MULTISENSOR SYSTEM FOR THE PROTECTION ABOVEWATER OF SEAPORT

MARIUSZ KASTEK, MAREK ŻYCZKOWSKI,
MIECZYSŁAW SZUSTAKOWSKI, PIOTR TRZASKAWKA,
WIESŁAW CIURAPIŃSKI, RAFAŁ DULSKI

Institute of Optoelectronics, Military University of Technology
gen. S. Kaliskiego Str. 2, 00-908 Warsaw, Poland
mkastek@wat.edu.pl

There are many separated infrastructural objects within a harbor area that may be considered „critical", such as gas and oil terminals or anchored naval vessels. Those objects require special protection, including security systems capable of monitoring both surface and underwater areas, because an intrusion into the protected area may be attempted using small surface vehicles (boats, kayaks, rafts, floating devices with weapons and explosives) as well as underwater ones (manned or unmanned submarines, scuba divers). The paper will present the concept of multisensor security system for a harbor protection, capable of complex monitoring of selected critical objects within the protected area. The proposed system consists of a command centre and several different sensors deployed in key areas, providing effective protection from land and sea, with special attention focused on the monitoring of underwater zone. The protection of surface area is based on medium-range radar and LLTV and infrared cameras.

INTRODUCTION

Geopolitical changes that the word saw at the turn of the centuries had also great impact on global security threats and challenges. The classic threats of full-scale war are now less likely to develop, replaced by asymmetric threats, like global terrorism as a number one peril. This shift in the whole concept of global security is also reflected on a regional scale, for example considering the security of Baltic Sea area. Here also the terrorism is considered as a major threat to the security of harbor facilities and shore infrastructure. Organized crime is rather underestimated in his respect, and other possible threats are illegal immigration and proliferation of weapons of mass destruction and dual-use materials. Piracy, however, which gets the worldwide attention nowadays, is virtually non-existent in this area. [1, 2].

The danger of terrorist attacks exists also during peace time, and naval forces are not always ready to counter the unexpected terrorist attack. Such attacks may occur during the force withdrawal phase of peacekeeping operations, when the state of alertness is somehow lowered. The threat of terrorist attack rises as the crisis situation is being developed and in such crisis situation the sabotage and espionage acts are also likely to take place.

The attacks conducted by terrorists or other groups or individual persons against naval bases, harbors and other infrastructure can be accomplished in the following manner [2]:

- surface attack with manned and unmanned vessels, used to carry explosives or as weapon platforms, also hijacked ships with dangerous materials (e.g. oil or chemical tankers) which can be used to ram other ships or harbor facilities [3];
- underwater attacks using divers, mini subs (manned or remote controlled) and explosives or sea mines (ground, magnetic or drifting) [1];
- land attacks using bombs installed in cars or trucks, suicide attacks, attacks with handguns, grenades, mortars, mail bombs, rising the riots in the harbor and attacks on anchored ships to hijack it or to capture the crew as hostages;
- aerial attacks with manned of unmanned (remote-controlled) crafts, balloons or kamikaze attacks;
- NBC attacks involving the use of nuclear, biological and chemical agents (aerosols, liquids), poisoning the food and water or directly the crews and/or passengers;
- cybernetic attacks aimed at disrupting the information systems, breaking the security protocols, sending false alarm messages, stealing the data, forging and blocking the information flow, unauthorized modifications of database content.

European Union has introduced the Regulation 725/2004 on enhancing ship and port facility security and the Directive 2005/65/WE on enhancing the port security. Security system for the protection of critical port infrastructure (e.g. gas or oil terminal) should conform to the requirements included in „Marine Terminal Physical Security" document, which describes the protection of oil terminals. The harbor security system is composed of several interacting components, like:

- Vessel Traffic System (VTS) with long-range radars manages the traffic in the covered area. Incoming ship makes contact with system operator, identifies itself and then it is guided to the port.
- Automatic Identification System (AIS) automatically confirms the ship's identity on the basis of its unique radio code and database information. The system tracks and locates the ships on a digital map and, in its more advanced version also provides visual identification in the range of system cameras.

Both systems mentioned above are now being integrated in single Port Management System (PMS) or Vessel Traffic Management and Information System (VTMIS). The main task of such systems is to assure safe traffic both in roadstead and in internal harbor zone. The land zone of the harbor should be also protected, including gates, fences and selected installations, like pipelines or tanks. As a result the security systems for the harbor protection include such solutions as:

- radar-camera system for the identification and tracking of personnel, land vehicles and surface vessels In order to provide perimeter protection, access control and visual monitoring of the area [4].
- active (sonar) and passive (magnetic barriers) systems to monitor the surface and underwater activity (including divers) [5, 6].

