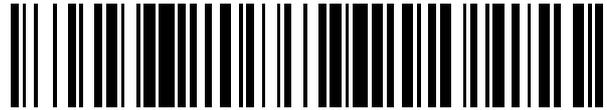


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 534 446**

51 Int. Cl.:

G08B 13/00 (2006.01)

G08G 3/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **03.08.2011 E 11754759 (6)**

97 Fecha y número de publicación de la concesión europea: **04.03.2015 EP 2601647**

54 Título: **Sistema antipiratería para la navegación marítima en áreas críticas y dispositivo para extracción de datos desde sensores a bordo**

30 Prioridad:

03.08.2010 IT RM20100434

03.08.2010 IT RM20100433

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

23.04.2015

73 Titular/es:

SELEX ES S.P.A (100.0%)

Piazza Monte Grappa, 4

00195 Roma (RM), IT

72 Inventor/es:

FIORINI, MICHELE;

GRAZIANO, GIOVANNI;

RULLI, ALBERTO y

BODO DI ALBARETTO, PAOLO

74 Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

ES 2 534 446 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema antipiratería para la navegación marítima en áreas críticas y dispositivo para extracción de datos desde sensores a bordo

5 La presente invención concierne a un sistema antipiratería para la navegación marítima en áreas críticas y un dispositivo para extracción de datos desde sensores a bordo.

Más en detalle, la presente invención concierne un sistema marítimo antipiratería basado en el análisis y seguimiento de objetivos. Tal sistema tiene en cuenta diferentes fuentes de información, para proporcionar al usuario final un canal de navegación seguro dentro de un área crítica y más en general en la Zona Económica Exclusiva (EEZ), gestionada por centros costeros o sistemas VTS (Servicios de Tráfico de Buques). La invención además
10 concierne un dispositivo para extracción de datos desde sensores a bordo de un barco que se utiliza en el sistema de la invención.

En los últimos 10 años, el Solicitante ha desarrollado, entre otros, los siguientes productos: el Servicio de Tráfico de Buques (VTS) y el Servicio de Gestión de Tráfico de Buques (VTMS), que explotan la búsqueda y patrimonio de saber hacer conseguido en la defensa de misiones críticas y en los campos de "Control de Tráfico Aéreo" (ATC), en
15 donde la sociedad está comprometida en la entrega de sistemas todo en uno, con respecto a un conjunto grande de consumidores en todo el mundo. El VTS y los sistemas de control de tráfico marítimo se han instalado en toda Italia, incluyendo un sistema particular para la gestión del tráfico en la laguna de Venecia y en diversos países del mundo, incluyendo Rusia, China, Polonia, Yemen y recientemente Turquía y Panamá. Además, la versión fluvial de los mismos sistemas, para el control de tráfico fluvial, está siendo instalada en Serbia en el río Danubio.

20 Cuando un sistema electrónico basado en sensores está acoplado con extensas capacidades de procesamiento de base de datos, el producto del Solicitante se llama Sistema de Gestión e Información de Tráfico de Buques (VTMIS).

El Solicitante está implementando actualmente el sistema de VTS nacional italiano que comprende:

- 73 emplazamientos de radar;
- 3 unidades de radar móviles;
- 25 - 39 centros de control local;
- 14 centros regionales;
- 1 centro nacional;
- 1 centro de formación.

30 El sistema tiene una organización de control y de comando en múltiples niveles, una cobertura redundante de áreas críticas, la posibilidad de integrar datos/servicios o Intercambiarlos con un cierto número de organizaciones externas (tanto civiles como militares): un ejemplo importante de esta capacidad de integración se da por la interconexión e intercambio de datos entre el Servicio Nacional de Viaje de Buques (NVTS) y el Sistema Nacional de Vigilancia Costera (NCSS), gestionado enteramente por la Marina Militar italiana.

35 Desde 1990 el Solicitante está presente activamente en las principales comisiones Internacionales (IMO – Organización Marítima Internacional, IALA – AISM Asociación Internacional de Ayudas Marinas a la Navegación y Autoridades de Faros, proyectos europeos, etc.), su negocio marítimo ha evolucionado de manera natural para satisfacer las necesidades recientes del mercado, incluyendo mejoras a la Gestión de Tráfico de Buques (VTM), e-Navegación, LRIT (Identificación y Seguimiento de Largo Alcance), vigilancia costera, vigilancia y gestión de navegación fluvial y sistemas de seguridad de embocaduras.

40 La piratería marina se ha doblado en 2009 como se indicaba por la Oficina Marítima Internacional (IMB). La IMB cree que la escalada de la piratería tendrá consecuencias económicas significativas para los países de economías emergentes. Como consecuencia, estos países deberían adoptar un sistema para asegurar ciertas rutas comerciales para evitar amenazas y establecer un Centro de Notificación de Piratería (PRC) de la IMB en Kuala Lumpur, Malasia. La mayor parte de los informes es relevante para el aumento de la actividad en el golfo de Aden y en las
45 aguas costeras de Somalia, en donde ocurrieron más de 150 accidentes en el pasado año.

