

A NEW HYBRID METHOD FOR SYNTHETIC APERTURE RADAR DECEPTIVE JAMMING

Jamal Saeedi

Electrical Engineering Department, Amirkabir University of Technology,
Tehran, Iran

ABSTRACT

Based on the synthetic aperture radar (SAR) geometric model, a novel, and fast algorithm of large scene deceptive jamming against different SAR systems is proposed. First, a template deceptive image is transformed into the time domain signal using inverse image formation algorithm. Then, the transformed signal is convolved with enemy's received SAR signal in order to cope with electronic counter-countermeasures (ECCM) techniques. Finally, the generated jamming signal is transmitted to enemy's SAR system for deceptive purpose. Specifically, we have proposed a hybrid method for SAR jamming, which uses a digital radio frequency memory (DRFM) system incorporating with SAR raw data simulation module. The experimental results for the proposed deceptive jammer demonstrate its ability to deceive SAR system.

KEYWORDS

Synthetic aperture radar; deceptive jamming; digital radio frequency memory; SAR raw data simulation.

1. INTRODUCTION

Synthetic aperture radar (SAR) is a powerful tool to discover targets under various kinds of conditions. SAR applications assist both the civilian and military subdivisions. Examples of SAR applications include: reconnaissance, surveillance, and targeting, treaty verification and non-proliferation, interferometry, foliage and ground penetration, navigation and guidance, moving target indication, change detection, and environmental monitoring [1]. The ability to produce images in day or night under all weather conditions is the most important feature of SAR.

In some military applications of SAR, the user encounters electronic warfare (EW). In these scenarios, the enemy employs a radar system to transmit a signal within the SAR system bandwidth to disturb the SAR system receiver, which is called SAR electronic counter measures (ECM) or jamming. The jamming signal goes through the SAR system receiver, which causes in severe distortions in the output image or formation of non-existent targets in the image. The methods used for suppressing the effect of the ECM jamming signal are called electronic counter-countermeasures (ECCM) [2]. The SAR ECM and ECCM are a pair of paradoxes, and they are developed with the advancement of modern SAR theories and technologies. Therefore, being familiar with all of the available ECCM methods is necessary for designing a SAR jamming system.

Generally, the SAR ECM technologies can be categorized into three kinds with respect to the jamming and the SAR transmitted signal relationship [3]. 1) Incoherent jamming such as a barrage jamming is referred when the jamming is within the same band of the SAR signal but incoherent in the range direction. 2) Partially coherent jamming such as a repeater jammer is called when the jamming is coherent in the range direction but incoherent in the azimuth direction [4]. 3) Coherent jamming, such as an active-decoy jamming is referred when the jamming is coherent in both the range and azimuth directions [5]. It can be generally said that coherency of jamming signal in two directions results in a false targets or deceptive image (in enemy's SAR image) with more quality and clarity. Therefore, coherent jamming is considered in this study.

There are different types of SAR ECCM techniques, e.g., the random waveform (such as the noise and chaotic waveform) method is now broadly utilized in the agile-waveform SAR, the space time adaptive processing technology is utilized in the multi-channel SAR [6], and the bi-static technology is also utilized in the bi-static SAR. Therefore, being familiar with all of the available ECCM methods is necessary for designing a SAR jamming system. An incoherent jamming can be easily generated but needs high-transmitted power, since it cannot obtain the signal processing gains of the linear frequency modulation (LFM) matched filtering during the SAR imaging process in both the range and azimuth directions. This kind of jamming can be easily detected by SAR due to its large transmitted power, and can be cancelled through a number of ECCM technologies, e.g., wideband sidelobe-cancellation, spatial filtering, and adaptive beam-forming. Partially coherent jamming needs relatively lower transmitted power comparing to the incoherent jamming. In order to achieve a good coherency with the SAR transmitted signal in the range direction, this kind of jamming usually utilizes a digital radio frequency memory (DRFM) based jammer structure. But it can still be easily detected by SAR due to its relatively high transmitted power which makes it to be distinguishable from the real targets in the imaging scene, and may be cancelled by the ECCM technologies mentioned above. Coherent jamming needs the least transmitted power comparing to the other two kinds of jamming mentioned above and is hard to be detected by SAR.

In this paper, a new hybrid method is proposed for deceptive jamming of SAR systems, which is robust against different SAR ECCM methods. This system can receive and store the signal emitted from a radar system, modify it by applying a target signature, and retransmit the modified signal towards the radar. This is done in real-time on each received radar pulse. The stored signal provides a high fidelity digital copy of the radar signal. The modifications or modulations applied can emulate the reflection processes that occur in real life so that the radar sees false targets with a natural radar signature. In addition, an idea based on sub-Nyquist sampling technology has been performed for jamming purpose, which can reduce the demands on sampling rate and processing speed.

The remainder of this paper is organized as follows. In Section 2, traditional methods of SAR deceptive jamming along with their pros and cons are presented. The proposed method based on large scene deceptive jamming and reconnaissance measurements is explained in Section 3. Section 4 illustrates experimental results for deceptive SAR jammer. Finally, conclusions are given in Section 5.

2. RELATED REVIEW

SAR deceptive jamming can be classified by three different groups including: DRFM-based approaches, SAR raw data generation based methods, and direct radio frequency processing (DRFP) based algorithms. In the following, we have reviewed some of previous works for deceptive jamming in the mentioned categories.