1. CONCEPT OF HARBOR SECURITY SYSTEM

There are many types of commercially available surveillance systems for the protection of such large-area objects like harbors [5-8]. However, some observations can be made regarding basic concepts of such systems, because there is a general tendency to include such components as:

- radar-visual observation systems with automatic target detection and tracking by a radar and then cueing the cameras for visual recognition;
- CCTV paired with thermal cameras for day and night observation capability;
- fusion of daylight and thermal camera images to obtain the easy to comprehend output for a system operator;
- Merging the radar and image data and visualization of the target trajectory on a digital map.

The above systems, primary developed for land surveillance, are adapted to sea surface monitoring tasks. It sometimes create problems, because radar-visual observation systems can produce significant noise in case of windy weather and rippled sea. As a result the noise filtration algorithms have to be implemented, both in radar and camera systems [9, 10]. Underwater and surface zones should be also monitored, which is provided by passive and active systems. Such solutions (sonars and magnetic barriers) are used in restricted harbor areas, highly sensitive to unauthorized access (entrance to gas and oil terminals, pipelines, ships anchored at terminals) [11]; The system with integrated passive and active sensors and the signal processing and fusion units should be able to detect and identify surface and underwater targets, including divers [12].

Both systems: radar-camera for land and sea surface monitoring and surface-underwater for sea area monitoring are autonomous and can be deployed independently in the protected area. By connecting them via a network a complex, perimeter protection system can be obtained. Such solution is then suggested by the authors as a coherent system for the protection of port area, managed by a single command and control center and connected by cable or radio Ethernet network.

The requirements on system architecture, functionality and instrumentation were formulated on the basis of broad analyses and studies, including the concepts presented in:

- Offshore Surveillance and Security Solution L3 Communications Klein Associates Inc.;
- Security Perimeters to Protect Against IED Attacks. PureTech Systems;
- Area Protection Network (APN) - A Concept for Autonomous Perimeter Surveillance and Protection with Demonstrator;
- A multi – sensor scenario for costal surveillance.

In a basic system concept, which emerged after the analysis, the protected areas cover the terrain and critical land infrastructure, shore installations and selected sea zone (Fig. 1).

The selected port area is covered by a perimeter protection system. On the land it is physical protection (fences, gates with access control) whereas on the sea it is a virtual fence created by a sensor system [14-18]. In addition to physical barrier on the land, this area is also monitored by radar-camera system [19-22]. The illustration of this protection concept is shown in Fig.1. The perimeter line (fence) is remotely monitored and additionally the inside area is also under surveillance, including the restricted areas. Detailed requirements for radar-camera system will be given in the next chapter [4, 5], but basic requirements are as follows:

- automatic broad-area surveillance;
- increased effectiveness by merging radar and day/night image data;

- detection and tracking of the intruder, visualization on a digital map with movement information (speed, direction) which add to the threat assessment by a system operator;
- cost-effective solution, considering the size of the protected area, maintenance and running costs.

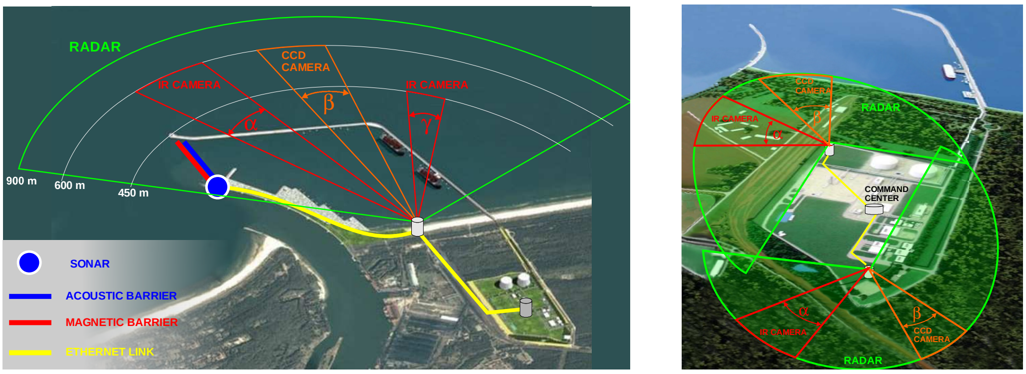


Fig.1. Sea and land zones protected by the proposed system.