El documento de patente US2009045983 describe un sistema de reconocimiento amigo/enemigo en el mar se describe (WFSS) que utiliza una tarjeta SIM ("Módulo de Identidad de Abonado") con un lector de SIM a bordo de una embarcación. Un transmisor, que está acoplado con el lector de SIM, transmite información desde la tarjeta SIM, así como información de posicionamiento, a una estación de seguimiento del sistema. La ventaja de este sistema
50 sería que evita modificaciones no autorizadas de la información de la embarcación cuando se utiliza junto con el estándar AIS, así como la autoidentificación de un gran número de embarcaciones sin rehacer los estándares globales AIS y GMDSS. No obstante, se describe la transmisión del ID pero no de toda la autenticación de todos los mensajes AIS por la pertinente clave a la ID. En particular, se utiliza una RFID, para la información de ID y tal

información se transfiere descifrada a través del AIS. Todo esto presupone una infraestructura de red (GSM o equivalente) presente actualmente solamente cerca de las costas.

5 La patente US 2003233176 describe un sistema de recogida y distribución de datos marítimos que comprende un barco configurado para transmitir una señal (por satélite) que corresponde a la posición actual del barco o a la posición prevista del barco, una red informática que incluye una o más bases de datos, cada una que comprende una o más zonas de interés, en donde la zona de datos de interés corresponde a una zona de controlador y un proveedor de servicios configurado para recibir la señal, recuperar uno o más datos de las zonas de interés a partir de la red informática sobre la base de la señal y transmite al barco una o más zonas de datos de interés para el barco. La zona de datos de interés está constituida por marítimas que son favorables a una utilización segura y económica del barco. La zona de interés es un área tridimensional que rodea el barco o una zona de tiempo limitado que rodea el barco.

10 El documento de patente US2008079608 describe un método para la optimización de la programación de los barcos que entran y se dirigen dentro/fuera del puerto, el método que comprende los pasos de:

- 15 a. combinar la información de un sistema de identificación automático en cada barco con la planificación de información de cada barco de un sistema de envío para producir una programación/ID combinados para cada barco;
- b. hacer el seguimiento de la latitud y longitud de cada barco por GPS para la producción de la latitud y longitud rastreadas para cada barco;
- c. comparar la latitud y longitud rastreadas de cada barco con los mapas de puerto existentes;
- 20 d. comparar continuamente la programación/ID para cada barco con la latitud y longitud rastreadas de cada barco.

La señalización se envía cada vez que la latitud y longitud rastreadas no corresponden a la latitud y longitud esperada de cada barco en un instante dado. El método hace el seguimiento y graba cada vez que un piloto embarca o desembarca de un barco.

25 El documento "Operational use of satellite SAR at EMSA" de Marin Chintoan-Uta, páginas 1-45, presentado en el Taller ESRIN de SEASAR, Frascati, 25 de enero de 2010, menciona la antipiratería en conexión con la vigilancia de embarcaciones.

30 Es un objeto de la presente invención un sistema antipiratería avanzado que se adapta perfectamente a las arquitecturas de VTMS funcionales y constituye una función complementaria para la defensa de áreas extendidas que están amenazadas por piratas y terroristas. El objeto del sistema de la invención también se puede utilizar en todos los sistemas de control de fronteras, seguridad/protección nacional y Zona Económica Exclusiva (EEZ).

Es un objeto de la presente invención un sistema antipiratería marítima, para el reconocimiento de embarcaciones sospechosas alrededor de uno o más barcos cooperantes a ser protegidos, que comprende:

- un sistema de control con base en tierra, que comprende:
- 35 - uno o más centros, distribuidos geográficamente, que comprenden sensores en tierra para detectar datos de vigilancia de embarcaciones;
- una estación central para recoger y elaborar datos de vigilancia de embarcaciones;
- 40 el sistema de control con base en tierra que comprende una red de comunicación bidireccional entre dichos uno o más centros y dicha estación central, de tal forma que la estación central sea capaz de enviar comandos a dichos sensores con base en tierra;
- un sistema de comunicación entre dichos uno o más centros y dichos uno o más barcos cooperantes a ser protegidos,

el sistema antipiratería que se caracteriza por que comprende:

- 45 - uno o más dispositivos, montados a bordo de dichos uno o más barcos cooperantes correspondientes a ser protegidos, para extracción de datos de vigilancia marítima desde sensores de vigilancia marítima, que están montados a bordo de dichos uno o más barcos cooperantes correspondientes a ser protegidos y son adecuados para vigilar el espacio alrededor de dichos uno o más barcos cooperantes, dichos uno o más dispositivos para extracción de datos que son adecuados para enviar dichos datos de vigilancia marítimos a al menos uno de dichos uno o más centros a través de dicho sistema de comunicación;

- un sistema de identificación y autenticación de dichos uno o más barcos cooperantes a ser protegidos, que funciona a través de dicho sistema de comunicación y se comparte entre dichos uno o más centros y cada uno de dichos uno o más barcos cooperantes a ser protegidos, en donde

5 dicha estación central para recoger y elaborar datos elabora los datos que llegan desde dichos uno o más centros y por lo tanto también desde dichos uno o más barcos cooperantes a ser protegidos y lanza las alarmas pertinentes en el caso de reconocimiento de embarcaciones sospechosas.

Aquí por "vigilancia marítima" se entiende la vigilancia de las embarcaciones en una zona marítima.

10 La ejecución de la elaboración por la estación central puede comprender el cruce de todos los datos a fin de individualizar la embarcación sospechosa o reconocer siluetas de embarcaciones que no están entre las formas de los barcos cooperantes, con referencia particular al procesamiento de la cinemática de todas las embarcaciones con el final de asignar a cada una de ellas un nivel de amenaza que puede ser de manera simplista amigo, enemigo, neutral, basado en sistemas heurísticos e inteligentes que aprenden y mejoran por la experiencia la fiabilidad del resultado propuesto.