In a DRFM-based jammer, it is assumed that the centre frequency of the intercepted waveform is known to the jammer. A local oscillator generates an exponential at the known centre frequency that is then mixed with the intercepted radar. The baseband waveform enters an analogue to digital (A/D) converter where it is sampled at the sampling interval T_s to produce the discrete signal. A delay is introduced to the discrete signal creating a false range offset by means of a controller and is then stored in memory until the next predicted pulse repetition interval (PRI) [5]. The discrete delayed signal passes through a digital to analogue (D/A) converter and is mixed with an exponential at the known centre frequency resulting in the transmitted jammer signal. DRFM jammer simulation will consist of copying and delaying the radar signal (n number of samples) at the first PRI to introduce the false range offset. The DRFM-based jammer can be coherent or partly coherent. In coherent jamming, Doppler frequency information of SAR system

should be used to generate false target in azimuth direction of SAR image. In [6] a new generation DRFM-based system is being developed to introduce false targets in a high-range-resolution (HRR) radar and other high-resolution imaging radars. This paper describes a new type of DRFM-modulator that uses digital signal processing in the frequency-domain for generation of false targets [7]. The modulator is being implemented using parallel digital logic in a number of field programmable gate arrays (FPGA) on a single printed circuit board (PCB) for use in an experimental radar jammer named EKKO II [8]. In the EKKO II experimental radar jammer the synthesis of false targets are realized with direct modulation and are implemented in FGPA [8]. The main drawback of DRFM-based jamming is incapability to produce large deceptive image. It is only capable of generating isolated targets in the enemy's SAR image, which cannot properly protect distributed targets.

In SAR raw data generation-based methods, usually an inverse SAR image formation algorithm is used to generate raw data in time domain from an arbitrary deceptive image. Then the digital raw data is transformed to analogue using a D/A block. After that, the based-band signal is mixed with an exponential at the known centre frequency of SAR system resulting in the transmitted jamming signal [9]. In [10] Zhou et.al proposed a fast method to generate deceptive jamming signal for space-borne SAR. This method can be included in the category of raw data generation-based methods. It is mentioned in the paper that recently, several schemes were provided to achieve effective deceptive jamming of point targets in a short time; however, they are not applicable to the distributed targets [11]. In [12], a fast deceptive jamming method by retransmitting SAR echoes was proposed, but it is only applicable for small scene. The main issue concerned with this kind of jamming method is the complexity of the raw data simulation algorithm. In addition, the reconnaissance system should provide more detailed information of SAR system including the transmitting waveform.

DRFP is a new method in which both down-conversion and up-conversion modules are no longer needed as compared to DRFM-based jammer. Since no down-conversion is needed, the SAR signal received by jammer should be expressed in a form of Radio Frequency (RF) [13]. One can find that both DRFP-based and DRFM-based jamming have similar imaging output. That is, DRFP can achieve similar performance of DRFM but has a more simplified jammer structure, owing to its direct modulation in RF. Therefore, it has the same limitations as DRFM-based method.

In all of the mentioned methods, there should be a reconnaissance system to estimate SAR system parameters for jamming signal generation. Measurement errors may result in decreasing jamming performance in different scenarios.

3. PROPOSED METHOD

In this Section, we have presented the proposed deceptive SAR jammer. In a general jamming plan, different sources of SAR systems should be firstly identified. After identification of different threat sources using a reconnaissance system, the jammer should separately generate and send the jamming signal for each threat source, simultaneously. Different threat sources should be separated to air and space divisions. In the space division, since satellites travel in specific altitudes with approximately constant velocities, there is no need for a Doppler radar for real-time tracking. However, for the air division, since different airplanes flies at different speeds and altitudes, therefore there should be a Doppler radar for real-time tracking to provide range and velocity of different threat sources. In this strategy, all of the received signals are analysed in different frequency channels using an interception system, and in case of existing an effective signal, the jamming signal should be generated for it. We can receive and separate signals from different sources of radar systems using an active Doppler radar and a passive wideband receiver. If one can get the Doppler shift of every platform, then it is possible to use it for distinguishing

the different signal sources received by the wide-band receiver (since we have known Doppler shift of different platforms using the Doppler radar system). This can be accomplished by spectrum analysing of the received signal. The Doppler shift appears as a frequency displacement around a nominal carrier frequency.

A space-borne SAR sensor is installed on a satellite platform. In this case, the altitude and velocity of the platform are approximately constant. However, for an airborne SAR, it is possible to take image at different altitudes and velocities. Therefore, there is a need for a radar tracking system, which simultaneously provides range and velocity information of platform to the jamming module. Here, we have proposed a hybrid method for SAR jamming, which uses a DRFM system incorporating with SAR raw data generation module. First, platform range and velocity along with SAR system parameters including bandwidth, carrier frequency, pulse width, etc. should be estimated by an interception system. For detecting range and velocity of SAR platform, a Doppler radar can be used. An example of the interception system used for SAR system parameters estimation is shown in Fig. 1 (a). In this method, first, the existing signals are received using a wideband antenna. In next step, the received signals are passed through a low noise amplifier. Now, different frequency bands of the amplified signal are separated using a switching frequency. The signal is then passed through a bandpass filter in order to get better frequency spectrum isolation after switching. Then, the result signal is amplified and is separated into two branches using a power divider. One branch is used for carrier frequency detection and the second one is connected to a mixer. Given the overall block diagram shown in Fig. 1 (a), the baseband signal can be separated from the carrier frequency after mixer. The baseband signal is amplified and is digitized using an analogue to digital converter. The digital signal is analysed in processing unit in order to estimate other SAR system parameters including pulse repetition frequency, pulse width, bandwidth, imaging mode, etc.

Doppler radar is used to determine the approximate geometry of protected area with respect to the SAR platform. It is important to detect the SAR platform before entering the protected area. Having the SAR system parameters and geometry of the protected area, raw SAR data is generated by a predefined image for deception. Using inverse SAR signal processing algorithm we can obtain raw data for a sample image, which is used for deception. This procedure can be implemented in a FPGA board to incorporate with DRFM system. After that, raw SAR data are convolved with the intercepted SAR signals using DRFM system simultaneously.

After convolution, the resulting signal is transferred to D/A module and then goes through the mixer. After transferring signal into the frequency band of SAR system, it is transmitted through the antenna to the enemy's SAR receiver for deception. Block diagram of the whole jamming system is shown in Fig. 1 (b). In the proposed method, there is no need to identify the type of the transmitted waveform of enemy's SAR system. Therefore, it is superior as compared to the raw data generation-based method. In the following sub-sections, first we have presented basic principle of SAR signal modelling and processing. Then, the deceptive signal generation using inverse SAR image formation is described. Finally, details of signal reception and transmission in the proposed jamming method will be demonstrated.