Automatic surface monitoring is assured by radar scanning in the full (360^o) or selected horizontal angle in 24/7 regime. System is continuously scanning the protected zones and triggers the alarm in case of intruder detection. As it was already mentioned, the sea environment generates significant amount of noise, and the radar signals have to be filtered in order to minimize false alarm rate. Currently the radars used in the security systems are modified versions of short range sea radars. They have ranges from 200 m to 3 km and work at the frequencies from 9 GHz to 77 GHz, (millimeter radars). The signal processing hardware should have network interface to transmit radar data to target tracking system [23, 24]. Software layer of a tracking system should provide:

- user-definable protected zones;
- rejection of background reflections (both land and sea background);
- definable number of reflections from target that initiate or stop tracking;
- sensitivity adjustment according to disturbance level;
- transfer the target data to the radar system processor.

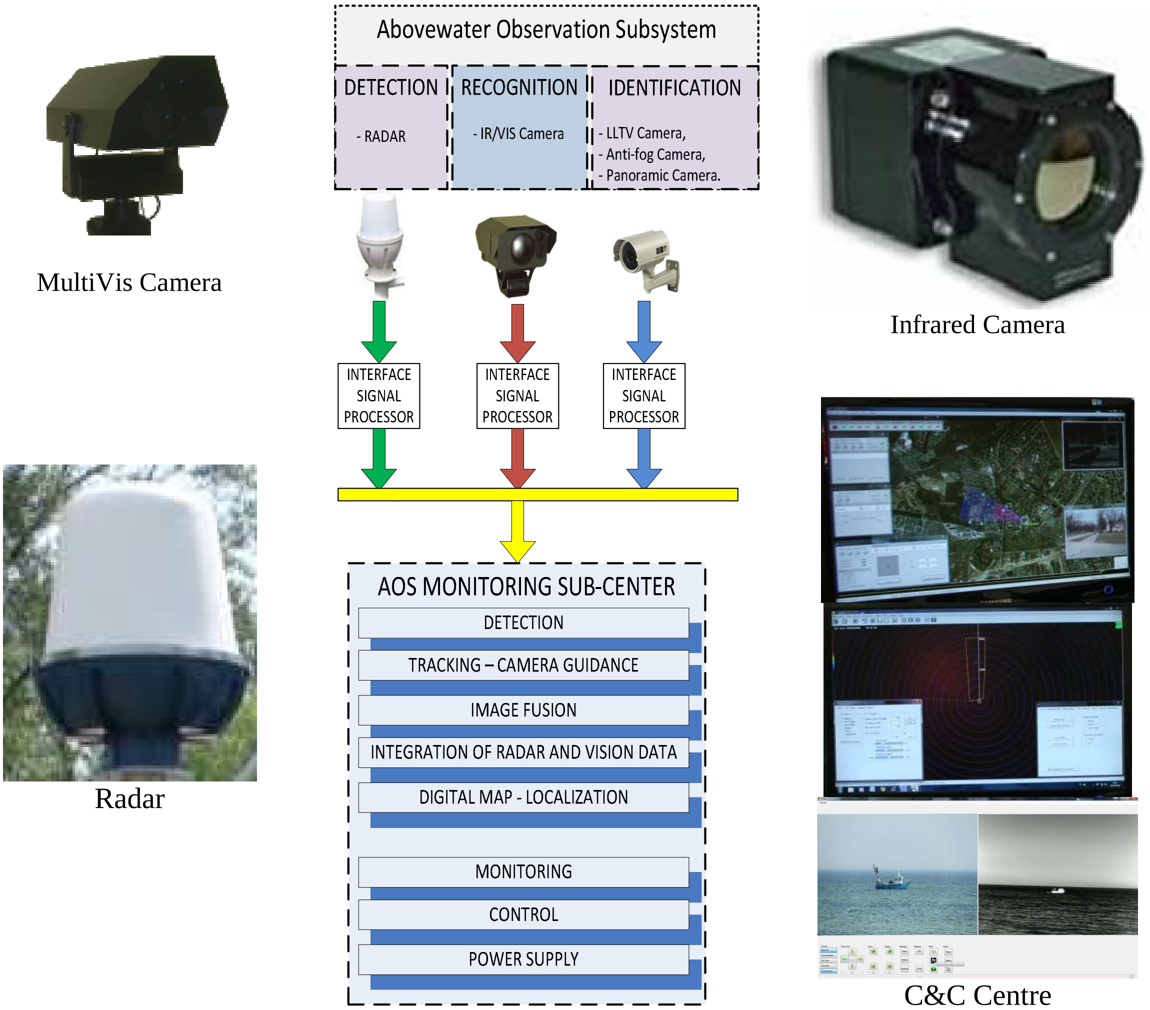
The object (target) type is determined on the basis of radar track data and harbor AIS system. Surface vessels not identified by AIS are considered as threats, which riggers the alarm on the operator's console and cue the cameras automatically to target. The target is viewed simultaneously by daylight and thermal cameras. Both should have automatic focusing aided by the distance information provided by the radar. In order to obtain best possible image quality the image fusion ids performed and the background clutter is filtered out [20, 21, 25]. The surface surveillance system should then provide:

- estimation of target movement and position;
- reception of AIS data;
- target identification (recognized – unrecognized – threat);
- rising the alarm and camera cueing;
- image filtering and fusion;
- sending the final visual data to the operator's console.