15 Preferiblemente según la invención, dichos sensores de vigilancia marítima comprenden el radar montado a bordo de dichos uno o más barcos cooperantes a ser protegidos.

De tal forma, ampliando, por medio del radar a bordo y opcionalmente también la(s) cámara(s), la cobertura de los sistemas en tierra, uno disminuye drásticamente los tiempos de reacción para las posibles contramedidas (el factor tiempo es fundamental como se mencionó anteriormente).

20 Preferiblemente según la invención, dicho sistema de identificación y autenticación comprende uno o más dispositivos de transmisión de AIS montados en dichos uno o más barcos cooperantes correspondientes y al menos un dispositivo de recepción de AIS en tierra, dichos uno o más dispositivos de transmisión de AIS que son adecuados para transmitir información de autenticación de la identidad de dichos uno o más barcos cooperantes correspondientes a dicho al menos un dispositivo de recepción de AIS.

25 Preferiblemente según la invención, a cada uno de dichos uno o más dispositivos de transmisión de AIS y dicho al menos un dispositivo de recepción de AIS en tierra se asocia una unidad de cifrado, que genera una clave para la autenticación de los mensajes de AIS, sin cargar la estructura de los mensajes intercambiados, es decir dentro de los estándares del sistema AIS.

Preferiblemente según la invención, dicho sistema de identificación y autenticación comprende o está constituido por una comunicación VHF sin firma cifrada.

30 Preferiblemente según la invención, dichos sensores con base en tierra comprenden al menos una cámara en tierra y dichos sensores de vigilancia marítima comprenden al menos una cámara, dicha estación central que elabora los datos de vídeo que llegan desde dichos sensores con base en tierra y dichos sensores de vigilancia marítima para obtener trazas de vídeo de embarcaciones, que incluyen dichas embarcaciones sospechosas y dichos uno o más barcos cooperantes, que se elaboran juntos con al menos una traza que llega desde dicho al menos un dispositivo de recepción de AIS en tierra y dicho radar pertinente para las mismas embarcaciones, con el fin de mejorar el reconocimiento de las mismas embarcaciones.

35 Esta es una novedad en el campo, debido a que hasta ahora la información electroóptica no se ha integrado con las de los radares. Uno puede integrar los datos de cámaras en tierra y/o cámaras a bordo. En particular, uno integra información que llega del análisis óptico de los flujos de vídeo de las cámaras (alta sensibilidad, cotidiana y de infrarrojos) con la información obtenida a partir del procesamiento de las señales electromagnéticas proporcionadas por radares y las señales de radar de AIS.

Preferiblemente según la invención, dicha estación central elabora datos de vídeo de una cámara para obtener adicionalmente las siluetas de embarcaciones y las compara con una serie de siluetas predefinidas pertinentes a barcos conocidos.

45 Esto aumenta la confianza del reconocimiento y añade información de siluetas de la embarcación bajo examen. Esta también es una novedad, dado que aún el reconocimiento de la silueta de la embarcación se ha comprometido al análisis de datos de satélite de difícil realización (y cara) y ciertamente no en casi tiempo real. Típicamente uno recoge datos de satélite durante un periodo de tiempo largo y entonces los elabora fuera de línea, obteniendo las siluetas de las embarcaciones bajo examen.

50 Uno integra de esta manera información a partir del análisis óptico de los flujos de vídeo de las cámaras (alta sensibilidad, cotidiana y de infrarrojos) con la información obtenida a partir de la elaboración de las señales electromagnéticas proporcionadas por los radares y las señales de radar de AIS.

Preferiblemente según la invención, cada uno de dichos uno o más dispositivos para extracción de datos comprenden:

- un módulo para conectar a dichos sensores de vigilancia marítima, por medio de un canal principal de datos o por conexión directa;

- un módulo de pasarela para conectar a un módulo de transmisión de datos montado a bordo de dichos uno o más barcos cooperantes para el envío de los datos extraídos a tierra a través de dicho sistema de comunicación.

- 5 Sin el módulo de conexión directa (rastreador), un pierde la gran mayoría de casos en donde hay embarcaciones que funcionan con un formato que no es estándar y no pueden transmitir por lo tanto a tierra los datos obtenidos desde los sensores a bordo (el operador humano en tal caso comunica el reconocimiento, por ejemplo por teléfono).

Gracias al dispositivo según la invención, uno agranda el rango de acción de la localización marítima (observación), dado que los sensores a bordo extienden y detallan la localización más allá del alcance de los sensores en tierra.

- 10 Preferiblemente según la invención, cada uno de dichos uno o más dispositivos para extracción de datos comprenden un módulo de elaboración de datos extraídos, que es adecuado para preparar los datos elaborados a ser transmitidos a través de dicho módulo de pasarela.

Preferiblemente según la invención, el módulo de elaboración de datos extraídos funciona como un rastreador a bordo, en particular en el caso de datos extraídos de sensores de radar a bordo.

- 15 En realidad muchos barcos trabajan con un formato no estándar, fallando dicho módulo de seguimiento y por lo tanto no pueden transmitir los datos obtenidos desde sensores a bordo (el operador humano, en tal caso, tiene que comunicar el reconocimiento, por ejemplo por teléfono).

Gracias al dispositivo según la invención, uno agranda el rango de acción de la localización marítima (observación), dado que los sensores a bordo extienden y detallan la localización más allá del alcance de los sensores en tierra.

