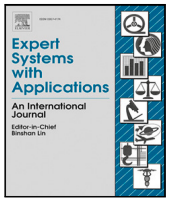
Expert Systems With Applications 249 (2024) 123670

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa



# Exploring an early warning system for maritime security risks: An approach based on compressed sensing

Xinran Li [a], Wei Wang [a,*], Hao Gu [b], Kun Jin [a]

[a] School of Transportation, Southeast University, No. 2 Southeast University Road, Jiangning District, Nanjing 211189, China
[b] No. 723 Institute, China State Shipbuilding Corporation, No. 186 Wuzhou East Road, Yangzhou 225000, China

ARTICLE INFO

*Keywords:*
Maritime security
Piracy threat
Risk warning
Ship detection
Compressed sensing

ABSTRACT

Piracy has posed intractable challenges to maritime security and the global economy. This study introduces a real-time early warning system designed to monitor piracy activity in the vicinity of merchant vessels, thereby facilitating the assessment and countermeasure of potential attacks. The approach employs frequency agile radar to identify pirate ships characterized by aggregation and jamming behavior. To address the computational difficulties caused by changing frequencies, compressed sensing with a tailored target information processing procedure is applied to reconstruct the radar observation scene. The developed target detection algorithm yields precise information about nearby pirate ships, enabling a comprehensive evaluation of the risk level and the subsequent recommendation of an appropriate security scheme. Extensive experiments have shown that the proposed early warning model can provide best warning performance compared to other benchmark models, with an average accuracy of 0.964, precision of 0.966, recall of 0.955, F1 score of 0.960.

## 1. Introduction

Maritime transportation is the dominant mode of intercontinental logistics and has gained a continuing growth over the past decades. Since maritime transportation operates mostly in international trades, vessels need to cross multiple national jurisdictions, thus posing new security challenges to operators (Christiansen et al., 2007). As the international maritime organization's (IMO's) slogan "*Safe, secure and efficient shipping on clean oceans*" reflects, maritime security research has always been a remarkable focal point. Pirate attack, due to the substantial economic loss and even human life threats, is recognized as a representation of non-traditional attacks and one of the most critical maritime security issues nowadays (Bryant et al., 2014; Lee & Song, 2017).

Acquisitive piracy crime has long been a notable risk factor when traveling the less regulated areas. As shown in Fig. 1, there occurred more than 200 incidents with regard to pirate attacks each year. Taking high-value oil transportation as an example, the number of piracy attacks on crude oil tankers peaked at 61 in 2011 and 19 in 2017 (Jin et al., 2019). The severe consequences, including cargo loss, ransom payments and kidnapping of seafarers, pose enormous economic pressure to ship operators. It is documented that the piracy-related costs of Maersk Line were at least USD 20 million in 2011 to cover insurance premiums, hardship allowances, and the costs of rerouting vessels (Leach, 2011).

Authorities and the shipping industry are investing significant amounts of capital and effort into the improvement of maritime security. For instance, deploying foreign naval to escort ships and designing the best management practices (BMP) to give guidelines on dealing with pirate attacks (Vespe et al., 2015). However, these efforts are implemented only partly due to the expensive costs. A marine piracy prediction and prevention framework to better coordinate risks and costs is thus highly anticipated. In this study, the challenge is responded by designing an early warning system that can monitor and report pirating activities in real-time.

An important prerequisite task of the early warning system design is to select a suitable sensing modality for detecting pirating activities. In this regard, the main features in the typical pirate attack scenario are worth highlighting (Bryant et al., 2014; Tumbarska, 2018): (i) probably occurring in darkness and inclement weather conditions; (ii) pirate ships are usually small and sail fast; (iii) detection of pirate ships may be disturbed by sea conditions; (iv) pirate ships may use jamming measures to mislead the detection.

Feature (i) implies that the selected sensing modality should not be vulnerable to light and weather. Thus cameras, lidar and infrared sensors are ruled out. Feature (ii) suggests that the scenarios under consideration require the detection of small moving targets at long ranges, making millimeter-wave radar with a shorter detection range

* Corresponding author.
*E-mail addresses:* xinran.li@seu.edu.cn (X. Li), wangwei@seu.edu.cn (W. Wang), guhao723@outlook.com (H. Gu), jinkun@seu.edu.cn (K. Jin).

https://doi.org/10.1016/j.eswa.2024.123670
Received 9 January 2023; Received in revised form 9 December 2023; Accepted 12 March 2024
Available online 21 March 2024
0957-4174/© 2024 Elsevier Ltd. All rights reserved.

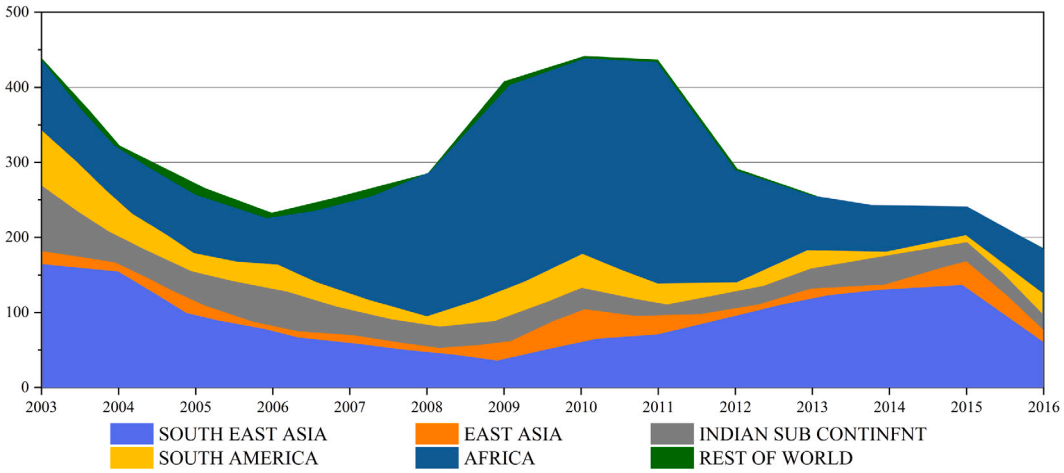



**Fig. 1.** Global pirate attack statistics.
*Source:* Watanabe et al. (2017).

unsuitable. In this context, pulse radar, which can offer long-range real-time detection, is an applicable sensor. Moreover, features (iii) and (iv) pose additional disturbances to radar detection. A specific pulse radar, frequency agile radar, is thus selected for its stable detection and anti-jamming performance (Quan et al., 2016).

Despite the benefits offered by frequency agile radars, the changing frequencies bring difficulties to the signal processing process. Generally, the detection performances of frequency agile radars rely on the prior information on the number of targets (Huang et al., 2018). The pirating activities, however, are unpredictable and full of uncertainties. To the best of our knowledge, researchers have not treated the problem in much detail, which hinders the adoption of frequency agile radars in pirate attack detection. These practical necessities provide strong motivations for the investigation into a tailored algorithm to assist the target information processing in this study.

This study aims to design an early warning system for maritime security risks, especially pirate attacks. The proposed system alarms for merchant vessels based on the moving target detection technique. The vessels receiving warning signals could activate an appropriate security scheme to defend against potential attacks. The main contributions of this study are summarized as follows:

- A practical systematic framework is proposed to tackle the challenging problem of real-time early warning for pirate attacks.
- A tailored target information processing algorithm is developed to improve moving target detection results.
- Extensive experiments are conducted to reveal that the proposed system enables accurate warning levels and outperforms baseline models.

The remainder of this paper is organized as follows. Section 2 reviews relevant literature. Section 3 proposes the methodologies, including an overview of the system framework, moving target detection, risk level assessment and decision-making support. Simulation results are presented in Section 4, and conclusions are provided in Section 5.

## 2. Literature review

As has been the case for other warning systems, identifying risk factors is paramount. In the case of preventing piracy, risk factor refers to the activity of pirate ships (Bryant et al., 2014). Thus, the first objective of this study is to monitor pirating activities precisely and timely. The second objective is to assess and report the potential threat level based on the obtained piracy information. In this section, the relevant literature on these domains is reviewed.

### 2.1. Maritime ship detection

Due to its essential role in maritime security, ship detection has been the topic of extensive research over the last decades. Ship detection via sensors, such as surveillance video systems, Satellite remote sensing and Synthetic Aperture Radar (SAR), have attracted significant attention in the past decades. Table 1 lists the comparison of sensors that have been selected in previous studies. It is noted that machine learning approaches have been in ship detection recently. For example, Chen et al. (2020) proposed a hybrid deep learning method that combines a modified Generative Adversarial Network (GAN) and a Convolutional Neural Network (CNN)-based detection approach to detect small ships based on video surveillance systems. Alghazo et al. (2021) proposed a CNN-based model to improve the ship identification accuracy from satellite images. Zhang et al. (2021) published a public ship detection dataset with accurate labels, in which several state-of-the-art detection algorithms are evaluated to give a benchmark for deep-learning-based ship detection methods.

To the best of our knowledge, few studies have focused on the detection of pirate attacks. Although machine learning models have been used in ship detection and achieved good performance, they are not applicable in pirate ship detection. The performances of machine learning based methods are highly dependent on the quality of training datasets. Risky pirate attack scenarios make it difficult to obtain available data and afford time-consuming training process. Some studies have attempted to find more tailored solutions. Touchton et al. (2013) implemented an automated system to track and identify piracy threats using a low-cost commercial radar. Motivated by the portability and flexibility of Unmanned Aerial Vehicle (UAV), (Watanabe et al., 2017) conducted an experimental study on adopting UAV drones to prevent pirate attacks. However, these selected sensors are not competent for pirate ship detection, as shown in Table 1. The comparison motivates us to select the frequency agile radar as the sensing modality of the proposed early warning system and develop an efficient detection method for monitoring pirating activities.