The actual situation in the harbor area (sea and land) is presented on a digital map with marked infrastructure objects and protected, restricted zones. All detected objects are displayed (tracked by radar, recognized by AIS, unrecognized-threats) using the color code.

Data visualization system presents also video images of the tracked objects to aid the operator's decision on the course of action. The operator upon receiving the alarm signal is obliged to act according to the defined security procedures. If the operator is not reacting, the system should initiate threat countering actions automatically, sending the information to the patrol units in the protected area. The patrol units are equipped with GPS modules and their position is also visualized on a digital map. Apart from automatic mode, the operator should he the option to control the system manually.

Physical location of surface and underwater area monitoring systems id determined by the configuration of a protected area (Fig.1.). For example the radar-camera sensors (range 500-800m) can be located on a single platform at the seaside or on breakwater. Location of underwater monitoring system is more complicated, because the barriers (acoustic and magnetic) must be placed at seabed in the protected zone and the location of active sonar depends on the sea bottom configuration and required angle of observation. Both underwater systems operate on different principles, so they require separate signal processing units and command sub-centers for data processing and visualization. Main Command Center should integrate the data from all the subsystems (sub–centers) and it should be located in the Harbor Security Center, which supervises all the security–related activities in the harbor area. The diagram of a monitoring system for the protection of selected infrastructure in the port area is presented in Fig. 2 and it includes the underwater and surface monitoring system and a command center.



MultiVis Camera

Infrared Camera

Radar

C&C Centre

Fig.2. System for the monitoring of underwater situation.

2. HARBOR WATERSIDE SURFACE SECURITY SYSTEM

Analyzed waterside harbor area is separated from an open sea by a 3 km long breakwater and on the other side there is another breakwater with 250 meters long repelling spur. The harbor entrance is about 350 meters wide and it is one of key areas to be protected. Another critical element is cargo unloading area, which is exposed to attacks from the entrance, and from the land and sea. The proposed surface monitoring system will include land and sea surface monitoring platform, fitted with the following sensors (Fig. 2):

- ground radar for the detection of small land and sea objects;
- Infrared and daylight cameras (radar cued);
- Multi-Vis camera system, comprising of LLTV camera, anti-fog camera and wide angle camera for panoramic view.

Multi-Vis camera will be pointed to a desired direction by showing the target on a digital map. Every system (radar and camera systems) will have its own software for signal processing and sending data to the Command Center (panel of control parameters of cameras is presented on Fig. 3).

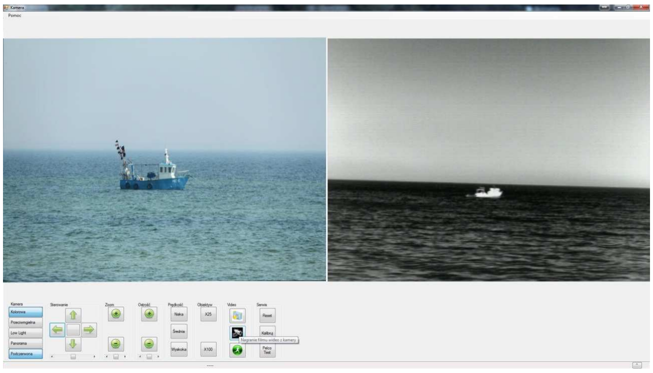


Fig.3. Panel control used for changing parameters of cameras.

Radar sensor has the range of 1200-1600 m and its location 6-10 meters above sea level small objects can be detected even on rippled sea. This sensor is a primary target detection device and it will be used to cue infrared/daylight cameras. The image from those cameras will be transferred directly to Command Center along with the data from automatic target identification system [26, 27]. The fusion of infrared and VIS images from the cameras will be performed and the processed image will also be presented to the system operator. In suitable conditions this will be enough to perform visual target identification. In harsh condition the Multi-Vis camera system will be also used for the target identification.

Fig.4. Sample images recorded during the summer season (temp. 23°C, humidity 87%, night) by anti-fog camera (a) and LLTV camera (b).