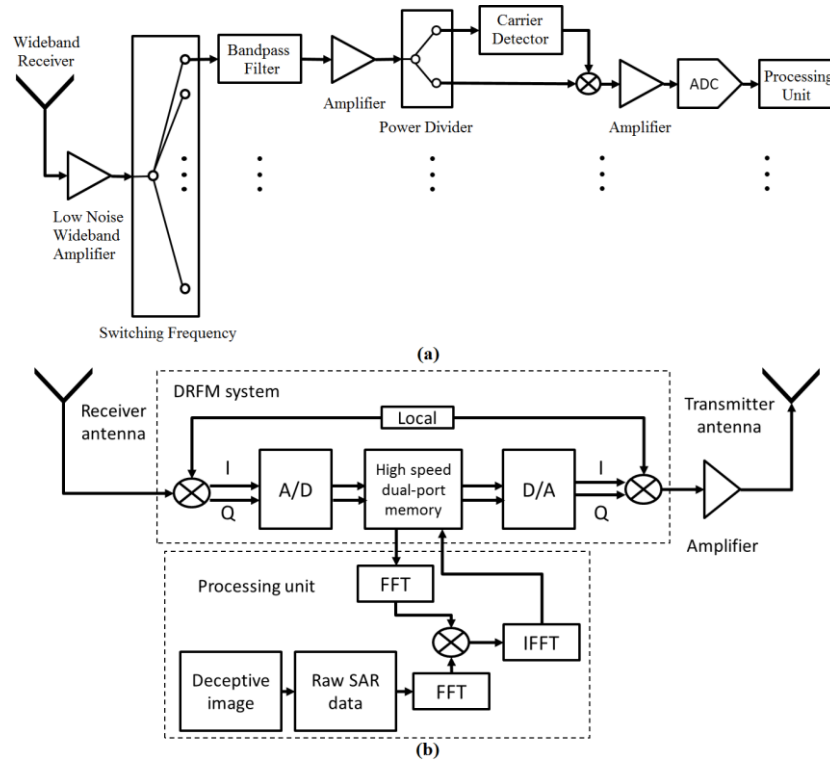


Figure 1. Block diagram of (a) the interception system, and (b) the proposed SAR deceptive jamming.

3.1. Basic principle of SAR signal modelling

This sub-section presents the fundamentals of SAR signal modelling. Before the SAR signal is generated, a number of important system parameters should be determined, including carrier frequency, bandwidth, pulse length, and pulse repetition frequency (PRF). The transmitted signal is a LFM waveform, where the signal spans the bandwidth over the pulse length. This cycle is repeated at the PRF. The SAR signal is usually generated at or near baseband and then mixed up to the desired operating frequency before transmission. The LFM transmit signal can be expressed as:

$$s_t(t) = A(t) \cdot \exp(j(2\pi f_0 t + \pi k_r t^2 + \varphi_0)) \quad (1)$$

where $A(t)$ is the signal amplitude and defines the pulse length with a rect function, f_0 is the frequency at the beginning of the chirp, k_r is chirp rate, and φ_0 is the starting phase which can usually be neglected

A power amplifier increases the signal power to a specified level in the transmission chain. An antenna propagates the amplified signal to the target area [14-16]. A very small portion of the transmit signal is reflected back to the radar. By neglecting the time-scaling influences on the pulse envelope, the echoed signal from target can be expressed as:

$$s_r(t, \eta) = A'(t) \cdot \exp(j(2\pi f_0(t - \tau) + \pi k_r(t - \tau)^2)) \quad (2)$$

where t is the fast time, η is the slow time (or azimuth time), and $A'(t)$ is an attenuated version of $A(t)$ and τ is the two-way time of flight to the target at range, $\tau = 2R/c$, where c is light speed.

The received signal is amplified with a low-noise amplifier (LNA) and mixed down to an appropriate band for sampling. After the signal from (2) is mixed down by a frequency, f_m , the signal ready to be recorded is as:

$$s_{rmd}(t) = A''(t) \cdot \exp(j(2\pi(f_0 - f_{md})t + \pi k_r(t - \tau)^2 - 2\pi f_0 \tau)) \quad (3)$$

where $A''(t)$ is an amplified version of $A'(t)$. For simplification let $f_m = f_0$, therefore,

$$s_{rm}(t, \eta) = A''(t) \cdot \exp(j(-2\pi f_0 \tau + \pi k_r(t - \tau)^2)) \quad (4)$$

SAR systems digitize this data and either store it on board, transmit it to a ground station, or process it on-board. In the following, a frequency domain algorithm for processing raw data will be described. The most frequently used algorithm for SAR signal processing is the range-Doppler algorithm (RDA) [17-18]. It was developed for processing SEASAT SAR data in 1978. There are three main steps to correctly focusing the data using RDA: range compression, range cell migration correction, and azimuth compression.

3.2. Deceptive signal generation using inverse SAR image formation

Here, we have used a method based on inverse SAR signal processing algorithm to generate jamming signal from deceptive image. The signal processing algorithm for image formation from raw data is discussed in previous sub-section. In order to generate a signal, which deceives enemy's SAR receiver, a similar process in opposite direction is performed using a deceptive image.

As it has mentioned in previous sub-section, the final step of image formation algorithm is azimuth compression. Therefore, the first step for raw data or deceptive signal generation is inverse azimuth compression. In the next step, the range cell migration is performed. Then, the resulting signal is transferred into the range-slow time domain using inverse FFT transform. At the end, an inverse matched filtering operation is performed with the transmitted signal as range reference function to obtain signal in fast time-slow time domain for deceptive jamming purpose. This signal should be transmitted in each period of pulse to the enemy's SAR receiver. The detailed information about the receiving and transmitting signal will be discussed in the next sub-section.

