSK modulated LFM AF plot—top view.

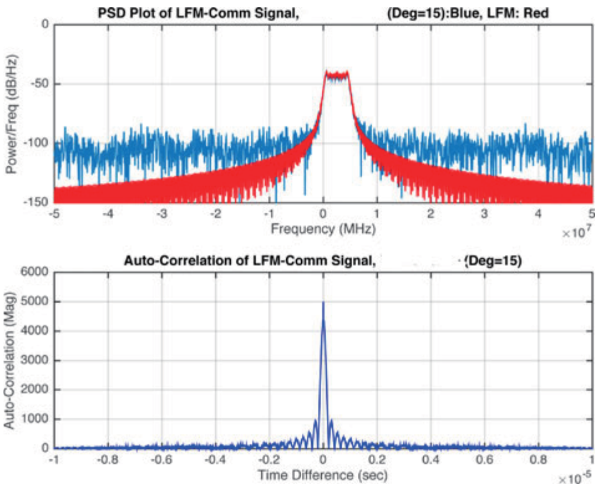
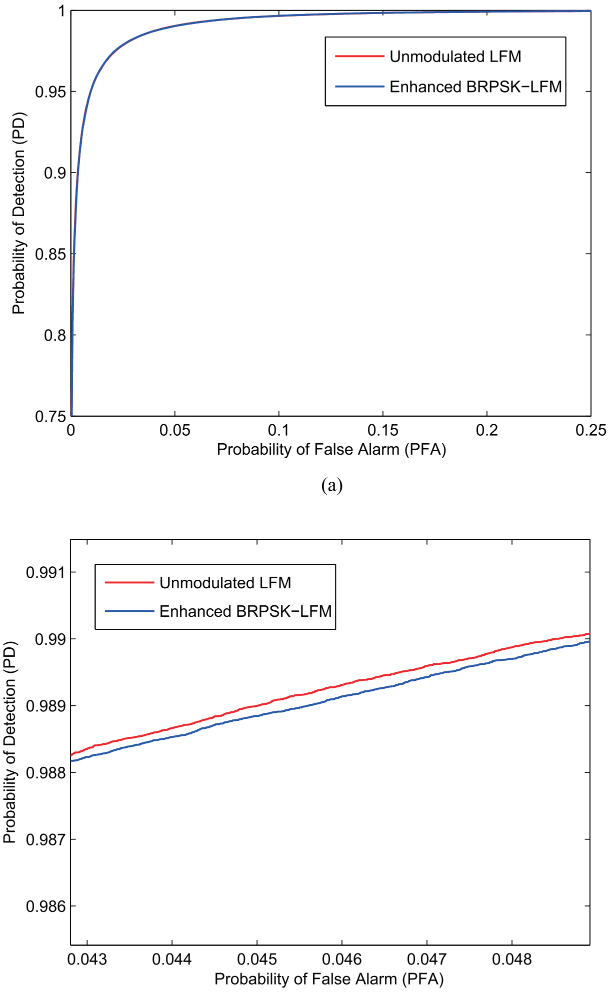


Fig. 21. PSD/autocorrelation of LFM chirp and BRPSK modulated LFM chirp.



(a)

(b)

Fig. 22. ROCs of LFM chirp and BRPSK modulated LFM chirp. (a) ROC. (b) Zoomed in ROC.

The result in Fig. 22(a) confirms that the difference between the two ROC curves is very small. Only in a zoomed in version of the plot shown in Fig. 22(b), a negligible difference is observed which reveals an insignificant performance loss with the newly designed waveform.

VI. CONCLUSION

In this paper, we have developed a novel RF steganography by hiding communication information in an LFM chirp radar signal. By exploiting a new RPSK modulation, the modulated chirp signal becomes very similar to the unmodulated chirp signal. Furthermore, by adopting variable symbol durations, we further enhance the security of the hidden communication signal by eliminating the cyclostationary features. The resulting reduced PSK modulated chirp signal then serves a hybrid radar/communication purpose, while it is difficult for the enemy to detect the existence of the modulation embedded in the chirp signal.

ACKNOWLEDGMENT

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

REFERENCES

[1] R. Schoolcraft
Low probability of detection communications-LPD waveform design and detection techniques
In *Proc. IEEE Mil. Commun. Conf.*, 1991, vol. 2, pp. 832–840

[2] F. C. Lau and C. K. Tse
Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation. New york, NY, USA: Springer, 2003.