### 2.2. Pirate attack risk assessment

Maritime accident analyses, including accident causation analysis (Chen et al., 2013; Goossens & Glansdorp, 1998), analysis on spatial–temporal characteristics (Huang et al., 2013; Sui et al., 2023) and navigation risk assessment (Li et al., 2012, 2014; Panahi et al., 2020; Wu et al., 2015), have become highly discussed topics (Luo & Shin, 2019; Psarros et al., 2010). To classify broadcast navigational warnings efficiently and accurately, Liu et al. (2018) presented

**Table 1**
Comparison of sensors (See Chen et al. (2020, 2021), Cui et al. (2019), Felzenszwalb et al. (2009), Henschel et al. (1998), Pieralice et al. (2017), Prayudi et al. (2020), Touchton et al. (2013), Tran and Le (2016), Wackerman et al. (2001), Watanabe et al. (2017), Xu et al. (2014), Yang et al. (2018) and Yao et al. (2017)).

| | Surveillance video | SAR | Satellite remote sensing | UAV drone | MMWR | GNSS-based radar | SFAR |
|---|---|---|---|---|---|---|---|
| | Felzenszwalb et al. (2009)<br>Tran and Le (2016)<br>Chen et al. (2020) | Henschel et al. (1998)<br>Wackerman et al. (2001)<br>Cui et al. (2019) | Yao et al. (2017)<br>Yang et al. (2018)<br>Chen et al. (2021) | Xu et al. (2014)<br>Watanabe et al. (2017)<br>Prayudi et al. (2020) | Touchton et al. (2013) | Pieralice et al. (2017) | This paper |
| Adverse weather conditions | ✕ | ● | ✕ | ✕ | ● | ● | ● |
| Harsh lighting conditions | ✕ | ● | ● | ○ | ● | ● | ● |
| Complex sea conditions | ○ | ○ | ○ | ✕ | ○ | ○ | ● |
| Contour detection | ● | ○ | ○ | ● | ✕ | ✕ | ✕ |
| Penetrating power | ✕ | ● | ● | ● | ● | ● | ● |
| Radia distance | ○ | ● | ● | ○ | ○ | ● | ● |
| Resolving power | ● | ● | ● | ● | ● | ○ | ● |
| Anti-jamming capability | ○ | ○ | ● | ✕ | ○ | ○ | ● |

Notes: ✕ denotes limited, ○ denotes average and ● denotes good.

a well-performed classifier by comparing several machine-learning approaches. Kretschmann (2020) proposed a machine learning-based approach to calculate leading maritime risk indicators for ships. However, as an important branch, the risk assessment methods of pirate attacks are currently not well researched by the maritime community, which may lead to potential disastrous consequences. Through historical statistics analyses based on the logistic regression, Jin et al. (2019) and Psarros et al. (2011) attempted to estimate the probability of a vessel being attacked by pirates and the success rate of piracy. They focused on risk factor identification of pirate attacks. Focusing on the situational factors that help prevent pirate attacks, Bryant et al. (2014) and Shane and Magnuson (2016) analyzed the impact of countermeasures taken on the success probability of such attacks. These valuable studies supports the development of real-time risk assessment model for pirate attacks in this study.

## 3. Methodology

In this section, an early warning system customized for pirate attacks is designed. Specifically, Section 3.1 describes the system framework. Subsequently, Section 3.2 introduces a tailored target detection method, followed by quantitative risk assessment in Section 3.3. Finally, Section 3.4 details decision-making support, including countermeasure recommendation and customized warning interface design.

### 3.1. Overview of the system framework

The overview of the system framework is expressed in Fig. 2. The entire operation is fully automated. The proposed early warning system can be considered as composed of three subsystems: target detection subsystem, data processing subsystem and decision support subsystem. As depicted, the operating procedure starts with detecting threat targets. Potential targets are detected accurately with the location and speed information using the target detection subsystem. To enhance the reliability of the warning reports, the threat targets can also be tracked in time. Once the threat targets have been identified, the target data will be embedded in map services and the potential attack will be assigned a risk level. The decision support subsystem then reports the early warning and provides a suite of countermeasures on the warning interface to engage the attack.

Three main stages in the operating procedure are listed below, in which the detailed methodologies are described in the following section.

(1) *Target detection and identification.* Small, clustered and fast-moving targets are typically identified as threat targets. The target detection system identifies the targets in time using selected sensors.

(2) *Data processing and risk level assessment.* The data processing platform aggregates and incorporates the target information into the positioning services. Then a risk level will be determined, which are dictated by piracy capabilities.

(3) *Decision-making support.* Upon receiving a warning signal, the decision-making subsystem will offer valuable guidance on the customized warning interface to help crews defend against the impending attack.

### 3.2. Moving target detection

One key task in the early warning system is to identify potential threatening targets as accurately as possible. Despite the benefits offered by random hopping of carrier frequency between pulses, the changing echo Doppler brings difficulties to the signal processing process. This section thus develops a compressed sensing based approach to assist the signal processing.

First, an empirical echo signal model is introduced to describe the dynamics of sea conditions. Then, the compressed sensing (CS) model and the Orthogonal matching pursuit (OMP) algorithm are utilized to reconstruct the radar observation scene. Lastly, a tailored target information processing algorithm is developed to obtain the number, location and speed of targets from the reconstructed scene.

#### 3.2.1. Signal model in sea wave environments

Different from common radars, frequency agile radars transmit a series of pulses with randomly varying carrier frequencies. As depicted in Fig. 3, there are $N$ pulses in a coherent processing interval (CPI). The frequency $f_n$ at pulse $n$ is determined by the following equation:

$$f_n = f_c + d_n \Delta f, n = 0, 1, \ldots, N-1 \tag{1}$$

where $f_c$ is the initial carrier frequency, $\Delta f$ is the frequency step, and $d_n$ denotes the frequency modulation code. For each frequency agile radar, there can be $M$ different types of frequency levels: $d_n$ is randomly selected from a discrete integer set $D_n = \{0, 1, \ldots, M-1\}$. Thus $B_s = M\Delta f$ is the called frequency hopping bandwidth.

The $n$th transmitted monotone pulse signal at time $t$ is dependent on the frequency $f_n$, which can be calculated using the standard rectangle function $\mathrm{rect}(\cdot)$:

$$S_t(n,t) = \mathrm{rect}(\frac{t - nT_r}{T}) e^{j2\pi f_n (t - nT_r)} \tag{2}$$

where $T$ is the pulse width and $T_r$ is the pulse repetition interval.

Taking multiple moving targets in a certain coarse range cell contains $G$ into account, the received signal in the cell can be stated as

$$S_r(n,t) = \sum_{g=1}^{G} \beta_g e^{j2\pi f_n (t - nT_r - \frac{2(r_g + v_g n T_r)}{c})} \tag{3}$$

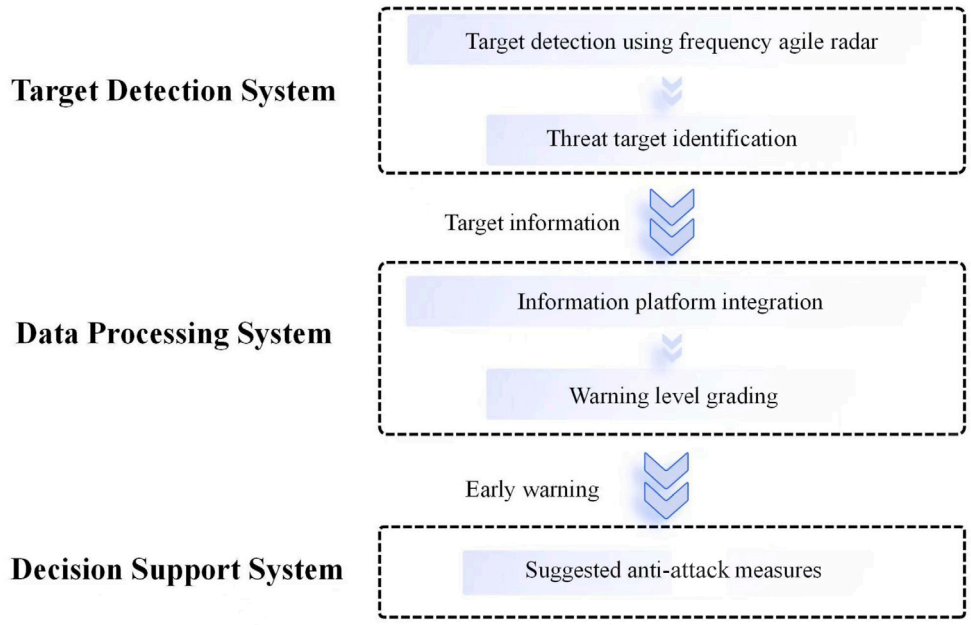



**Fig. 2.** Illustration of the risk warning system.

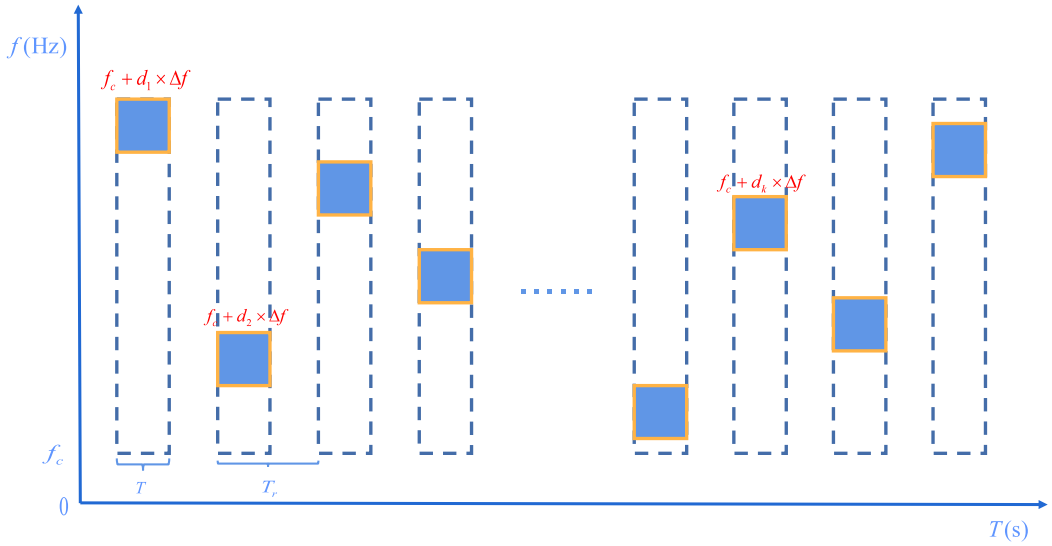



**Fig. 3.** Illustration of the broadband signal waveform of the frequency agile radar.

where $c$ is the light speed, $\beta_g$, $r_g$, $v_g$ denote the backscattering coefficient, range and velocity of the $g$th target, respectively.