- 20 Preferiblemente según la invención, dicho módulo de pasarela es adecuado para operar hacia un módulo de transmisión de datos radio VHF montado a bordo de dichos uno o más barcos cooperantes.

Preferiblemente según la invención, dicho módulo de pasarela es adecuado para operar hacia un módulo de transmisión radio U/VHF y/o por satélite, montado a bordo de cada uno dichos uno o más barcos cooperantes para el envío de datos al sistema de control en tierra.

- 25 Preferiblemente según la invención, dicho módulo de pasarela comprende un submódulo para la gestión de comandos y parámetros pertinentes a la comunicación radio, tales como por ejemplo el traspaso en la selección de las frecuencias y canales radio a ser utilizados en dicho sistema de comunicación.

Preferiblemente según la invención, cada uno de dichos uno o más dispositivos comprende dos módulos de conexión a dichos sensores de vigilancia marítima:

- 30 - un módulo de conexión directa, que extrae los datos y los representa en un formato predefinido;
- un módulo de conexión indirecta de canal principal (ETH), que es un olfateador para extracción de datos y representación de datos en un protocolo estándar.

Preferiblemente según la invención, dicho sistema de identificación y autenticación utiliza indiferentemente o bien el mensaje N° 8 o bien el 6 del estándar de AIS, que proporcionan medios de elaboración electrónica que añaden una información secreta a la cadena de los 24 mensajes de AIS y calculan una función de generación de claves de la cadena entera así obtenida, dicha función de generación de claves que se inserta o bien en el citado mensaje 8 o bien 6, la cadena de 24 mensajes así obtenida que es finalmente enviada a través de dicho sistema de comunicación.

Preferiblemente según la invención, dicha información secreta es una clave criptográfica.

- 40 Preferiblemente según la invención, cada uno de dichos uno o más dispositivos utilizan un GPS y un módulo de localización geográfica, que es adecuado para detectar cualquier desviación del barco cooperante correspondiente a ser protegido de los límites de un área de seguridad predeterminada y/o el plan de navegación en caso de captura del barco cooperante por piratas y también es adecuado para transmitir tal desviación a un sistema de control con base en tierra.

- 45 Es un objeto adicional de la presente invención un dispositivo para extracción de datos de vigilancia marítima desde sensores de vigilancia marítima montados en un barco según la reivindicación 18.

La invención se describirá ahora, a modo de ilustración pero no a modo de limitación, haciendo referencia a las figuras de los dibujos anexos, en los cuales:

- la figura 1 muestra la arquitectura general del sistema según la invención;

- 50 - la figura 2 muestra el flujo de elaboración de información en el sistema según la invención (parte en tierra);

- la figura 3 muestra una cadena de elaboración de procesamiento de vídeo, en el dominio de píxeles, es decir dominio óptico (segmentación del fondo/primer plano, seguimiento de objeto y clasificación/extracción de rasgos al dominio semántico (fusión de datos y descripción de escena) según la invención;

- la figura 4 muestra la técnica de extracción de rasgos para la clasificación de barcos;

5 - la figura 5 muestra la conexión de un dispositivo de “caja de seguridad” según la invención;

- la figura 6 muestra los módulos de la caja de seguridad según la invención.

La ejecución de la función por el sistema 100 según la presente invención (función antipiratería naval) se basa en el análisis y seguimiento de objetivos en base a varias fuentes de información acerca de objetivos dispersos 30, 31, 50, para proporcionar al usuario final la posibilidad de obtener un canal de navegación segura en la zona exclusiva económica EEZ, gestionada por los centros de VTS o centros costeros equivalentes.

10

Haciendo referencia a la figura 2, el sistema utiliza, según una realización preferida, tres fuentes de datos diferentes:

- cámaras 11 (típicamente cámaras de alta sensibilidad adaptadas a bajo nivel de luz e infrarrojos) al nivel de tierra y/o a bordo;

- radar en tierra 12 y radar a bordo 12’;

15

- Sistema de Identificación Automática AIS 13.

Tradicionalmente, solamente el radar en tierra y más recientemente el AIS se han utilizado para obtener la posición del objetivo y su identificación. Tales sistemas tradicionales tienen la desventaja de usar solamente datos cinemáticos y por lo tanto no permiten una identificación precisa de las embarcaciones de diversa naturaleza (comercial o potencialmente pirata) en la zona observada. El AIS es obligatorio solamente en grandes barcos mayores de 15t, por lo tanto se pueden detectar los objetivos pequeños potencialmente más peligrosos solamente por el radar que no permite una identificación precisa dado a que maneja solamente información cinemática.

20

El sistema según la invención utiliza en su lugar también los datos que llegan desde el radar del barco y opcionalmente desde las cámaras a nivel de tierra y/o a bordo, para permitir la mejora de la fusión de datos que llegan desde todos los sensores y por lo tanto mejorar la posibilidad de una identificación y posicionamiento correctos tanto del barco observado como de las embarcaciones que lo rodean con el fin de efectuar una alerta temprana acerca de la presencia de amenazas piratas potenciales.

25

También se debería observar que dentro de un área ya vigilada por un sistema de VTS clásico, la presente invención proporciona la funcionalidad antipiratería sin la necesidad de añadir sensores adicionales en el área de vigilancia (debido al hecho de que cada embarcación de interés ya posee al menos un radar a bordo). Hace uso de información complementaria que llega desde diferentes sensores (radar, AIS, cámaras).