3.3. Details of signal reception and transmission

As described in sub-section 3.1, SAR in pulsed mode transmits frequency modulation signal with bandwidth of t_p . Then, it receives the echo signal between t_s and t_f times related to the minimum and maximum ranges. In order to generate deceptive signal there should be an interception system to detect transmitted signal from enemy's SAR system, transfer it to the baseband, and then digitize it using a DRFM system. Having the transmitted SAR signal samples and other system parameters, jamming signal can be generated using inverse SAR image formation. It should be mentioned that the received signal in interception system is used as range reference signal. In plan A of the proposed method, it is supposed that the transmitted signal waveform from enemy's SAR system does not change in each pulse.

When the enemy's SAR signal is intercepted along with system parameters, the jamming signal can be generated after a delay time τ . Now, we can send back the jamming signal to the receiver antenna of enemy's SAR system pulse to pulse. The details of transmitting jamming signal in each period are graphically shown in Fig. 2 (a). The methods used for suppressing the effect of the ECM jamming signal are called ECCM. An effective ECCM against DRFM repeat jammer-type systems is to measure the SAR signature of a target scene using a radar system that varies its transmitted pulse in the slow-time domain (from one PRI to another) [2, 19-20]. In this system,

the radar maintains the same band (carrier and bandwidth); however, the pulses are coded (diversified) to be approximately orthogonal to each other.

Such a radar is less susceptible to a DRFM repeat or adaptive jammer due to the following reasons: 1) the jammer cannot adapt easily since the radar signal is varying in the PRI (slow-time) domain, and/or 2) the signal transmitted by a DRFM repeat jammer at a given PRI (i.e., the radar signal that is used by the SAR system at the previous PRI) is approximately orthogonal to the radar signal that the SAR system is utilizing at the current PRI and, thus, a matched filtering with the updated (current PRI) radar signal would weaken the DRFM repeat jammer signal.

In plan B of the proposed method, it is assumed that the transmitted waveform of enemy's SAR system is changed in different periods or pulse-to-pulse. In this case, the transmitted signal should be extracted in each period using the interception system, and then the deceptive signal information should be modulated on this signal. To aim this, first the jamming signal in range frequency-slow time domain is generated from a deceptive image using intercepting of enemy's SAR system parameters. Then, the transmitted SAR signal is received and digitized in each period using the interception system. Finally, each pulse of generated jamming signal is convolved with the received signal and it is sent back to the enemy's SAR system antenna, respectively. Graphical representation of transmitting deceptive jamming signal in plan B is shown in Fig. 2 (b).

A key parameter in plan B of the proposed method is maximum time allowed for convolving jamming signal with the received signal from enemy's SAR system. The time limit for processing can be calculated with respect to Fig. 3 as follows:

$$t_{R_{jam}} = \frac{(2 \times R_{jam})}{3e^8}, t_{R_{min}} = \frac{(2 \times R_{min})}{3e^8} \rightarrow T_{limit} = t_{R_{min}} - t_{R_{jam}} \quad (5)$$

As shown in Fig. 2 (b), in order to modulate jamming signal we need a FFT, a phase multiply and an IFFT. Implementation time of these three steps in plan B of the proposed method should be less than the estimated time in (5). One direct method to decrease the computational cost for jamming signal modulation with the received signal samples is sub-Nyquist sampling.

The theory of Shannon–Nyquist has indicated that a signal can be recovered exactly from measurements uniformly sampled by an A/D whose sampling frequency is no less than twice of the signal bandwidth. Thus, a high quality A/D is extremely needed to achieve the optimal reconstruction of the broadband radar signal, which may become practically infeasible. Actually, there is no need for a jammer to sample the radar signal at such a high rate since the purpose of the jammer is not to reconstruct it but to interfere it. Sub-Nyquist sampling has been developed and utilized in several applications such as data compression, medical imaging and radar imaging. Under-sampling at low rates will lead to aliasing and corresponding reconstruction algorithm

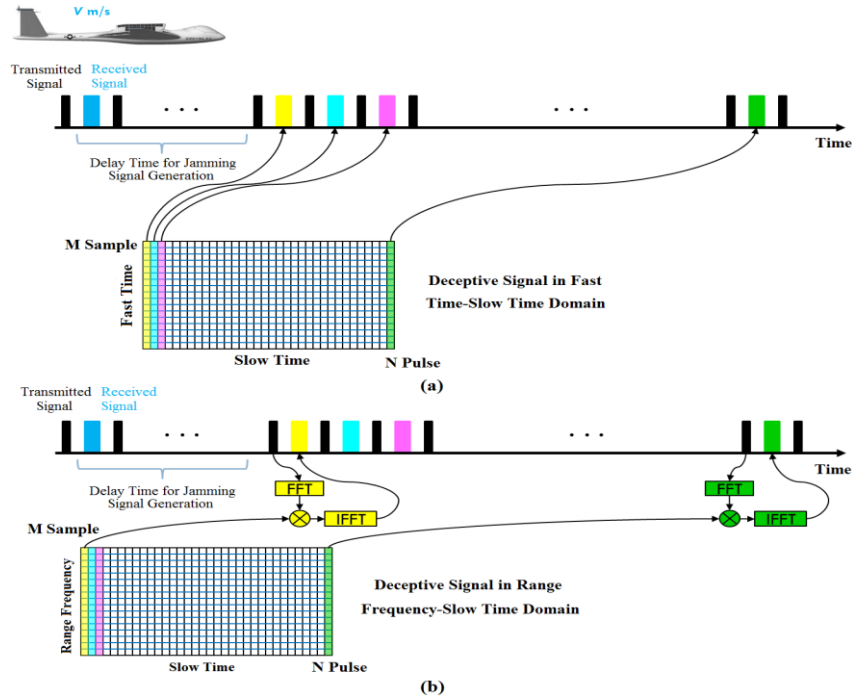


Figure 2. Graphical representation of transmitting generated jamming signal in each period of (a) plan A, and (b) plan B of the proposed method.

should be addressed as a prior condition. However, this is usually impractical in the electronic warfare since the jammer and the radar are non-cooperative.

