

Multispectral Systems of Imaging Scenery in Critical Infrastructure Protection, Threat Identification and Recognition

M. KAROL, M. SZUSTAKOWSKI, M. ŻYCKOWSKI*, P. MARKOWSKI AND W. CIURAPIŃSKI

Military University of Technology, Institute of Optoelectronics, S. Kaliskiego 2, 00-908 Warsaw, Poland

The surveillance system more often uses devices working on different bands that are used not only for detection but also to recognize and identify threats. The paper presents the possibility of protection, detection and identification of risks, achieved through the use of multispectral detection systems in critical infrastructure facilities. The authors consider the benefits of active sensors based on other wavebands, such as millimeter wave radar, terahertz cameras, infrared camera and shows the ability to detect and identify the target using data collected by the sensors. Also discussed the issue of fusion data from different sensors and opportunities that the whole system obtained by application of data fusion.

DOI: [10.12693/APhysPolA.124.459](https://doi.org/10.12693/APhysPolA.124.459)

PACS: 42.30.Wb, 87.57.-s, 42.79.Qx

1. Introduction

At present, many non-military materials and resources are available and because of that many organizations in the world are trying to become well-known by carrying out terrorist attacks. These organizations use their acts to get the world's attention on specific problems. Typically, such attacks are a serious threat to civilian population and critical infrastructure objects, because they are designed to cause maximum damages. In the Baltic Sea the terrorist attacks on seaports are considered as one of major threats [1].

Considering seaport as a critical infrastructure object, we can identify several ways of plausible terrorists attacks.

- Attack from the sea surface using manned and unmanned boats that can carry armed men and explosives.
- Hijacking of ships transporting dangerous materials and using materials as weapons.
- Underwater attacks using divers or miniature submarines.
- Land attacks on ships docked at the port using improvised explosive devices, suicide attacks, firing docks using handheld rocket launchers or mortars.
- Attacks from the air using manned or unmanned aircraft.
- NBC attacks (with nuclear, biological or chemical weapons), sabotage food supplies for ships passengers.

- Cyber-attacks targeting port security systems such as traffic control system, security system, and interference in database (read, modification and destruction).

According to the recent standards, security systems of critical infrastructure objects should be implemented in accordance with guidelines contained in "Marine Terminal Physical Security". The system includes subsystems such as vessel traffic system (VTS) and automatic identification system (AIS). Both of these subsystems are part of port management system (PMS) or vessel traffic management and information system (VTMIS). In order to ensure complete safety of objects like seaports, and to ensure protection against all threats mentioned above, it is necessary to connect under and above water threat detection systems. Such systems should include radar-camera units (allowing for identification and tracking of port personnel, vehicles and vessels [3]) and active and passive monitoring systems of underwater activities such as sonar and magnetic barriers [4, 5]. As a part of a research lead in the Military University of Technology, demonstrator of a seaport security system based on these assumptions was developed.

2. Critical infrastructure protection system — concept

There are many individual sensors for large areas protection on both military and civilian markets [4–11]. According to their technical characteristics, and specific physical phenomena, features of electronic security system for large area protection are highlighted:

- Radar-vision automatic detection and tracking of target [12–14],
- Connection of VIS and IR cameras to extend the observation capabilities during night and day [15],

*corresponding author; e-mail: mzyckowski@wat.edu.pl

- Fusion of data from cameras [16],
- Combination of data acquired from multiple systems on a digital map [17].

Taking into account the specific marine conditions, such system should be resistant to false alarms generated by strong wind and high waves. The base conception of seaport security system (Fig. 1) has been developed on the concept of newly built regasification terminal in Świnoujście.

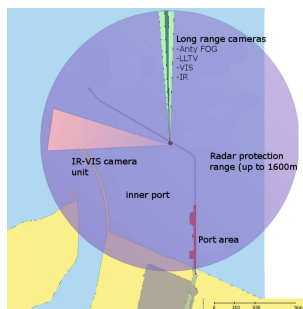


Fig. 1. Conception of seaport security system.

Particular areas should be protected by dedicated technical protection system. At the land area there are mechanical protection (fences, gates with access control, etc.) and monitoring by radar-camera units. In the water, the protection is realised by virtual barrier formed with various sensors. Sensors used in the system allow for monitoring of the entire protected area, not just the fence line.