30

Aquí se tiene que hacer hincapié que el uso del único radar a bordo para fines antipiratería es todo ya solo una innovación destacable con respecto a la técnica anterior, debido a que esto extiende el campo de investigación del radar sin la necesidad de montar sensores adicionales en cualquier parte del sistema. Como veremos a continuación, esta funcionalidad se asegura por la “caja de seguridad” (o dispositivo 90 para extracción de datos de vigilancia marítima) según la invención, que opcionalmente también puede explotar los datos de la cámara a bordo.

35

En un escenario real, son ciertas las siguientes afirmaciones:

- el AIS 70 es obligatorio normalmente para barcos mayores de 15t según la regulación de la IMO y por lo tanto no proporciona ninguna información para los barcos más pequeños;

- el AIS 70 se podría manipular ilícitamente para proporcionar información engañosa;

40

- el radar 12 o el de a bordo 12’ proporcionan información cinemática, normalmente sin información que concierne a la identidad de los objetivos de los mismos objetivos (por ejemplo, es difícil discriminar, con la ayuda del único radar, entre una embarcación pequeña inmóvil y una boya);

45

- la cámara en tierra 11 o las de a bordo proporcionan la información de vídeo acerca del objetivo desde donde se pueden extraer los datos de identificación para cualquier objetivo específico (en el ejemplo anterior, la posibilidad de añadir la información óptica, por medio del uso de las cámaras, a los datos del radar permite discriminar inmediatamente entre un barco inmóvil incluso si es de tamaño pequeño y una boya).

Los datos de entrada se elaboran en un módulo llamado módulo de Fusión de datos Multisensor mejorada (e-MSF) 21 con el fin de proporcionar una evaluación de la amenaza que corresponde al escenario operativo 22, que se usa por el operador de la sede en tierra 20.

50

Nivel con base en tierra

El nivel con base en tierra (primer nivel) 20 está instalado en los nodos de cálculo del sistema de VTS o sistema equivalente de vigilancia costera y se dedica a la realización de las funcionalidades antipiratería mencionadas a continuación, que tienen como entrada el radar 12, 12', el AIS 13 ("Sistema de Identificación Automática") y los datos electroópticos 11, 11' como se muestra en la figura 2. Este nivel comprende por lo tanto los datos recibidos desde los sensores del barco cooperante.

El procesamiento de las imágenes ópticas 11, 11' define los pasos de elaboración de señales de vídeo desde niveles de significado semántico bajo (flujo de datos en bruto que llegan de la(s) cámara(s)) a los niveles semánticamente más descriptivos. Este proceso electroóptico se compone de (véase, la figura 3):

- 10 - un módulo de segmentación 23 cuyo propósito es el aislamiento de los objetivos de interés del segundo plano;
- un módulo de seguimiento óptico 24 cuyo propósito es atribuir a cada uno de los objetos aislados en el paso previo un identificador unívoco que se necesita para identificar el mismo objeto en imágenes posteriores del flujo de vídeo;
- 15 - un módulo de extracción de rasgos 25 cuyo propósito es el cálculo de los rasgos principales de los objetivos aislados;
- un módulo de clasificación de objetivos 26 que trabaja en las siluetas de los objetivos. Los rasgos obtenidos desde el módulo de extracción de rasgos (matrícula, color, forma) son la entrada para este módulo, que comparará la silueta del objetivo con las siluetas de los barcos en una base de datos (DB) de referencia 27 (véase la figura 4).

20 Después del paso de elaboración de imágenes, el sistema según la invención efectúa la fusión de la información óptica con la información del AIS y radar, en el módulo de e-MSF 21. Con este fin, se ha desarrollado un algoritmo para usar datos ópticos en el proceso de fusión. La dificultad de tal proceso es la de asociar correctamente los datos de imágenes con las trazas de AIS o radar correspondientes, dado que los datos de imágenes no contienen la información de distancia. Para superar esta dificultad, se ha implementado un algoritmo, que usa puntos de referencia georreferenciados que se definen por el operador y, por medio de transformaciones geométricas, tiene éxito al asociar información de posición con un objetivo óptico.

La fusión de datos tiene una funcionalidad doble: por una parte, se asocia información al objetivo, que es funcional a los procesos de evaluación de amenazas posteriores 22 (ver más adelante), por otra parte la interacción con las imágenes ópticas permite validar la información de radar. El esquema de validación proporciona que, comenzando desde la traza de radar única, una vez que las cámaras están colocadas para enmarcar el punto donde la misma traza de radar se encuentra a sí misma, se ejecuten los algoritmos tradicionales para la detección del objeto, de tal forma que se verifica con eficacia que la traza del radar es correspondiente a una embarcación.

Como ya se dijo, después del proceso de fusión de datos, cada traza se asocia a información de posición (AIS o radar) y por lo tanto cada objeto también se correlaciona con datos de extensión (longitud, altitud).

- 35 Comenzando a partir de toda la información disponible:
- datos que se derivan a partir de vídeo (matrícula, color, forma);
 - datos cinemáticos de radar o AIS (posición, rumbo y velocidad);
 - datos pertinentes para la unión de información de posición de vídeo y radar/AIS (longitud, altitud);
 - datos que llegan de archivos disponibles (por ejemplo bases de datos de embarcaciones de Lloyd u otras),

40 el módulo de evaluación de amenazas puede operar en dos modos.