Inspired by this characteristic, Pan et al. [21] propose an inverse SAR (ISAR) jamming idea based on the sub-Nyquist sampling technology which can reduce the demands on sampling rate and processing speed. The transmitted pulses of radar are sampled under the sub-Nyquist sampling theorem by the jammer and the signals formed by the samples are modulated by a target template. After that, the jamming signals are sent to the radar imaging system and a train of false-target images will be induced in the RD imaging plane. Here, we have used the same procedure proposed in [21] for jamming signals modulation in order to decrease the computational cost. However, other methods can be used for improving the accuracy and quality. In the next Section, the results of generating jamming signal with lower Nyquist rate for decreasing computational cost has been shown.

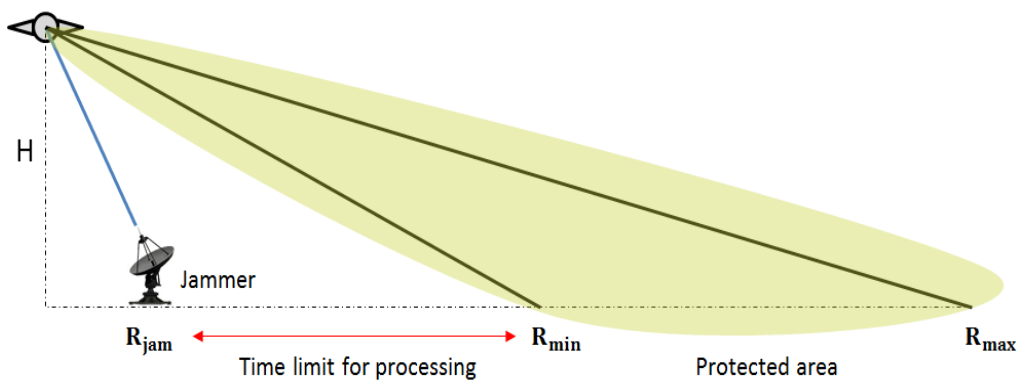


Figure 3. Graphical representation of time limit calculation for transmitting jamming signal in plan B of the proposed method.

4. EXPERIMENTAL RESULTS

In this Section, the experimental results of the proposed SAR deceptive jammer are presented. In order to evaluate the proposed deceptive jammer, two synthetic images along with two real SAR images are used to generate raw signals as the real and deceptive SAR signals (see Fig. 4). SAR system parameters used in the experiment are shown in Table 1. The SAR system works in the Stripmap mode and it is assumed that the SAR system parameters are fully known by jammer module in order to generate deceptive signal. In the following, we have also discussed about the errors in parameters estimation using interception module and its effects on the jamming performance. It should be mentioned that the inverse SAR signal processing method is used for generating raw signal for deceptive signals from deceptive image, which is discussed in previous chapter. However, we have used the traditional method of raw signal generation from real SAR image in the experiment. To generate raw signal from real SAR image, SAR image should be resampled (or interpolated) based on the simulation

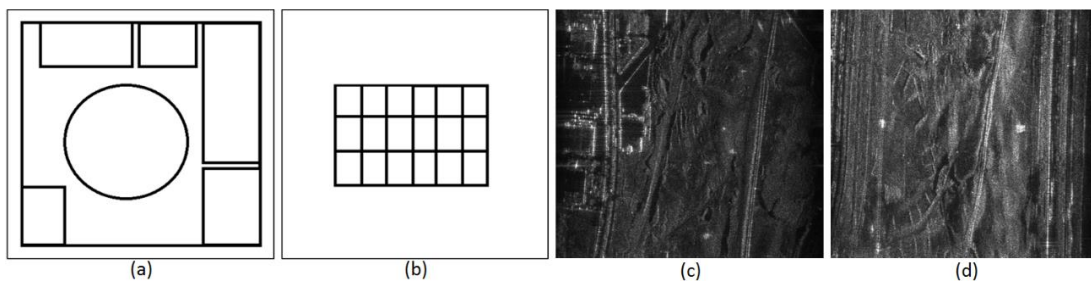


Figure 4. The synthetic and real SAR images used for raw signal generation as (a) ,(c) real and (b), (d) deceptive images.

Table 1. Two sets of SAR system parameters used for simulations.

Parameter	Value	Parameter	Value
Velocity (m/s)	120, 90	Carrier frequency (GHz)	9, 5
Bandwidth (MHz)	200	Sampling frequency (MHz)	500
Pulse width (μ s)	30		28
Swath width (m)	700	Flight time (s)	45350, 28713
PRF (Hz)	150, 100	Minimum Range (m)	46108, 29062
Altitude (km)	35, 25	Maximum Range (m)	2
Incident Angle (deg)	40, 30	Elevation beamwidth(deg)	1
		Azimuth beamwidth(deg)	

parameters including the swath width, flight time, and range and azimuth resolutions. After resampling, each sample in the image should represent a resolution cell on the ground for SAR echo simulation. Then, delay time τ should be obtained for each point target or image sample using the SAR imaging geometry, and the raw signal is obtained using the model described in (4). Finally, all of the raw signals for image samples are weighted summed with their corresponding amplitudes in the resampled SAR image.

The deceptive jamming results for different jammer-to-signal ratios (JSRs) are shown in Figs. 5 and 6. The vertical direction is azimuth, and the horizontal direction is ground range. For these experiments, raw signals are generated for both real and deceptive images using the proposed scheme and then they have added with different JSRs. Finally, the output image is obtained using the signal-processing algorithm (RDA) on the added signal. As it can be seen from the results, the JRS around 20 dB is required to have a deceptive image with good quality in the enemy's SAR system. In order to determine the required power for transmitting jamming signal on the ground,

the power of received SAR signal should be measured. Considering 20 dB JSR and signal attenuation in antenna sidelobe level about 20 dB, the jamming transmitting power should be more than 40 dB of received SAR signal power.