Monitoring of the surface will be realized by a millimeter-wave radar (9–77 GHz) operating in continuous mode in scanning area with angular range up to 360°. The coverage of such surveillance system should be limited to 3000 m. Objects not recognized by AIS system are automatically considered as a threat, triggering the alarm procedure. The VIS and IR cameras are remotely guided to the target position with automatic settings of observation parameters, depending on the distance between camera and target. For obtaining the best image quality image fusion and background noise reduction (clutter) is performed.

The increasing technological capabilities allow terrorists to use more advanced water transport equipment such as speedboats, miniature submarines and remotely operated vehicles and submarines. Equipment used in attacks forces to build both surfaced and underwater security systems at the seaport. Underwater protection system, according to the principles of protection concept should allow detection and identification of underwater objects, tracking their movements and finally neutralization of threat. These subsystems should be built based on devices such as active sonar, acoustic barriers, magnetic barriers, optical and chemical sensors supported by physical underwater obstacles.

Current situation at the seaport should be fully presented on a digital map. All protected areas should be plotted and positions of all detected objects should be marked on a map. The patrols are equipped with GPS modules communicating with the system. Their position is also displayed on the map in real time. Except the positions of objects, operator panel presents images from the target tracking cameras, which helps to decide which actions should be taken in current situation.

The aim of surveillance centre integration is to minimize amount of personnel necessary to control each subsystem.

3. Security system demonstrator

As a part of the project the technology demonstrator for presentation of capabilities of large area critical infrastructure protection systems was developed. The demonstrator includes the visual and infrared camera, a set of long range cameras and a millimeter-wave radar. Multiple tests run in the real conditions allowed to eliminate errors in demonstrator. Each of performed test procedure beside checking operation and cooperation between different systems was focused on improving the operator interface in order to make it more efficient and help it to identify and handle as many alarms events and technical incidents as possible. Operator interface of the protection system demonstrator allows to visualize information about presence and location of an intruder on a digital map (calibrated with the GPS module), guide the cameras on targets, present images from visual and thermal cameras and perform the image fusion. In addition, the operator has the ability to control all the devices parameters. That allows to customize the system according to the actual needs and conditions. Additionally, the operator has the ability to specify more advanced features of system such as tracking based on image data, motion detection in the picture, control of advanced image enhancing methods, image fusion, and enabling image transfer to emergency services equipped with PDA. Underwater protection systems functionalities are presented as parts connected with blue line, above water/ground systems functionalities are connected with green line. For the correct interpretation and analysis of information obtained by system demonstrator, Command Centre for visualization of the data of each used subsystem was developed.

The main feature of the developed system is the universality. Based on a consistent, open source software, an operator interface for supervising a number of different protection systems based on optoelectronic sensors was developed. These sensors generally have closed protocols different for each producer. The developed system uses a set of TCP/IP interfaces, and brings together sensors to overall operation system. The main function of system is visualization of information about action of devices, controlling, testing and trigger actions of physical security groups on a digital map. Uniform software interface supports only these technologies which are characterized

by suitable properties allowing to maximize threats detection, as well as matching system performance to protected area. Distinctive feature of technology demonstrator is use of intuitive operating system mechanisms known from e.g. web browsers.

4. System tests

The principle of operation of multispectral above and underwater protection system is based on multisensor platform including such devices like millimeter-wave radar, VIS and IR cameras, and set of long range cameras. Main assumption of system operation is early detection of target in selected protection zones. In the next step, geographical position of detected target is calculated based on radar position and information about detected target. The last step is calculation of rotation angle (in azimuth and elevation) of cameras.

Calculation of rotation parameters is determined dynamically in case of camera selected by the system operator (cameras have various parameters values e.g. field of view). However, the position is determined to be sure that detected object is placed in the area used for calculating object tracking parameters. During the investigations, many series of measurements for different detected objects, on sea and land were performed. Tests were carried out not only at different targets, but with various weather conditions and for each camera included in demonstrator. Sample during the measurements, test procedures of automatic image contrast, and sharpness adjustment were tested. These procedures are based on measurements of contrast and phase shift between details in the image frame. Maximum contrast is equivalent to proper focus settings.