En el primer modo, el sistema se entrena para reconocer comportamientos anómalos sin la intervención del operador. En tal modo, el operador debería definir solamente rasgos importantes a seguir (por ejemplo la posición, velocidad y rumbo) y el sistema:

- 45 1) aprenderá (fuera de línea) el comportamiento "normal" del sistema (a fin de hacer al sistema entender lo que es un comportamiento normal, el sistema se entrena sobre datos reales sin situaciones anómalas);
- 2) detectar situaciones anómalas comparando los datos actuales con los datos utilizados durante las sesiones de entrenamiento.

En el segundo modo, el operador define (pero usando un lenguaje con reglas predefinidas) la situación anómala que se desea evitar.

La tecnología utilizada para implementar tal sistema se basa en la Lógica de Descripción (DL). El sistema Basado en Conocimiento (KB) contendrá un conjunto de afirmaciones predefinidas (normalmente llamadas afirmaciones de caja T) construido (solamente una vez) por un experto en la técnica. Los datos que llegan desde los sensores, una vez elaborados adecuadamente, proporcionarán información en el estado real del sistema (afirmación de caja A).
5 Comenzando a partir de estas estructuras, el sistema proporcionará una descripción semántica de la situación actual.

Sobre la base de la evaluación de la amenaza 22, la función antipiratería se activa y gestiona directamente por el componente de soporte de decisión del sistema de VTS o centro de control costero equivalente, para:

- indicar las herramientas más adaptadas para enfrentarse a la amenaza;

10 - indicar el camino mínimo para alcanzar el objetivo razonable;

- evaluar el posible camino de escape y comenzar la misión de caza.

Conexión de comunicación segura (segundo nivel)

15 El nivel de conexión segura 60 define un camino de aproximación segura a través de un canal de tránsito seguro (de cualquier extensión y forma, posiblemente incluso un área) dentro de un área certificada de AIS. Esta área certificada tiene una extensión igual al alcance de radar de AIS normal (el hecho de "certificar los datos de AIS no disminuyen la eficiencia intrínseca del sistema de AIS). El AIS 13, 70 es un transpondedor de cooperación que proporciona un canal de comunicación barco-tierra sobre una conexión de VHF que es intrínsecamente insegura (todos los detalles de la estructura de los mensajes están en la regulación ITU-R, M.1371-1).

20 Dicha conexión insegura de AIS permite el olfateado, la simulación y suplantación de identidad, por ejemplo los paratas podrían simular un ataque a un barco no existente para distraer la atención haciendo a los medios de emergencia y las unidades aliadas converger en una zona geográfica que está distante del punto donde se realiza realmente el ataque. El "factor tiempo" puede ser altamente determinante para el resultado de un ataque (normalmente los piratas no tienen medios adecuados para enfrentarse a una reacción de los medios de refuerzo, juegan en su lugar con el factor sorpresa para atacar un barco mercante, petrolero o similar). El concepto innovador de "traza certificada" se introduce con el fin de validar cualquier información pertinente a una traza.

25 En el marco del estándar de AIS mencionado anteriormente (24 mensajes), la presente invención usa algunos de los mensajes para asegurar la integridad de la comunicación. Con este fin, la invención utiliza indiferentemente uno o el otro de los mensajes N° 8 y 6, que están disponibles como mensajes de texto libremente utilizables por cualquiera. Una información secreta (por ejemplo una clave) se adjunta a la cadena de los 24 mensajes y se calcula una función de generación de claves de la cadena entera. Después, esta función de generación de claves se inserta en el
30 mensaje elegido (o bien el N° 8 o bien el N° 6) y la cadena de 24 mensajes se envía al usuario deseado (sedes en tierra).

La información secreta se comparte con el usuario deseado, de manera que puede reconocer el barco que está comunicando.

35 El mensaje 6 se usa en la técnica anterior para dirigirse uno mismo al destinatario, el mensaje 8 se utiliza para difundir la información (todos los aparatos de AIS). Se puede utilizar un mensaje adicional 7 por las sedes para acuse de recibo de la recepción.

40 De esta forma, el AIS según la invención no funcionará solamente para identificar el barco cooperante en el sistema antipiratería, más bien también para autenticar la identidad proporcionada por el AIS de la técnica anterior. El VTS solo no puede proporcionar esta autenticación, debido al hecho de que el AIS podría haber sido robado o clonado o manipulado e instalado en un barco que desea simular ser cooperante. Esto es debido a que la información de identificación no se mantiene en el AIS.

45 Aquí se tiene que especificar que la elección de los mensajes 6 y 8 es solamente una realización preferida de la autenticación (preferida dado que permite no modificar el estándar actual de los mensajes de AIS y por lo tanto la infraestructura de AIS instalada hoy en día, que permanece absolutamente compatible con todas las instalaciones existentes, utilizando con precisión esos mensajes que en el estándar de AIS se reservan como "texto libre"). Se puede hacer de muchas maneras diferentes, alcanzando la misma meta (por ejemplo en caso de evolución del estándar).

50 Además de los detalles técnicos utilizados para asegurar la conexión de AIS, es posible comparar la información disponible en los puertos de partida o en los registros internacionales tal como el plan de navegación (trayectoria espacial y programación de tiempo) y el protocolo de inicio con la información intercambiada a través de la conexión de AIS y los datos que llegan desde el procesamiento óptico (trayectoria de navegación actual) para validar la correspondencia de la información dinámica con la información estática (por ejemplo el plan de navegación) en tiempo real.