Multi-Vis camera systems has four main components: pan-tilt mount, daylight camera, night camera and anti-fog camera. Night camera can operate at the illumination as low as 0.00003 lux (no infrared emitters are required) and produces grayscale images with the resolution of 570 lines. Anti-fog camera sees through fog, smoke, drizzle and snow and it features 15dB contrast enhancement for improved image quality. Color daylight camera has the resolution of 540 lines and it is used for viewing well illuminated objects. The cameras have advanced optics, offering zoom capability from 6x to 100x and they are mounted on pa pan-tilt platform for effective target tracking. Long zoom range is achieved by using two separate, switchable lenses: lens 1: (zoom from 6 x to 25x, diameter 25mm) and lens 2 (zoom from 25x to 100x, diameter 115mm). Both lenses are electronically stabilized. The last camera is a wide angle device (with 8 mm focal length) for panoramic viewing. Sample images recorded by those cameras are shown in Fig. 4. Multi-Vis camera system is also equipped with image enhancement module, which increases the observation capability and probability of threat detection. The effects of application of different implemented algorithms on output camera images are presented in Fig. 5 [28-30].

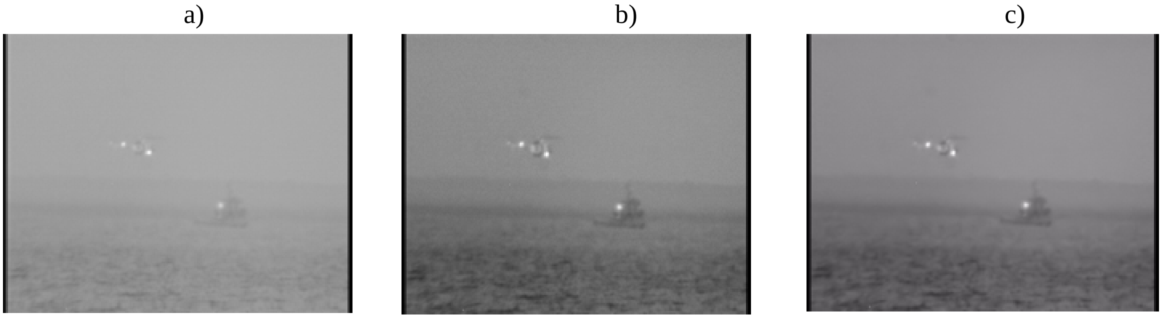


Fig. 5. Image enhancement algorithms for LLTV camera: unprocessed image (a), histogram equalization (b) and image filtering (c) (summer season, temp. 23°C, humidity 87%, night)

Daylight camera system is complemented with a thermal camera with VOx microbolometer focal plane array (640x480 pixels). The thermal camera has two switchable fields of view (focal length 35 mm and 100 mm) and electronic image magnification (two or four times). There is also an own image enhancement algorithm implemented in the camera, based on the histogram equalization method. Sample images recorded by this thermal camera are shown in Fig.6.

Fig. 6. Thermal images of a RIB boat: distance 600 m (a) and distance 1200 m (b). (summer season, temp. 23°C, humidity 87%, night)

3. DATA FUSION OF SECURITY SYSTEM

Effective exploitation (by a system operator) of all available information in all data channels requires the effective synthesis of sensor data to be applied [31-34]. Final effectiveness of a multi-sensor system should be (and usually is) better than the that of a simple set of individual, independent sensors. The real benefit of multi-sensor setup is achieved only when the sensors provide information complementary to each other.

Fig. 11 shows the diagram of data processing from all the system sensors from surface and underwater components. Both sub-systems have fully functional, separate data analysis modules, but the data fusion improves the target detection and lowers the false alarm rate.

The application of a multi-sensor system diminishes the possibility of losing a target track due to loss of signal (e.g. when one sensor loses the sight of a target, others may still see it). Another example of complementary sensor operation can be observed due to different spectral bands and principles of operation of particular sensors. For example, radar sensor and INFRARED camera have different properties (e.g. field of view, spectral band, spatial resolution). In a multi-sensor setup an omnidirectional sensor (radar) can be used to detect the target and then cue the high-resolution camera for final target identification. As it was already mentioned, the effectiveness of particular sensors depends on many factors, like weather conditions, background properties, distance and countermeasures used by an intruder. It may happen that single sensor has to operate in conditions far from optimal. The application of different sensors that are differently influenced by those external conditions assures constant proper system operation. Passive IR sensors (and VIS cameras) do not provide distance information, only angular dimensions can be extracted. The combination of radar sensor and a camera gives both the distance and target size data.