### 3.2.2. Compressed sensing

Compressed sensing (CS), first proposed by Candès et al. (2006) and Donoho (2006), has been one of the most popular and effective signal processing models. CS has successfully been applied to a variety of sparse recovery problems, including magnetic resonance imaging (Lustig et al., 2008), compressive sampling (Mishali et al., 2011) and frequency agile radar signal processing (Huang et al., 2018).

As depicted in Fig. 4, the cells containing targets take up only a fraction of whole range–Doppler coordinates. In these cases, the CS approach can be used to obtain the signal vector $\boldsymbol{x}$ based on the observation vector $\boldsymbol{y}$ and the observation matrix $\boldsymbol{A}$. As the signal can be regarded as sparse in the considered scenario, the CS model is adopted to reconstruct the echo signal.

Without loss of generality, an interested coarse range cell is focused on. The echo signal is sampled with frequency $\frac{1}{T}$ after down-conversion. The echoes of multiple pulses transmitted successively on the interested coarse range cell are collected, and the $n$th sampled echo can be approximated as

$$S_r(n) \approx \sum_{g=1}^{G} \beta_g e^{-j4\pi \frac{r_g + v_g n T_r}{c}(f_c + d_n \Delta f)} \tag{4}$$

For ease of presentation, auxiliary variables scattering intensity $\gamma_g$, range term $p$ and Doppler term $q$ are introduced:

$$\begin{cases} \gamma_g = \beta_g \cdot e^{-j4\pi f_c r_g / c} \\ p = -4\pi \Delta f r_g / c \\ q = -4\pi f_c v_g T_r / c \end{cases} \tag{5}$$

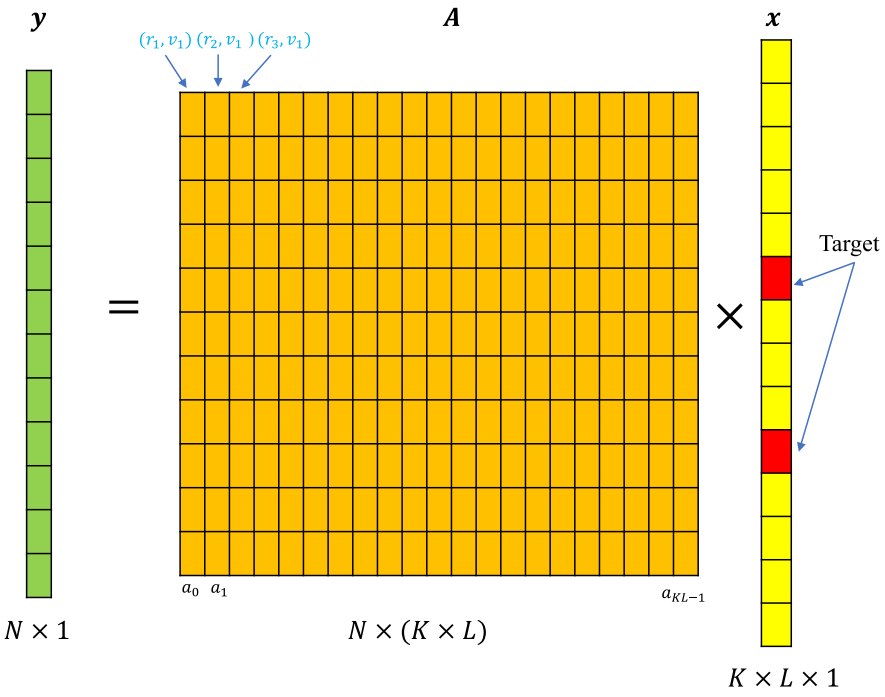



**Fig. 4.** Compressed sensing model of the frequency agile radar.

Then, the echo signal model in Eq. (4) can be rewritten as

$$S_r(n) \approx \sum_{g=1}^{G} \gamma_g \cdot e^{jpd_n} \cdot e^{jq(1+d_n \frac{\Delta f}{f_c})n} \tag{6}$$

In order to detect the position and velocity of all targets in the interested coarse range cell, the high resolution range - Doppler frequency scope plane $(p, q)$ is discretized into $K \times L$ grids uniformly. The values of $K$ and $L$ depend on the desired granularity of the reconstructed scene and a typical value taken are $K = M$ and $L = N$. The $n$th echo signal $S_r(n)$ can be described by:

$$S_r(n) = \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} \gamma_{k,l} \cdot e^{jp_k d_n} \cdot e^{jq_l(1+d_n \frac{\Delta f}{f_c})n} \tag{7}$$

where $\gamma_{k,l}$ is the scattering intensity of the target presented at $(p_k, q_l)$. The intensity matrix $\Gamma = [\gamma_{k,l}] \in \mathbb{C}^{K \times L}$ can be vectorized in column and transformed into vector $x \in \mathbb{C}^{KL}$:

$$\boldsymbol{x} = \left[\gamma(p_0, q_o), \ldots, \gamma(p_{K-1}, q_o), \ldots, \gamma(p_{K-1}, q_{L-1})\right]^{\mathrm{T}} \tag{8}$$

Define a steering vector for the element of vector $x$ as $a_m \in \mathbb{C}^N$, whose $n$th element can be stated as

$$a_m(n) = e^{jp_{m_k} d_n + jq_{m_l}(1+d_n \frac{\Delta f}{f_c})n} \tag{9}$$

Then Eq. (4) can be rewritten as

$$S_r(n) = \left[a_0, a_1, \ldots, a_{KL-1}\right] \cdot x \tag{10}$$

With the observation vector $\mathbf{y} = [S(0), S(1), S(2), \ldots, S(N-1)]^{\mathrm{T}}$ in the interested coarse range cell, the matrix form of the radar observation equation is obtained:

$$\begin{bmatrix} S(0) \\ \vdots \\ S(N-1) \end{bmatrix} = \begin{bmatrix} a_{0,0} & \cdots & a_{0,KL-1} \\ \vdots & \vdots & \vdots \\ a_{N-1,0} & \cdots & a_{N-1,KL-1} \end{bmatrix} \begin{bmatrix} x_0 \\ \vdots \\ x_{KL-1} \end{bmatrix} \tag{11}$$

Considering the sea clutter, Eq. (11) can be recast as

$$\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{\omega} \tag{12}$$

where $\boldsymbol{A} = [a_m] \in \mathbb{C}^{N \times KL}$, and $\boldsymbol{\omega}$ is the sea clutter vector.

In the considered scenario, sea clutter is a notable disturbance. Sea clutter is defined as the radar electromagnetic wave received when it strikes the sea surface Backscattered echoes from the sea surface (Conte et al., 2004; Farina et al., 1997). Since the sea clutter is space/time-dependent, the features are hard to capture and exhibits distinctly non-Gaussian properties (Conte & De Maio, 2004). Gini and Greco (2002) argued that the sea clutter can be modeled as a Compound Gaussian Model (CGM), which is represented by the following texture component and scatter component:

$$\boldsymbol{\omega}(m) = \sqrt{\boldsymbol{\tau}(m)} \times \boldsymbol{u}(m) \tag{13}$$

where $m$ is the $m$th CPI. In a single CPI, the CGM model can be expressed as a spherically invariant random vector (SIRV) model:

$$\boldsymbol{\omega} = \sqrt{\boldsymbol{\tau}} \times \boldsymbol{u} \tag{14}$$

where the texture component is a positive random constant and the scatter component follows a complex Gaussian distribution.

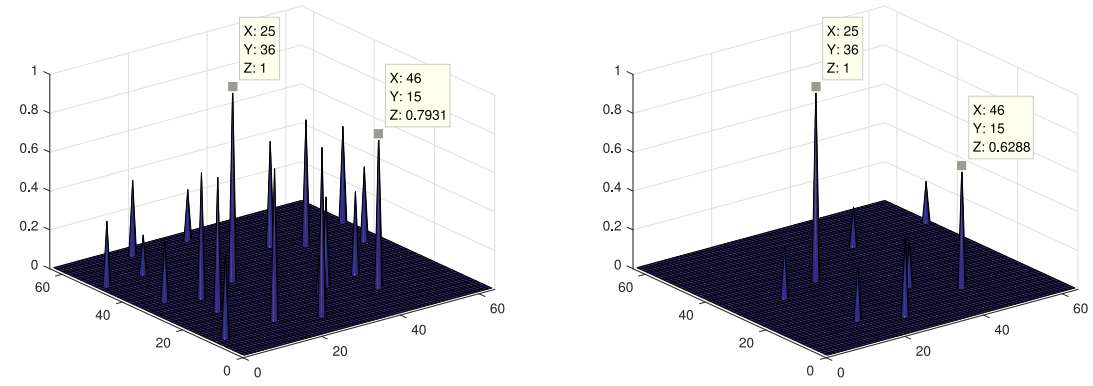
### 3.2.3. Scene reconstruction

The signal vector $\boldsymbol{x}$ can be recovered from the contaminated measurements using Eq. (12). Then the range and velocity information of targets can be inferred from locations of nonzero elements in Herman and Strohmer (2009). Many efficient methods are developed to recover targets based on the CS model (Chen et al., 2001; Ni et al., 2022). In the following experiments, the Orthogonal matching pursuit (OMP) algorithm (Tropp & Gilbert, 2007) is employed, which is one of the most popular algorithms in target recovery.

As a typical greedy tracking algorithm, the OMP algorithm iteratively selects a column from the observation matrix $\boldsymbol{A}$ that has the maximum correlation with the residual $\boldsymbol{r}$. By adding the selected column to the matrix $A_{T^i}$, the recovering signal vector $\boldsymbol{x}^i$ and the residual $\boldsymbol{r}$ can be updated using the least square method. The details of the OMP algorithm are presented in Algorithm 1.

### 3.2.4. Target information processing

Despite the accurate recovery of the range and velocity information, the number detection performance of the OMP algorithm is highly dependent on the prior information on the exact number of targets (Huang et al., 2018). If the pre-set maximum number of iterations is lower than the real number of targets, some targets are likely to be missed.