Another experiment has been conducted here to show the effect of noise in jamming results. After generating the SAR raw signal, radio frequency (RF) noise is added to it (RF noise is simulated through filtering the Gaussian noise). It should be mentioned that because of the randomness property of noise, RF noise is generated once, and it is used similarly for different this experiment. It can be seen from Fig. 7 that apart from the signal-to-noise-ratio (SNR) the jamming results are depended to the JSR, because the noise has similar effect on both jamming and real SAR signals.

As we have discussed in previous Section, sub-Nyquist sampling can be used for decreasing computational cost of the signal modulation step in the plan B of the proposed method. The results of jamming signal generation with sub-Nyquist sampling in the proposed method are shown in Fig. 8. From the results, one can see that with reducing 8 times of Nyquist criteria for sampling, the deceptive image is still visible over the real SAR image.

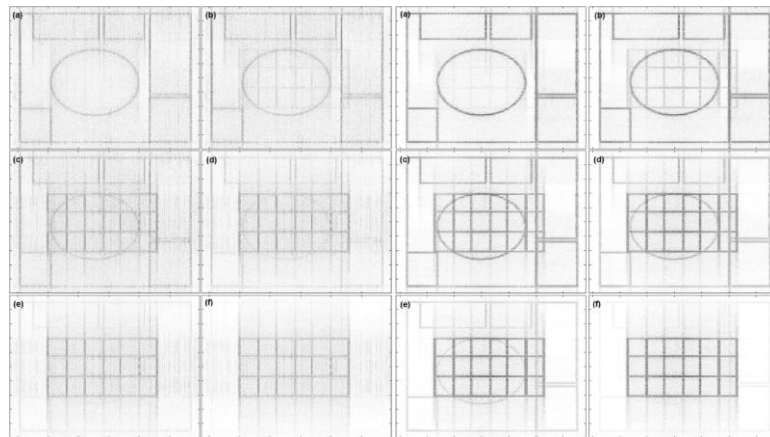


Figure 5. The results of proposed jamming scheme using synthetic images obtained with two sets of simulation parameters (left: X band, right: C band) for different JSRs (a) -20, (b) -10, (c) 0, (d) 5, (e) 10, and (f) 20 (dB).

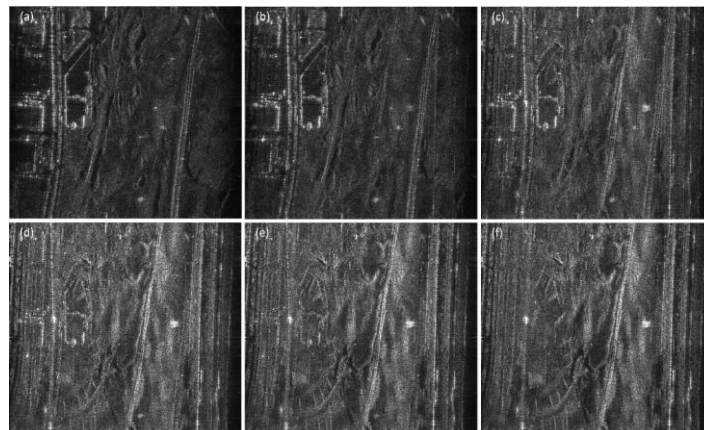


Figure 6. The results of proposed jamming scheme using real SAR images for different JSRs (a) -20, (b) -10, (c) 0, (d) 5, (e) 10, and (f) 20 (dB).

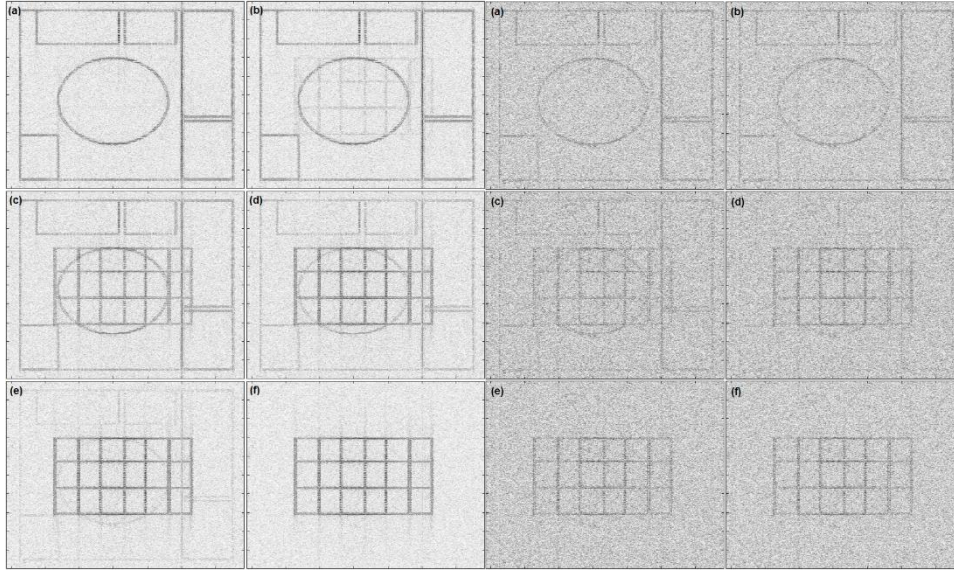


Figure 7. The results of proposed jamming scheme using synthetic images obtained by set two (C band) of simulation parameters (left: -10 SNR, right: -20 SNR) for different JSRs (a) -20, (b) -10, (c) 0, (d) 5, (e) 10, and (f) 20 (dB).

We can divide SAR system parameters into two groups, which are important for jamming signal generation. First group of parameters is obtained using Doppler radar including range to target and platform speed. The mentioned parameters are directly used in deceptive jamming signal generation. However, second group of parameters including pulse repetition frequency, carrier frequency, bandwidth, and pulse width has important role in accurately extracting of the received SAR signal. The second group of parameters is estimated using the interception system. Small errors for these parameters can decrease the performance of deceptive image. However, for large errors, the received SAR signal cannot correctly be extracted and therefore the deceptive image is no longer dominant in the enemy's SAR system image. Here, we have only analysed errors in the first group of parameters, which is estimated using Doppler radar. Simulation and error analysis of the second group of parameters requiring hardware implementation of the system, which is beyond the scope of this paper.