Data synthesis is a multi-layer process [34]. In case of the perimeter protection system the initial data processing has to be performed and the target status has to be determined. The estimation of target status comprises of the characterization of an object itself and its movement. Object characterization is a process of data evaluation (not only sensor signals) that leads to complete target recognition: detection, direction, classification and identification [31]. Detection is defined as confirmation of the presence of the target. Classification means that the detected target is assigned to one of the pre-determined classes of objects (e.g. human, boat, truck, ship). Identification level is achieved when the precise object description within its class can be made (human: armed assailant, boat: fishing cutter). Higher level of target discrimination imposes higher requirements on sensor resolution and signal-to-noise ratio at its output. The application of particular data synthesis algorithms in a multi-sensor security system depends on the overall system concept of operation. For example, object tracking relies usually on raw sensor data processing performed by a central system processing unit, whereas identification algorithms use complex data analysis at every functional level of the system. The general scheme of operation is presented in Fig. 7 and the detailed description of main stages and algorithms of data synthesis in the proposed security system for perimeter protection will be described below.

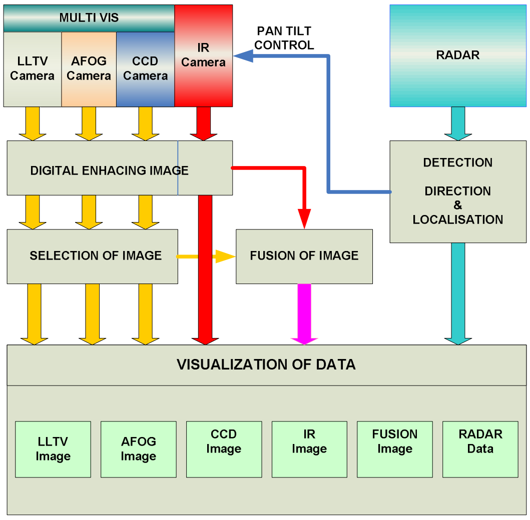


Fig.7. Concept of sensor data synthesis using radar, MultiVIS and infrared cameras.

At the moment when radar sensor detects the possible target [25] the range and bearing data are used to direct the cameras mounted on the sensor platform. Image analysis module matches the fields of view of both infrared and VIS cameras [35]. At this time the image fusion process (synthesis of images) is initiated. It can be seen from the above image that cameras have different fields of view and resolution. The synthesis of such images can be performed in a following way: [33, 34]:

$$f = f_i^{VIS} \oplus \tilde{f}_i^{IR}(s,\theta,t), \tag{1}$$

where $\tilde{f}_i^{IR}(s,\theta,t)$ is a processed image f_i^{IR} from infrared camera after the following transformations: resizing by a factor s, shifting by a vector t and rotation by an angle θ. In order to overlay two images the values of s and θ have to be calculated as well as operator of the synthesis $\oplus$. When the aforementioned coefficients are determined, the image synthesis is performed using discrete wavelet transform (DWT) [35]. For a visual image I^{VIS} and infrared image I^{IR}, the DWT-based image synthesis algorithm can be described as [36]:

$$f = \omega^{-1}(\phi(\omega(I^{VIS}), \omega(I^{IR}))), \tag{2}$$

where ω is a DWT, ω-1 is inverse DWT, φ is a certain rule of image synthesis and f is a final synthesized image.

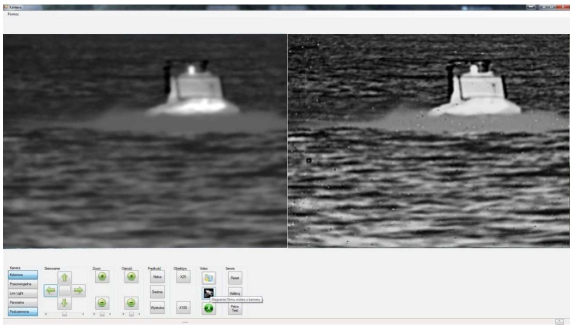


Fig.8. Results of procedure of enhancing imaging processing used in infrared camera: unprocessed image (left), histogram equalization (right).

Every image is analyzed and as a result some areas are marked, in which the presence of a target is suspected. infrared image is “binarized” using pre-defined detection thresholds and after that the mask distinguishing certain objects is obtained. Mask is created by assigning high brightness level (white color) to any area above detection threshold and low level (black color) to the rest of the image. In order to distinguish target from background the detection threshold (temperature value) is adaptively calculated – objects of temperatures lower than threshold are treated as background. Algorithms used for defining threshold brightness value are, in case of visual images, usually based on histogram analysis [36, 37]. For thermal images the application of the probability density function describing the occurrence of certain temperature values is more appropriate. This function is then discretized in the temperature domain and the histogram showing the occurrence of certain temperature ranges is obtained. During initial tests the histogram-based analysis was yet not applied and arbitrary threshold level at 60% of dynamic range was used instead. Final image is created by appropriate merging of the image obtained according to the above procedure with an infrared image.