Nivel naval (tercer nivel)

A fin de enfrentarse a los eventos más críticos, el sistema según la invención propone utilizar un dispositivo dedicado en lo sucesivo llamado “caja de seguridad” (SB) 90, que tiene que ser conectada al radar (y/u otros sensores) ya instalados en el barco (típicamente utilizando un conjunto limitado de interfaces estándar) por ejemplo con el fin de:

- 5 - localizar el barco en cualquier momento;
- detectar cualquier desviación de los límites del área segura y/o el plan de navegación (en caso de captura del barco por los piratas) y posiblemente transmitirla a los centros de VTS;
- transmitir a los centros de VTS los datos de vigilancia acerca de las embarcaciones alrededor del barco, adquiridos para mejorar el marco táctico que extiende la cobertura del radar (véanse las figuras 5 y 6).

10 A fin de realizar la segunda operación de la lista, la caja de seguridad puede comprender un GPS o explotar el ya montado a bordo y comprender un módulo de localización geográfica que comprende todos los mapas adecuados para el fin.

15 También se utiliza para extender la cobertura del radar desde tierra con las trazas a bordo de “ARPA” (Ayuda de Trazado de Radar Automatizado) que llegan desde el barco hacia tierra (haciendo uso de la caja de seguridad como se describe a continuación). La caja de seguridad (SB) es un dispositivo informatizado (PC de Windows® o Linux comercial) que está equipado con módulos software dedicados.

En particular, hay dos módulos software de interés:

- el rastreador 91 y
- 20 - la pasarela 92 para la interfaz del subsistema de VHF, llamada VHF-GW (que también podría ser una pasarela para una conexión por satélite para la transmisión de datos).

25 La caja de seguridad 90 recibe datos desde dos interfaces de entrada, una para el rastreador 91 y otra 92 directamente desde la LAN (Red de Área Local) del barco, también llamada canal principal de datos del barco (por ejemplo un canal principal de datos serie a 4.800 baudios) y envía su salida a la consola de VHF (es decir la consola o interfaz para el sistema por satélite), que es la consola del subsistema de VHF, de nuevo a través de la LAN del barco.

30 La comunicación en la LAN del barco se basa en tecnologías Ethernet con protocolos estándar tales como los mensajes NMEA (NMEA 0183 y 2000 gestionados por la asociación nacional de electrónica naval, www.nemea.org). Por otra parte, si el barco no tiene un canal principal de datos moderno (LAN) sino solamente un radar a bordo conectado directamente a la consola de ARPA, se utiliza una segunda interfaz de entrada de la caja de seguridad para conectar tal consola de ARPA directamente al rastreador dentro de la caja de seguridad, que produce trazas de radar por medio de un rastreador 91 dentro de la caja de seguridad. Tales trazas se producen en un formato predefinido y se envían a la VHF-GW 92, que puede transformarlas en un mensaje estándar tal como el NMEA y entonces la pasa a la consola de VHF del subsistema de VHF o las envía directamente a través de una interfaz dedicada siempre que el subsistema de VHF esté predispuesto y sea compatible. En este segundo escenario, la conexión entre la consola del barco (o del barco mercante) y la caja de seguridad se realiza usando una conexión serie tal como la conexión estándar RS-232 que podría ser adecuada considerando la corta distancia a cubrir. Uno observa aquí que la caja de seguridad está instalada a bordo del barco y normalmente podría estar colocada cerca de la consola del barco.

40 Resumiendo, el propósito de la caja de seguridad 90 es producir trazas de radar y/u ópticas (o de diferente tipo si los sensores a bordo son diferentes) preferiblemente en un formato estándar (por ejemplo NMEA). Con este fin, si el barco es –supongamos – un barco moderno y ya tiene trazas de radar en el formato comercial (por ejemplo NMEA) y una red local (tecnología Ethernet), la caja de seguridad se conecta simplemente a la LAN del barco y las trazas se reenvían al subsistema de VHF usando un olfateador. Por el contrario, en todos los otros casos donde no hay un rastreador en el barco o no hay ninguna unidad de procesamiento de radar estándar en el barco, la caja de seguridad se conecta usando un cable serie (RS-232 o equivalente) directamente a la consola naval (ARPA) manteniendo los datos de radar en bruto y realizando la misma función de seguimiento. En ambos casos, la salida de la caja de seguridad está constituida por trazas de radar estándar (por ejemplo en el formato NMEA) o en un formato propietario, que se envían al sistema en tierra de la presente invención utilizando el subsistema de VHF.

50 La idea comercial se basa en la observación de que la protección contra la piratería es una oportunidad económica que es atractiva para los clientes y podría ser de interés para la administración nacional de VTS y los propietarios de los barcos. Además, las compañías de seguros podrían reducir las tarifas para la navegación de carga y barcos dentro de las áreas afectadas por la piratería tan pronto como acepten abonarse a dicho servicio de seguridad.