The jamming results for error analysis of range to platform and platform speed estimations are shown in Figs. 9 and 10. From the results, one can see that error in platform range causes to shift the deceptive image in the range direction. This means that the protected area on the ground is not correctly covered with deceptive image. It can be seen in Fig. 9 that with increasing the error in platform range, the deceptive image is shifted with the same amount along the range axis. As a result, one can conclude that the jamming system is not sensitive to the platform range error up to few meters. From the results related to speed error analysis shown in Fig. 10, one can see that error in speed estimation results in target blurring in azimuth direction. This is because the error in platform speed estimation causes error in Doppler bandwidth in the deceptive signal generation step. Therefore, azimuth compression cannot be efficiently performed in enemy's SAR system and results in target blurring in azimuth direction.

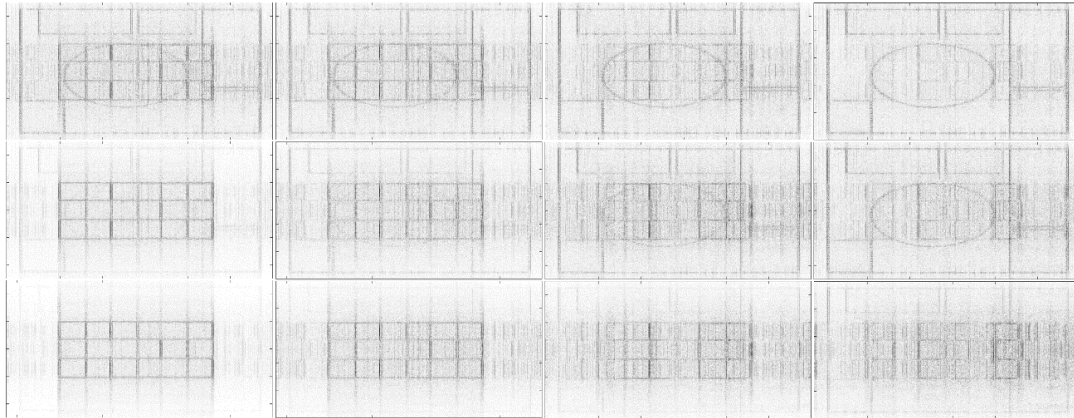


Figure 8. The results of proposed jamming scheme obtained by set one of simulation parameters (X band): top to bottom: 5, 10 and 20 dB JSR and left to right: different sampling rates f_s , $f_s/2$, $f_s/4$, and $f_s/8$.

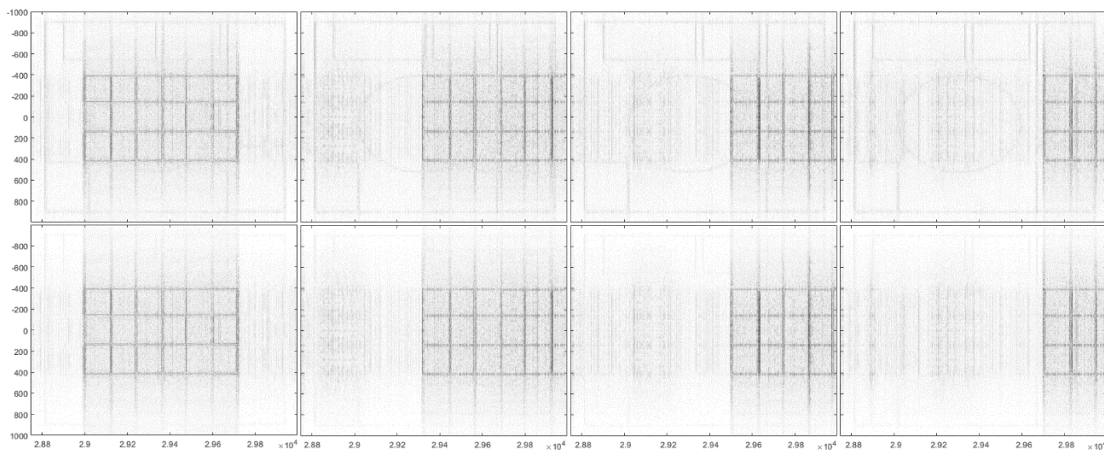


Figure 9. The results of proposed jamming scheme obtained by set one of simulation parameters (X band) for different errors in platform range estimation from left to right: 0, 150, 250, and 350 meters, top to bottom: 10 JSR and 20 JSR.

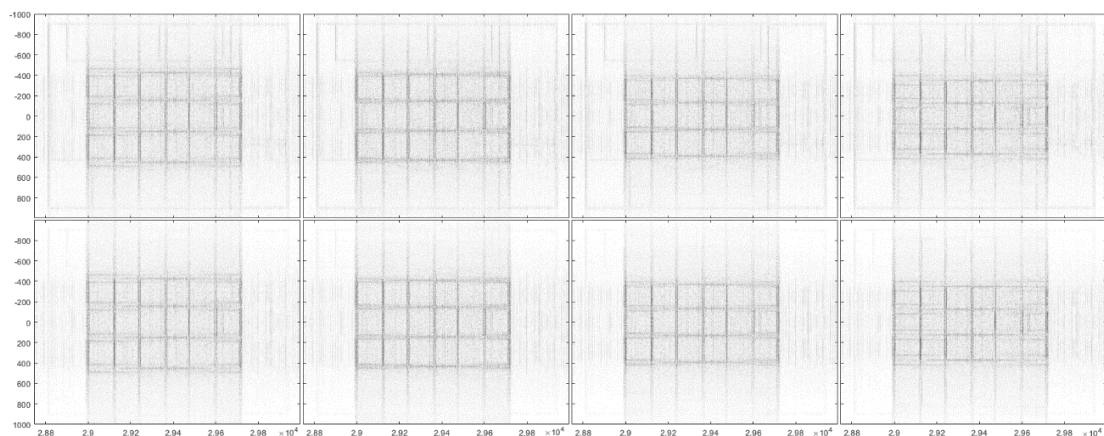


Figure 10. The results of proposed jamming scheme obtained by set one of simulation parameters (X band) for different errors in platform velocity estimation from left to right: -10, -5, +7, and +14 m/s, top to bottom: 10 JSR and 20 JSR.