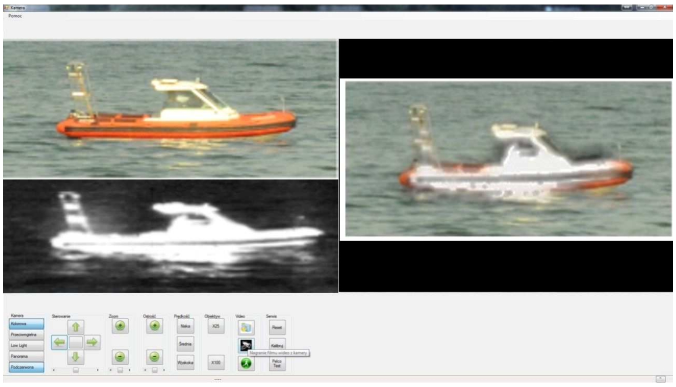


Fig.9. Results of procedure of image fusion used in visible and infrared camera: visible and infrared image (left), fused image (right).

The presented concept of radar and camera data fusion is only one of many possible solutions. The Security system for the protection of selected critical infrastructure interacts (on the Command and Control center level) with other security related systems of a seaport (like AIS) thus giving the operator full situational awareness in the vicinity of a protected zone.

4. CONCLUSIONS

The presented concept of a multisensor security system for the protection of critical infrastructure in the harbor area, comprising of underwater and surface monitoring sensors follows the current trends in contemporary security systems. The application of unique underwater sensor layout and the data fusion with surface sensors increases the probability of intruder detection in an attempt to violate the protected zone. Such solution is particularly important bearing in mind the threats and dangers of the present world.

Sensor data fusion demonstrated in the surface system components (daylight cameras, thermal cameras and radars) increases the probability of detection of small, fast surface objects like RIB boats, which are often used by terrorists in their attacks. The application of image enhancement techniques and fusion of thermal and daylight images may further increase the detection and visual identification range of small, fast-moving objects. The presented camera set-up and image processing algorithms were field tested with promising results, and the application of such camera configuration in security and surveillance systems is highly advisable.

The presented complex, multisensor system can be deployed for the protection of real harbor area become valuable security component. The test results indicate its effectiveness in detecting all kinds of objects that can be a threat to the seaport area.

ACKNOWLEDGEMENT

The presented research project is supported by Polish National Centre for Research and Development in the frame of research programs funding plan for the years 2009-2011.

REFERENCES

[1] K. Kubiak, www.wns.dsw.edu.pl/fileadmin/user_upload/wszechnica/04.pdf, (in Polish) (2010).

[2] B.J. Rhodes, N.A. Bomberger and all, “Maritime situation monitoring and awareness using learning mechanisms”, Proceedings of IEEE MILCOM 2005 Military Communications Conference Atlantic City NJ USA, 2005.

[3] D. Suchman, “Basic Do's and Don'ts of Designing, Installing and Operating a Harbor Protection system”, Proceedings of TICA'05, (2005).

[4] A.C. Van Den Broek, S.P. Van Den Broek and all, “A multi-sensor scenario for coastal surveillance”, Proc. of SPIE, 6736, 67360P (2007).

[5] M. Seibert, B.J. Rhodes, N.A. Bomberger and all, “SeeCoast port surveillance”, Proc. of SPIE 6204, 62040B (2006).

[6] G.a Yan, B.B.b Bista, D.B.c Rawat and all, “General active position detectors protect VANET security”, Proceedings - 2011 International Conference on Broadband and Wireless Computing Communication and Applications 6103009, 11-17 (2011).

[7] R. Dulski, M. Szustakowski, M. Kastek and all, “Infrared uncooled cameras used in multi-sensor systems for perimeter protection”, Proc. of SPIE, 7834, 783416 (2010).

[8] M. Zyczkowski, M. Szustakowski, W. Ciurapinski and all, “Integrated optoelectronics security system for critical infrastructure protection”, Przegląd Elektrotechniczny 86 (10), 157-160 (2010).

[9] G. Fasano, L. Forlenza, D. Accardo and all,”Integrated obstacle detection system based on radar and optical sensors”, AIAA Infotech at Aerospace 2010, 3421 (2010).

[10] G. Fasano, D. Accardo, A. Moccia and all, “Flight Test results for a multi sensor obstacle detection and tracking system for sense and avoid applications”, AIAA Infotech and Aerospace 2009, (2009).

[11] A. Asada, K. Kuramoto, T. Tanaka and all, “Development of underwater security sonar system”, OCEANS 2006 - Asia Pacific, 4393879 (2007).