(a) Scene reconstruction without correlation modulation (b) Scene reconstruction with correlation modulation

**Fig. 5.** Comparison of scene reconstruction.

**Algorithm 1:** The OMP algorithm.

**Input:** observation matrix $\boldsymbol{A}$, observation vector $\boldsymbol{y}$, maximum number of iterations $I$

**Output:** recovered signal vector $\boldsymbol{x}$

1 **Step 0:** Initialize residual $\boldsymbol{r}^0 = \boldsymbol{y}$, index set $T^0 = \emptyset$, the matrix of chosen atoms $\boldsymbol{A}_{T^0} = [\ ]$, and the iteration counter $i = 1$.

2 **Step 1:** Calculate the correlation vector between observation matrix $\boldsymbol{A}$ and residual $\boldsymbol{r}^{i-1}$:

$$\boldsymbol{g}^i = \langle \boldsymbol{A}, \boldsymbol{r}^{i-1} \rangle \tag{15}$$

3 **Step 2:** Select the index $j^i$ with the maximum value of $\boldsymbol{g}^i$:

$$j^i = \underset{j=1,2,\ldots,KL}{\arg\max} \left| g^i(j) \right| \tag{16}$$

4 **Step 3:** Add the index $j^i$ into index set $T^i$:

$$T^i = T^{i-1} \cup j^i \tag{17}$$

5 **Step 4:** Solve a least squares problem:

$$\hat{\boldsymbol{x}}^i = \underset{\boldsymbol{x}^i}{\arg\min} \| \boldsymbol{y} - \boldsymbol{A}_{T^i} \boldsymbol{x}^i \|_2 \tag{18}$$

6 **Step 5:** Update the residual using:

$$\boldsymbol{r}^i = \boldsymbol{y} - \boldsymbol{A}\hat{\boldsymbol{x}}^i \tag{19}$$

7 **Step 6:** Increment $i$. If $i \leq I$, go to Step 1.

8 **Step 7:** Return the recovered signal vector $\boldsymbol{x} = \hat{\boldsymbol{x}}^I$.

Therefore, the pre-set maximum number of iterations of the OMP algorithm is generally considered as a relatively large value. This trick in turn increases the probability of noises being recovered as targets. An efficient target information processing algorithm is thus highly needed.

The detailed target information processing algorithm is shown in Algorithm 2. While detecting multiple targets, it is difficult to distinguish between real targets with lower echo signals and noises using a constant threshold. An efficient way is to increase the amplitude gap between these signals and then filter the noises using a adaptive threshold. First, the correlation $\boldsymbol{b}$ between the observation matrix $\boldsymbol{A}$ and the observation vector $\boldsymbol{y}$ is calculated. Then the recovered signal $\boldsymbol{x}$ can be modulated using the correlation $\boldsymbol{b}$. By doing so, the signal amplitude of real targets will be significantly higher than the noises (Determe et al., 2016), as shown in Fig. 5.

Otsu algorithm, a popular threshold segmentation algorithm, is adopted to identify targets from the recovered scene (Otsu, 1979). The performances of the Otsu algorithm are sensitive to noise, especially for multi-target detection. An adaptive procedure is thus introduced to adjust the thresholds obtained from the Otsu algorithm. Specifically, if the first detection identifies a single target, the threshold will be reduced by $\gamma$. The updated threshold allows some signals with lower amplitudes to be identified as targets. If only one target is identified with the lower threshold, the scenario can be regarded as existing one single target. On the contrary, if more than 5 targets are identified for the first time, the threshold will be increased by $\gamma$ to filter signals with lower amplitudes. The scenario can be considered to contain more than 5 targets in case more than 5 targets are still identified. The threshold will increase or decrease by $\gamma$ randomly when 2–5 targets are identified. The motivation is that conducting multiple detections with different thresholds is a promising way to improve warning accuracy.

### 3.3. Risk level assessment

The risk level of pirate attack is indicated by the piracy capability index which is directly related to the probability of a successful boarding. The capability of pirates is often evaluated by the number of pirate ships, the number of pirates, and the types of weapons (Psarros et al., 2011; Shane & Magnuson, 2016; Wong & Yip, 2012). Since the latter two are difficult to ascertain before the pirates board the vessel, they are replaced with the range and velocity of the pirate ships. According to Jin et al. (2019) and Zou and Xi (2011), the following grading rules shown in Table 2 are adopted in this study.

Considering that the number of pirate ships is the key factor in the piracy capability index, the risk levels for the scenarios with a single ship are assessed as Level 1 and that for scenarios with more than 5 ships are assessed as Level 3. For the cases with medium-number pirate ships, the risk level can be obtained by borrowing the idea of the fuzzy comprehensive evaluation method. Let $r_{ij}$ denotes the membership of variable $i$ to level $j$, where $r_{ij} = \frac{m}{n}$ indicates that there are $m$ of $n$ targets whose metric $i$ belongs to level $j$. $\boldsymbol{R}$ is the membership matrix

$$\boldsymbol{R} = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix} \tag{25}$$

The comprehensive risk level can be determined as the index corresponding to the largest element in vector $\boldsymbol{B}$, which can be calculated as

$$\boldsymbol{B} = \boldsymbol{\psi} \circ \boldsymbol{R} = = \begin{bmatrix} b_1 & b_2 & b_3 \end{bmatrix} \tag{26}$$

where $\boldsymbol{\psi} = \begin{bmatrix} \psi_1 & \psi_2 & \psi_3 \end{bmatrix}$ is the pre-specified weight vector.

**Algorithm 2:** Target information processing algorithm.

**Input:** observation matrix $\boldsymbol{A}$, observation vectors $\boldsymbol{y}_n$, adjustment coefficient of the threshold weighting factor $\gamma$

**Output:** warning level

**Step 0:** Initialize the threshold adjustment factor $\lambda$ and the detection counter $n = 1$.

**Step 1:** Obtain recovered signal vector $\boldsymbol{x}$ with observation matrix $\boldsymbol{A}$ and observation vector $\boldsymbol{y}_n$ using Algorithm 1.

**Step 2:** Compute the correlation vector between observation matrix $\boldsymbol{A}$ and observation vector $\boldsymbol{y}_n$:

$$\boldsymbol{b} = \langle \boldsymbol{A}, \boldsymbol{y}_n \rangle \tag{20}$$

and construct a diagonal matrix $\boldsymbol{W}$:

$$\boldsymbol{W} = diag(\boldsymbol{b}) = \begin{bmatrix} b_0 & 0 & \cdots & 0 \\ 0 & b_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{KL-1} \end{bmatrix} \tag{21}$$

**Step 3:** Modulate $\boldsymbol{x}$ by $\boldsymbol{W}$ and normalize it:

$$\boldsymbol{x} = \boldsymbol{W}\boldsymbol{x} \tag{22}$$

$$\boldsymbol{x} = \frac{|\boldsymbol{x}|}{|\boldsymbol{x}|_{\max}} \tag{23}$$

**Step 4:** Compute threshold $Th$ using Otsu method:

$$Th = Otsu(\boldsymbol{x}) \tag{24}$$

**Step 5:** Let elements in $\boldsymbol{x}$ less than $\lambda \cdot Th$ equal to 0.

**Step 6:** Transform $\boldsymbol{x}$ into range-Doppler matrix $\boldsymbol{H}$ to get number, range and velocity of targets.

**Step 7:** Evaluate the $n$-th risk level according to Section 3.3.

**Step 8:** Update the threshold weighting factor $\lambda$:

```
if number == 1 then
    λ = λ − γ
else
    if number ≥ 6 then
        λ = λ + γ
    else
        random{λ − γ, λ + γ}
```

**Step 9:** Increment $n$. If $n \leq N$, go to Step 1. Note that $N$ denotes the pre-set maximum number of detection times.

**Step 10:** Determine the warning level based on the results of $n$-times risk level assessments:

```
if Count(risk level == 1) > 1 then
    warning level = 1
else
    if Count(risk level == 3) > 1 then
        warning level = 3
    else
        warning level = 2
```

### 3.4. Decision-making support

As an integral part of the early-warning system, the decision-making support module directly helps the crew combat pirate attacks by recommending appropriate countermeasures. Details on how the early warning system determines and recommends the appropriate countermeasures are presented in Section 3.4.1. To display the warning information clearly, a customized warning interface is designed and implemented in Section 3.4.2.

**Table 2**
Measurement conversion.

| Rating variables | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| Number of boats | 1 | 2–5 | More than 5 |
| Range of boats (n mile) | [7,9] | [5,7) | [3,5) |
| Velocity of boats (knot) | [10,20) | [20,40) | [40,60] |

#### 3.4.1. Countermeasure recommendation

As suggested by BMP, defensive schemes would transfer from passive anti-piracy measures to active anti-piracy measures as warning levels increase. By conducting a comprehensive search of the relevant literature (Bryant et al., 2014; Jin et al., 2019; Psarros et al., 2011; Shane & Magnuson, 2016; Wong & Yip, 2012; Zou & Xi, 2011), the recommended countermeasures based on warning levels are given in Table 3.

#### 3.4.2. Warning interface design

To better report warning signals and risk information for vessels, a warning interface is designed. The input is real-time target detection data, and the output is detailed warning information. The warning interface is developed using the HTML5 technique based on Dreamweaver CC software.

Fig. 6 shows a capture of the warning interface depicting three threat target presence. The warning interface contains five modules. The top left module displays the current position obtained from the GPS service, including latitude, longitude and sea area information. In the middle, a map illustrates sailing direction, sailing speed and location of threat targets. Detailed information about the targets, including their range and velocity, is acquired from the detection results and presented in the bottom left module.

The risk level is reported in the top right module. For clear crew alerts, Warning Level 1, 2, 3 illuminates a yellow dot, an orange dot, and a red dot, respectively. In the illustrated attack scenario, an orange dot is lit, indicating a Level 2 rating. The bottom right module consists of two push buttons. Click on the first button can display specific counter decisions. The second button enables the crew to call the escort team nearby at the touch of a button in case of emergency.

## 4. Results of simulation experiments

Extensive simulation experiments are conducted to evaluate the performance of the proposed system under multiple scenarios. In this paper, the algorithms presented in this paper are implemented in MATLAB. All experiments are conducted on a personal computer with an IntelCore Duo 2.9 GHz Processor and 16 GB RAM.