[3] H. Lu, L. Zhang, M. Jiang, and Z. Wu
High-security chaotic cognitive radio system with subcarrier shifting
IEEE Commun. Lett., vol. 19, no. 10, pp. 1726–1729, Oct. 2015

[4] W. A. Gardner and C. M. Spooner
Signal interception: Performance advantages of cyclic-feature detectors
IEEE Trans. Commun., vol. 40, no. 1, pp. 149–159, Jan. 1992.

[5] W. A. Gardner
Cyclostationarity in Communications and Signal Processing. Piscataway, NJ, USA: IEEE Press, 1993.

[6] W. Gardner, W. Brown, and Chih-Kang Chen
Spectral correlation of modulated signals: Part II - Digital modulation
IEEE Trans. Commun., vol. 35, no. 6, pp. 595–601, Jun. 1987.

[7] W. A. Gardner
Signal interception: A unifying theoretical framework for feature detection
IEEE Trans. Commun., vol. 36, no. 8, pp. 897–906, Aug. 1988.

[8] A. Fehske, J. Gaeddert, and J. Reed
A new approach to signal classification using spectral correlation and neural networks
In *Proc. IEEE 1st Int. Symp. New Frontiers Dyn. Spectrum Access Netw.*, Nov. 2005, pp. 144–150.

[9] M. Tsatsanis and G. Giannakis
Blind estimation of direct sequence spread spectrum signals in multipath
IEEE Trans. Signal Process., vol. 45, no. 5, pp. 1241–1252, May 1997.

[10] E. C. Like, V. Chakravarthy, and Z. Wu
Signal classification in fading channels using cyclic spectral analysis
EURASIP J. Wireless Commun. Netw., vol. 2009, 2009, Art. no. 879812.

[11] Z. Wu and T. C. Yang
Blind cyclostationary carrier frequency and symbol rate estimation for underwater acoustic communications
IEEE MMTC E-Lett. Spec. Issue Acoust. Audio Commun., vol. 7, no. 2, pp. 25–29, Feb. 2012

[12] M. C. Wicks, D. Erricolo, L. Teng, and L. LoMonte
On spectrum sharing between radar and communications
In *Proc. IEEE Top. Conf. Antenna Propag. Wireless Commun.*, Palm Beach Aruba, Aug. 2014, pp. 890–893.

[13] H. D. Griffiths *et al.*
, Radar spectrum engineering and management: technical and regulatory approaches
Proc. IEEE., vol. 103, no. 1, pp. 85–102, Jan. 2015.

[14] M. C. Wicks
Spectrum crowding and cognitive radar
In *Proc. IAPR 2nd Workshop Cogn. Inf. Process.*, Elba Island, Italy, Jun. 2010, pp. 452–457.

[15] Shared Spectrum Access for Radar and Communications (SSPARC), DARPA. 2015. [Online]. Available: http://www.darpa.mil/program/shared-spectrum-access-for-radar-and-communications

[16] Y. L. Sit, C. Sturm, L. Reichardt, T. Zwick, and W. Wiesbeck
The OFDM joint radar-communication system: An overview
In *Proc. 3rd Int. Conf. Adv. Satell. Space Commun.*, 2011, pp. 69–74.

[17] Y. L. Sit, L. Reichardt, C. Sturm, and T. Zwick
Extension of the OFDM joint radar-communication system for a multipath, multiuser scenario
In *Proc. IEEE RadarCon*, 2011, pp. 718–723.

[18] M. Braun, C. Sturm, A. Niethammer, and F. K. Jondral
Parametrization of joint OFDM-based radar and communication systems for vehicular applications
In *Proc. IEEE 20th Int. Symp. Pers., Indoor Mobile Radio Commun.*, 2009, pp. 3020–3024.

[19] C. W. Rossler, E. Ertin, and R. L. Moses
A software defined radar system for joint communication and sensing
In *Proc. IEEE RadarCon*, 2011, pp. 1050–1055.

[20] N. Levanon and E. Mozeson
Radar Signals. New York, NY, USA: Wiley, 2004.

[21] S. Darlington
Pulse Transmission (chirp)
U.S. Patent 2,678,997, 1954.