During the process of system demonstrator development, procedures of facilitating the operation of the automatic threat detection system were developed. The most important procedure is the methodology of fusing images from VIS with IR cameras. Assuming simplified model of camera perspective, the process of fusion of visible and thermal images can be reduced to three operations executed sequentially. The first operation is a transformation of image to highlight distinctive elements (e.g. thresholding with two thresholds), the second operation is calculation of geometric image transformation coefficients. Final step is reverse geometric transformation of one image to another and superimposing images. In Fig. 2a–c results of fusing recorded images are presented.

In the system of processing and controlling of observation cameras, a novel method of tracking the detected object based on two tracking algorithms was applied. The first method is a standard motion detection algorithm using images from VIS camera. Second algorithm is responsible for tracking objects in IR images. It is based on object attributes mean-shift algorithm connected with gradient algorithm sum-of-squared-differences (SSD). The results of that procedure for various observation distances

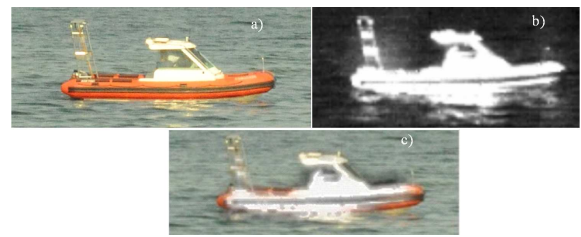


Fig. 2. Result of image fusion algorithm: (a) VIS image, (b) IR image, (c) fusion image.

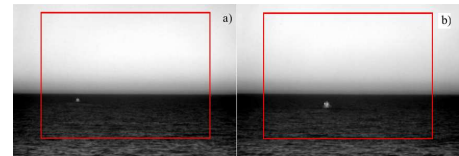


Fig. 3. Result of motion detection and tracking algorithms at distance of (a) 2400 m, (b) 900 m.

are shown in Fig. 3. Except using algorithms for tracking moving objects, also algorithms of image quality improvement have been applied. Examples of using algorithms during field tests are presented in Fig. 4.

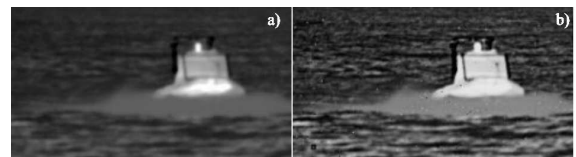


Fig. 3. Results of image enhancing algorithms (a) original, (b) enhanced.

During the demonstrator development, long ranged cameras were tested. Results of laboratory tests shown that with use of these cameras it is possible to recognize a human from a distance of 7600 m, and identify objects at the distance of 3800 m. Besides the laboratory measurements, cameras were tested in real conditions. Figure 4 presents plots of MTF parameter of the long range cameras. Comparison of images recorded under different weather and illumination conditions using various cameras are shown in Table.

5. Conclusions

Demonstrator of multispectral system for protection of seaport was developed according to the latest trends and technologies used in security systems of critical infrastructure objects. The main issue in construction of technical protection system turns out to be the accurate analysis of the physical phenomena used by particular optoelectronic sensors. Ensuring complementarity of physical threats detection and their disclosure from background determines maximum probability of intrusion detection.

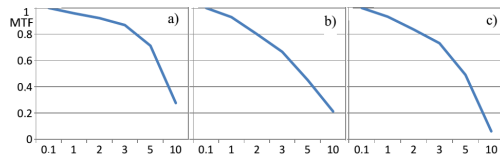




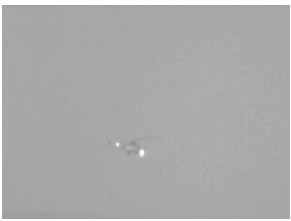



Fig. 4. MTF characteristics of long range cameras set: (a) VIS, (b) LLTV, (c) Anti-FOG.

TABLE

Long range camera tests results.

LLTV, zoom 25, 4 km	VIS, zoom 25, 1 km
	
Anti-FOG, zoom 100, 15 km	LLTV, zoom 100, 1 km
	
LLTV, zoom 100, 8 km	LLTV, zoom 25, 0.3 km
	

This is possible only by using a number of different technologies. Moreover, tests results showed that parameters values included in manufacturer's technical specifications very often differ from real values, thus before installing the equipment complete tests should be run in order to determine real values of parameters like range and sensitivity. Capabilities of intrusion detection and identification obtained with current systems allow to develop more precise and reliable systems for protection of critical infrastructure objects only when using additional features. Therefore, the developed system uses algorithms for image fusion and image quality improvement for more accurate and more precise objects identification.