### 4.1. Illustrative case

An illustrative case is provided to describe the proposed early warning system. In the proposed early warning system, the frequency agile radar mounted on the merchant vessel detects threatening pirate ships by continuously transmitting and receiving signals. The values for each parameter employed in the selected frequency agile radar are summarized in Table 4.

In the illustrative case, there are six pirate ships about 4 n mile from the merchant vessel. As the attack is carried out in a cluster style, the pirate ships are close to each other and at similar sailing speeds. Detailed information on the pirate ships are as follows:

Number of pirate ships: 6
Pirate ship 1: range 3.972 n mile, velocity 52.48 knot;
Pirate ship 2: range 3.978 n mile, velocity 42.76 knot;
Pirate ship 3: range 3.984 n mile, velocity 40.82 knot;
Pirate ship 4: range 3.987 n mile, velocity 46.65 knot;
Pirate ship 5: range 3.994 n mile, velocity 40.82 knot;
Pirate ship 6: range 4.001 n mile, velocity 48.60 knot.

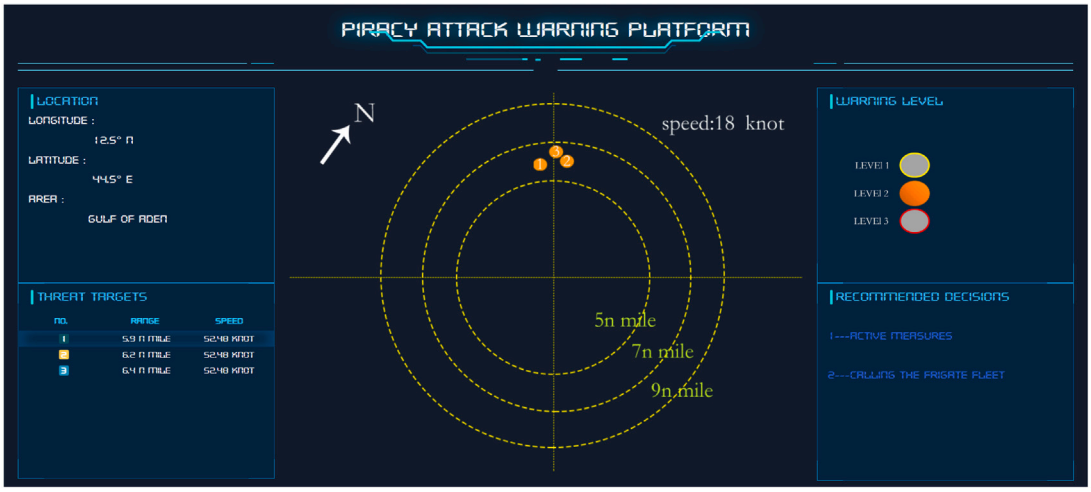



**Fig. 6.** Illustration of the risk warning system.

**Table 3**
Recommended countermeasures.

| Warning level | Measure type | Specific countermeasures |
|---|---|---|
| Level 1 | Passive | • alarm raised<br>• crew assembled<br>• being vigilant |
| Level 2 | Passive+active | • all passive measures<br>• hoses, lights, flares and electric perimeter fence used<br>• evasive maneuvers performed<br>• sailing speed increased |
| Level 3 | Passive+active+call for help | • all passive measures<br>• all active measures<br>• call for escort fleet |

**Table 4**
Values of the parameters used in the experiments.

| Parameters | Values |
|---|---|
| LFM bandwidth $B$ | 2 MHz |
| Sampling frequency $f_s$ | 20 MHz |
| Carrier frequency $f_c$ | 10 GHz |
| Frequency step $\Delta f$ | 2 MHz |
| Pulse repetition time $T_r$ | 120 μs |
| Pulse number in a CPI $N$ | 64 |
| Pulse width $\tau$ | 4 μs |
| Maximum frequency code $M$ | 64 |
| Coarse range cell $\Delta R$ | 0.04 n mile |
| Speed resolution $\Delta v$ | 3.79 knot |
| Frequency hopping bandwidth $B_s$ | 128 MHz |
| High range cell $\Delta R'$ | 0.000625 n mile |

After receiving the echo signal with target information, the coarse range cells which contain the targets can be obtained using the pulse compression technique. The approximate ranges of the targets are determined to be between 3.97 n mile and 4.10 n mile. The CS algorithm is adopted to identify the targets more exactly. The results are presented in Fig. 7. As depicted, the six signals with the highest amplitudes are considered to have detected the targets, whereas the others are filtered out as noise. Therefore, the attack scenario can be considered well recovered.

Fig. 8 displays the warning interface of the illustrative case. The map in the middle shows the six threat targets. According to Table 2, the number of pirate ships belongs to Level 3, which indicates that the risk level of the case is Level 3. The red light representing Level 3 is illuminated, as shown on the right-hand side. As the potential attack is assessed at the highest risk level, the bottom right module suggests active defensive measures. The specific policies can be displayed by clicking on the button *ACTIVE MEASURES*. The *MAYDAY* button is also active for the crew to call the frigate fleet nearby.

### 4.2. Warning performance

In this section, extensive computational experiments are conducted to assess the performance of the proposed early warning system. Specifically, 27 instance types representing multiple attack scenarios based on the criteria presented in Table 2 are generated. To capture the group behavioral characteristics of pirate attacks, pirate ships are set to be within 75 m (0.04 n mile) of each other in all instances. Note that it is a very strict assumption and the results can thus reflect the robustness of the proposed model. For each instance type, 1000 replications are randomly generated.

In Table 5, the column *Risk Level* represents the real risk level of the given scenario. Considering that the number of pirate ships usually has a significant impact on the severity of the potential attack, the weight vector $\boldsymbol{\psi}$ is assumed to be $\begin{bmatrix} 0.4 & 0.3 & 0.3 \end{bmatrix}$ in the experiments. The metric $Accuracy$, indicating the percentage of the instances where the warning level matches the real risk level out of the total instances, is used to evaluate the warning performance. The allowed detection number (i.e., $N$ in Algorithm 2) is set to be 1 and 4, and the warning accuracy is denoted as $Acc-1$ and $Acc-4$ respectively. The computing time for the four detections (in 1s) is acceptable as response time in seconds can satisfy the requests of the pirate attack scenarios. In the following experiments, $\lambda$ is set to be 0.4 and $\gamma$ is set to be 0.1.

As shown in Table 5, the results reveal that the early warning system provides good performance in all scenarios. Specifically, the proposed warning method achieves high accuracy showing an average $Acc-1$ of 0.899 and an average $Acc-4$ of 0.964. The warning algorithm performs best on instances with a single target, which has an average $Acc-1$ of 0.990 and an average $Acc-4$ of 0.996. The reason is

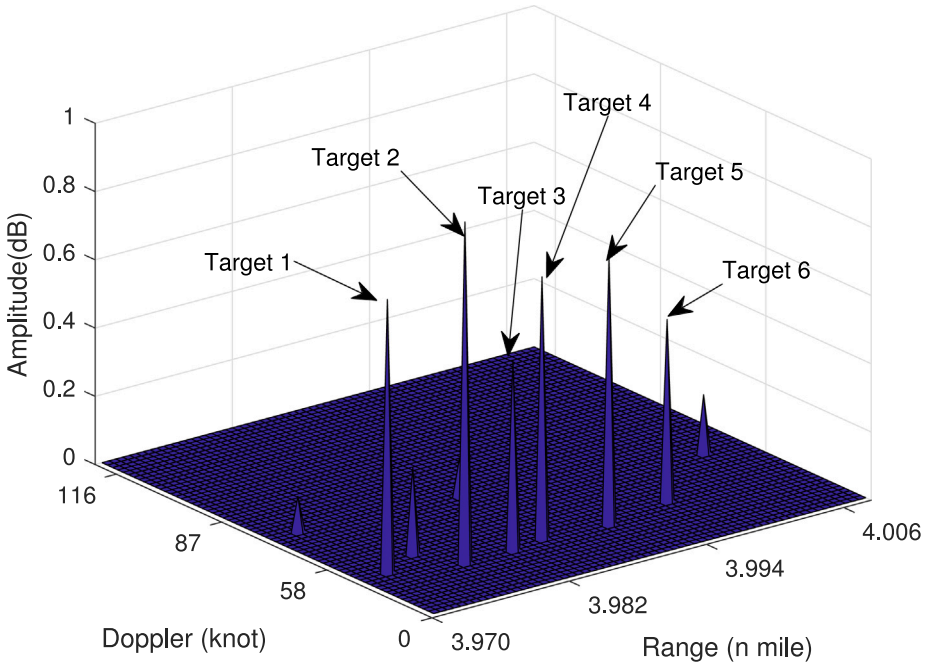



**Fig. 7.** Scene reconstruction for the illustrative case.

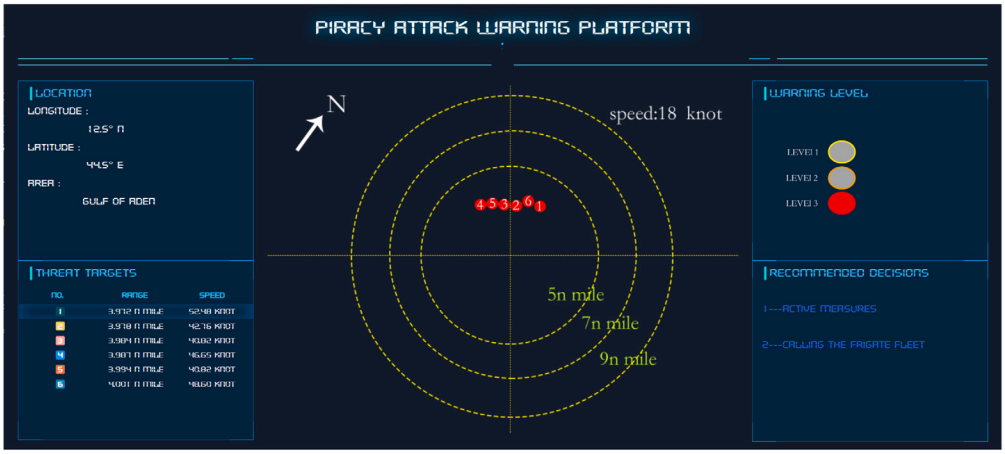



**Fig. 8.** Warning interface for the illustrative case.

that the employed OMP algorithm in the target detection could deliver better results when recovering only one target. In terms of the instances with high-number targets, the warning performance is also better than that of the instances with medium-number targets. By checking the assessment process, the possible reason is: since more than 5 targets will be rated at level 3, the accuracy of the warning level would not be affected even if some noise is mistaken as targets (i.e., false alarms).