[12] E. Belcher, W. Hanot, J. Brush, “Dual-Frequency Identification Sonar (DIDSON)” UT2002, 187-192(2002).

[13] T. Sosnowski, H. Madura, M. Kastek and all, “Method of objects detection employing passive IR detectors for security systems”, Proc. of SPIE 7113, 71131G (2008).

[14] M. Kastek, T. Sosnowski, H. Polakowski and all, “Long-range PIR detector used for detection of crawling people”, Proc. of SPIE 7113, 71131F (2008).

[15] P. Lindquist, “Area Protection Network (APN) - A concept for autonomous perimeter surveillance and protection with demonstrator”, Proc. of SPIE 6736, 67360N, (2007).

[16] M. Kastek, T. Sosnowski, T. Piatkowski, “Passive infrared detector used for detection of very slowly moving of crawling people”, Opto-electronics Review 16 (3), 328-335 (2008).

[17] M. Kastek, H. Madura, T. Sosnowski, “Passive infrared detector used for infrastructure protection”, WIT Transactions on the Built Environment 108, pp. 61-70 (2009).

[18] M. Szustakowski, W. Ciurapinski, M. Zyczkowski and all, “Multispectral system for perimeter protection of stationary and moving objects”, Proc. of SPIE 7481, 74810D (2009).

[19] C.J. Baker, H.D. Griffits, “Bistatic and Multistatic Radar Sensor for Homeland Security”, www.natoasi.org/sensors2005/papers/baker.pdf.

[20] P. Cory and all, “Radar – Based Intruder Detector for a Robotic Security System”, www.nosc.mil/robots/pubs/spie3525b.pdf.

[21] Lipton and all, “Critical Asset Protection, Perimeter and Threat Detection Using Automated Video Surveillance”, www.objectvideo.com.

[22] G.Yan, W. Yang, J. Lin and all, “Active location security through dynamically tunable radar in vanet”, Proc. of the 7th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2010) San Francisco USA, 2010;

[23] W. Butler, P. Poitevin, J. Bjornholt, “Benefits of wide area intrusion detection systems using FMCW radar”, Proc. of SPIE 6943, 69430Q (2008).

[24] Seastrand, M.J., “Maritime microwave radar and electro-optical data fusion for homeland security”, Proc. of SPIE, 5403 (PART 2), 673-682 (2004).

[25] M. Zyczkowski, N. Palka, T. Trzcinski and all, “Integrated radar-camera security system - Experimental results”, Proc. of SPIE 8021, 80211U (2011).

[26] M. Zyczkowski, M. Szustakowski, W. Ciurapiński and all, “Integrated mobile radar-camera system an airport perimeter security”, Proc. of SPIE 8184, 818406 (2011).

[27] G. Bieszczad, T. Sosnowski, H. Madura and all, “Image processing module for high speed thermal camera with cooled detector”, Proc. of SPIE 8012, 80120L (2011).

[28] R. Dulski, P. Powalisz, M. Kastek and all, “Enhancing image quality produced by IR cameras”, Proc. of SPIE 7834, 783415 (2010).

[29] G. Bieszczad, T. Sosnowski, H. Madura and all, “Adaptable infrared image processing module implemented in FPGA”, Proc. of SPIE 7660, 76603Z (2010).

[30] S.P. Van Den Broek, “Detection and classification of infrared decoys and small targets in a sea background”, Proc. SPIE 4029, 70-80 (2000).

[31] M. Kastek, R. Dulski, M. Zyczkowski and all, “Multisensor systems for security of critical infrastructures - Concept, data fusion, and experimental results”, Proc. of SPIE 8193, 81933X (2011).

[32] D. L. Hall, J. Llinas,”An introduction to multisensor data fusion”, Proc. IEEE vol. 85 no. 1, 6-23 (1997).

[33] L. A. Klein, Sensor and Data Fusion Concepts and Applications. SPIE (1993).

[34] R. Dulski, S. Milewski, M. Kastek and all, “Detection of small surface vessels in near, medium and far infrared spectral bands”, Proc. of SPIE 8185, 81850U (2011).

[35] Burt, P. J., Adelson, E., “The Laplacian pyramid as a compact image code”, IEEE Trans. Communications vol. 31 no. 4, 532-540 (1983).

[36] R. Dulski, M. Kastek, G. Bieszczad, and all, “Data fusion used in multispectral system for critical protection”, WIT Transactions on Information and Communication Technologies 42, 165-172 (2009).

[37] W. Ciurapinski, R. Dulski, M. Kastek and all, “Data fusion concept in multispectral system for perimeter protection of stationary and moving objects”, Proc. of SPIE 7481, 748111 (2009).