However, development of a common operator interface of optoelectronic sensors is possible only with breaking the barriers between hardware manufacturers (problems of individual control commands, closed protocols and software drivers, personalized service and data analysis programs).

Acknowledgments

The system presented in this paper was developed during project funded by the Polish Ministry of Science and Higher Education (project OR00 0028 12).

References

- [1] K. Kubiak, www.wns.dsw.edu.pl/fileadmin/user_upload/wszechnica/04.pdf, 2010.
- [2] B.J. Rhodes, N.A. Bomberger, M.C. Seibert, A.M. Waxman, in: *Proc. IEEE MILCOM 2005* **1**, 646 (2005).
- [3] A.C. Van Den Broek, S.P. Van Den Broek, J.C. Van Den Heuvel, P.B.W. Schwing, A.W.P. Van Heijningen, *Proc. SPIE* **6736**, 67360P (2007).
- [4] M. Seibert, B.J. Rhodes, N.A. Bomberger, P.O. Beane, J.J. Sroka, W. Kogel, W. Kreamer, C. Stauffer, L. Kirschner, E. Chalom, M. Bosse, R. Tillson, *Proc. SPIE* **6204**, 62040B (2006).
- [5] G. Yan, B.B. Bista, D.B. Rawat, E.F. Shaner, in: *Proc. 2011 Int. Conf. on Broadband and Wireless Computing Communication and Applications* 6103009 (2011), p. 11.
- [6] R. Dulski, M. Szustakowski, M. Kastek, W. Ciurapiński, P. Trzaskawka, M. Zyczkowski, *Proc. SPIE* **7834**, 783416 (2010).
- [7] M. Zyczkowski, M. Szustakowski, W. Ciurapiński, N. Palka, M. Kastek, *Przegląd Elektrotechniczny* **86**, 157 (2010) (in Polish).
- [8] M. Kastek, R. Dulski, M. Zyczkowski, M. Szustakowski, P. Trzaskawka, W. Ciurapiński, G. Grelowska, K. Listewnik, *Proc. SPIE* **8388**, 83880M (2012).
- [9] M. Szustakowski, W. Ciurapiński, M. Zyczkowski, N. Palka, M. Kastek, R. Dulski, G. Bieszczad, T. Sosnowski, *Proc. SPIE* **7481**, 74810D (2009).
- [10] M. Życzkowski, A. Arciuch, W. Ciurapiński, in *Real-time Systems, Advances in Research and Application*, WKŁ, Warsaw 2009, p. 431 (in Polish).
- [11] M. Życzkowski, M. Szustakowski, M. Kastek, W. Ciurapiński, T. Sosnowski, *WIT Trans. Inform. Commun. Techn.* **42**, 123 (2009).
- [12] M. Zyczkowski, M. Szustakowski, W. Ciurapiński, M. Karol, P. Markowski, *Proc. SPIE* **8361**, 83611G (2012).
- [13] M. Zyczkowski, M. Szustakowski, W. Ciurapiński, R. Dulski, M. Kastek, P. Trzaskawka, *Proc. SPIE* **8184**, 818406 (2011).
- [14] M. Zyczkowski, N. Palka, T. Trzcinski, R. Dulski, M. Kastek, P. Trzaskawka, *Proc. SPIE* **8021**, 80211U (2011).
- [15] R. Dulski, S. Milewski, M. Kastek, P. Trzaskawka, M. Szustakowski, W. Ciurapiński, M. Zyczkowski, *Proc. SPIE* **8185**, 81850U (2011).
- [16] M. Kastek, R. Dulski, M. Zyczkowski, M. Szustakowski, W. Ciurapiński, K. Firmanty, N. Palka, G. Bieszczad, *Proc. SPIE* **8193**, 81933X (2011).
- [17] R. Dulski, M. Kastek, P. Trzaskawka, T. Piatkowski, M. Szustakowski, M. Zyczkowski, *Proc. SPIE* **8019**, 80190X (2011).