Table 5 also shows that the results of $Acc-4$ outperform that of $Acc-1$. It indicates that with the increase of detection counts, the accuracy of early warning level tends to be improved for all considered scenarios. This is particularly true for the scenarios with medium-number (i.e. 2–5) targets. One possible explanation could be that multiple detections in a short time can help avoid the random errors caused by the OMP algorithm. Another reason is that the in four detections scenarios, the threshold for the latter detection can be adjusted according to the previous detection result by introducing the adjustment coefficient $\gamma$. The results reveals the effectiveness of the tailored adaptive adjustment procedure in the target information processing algorithm.

To help better demonstrate the results, Precision, Recall and F1 Score are adopted as auxiliary performance metrics. Following the common definitions in performance measure, the Precision $P$ and the Recall $R$ can be calculated by:

$$P = \frac{TP}{TP + FP}$$

$$R = \frac{TP}{TP + FN}$$

For each risk level, a positive sample refers to an attack instance belonging to this risk level, while a negative sample refers to others. True Positive (TP) denotes the number of positive samples that are correctly predicted, False Positive (FP) denotes the number of negative samples that are falsely predicted, and False Negative (FN) denotes the number of positive samples that are falsely predicted.

The F1 Score for risk level $i$ is defined as:

$$F_{1,i} = \frac{2P_i \times R_i}{P_i + R_i}$$

then the F1 Score considers the all scenarios can be formulated as follows:

$$F_1 = \frac{1}{3}\sum_{i=1}^{3} F_{1,i}$$

**Table 5**
Computational performance for the test instances.

| Number | Range (n mile) | Velocity (knot) | Risk Level | Acc-1 | Acc-4 |
|---|---|---|---|---|---|
| 1 | [7,9] | [10,20) | Level 1 | 1.000 | 1.000 |
| 1 | [7,9] | [20,40) | Level 1 | 0.995 | 0.997 |
| 1 | [7,9] | [40,60] | Level 1 | 0.999 | 1.000 |
| 1 | [5,7) | [10,20) | Level 1 | 0.962 | 0.991 |
| 1 | [5,7) | [20,40) | Level 1 | 0.997 | 0.998 |
| 1 | [5,7) | [40,60] | Level 1 | 0.999 | 1.000 |
| 1 | [3,5) | [10,20) | Level 1 | 0.962 | 0.983 |
| 1 | [3,5) | [20,40) | Level 1 | 0.994 | 0.995 |
| 1 | [3,5) | [40,60] | Level 1 | 0.998 | 0.999 |
| 2–5 | [7,9] | [10,20) | Level 1 | 0.942 | 0.955 |
| 2–5 | [7,9] | [20,40) | Level 2 | 0.861 | 0.879 |
| 2–5 | [7,9] | [40,60] | Level 2 | 0.869 | 0.888 |
| 2–5 | [5,7) | [10,20) | Level 2 | 0.846 | 0.865 |
| 2–5 | [5,7) | [20,40) | Level 2 | 0.864 | 0.891 |
| 2–5 | [5,7) | [40,60] | Level 2 | 0.870 | 0.907 |
| 2–5 | [3,5) | [10,20) | Level 2 | 0.837 | 0.859 |
| 2–5 | [3,5) | [20,40) | Level 2 | 0.848 | 0.867 |
| 2–5 | [3,5) | [40,60] | Level 3 | 0.912 | 0.956 |
| >5 | [7,9] | [10,20) | Level 3 | 0.816 | 0.998 |
| >5 | [7,9] | [20,40) | Level 3 | 0.821 | 0.999 |
| >5 | [7,9] | [40,60] | Level 3 | 0.857 | 0.999 |
| >5 | [5,7) | [10,20) | Level 3 | 0.828 | 0.999 |
| >5 | [5,7) | [20,40) | Level 3 | 0.819 | 0.997 |
| >5 | [5,7) | [40,60] | Level 3 | 0.841 | 0.999 |
| >5 | [3,5) | [10,20) | Level 3 | 0.812 | 0.998 |
| >5 | [3,5) | [20,40) | Level 3 | 0.833 | 0.999 |
| >5 | [3,5) | [40,60] | Level 3 | 0.879 | 1.000 |

**Table 6**
Performance measure of the proposed early warning model.

| | Precision | Recall | F1 Score |
|---|---|---|---|
| Risk Level 1 | 0.971 | 0.992 | 0.981 |
| Risk Level 2 | 0.982 | 0.879 | 0.928 |
| Risk Level 3 | 0.946 | 0.994 | 0.969 |
| Macro average | 0.966 | 0.955 | 0.960 |

The Precision, Recall, and F1 Score are listed in Table 6, where the first three rows represent the performances of each risk level, and the row macro average represents an average of all scenarios. As shown in Table 6, the proposed early warning model performs well in almost all scenarios and, for the false-detected events, it tends to overestimate the high-risk level events instead of underestimating those low-risk events. Thus, from the perspective of risk warning, it could help to improve the security level of merchant ships. Specifically, for events with risk level 3, the proposed algorithm obtains the highest Recall value and a relatively low Precision value, which implies that it tends to miss-classified low-risk events as level 3 events, particularly for real risk level 2 events (i.e., 555 out of 572 FP events). Meanwhile, for events of risk level 2, though the Recall value is the lowest, experimental results reveal that about 65.8% of the FN events are miss-classified as risk level 3. Although overestimating the risk level may lead to higher operation costs in practice, it can help guarantee the security of ships, which is a more critical factor than monetary benefit.

### 4.3. Comparative analysis

In order to further demonstrate the superiority of the proposed method, comparative studies are conducted in this section. The first study assesses the benefits of selecting frequency agile radar by comparing the detection results with that of common radar in same basic parameters. The second study evaluates the improvement of warning capability brought by the proposed target information processing algorithm in Section 3.2.4, taking some popular algorithms as baseline models.

#### 4.3.1. Benefits of selecting frequency agile radar

In this section, we focus on the suitability of the frequency agile radar for detecting pirate boats. To this end, an experiment is conducted to compare the frequency agile radar with the fixed frequency pulse radar (called the common radar below). The parameters of the common radar are consistent with those of the selected frequency agile radar shown in Table 4, except the frequency step $\Delta f = 0$.

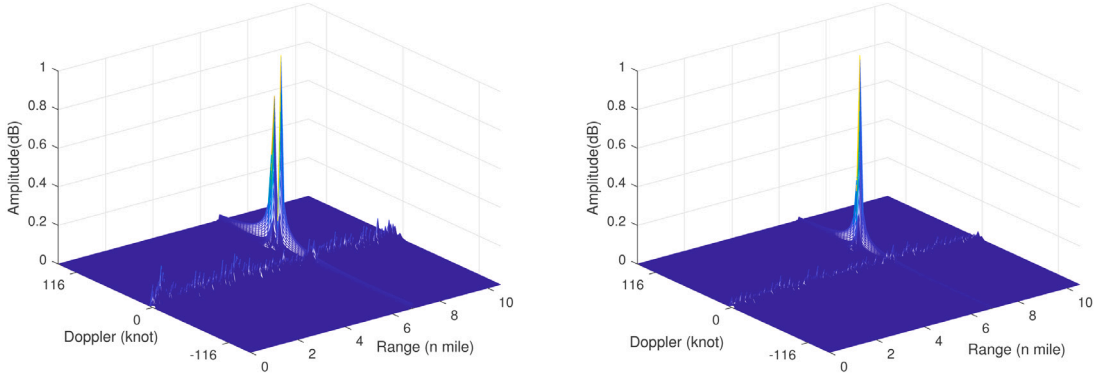
As shown in Fig. 9(a), the common radar detects two targets using pulse compression and coherence accumulation technique. Note that only one coarse range cell is identified, despite there being two targets. This is because the common radar has a range resolution of 0.04 n mile ($\Delta R = \frac{C}{2B} = 75$ m $\approx 0.04$ n mile), targets within 0.04 n mile of each other are in the same coarse range cell. The identified coarse range cell indicates the targets are in an approximate range of 6.844 n mile - 6.884 n mile. However, the exact locations of the two targets cannot be recovered due to the radar range resolution. Moreover, the two targets cannot be distinguished if they have the same speeds. As depicted in Fig. 9(b), only one target has been recovered. The reason is that the two targets are not only in the same range cell but also in the same Doppler cell. Therefore, they are treated as one target when the echo signal is processed. Considering that pirate boats are usually close together and sail at about the same speed, the utilization of common radar is prone to miss targets.

Fig. 10 shows that for the same scenario, the frequency agile radar performs a better reconstruction. As shown in Fig. 10(a), the frequency radar first identifies that the coarse range cell representing 6.844 n mile - 6.884 n mile may contain targets using the pulse compression technique. With the precise recovery of the CS algorithm, it is observed that the high range cells containing the targets are the 12th cell and the 22nd cell. Thus, the target ranges can be recovered as $12 \times \frac{75}{64} + 12675 = 12689.06$ m $= 6.8515$ n mile and $22 \times \frac{75}{64} + 12675 = 12700.78$ m $= 6.8579$ n mile respectively. The errors between the recovered range and the real range of the two targets are no more than 0.000625 n mile, which is the range resolution of the selected frequency agile radar. Fig. 10(b) also shows that the 11th Doppler cell contains the targets. The velocity of the targets can be estimated as $11 \times 3.79 = 41.69$ knot, while the real velocity is 42.7 knot. The results reveal that the proposed pirate boat detection method is able to identify the exact number of targets and an accurate estimate of their range and velocity, even when the targets are at a similar range and velocity.