[22] M. R. Winker
Chirp signals for communications
In *Proc. IEEE WESCon Conv. Rec.*, 1962.

[23] C. E. Cook
Linear FM signal formats for beacon and communication systems
IEEE Trans. Aerosp. Electron. Syst., vol. AES 10, no. 4, pp. 471–478, Jul. 1974.

[24] P. W. Baier, R. Simons, and H. Waibel
Chirp-PN-PSK-Signale als Spread-Spectrum-Signalformen geringer Dopplerempfindlichkeit und grober Signalformvielfalt
NTZ Archiv, vol. 3, pp. 29–33, Feb. 1981

[25] M. Kowatsch, F. J. Seifert, and J. T. Lafferl
Comments on transmission system using pseudonoise modulations of linear chirps
IEEE Trans. Aerosp. Electron. Syst., vol. AES-17, no. 2, pp. 300–303, Mar. 1981

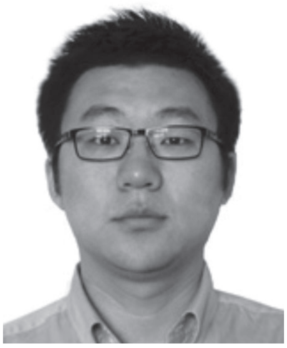
[26] M. Kowatsh and J. T. Laferal
A spread-spectrum concept combining chirp modulation and pseudonoise coding
IEEE Trans. Commun., vol. com-31, no. 10, pp. 1133–1142, Oct. 1983.

Zhiping Zhang (M'16) received the B.S. degree in electrical engineering from Nankai University, Tianjin, China, in 2001 and the M.S. and Ph.D. degrees in intelligence science from Peking University, Beijing, China, in 2004 and 2011, respectively.

From 2011 to 2013, he was a Postdoctoral Research Fellow with the Department of Computer Science and Technology, Peking University. Since 2013, he has been a Research Faculty Member and the co-director of Broadband, Mobile and Wireless Networking Laboratory with the Department of Electrical Engineering, Wright State University, Dayton, OH, USA.

Michael J. Nowak (M'16) received the B.S. degree in astronautical engineering from United States Air Force Academy, CO, USA, in 1979, the M.S. degree in aerospace engineering from the University of Texas at Austin, Austin, TX, USA, in 1992, and the Ph.D. degree in engineering from Wright State University, Dayton, OH, USA, in 2016.

He is currently a Technical Advisor of the Spectral Warfare Division of Sensors Directorate, Air Force Research Laboratory, Dayton, OH, USA.



Yang Qu (M'17) received the B.S degree in electrical engineering from DaLian Jiaotong University, DaLian, China, in 2010, the M.S. degree in electrical engineering from Wright State University, Dayton, OH, USA, in 2013. He is currently working toward the Ph.D. degree in electrical engineering at the Department of Electrical Engineering,Wright State University.

Michael C. Wicks (S'81–M'89–SM'90–F'98) received the B.Sc. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1981 and the M.Sc. and Ph.D. degrees in electrical engineering from Syracuse University, Syracuse, NY, USA, in 1985 and 1995, respectively.

He was with the U.S. Air Force Senior Scientist for sensors signal processing, specializing in the science and technology needed for superior air and space systems for intelligence, surveillance, reconnaissance, precision engagement, and electronic warfare. In 2011, he was with the University of Daytonwhere, as a Full Professor and an Endowed Chair, Ohio Scholar for Sensor Exploitation and Fusion, and a Distinguished Research Scientist.

Dr. Wicks received the 2013 IEEE Picard Medal for Radar Technologies and Applications.

John Ellinger received the Ph.D. degree in electrical engineering from Wright State University, Dayton, OH, USA, in 2016.

He currently with the Air Force Research Laboratory, Dayton, OH, USA.

Zhiqiang Wu (M’02–SM’16) received the B.S. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 1993, the M.S. degree from Peking University, Beijing, China, in 1996, and the Ph.D. degree from Colorado State University, Fort Collins, CO, USA, in 2002, all in electrical engineering.

From 2003 to 2005, he was an Assistant Professor with the Department of Electrical Engineering of West Virginia University Institute of Technology, Beckley, WV, USA. In 2005, he joined the Department of Electrical Engineering of Wright State University, where he is currently a Full Professor.