From the results, one can conclude that the jamming system is not sensitive to the platform speed error up to few meters per second and deceptive image is generated with good quality.

5. CONCLUSIONS

This paper presents a new method for large scene deceptive jamming against the SAR system. This new method is capable of deceiving SAR system by generating and transmitting a synthetic image. Specifically, we have added a new module in the proposed jammer structure, which modulates jamming signal with received SAR signal. As a result, the proposed jammer method will be robust with respect to the ECCM methods used by enemy's SAR system. The experimental results for the proposed deceptive jammer demonstrate its ability to deceive SAR system. In addition, parameters error analysis indicates low sensitivity of the proposed jammer system.

REFERENCES

- [1] Saeedi, J. (2015). Synthetic Aperture Radar Signal Processing Using Nonlinear Frequency Modulation and Phase Error Compensation. Ph.D. Dissertation, Electrical Engineering Dept., Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran.
- [2] Garmatyuk, D., Narayanan, R. (2002). ECCM capabilities of an ultrawideband bandlimited random noise imaging radar. *IEEE Trans on Aerospace and Electronic Systems*. 38(4), 1243-1255.
- [3] Hong-xu, H., Yi-yu, Z., Jing, W., Zhi-tao, H. (2010). A Frequency-based Inter/Intra Partly Coherent Jamming Style to SAR. *International Conference on Signal Processing Systems*, 434-438.
- [4] Wu, X., Dai, D., Wang, X., Lu, H. (2007). Evaluation of SAR jamming performance. *International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communication*, 1476-1479.
- [5] Dai, D., Wu, X., Wang, X., Xiao, S. (2007). SAR active-decoys jamming based on DRFM'. *IET International Conference on Radar System*, 1-4.
- [6] Klemm, R. (2002). *Principles of Space-time Adaptive Processing (3rd Edition)*. The Institution of Engineering and Technology, London, United Kingdom.
- [7] Saper, R.H., Dyck, D. (1999). A computed approach to electronic countermeasures for deception of high resolution radar. *International conference and exhibition on radar systems*, 1-4.
- [8] Kristoffersen, S., Thingsrud, O. (2004). The EKKO II Synthetic Target Generator for Imaging Radar'. *Proceedings of EUSAR*, 1-4.
- [9] Yu, M., Zhang, Z., Li, G., Li, J., Gao, P. (2008). SAR Interfering Based on Fast Simulation of SAR Raw Signal. *International Conference on System Simulation and Scientific Computing*, 652-654.
- [10] Zhou, F., Zhao, B., Tao, M., Bai, X., Chen, B., Sun, G. (2013). A Large Scene Deceptive Jamming Method for Space-Borne SAR. *IEEE Trans on geoscience and remote sensing*, 51(8), 4486-4495.
- [10] Long, S., Hong-rong, Z., Yue-sheng, T., Chang-yao, Z. (2009). Research on deceptive jamming technologies against SAR. *Proc of APSAR*, 521-525.
- [11] Sun, G., Zhou, F., Xing, M., Bao, Z. (2009). Deception-jamming technology against the SAR based on the deceptive scene and real-time analyses. *J Xidian Univ*, 36(5), 813-818.
- [12] Liu, Q., Dong, J., Wang, X., Xing, S., Pang, B. (2013). An efficient SAR jammer with direct radio frequency processing (DRFP). *Progress in Electromagnetics Research*, 137, 293-309.

- [13] Saeedi, J. (2017). Feasibility Study and Conceptual Design of Missile-Borne Synthetic Aperture Radar. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, PP(99), 1-12.
- [14] Liu, Y., Deng, Y., Wang, R., Yan, H., Chen J. (2012). Efficient and precise frequency-modulated continuous wave synthetic aperture radar raw signal simulation approach for extended scenes. *IET Radar, Sonar & Navigation*, 6(9), 858-866.
- [15] Saeedi, J., Alavi S.M. (2015). Improved navigation-based motion compensation for LFM-CW synthetic aperture radar. *Signal Image and Video Processing*, 10(2), 405-412.
- [16] Saeedi, J., Faez, K. (2016). Synthetic Aperture Radar Imaging Using Nonlinear Frequency Modulation Signal. *IEEE Transactions on Aerospace and Electronic Systems*, 52(1), 99-110.
- [17] Saeedi, J., Faez, K. (2016). A back-projection autofocus algorithm based on flight trajectory optimization for synthetic aperture radar imaging', *Multidimensional Systems and Signal Processing*, 27(2), 411-431.
- [18] Garmatyuk, D., Narayanan, R. (2002). ECCM capabilities of an ultrawideband bandlimited random noise imaging radar. *IEEE Trans on Aerospace and Electronic Systems*, 38(4), 1243-1255.
- [19] Kulpa, K., Lukin, K., Miceli, W., Thayaparan T. (2008). Signal Processing in Noise Radar Technology. *IET Radar, Sonar & Navigation*, 2(4), 229-232.
- [20] Pan, X., Wang, W., Feng, D., Liu, Y., Fu, Q., Wang, G. (2014). On deception jamming for countering bistatic ISAR based on sub-Nyquist sampling. *IET Radar, Sonar & Navigation*, 8(3), 173-179.

AUTHOR

Jamal Saeedi received the B.Sc. degree in Biomedical Engineering from Sahand University of Tabriz, Iran in 2007, and his M.Sc. and Ph.D. degrees in Electronic Engineering from Amirkabir University of Tehran, Iran in 2010 and 2015, respectively. He has over 18 publications in various areas, including signal and image processing, radar, and synthetic aperture radar. His current research interests include signal and image processing, specializing particularly in information fusion, pattern recognition, road traffic monitoring systems, and synthetic aperture radar signal processing.