Fig. 11 shows the results of pulse compression via the common radar and the frequency agile radar while encountering repeater jamming. Repeater jamming, a popular and efficient signal jamming approach, interferes with the propagation of target signals by replicating and then transmitting them again. If the pirate ships employ repeater jamming, the detection sensor will receive confused echo signals comprised of real signals and false signals. For the common radar, the false signal will be mistaken as a target. In Fig. 11(a), pulses in both the 1690th and 1900th range cells are identified as targets, but the latter is a false target created by the repeater jamming. For the frequency agile radar adopted in this study, only the real target will be identified, as shown in Fig. 11(b). The reason is that, the jammer is difficult to determine the frequency of the next pulse transmitted by the frequency agile radar as it changes randomly. If the jammer replicates and transmits a certain fixed frequency signal, it will be filtered by the matched filter of the frequency agile radar. Therefore, only real signals can be identified as targets.

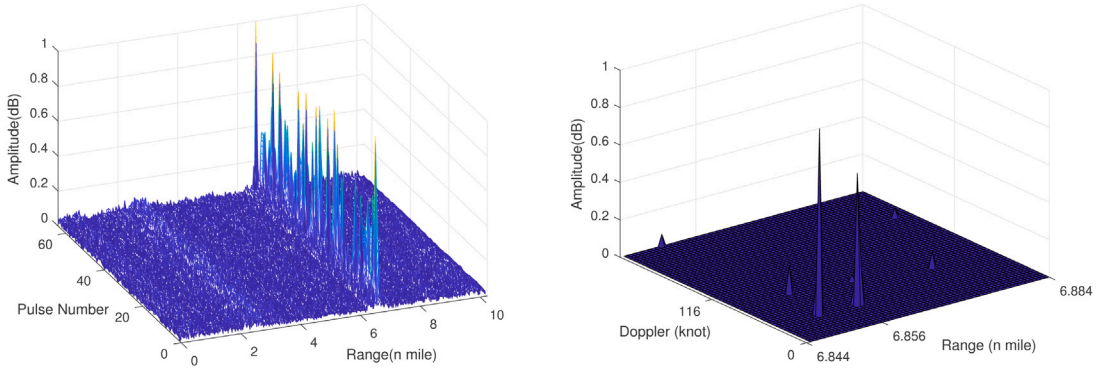
#### 4.3.2. Target information processing algorithm comparison

Considering commonly used processing methods in the previous target detection studies (Novak et al., 1993), constant thresholds are used as baseline models to distinguish targets and noises from the obtained recovered scene by the OMP algorithm. Constant threshold assumes that signals with amplitudes above the pre-set threshold are considered real targets, while the rest are filtered out as noises. In order to avoid the miss alarms due to high thresholds and false alarms due



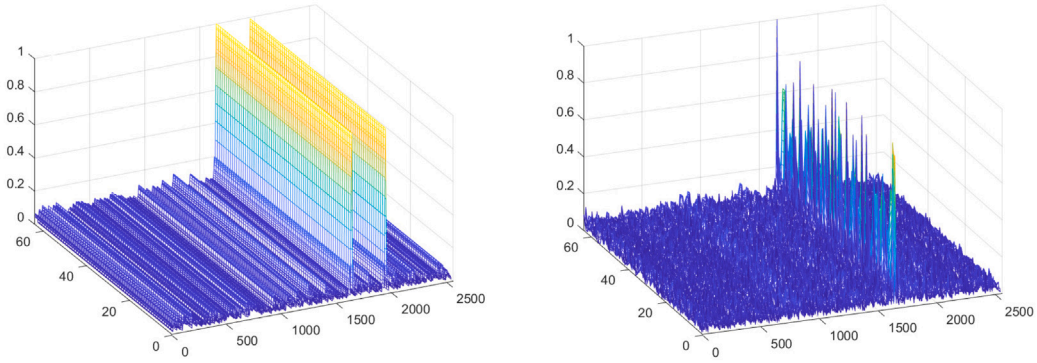

(a) Coherent integration for different speed targets (b) Coherent integration for same speed targets

**Fig. 9.** Scene reconstruction of common radar.




(a) Pulse compression for same speed targets (b) CS recovery for same speed targets

**Fig. 10.** Scene reconstruction of frequency agile radar.



(a) pulse compression via common radar (b) pulse compression via frequency agile radar

**Fig. 11.** Pulse compression results under repeater jamming.

to low thresholds, 0.4, 0.5, 0.6 and 0.7 are set to be thresholds in the following experiments. Besides the constant thresholds, a model whose threshold values are determined by the Otsu algorithm is also tested, referred to *Otsu* for short.

The results demonstrated in Table 7 are the average warning performance in multiple cases. It can be seen that the proposed target information processing model performs better warning performances in all test scenarios, showing warning accuracy of 96.4%, than all baseline models. The stable performances in different target number scenarios also reveal the robustness of the proposed algorithm.

Constant thresholds can deliver good warning performances in single target scenes. The reason is that the reconstructed scene obtained by the OMP algorithm makes it easy to distinguish real targets and noises due to the scene sparsity. However, constant thresholds perform poorly in multi-target scenes with lower sparsity. More specifically, thresholds of 0.4 and 0.5 show low warning capability in 2–5 target scenarios, whereas thresholds of 0.6 and 0.7 perform worse in more target scenarios. For scenarios containing 2–5 targets, a low threshold may lead to false alarms and the warning level would be misjudged to a higher level when the number of targets is misjudged to be 6 or more.

**Table 7**
Warning performance comparison on multiple scenarios.

| Target number | Model | Acc-4 |
|---|---|---|
| 1 | Constant threshold 0.4 | 0.778 |
| 1 | Constant threshold 0.5 | 0.935 |
| 1 | Constant threshold 0.6 | 0.988 |
| 1 | Constant threshold 0.7 | 0.998 |
| 1 | Otsu | 0.978 |
| 1 | Target information processing model | **0.996** |
| 2–5 | Constant threshold 0.4 | 0.545 |
| 2–5 | Constant threshold 0.5 | 0.768 |
| 2–5 | Constant threshold 0.6 | 0.904 |
| 2–5 | Constant threshold 0.7 | 0.902 |
| 2–5 | Otsu | 0.842 |
| 2–5 | Target information processing model | **0.896** |
| >5 | Constant threshold 0.4 | 0.997 |
| >5 | Constant threshold 0.5 | 0.916 |
| >5 | Constant threshold 0.6 | 0.558 |
| >5 | Constant threshold 0.7 | 0.211 |
| >5 | Otsu | 0.769 |
| >5 | Target information processing model | **0.999** |

The problem of missed alarms due to higher thresholds has less negative impacts on the warning capability in this scenario, as even if some real targets are not identified, the warning level cannot be misjudged to a lower warning level unless only one target is successfully identified. A similar but opposite mechanism works for more target scenarios.

It can be observed that adopting the Otsu model achieves stable warning performance with 86.3% accuracy, respectively. However, the warning performance of the Otsu model decreases as the number of targets increases. This is because the Otsu model is sensitive to noise especially in multi target detections, as discussed in Section 3.2.4. One can show that the warning capabilities of the baseline models are unstable and only perform well in some scenarios. The robust warning performance makes the proposed target information processing model more practical due to the unpredictability of the pirating activities.

## 5. Conclusions

To response a crucial practical challenge in maritime security-designing an efficient solution to prevent potential pirate attacks-this paper explores a real-time early warning system for maritime security risks. The system comprises a target detection subsystem, a data processing subsystem, and a decision-making support subsystem. By providing early warnings and management advice, the proposed system offers crews more response time to defend against potential attacks, thereby significantly reducing the risk in active area of pirate operations.

In order to detect the small moving targets in space–time dependent sea conditions, the target detection subsystem selects the frequency agile radar as the sensing modality, and a CS approach with a tailored target information processing algorithm is developed to identify targets. With the target information, a risk level assessment method is proposed to determine a reasonable warning level as well as appropriate defense measures. The proposed framework and algorithms are tested on typical illustrative scenarios. The results show that, for closely spaced targets (e.g., side-by-side pirate ship groups) and cases encountering repeater jamming, the developed approach outperforms common radar, and the early warning system can provide accurate warnings under multiple attack scenarios and outperforms baseline models.

In the future, we are interested in improving the early warning performance by introducing the cooperative sensing technique. The integration of multiple sensors, such as cameras or drones, not only enables more accurate information about pirate ships but also help vessels know the number of pirates and even their weaponry. Therefore, incorporating cooperative sensing technique can lead to a more accurate and comprehensive assessment of the piracy risk levels. Future research directions involve gathering accurately labeled image datasets across diverse scenes. Moreover, there is a high anticipation for the development of efficient detection algorithms tailored for small ships in complex sea conditions.

## CRediT authorship contribution statement

**Xinran Li:** Conceptualization, Methodology, Writing – original draft. **Wei Wang:** Conceptualization, Validation, Supervision. **Hao Gu:** Methodology, Software, Writing – review & editing. **Kun Jin:** Software, Validation, Writing – review & editing.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

Data will be made available on request.

## Acknowledgments

This study has been substantially supported by the research grants from the National Natural Science Foundation Council of China (51878166).

## References

Alghazo, J., Bashar, A., Latif, G., & Zikria, M. (2021). Maritime ship detection using convolutional neural networks from satellite images. In *2021 10th IEEE international conference on communication systems and network technologies* (pp. 432–437). http://dx.doi.org/10.1109/CSNT51715.2021.9509628.

Bryant, W., Townsley, M., & Leclerc, B. (2014). Preventing maritime pirate attacks: a conjunctive analysis of the effectiveness of ship protection measures recommended by the international maritime organisation. *Journal of Transportation Security*, *7*(1), 69–82.

Candès, E. J., Romberg, J., & Tao, T. (2006). Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Transaction on Information Theory*, *52*(2), 489–509.

Chen, Z., Chen, D., Zhang, Y., Cheng, X., Zhang, M., & Wu, C. (2020). Deep learning for autonomous ship-oriented small ship detection. *Safety Science*, *130*, Article 104812.

Chen, S. S., Donoho, D. L., & Saunders, M. A. (2001). Atomic decomposition by basis pursuit. *SIAM Review*, *43*(1), 129–159.

Chen, L., Shi, W., & Deng, D. (2021). Improved YOLOv3 based on attention mechanism for fast and accurate ship detection in optical remote sensing images. *Remote Sensing*, *13*(4), 660.

Chen, S.-T., Wall, A., Davies, P., Yang, Z., Wang, J., & Chou, Y.-H. (2013). A human and organisational factors (HOFs) analysis method for marine casualties using HFACS-maritime accidents (HFACS-MA). *Safety Science*, *60*, 105–114.

Christiansen, M., Fagerholt, K., Nygreen, B., & Ronen, D. (2007). Maritime transportation. *Vol. 14*, In *Handbooks in operations research and management science* (pp. 189–284). Elsevier.

Conte, E., & De Maio, A. (2004). Mitigation techniques for non-Gaussian sea clutter. *IEEE Journal of Oceanic Engineering*, *29*(2), 284–302.

Conte, E., De Maio, A., & Galdi, C. (2004). Statistical analysis of real clutter at different range resolutions. *IEEE Transactions on Aerospace and Electronic Systems*, *40*(3), 903–918.

Cui, Z., Li, Q., Cao, Z., & Liu, N. (2019). Dense attention pyramid networks for multi-scale ship detection in SAR images. *IEEE Transactions on Geoscience and Remote Sensing*, *57*(11), 8983–8997.

Determe, J.-F., Louveaux, J., Jacques, L., & Horlin, F. (2016). Improving the correlation lower bound for simultaneous orthogonal matching pursuit. *IEEE Signal Processing Letters*, *23*(11), 1642–1646. http://dx.doi.org/10.1109/LSP.2016.2612759.

Donoho, D. L. (2006). Compressed sensing. *IEEE Transaction on Information Theory*, *52*(4), 1289–1306.

Farina, A., Gini, F., Greco, M., & Verrazzani, L. (1997). High resolution sea clutter data: statistical analysis of recorded live data. *IEE Proceedings-Radar, Sonar and Navigation*, *144*(3), 121–130.

Felzenszwalb, P. F., Girshick, R. B., McAllester, D., & Ramanan, D. (2009). Object detection with discriminatively trained part-based models. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *32*(9), 1627–1645.

Gini, F., & Greco, M. (2002). Texture modelling, estimation and validation using measured sea clutter data. *IEE Proceedings-Radar, Sonar and Navigation*, *149*(3), 115–124.

Goossens, L., & Glansdorp, C. (1998). Operational benefits and risk reduction of marine accidents. *The Journal of Navigation*, *51*(3), 368–381.

Henschel, M. D., Rey, M. T., Campbell, J., & Petrovic, D. (1998). Comparison of probability statistics for automated ship detection in SAR imagery. *Vol. 3491*, In *1998 international conference on applications of photonic technology III: closing the gap between theory, development, and applications* (pp. 986–991). SPIE.

Herman, M. A., & Strohmer, T. (2009). High-resolution radar via compressed sensing. *IEEE Transactions on Signal Processing*, *57*(6), 2275–2284.

Huang, D.-Z., Hu, H., & Li, Y.-Z. (2013). Spatial analysis of maritime accidents using the geographic information system. *Transportation Research Record*, *2326*(1), 39–44.

Huang, T., Liu, Y., Xu, X., Eldar, Y. C., & Wang, X. (2018). Analysis of frequency agile radar via compressed sensing. *IEEE Transactions on Signal Processing*, *66*(23), 6228–6240.

Jin, M., Shi, W., Lin, K.-C., & Li, K. X. (2019). Marine piracy prediction and prevention: Policy implications. *Marine Policy*, *108*, Article 103528.

Kretschmann, L. (2020). Leading indicators and maritime safety: predicting future risk with a machine learning approach. *Journal of Shipping and Trade*, *5*(1), 1–22.

Leach, P. (2011). The rising costs of piracy. *Journal of Commerce*, *12*(17), 24–26.

Lee, C.-Y., & Song, D.-P. (2017). Ocean container transport in global supply chains: Overview and research opportunities. *Transportation Research, Part B (Methodological)*, *95*, 442–474.

Li, S., Meng, Q., & Qu, X. (2012). An overview of maritime waterway quantitative risk assessment models. *Risk Analysis: An International Journal*, *32*(3), 496–512.

Li, K. X., Yin, J., Bang, H. S., Yang, Z., & Wang, J. (2014). Bayesian network with quantitative input for maritime risk analysis. *Transportmetrica A: Transport Science*, *10*(2), 89–118.

Liu, H., Liu, Z., & Liu, D. (2018). Application of machine learning methods in maritime safety information classification. In *2018 tenth international conference on advanced computational intelligence* (pp. 735–740). IEEE.

Luo, M., & Shin, S.-H. (2019). Half-century research developments in maritime accidents: Future directions. *Accident Analysis and Prevention*, *123*, 448–460.

Lustig, M., Donoho, D. L., Santos, J. M., & Pauly, J. M. (2008). Compressed sensing MRI. *IEEE Signal Processing Magazine*, *25*(2), 72–82.

Mishali, M., Eldar, Y. C., & Elron, A. J. (2011). Xampling: Signal acquisition and processing in union of subspaces. *IEEE Transactions on Signal Processing*, *59*(10), 4719–4734.

Ni, T., Liu, S., Mao, Z., & Huang, Y. (2022). Information-theoretic target localization with compressed measurement using FDA radar. In *2022 IEEE radar conference* (pp. 1–5). IEEE.

Novak, L. M., Burl, M. C., & Irving, W. (1993). Optimal polarimetric processing for enhanced target detection. *IEEE Transactions on Aerospace and Electronic Systems*, *29*(1), 234–244.

Otsu, N. (1979). A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, *9*(1), 62–66.

Panahi, R., Ng, A. K., Afenyo, M. K., & Haeri, F. (2020). A novel approach in probabilistic quantification of risks within the context of maritime supply chain: The case of extreme weather events in the arctic. *Accident Analysis and Prevention*, *144*, Article 105673.

Pieralice, F., Santi, F., Pastina, D., Bucciarelli, M., Ma, H., Antoniou, M., & Cherniakov, M. (2017). GNSS-based passive radar for maritime surveillance: Long integration time MTI technique. In *2017 IEEE radar conference* (pp. 0508–0513). IEEE.

Prayudi, A., Sulistijono, I. A., Risnumawan, A., & Darojah, Z. (2020). Surveillance system for illegal fishing prevention on uav imagery using computer vision. In *2020 international electronics symposium* (pp. 385–391). IEEE.

Psarros, G. A., Christiansen, A. F., Skjong, R., & Gravir, G. (2011). On the success rates of maritime piracy attacks. *Journal of Transportation Security*, *4*, 309–335.

Psarros, G., Skjong, R., & Eide, M. S. (2010). Under-reporting of maritime accidents. *Accident Analysis and Prevention*, *42*(2), 619–625.

Quan, Y., Li, Y., Wu, Y., Ran, L., Xing, M., & Liu, M. (2016). Moving target detection for frequency agility radar by sparse reconstruction. *Review of Scientific Instruments*, *87*(9), Article 094703.

Shane, J. M., & Magnuson, S. (2016). Successful and unsuccessful pirate attacks worldwide: A situational analysis. *Justice Quarterly*, *33*(4), 682–707.

Sui, Z., Wen, Y., Huang, Y., Song, R., & Piera, M. A. (2023). Maritime accidents in the Yangtze river: A time series analysis for 2011–2020. *Accident Analysis and Prevention*, *180*, Article 106901.

Touchton, B., Hilands, T., & Rigsby, D. (2013). Automated maritime contact tracking and piracy threat identification using a low-cost commercial radar.

Tran, T.-H., & Le, T.-L. (2016). Vision based boat detection for maritime surveillance. In *2016 international conference on electronics, information, and communications* (pp. 1–4). IEEE.

Tropp, J. A., & Gilbert, A. C. (2007). Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Transaction on Information Theory*, *53*(12), 4655–4666.

Tumbarska, A. (2018). Current maritime piracy practices and anti-piracy protection. *Science Business Society*, *3*(3), 141–144.

Vespe, M., Greidanus, H., & Alvarez, M. A. (2015). The declining impact of piracy on maritime transport in the Indian ocean: Statistical analysis of 5-year vessel tracking data. *Marine Policy*, *59*, 9–15.

Wackerman, C. C., Friedman, K. S., Pichel, W. G., Clemente-Colón, P., & Li, X. (2001). Automatic detection of ships in RADARSAT-1 SAR imagery. *Canadian Journal of Remote Sensing*, *27*(5), 568–577.

Watanabe, K., Takashima, K., Mitsumura, K., Utsunomiya, K., & Takasaki, S. (2017). Experimental study on the application of UAV drone to prevent maritime pirates attacks. *TransNav, International Journal on Marine Navigation and Safety od Sea Transportation*, *11*(4).

Wong, M. C., & Yip, T. L. (2012). Maritime piracy: an analysis of attacks and violence. *International Journal of Shipping and Transport Logistics 4*, *4*(4), 306–322.

Wu, B., Wang, Y., Zhang, J., Savan, E. E., & Yan, X. (2015). Effectiveness of maritime safety control in different navigation zones using a spatial sequential DEA model: Yangtze river case. *Accident Analysis & Prevention*, *81*, 232–242.

Xu, C., Zhang, D., Zhang, Z., & Feng, Z. (2014). BgCut: automatic ship detection from UAV images. *The Scientific World Journal*, *2014*.

Yang, X., Sun, H., Fu, K., Yang, J., Sun, X., Yan, M., & Guo, Z. (2018). Automatic ship detection in remote sensing images from google earth of complex scenes based on multiscale rotation dense feature pyramid networks. *Remote Sensing*, *10*(1), 132.

Yao, Y., Jiang, Z., Zhang, H., Zhao, D., & Cai, B. (2017). Ship detection in optical remote sensing images based on deep convolutional neural networks. *Journal of Applied Remote Sensing*, *11*(4), 042611–042611.

Zhang, Z., Zhang, L., Wang, Y., Feng, P., & He, R. (2021). ShipRSImageNet: A large-scale fine-grained dataset for ship detection in high-resolution optical remote sensing images. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *14*, 8458–8472.

Zou, y., & Xi, X. (2011). Construction of dynamic early warning mechanisms against piracy. *World Shipping*, *34*(6), 46–49.