En lo precedente, se han descrito realizaciones preferidas y variaciones de la presente invención, pero se tiene que considerar que los expertos en la técnica serán capaces de hacer modificaciones y otras variaciones sin apartarse del alcance de la invención, que se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema antipiratería marítimo (100), para el reconocimiento de embarcaciones sospechosas (50) alrededor de uno o más barcos cooperantes (30) a ser protegidos, que comprende:
- un sistema de control con base en tierra (10, 20, 40), que comprende:
 - 5 - uno o más centros (10), distribuidos geográficamente, que comprende sensores en tierra (11, 12) para detectar datos de vigilancia de embarcaciones;
 - una estación central (20) para recoger y elaborar datos de vigilancia de embarcaciones;
- el sistema de control con base en tierra (10, 20, 40) que comprende una red de comunicación bidireccional (40) entre dichos uno o más centros (10) y dicha estación central (20), de tal forma que la estación central (20) sea capaz de enviar comandos a dichos sensores con base en tierra;
- 10 - un sistema de comunicación entre dichos uno o más centros (10) y dichos uno o más barcos cooperantes a ser protegidos (30),
- el sistema antipiratería que se caracteriza por que comprende:
- 15 - uno o más dispositivos (90), montados a bordo de dichos uno o más barcos cooperantes correspondientes a ser protegidos (30), para extracción de datos de vigilancia marítima desde sensores de vigilancia marítima (12', 11'), que se montan a bordo de dichos uno o más barcos cooperantes correspondientes a ser protegidos (30) y son adecuados para vigilar el espacio alrededor de dichos uno o más barcos cooperantes, dichos uno o más dispositivos (90) para extracción de datos que son adecuados para enviar dichos datos de vigilancia marítima a al menos uno de dichos uno o más centros (10) a través de dicho sistema de comunicación;
 - 20 - un sistema de identificación y autenticación (13, 70) de dichos uno o más barcos cooperantes a ser protegidos (30), que funciona a través de dicho sistema de comunicación y se comparte entre dichos uno o más centros (10) y cada uno de dichos uno o más barcos cooperantes a ser protegidos (30),
- en donde dicha estación central (20) para recoger y elaborar datos elabora los datos que llegan desde dichos uno o más centros (10) y por lo tanto también desde dichos uno o más barcos cooperantes a ser protegidos (30) y lanza las alarmas pertinentes en el caso de reconocimiento de embarcaciones sospechosas (50).
- 25 2. Un sistema según la reivindicación 1, caracterizado por que dichos sensores de vigilancia marítima comprenden el radar montado a bordo de dichos uno o más barcos cooperantes a ser protegidos (30).
3. Un sistema según la reivindicación 1 o 2, caracterizado por que dicho sistema de identificación y autenticación (13, 70) comprende uno o más dispositivos de transmisión de AIS (70) montados en dichos uno o más barcos cooperantes correspondientes (30) y al menos un dispositivo de recepción de AIS en tierra (13), dichos uno o más dispositivos de transmisión de AIS (70) que son adecuados para transmitir información de autenticación de la identidad de dichos uno o más barcos cooperantes correspondientes (30) a dicho al menos un dispositivo de recepción de AIS en tierra (13).
- 30 4. Un sistema según la reivindicación 3, caracterizado por que se asocia una unidad de cifrado a cada uno de dichos uno o más dispositivos de transmisión de AIS (70) y dicho al menos un dispositivo de recepción de AIS en tierra (13), que genera una clave para la autenticación de los mensajes de AIS, sin cambiar la estructura de los mensajes de intercambios, es decir dentro de los estándares de sistemas de AIS.
- 35 5. Un sistema según la reivindicación 3, caracterizado por que dicho sistema de identificación y autenticación comprende o está constituido por una comunicación de VHF con firma cifrada.
- 40 6. Un sistema según cualquier reivindicación 2 a 5, caracterizado por que dichos sensores con base en tierra (11, 12) comprenden al menos una cámara en tierra (11) y dichos sensores de vigilancia marítima comprenden al menos una cámara (11'), dicha estación central (20) que elabora los datos de vídeo que llegan desde dichos sensores con base en tierra y dichos sensores de vigilancia marítima para obtener trazas de vídeo de embarcaciones, incluyendo dichas embarcaciones sospechosas y dichos uno o más barcos cooperantes, que se elaboran junto con al menos una traza que llega desde dicho al menos un dispositivo de recepción de AIS en tierra (13) y dicho radar (12, 12')
- 45 pertinente para las mismas embarcaciones, con el fin de mejorar el reconocimiento de las mismas embarcaciones.
7. Un sistema según la reivindicación 6, caracterizado que dicha estación central (20) elabora datos de vídeo a partir de una cámara (11, 11') para obtener adicionalmente las siluetas de embarcaciones y las compara con una serie de siluetas predefinidas pertinentes a barcos conocidos.
- 50 8. Un sistema según cualquier reivindicación 2 a 7, caracterizado por que cada uno de dichos uno o más dispositivos para extracción de datos comprende:

- un módulo (91, 93) para conectar a dichos sensores de vigilancia marítima (12', 11'), por medio del canal principal de datos o por conexión directa;

5 - un módulo de pasarela (92) para conectar a un módulo de transmisión de datos montado a bordo de dichos uno o más barcos cooperantes (30) para el envío de los datos extraídos a tierra a través de dicho sistema de comunicación.

9. Un sistema según la reivindicación 8, caracterizado por que cada uno de dichos uno o más dispositivos para extracción de datos comprende un módulo de elaboración de datos extraídos, que es adecuado para preparar datos elaborados a ser transmitidos a través de dicho módulo de pasarela (92).

10. Un sistema según la reivindicación 9, caracterizado por que dicho módulo de elaboración de datos extraídos funciona como un rastreador a bordo, en particular en el caso de datos extraídos de sensores de radar a bordo.

11. Un sistema según cualquier reivindicación 8 a 10, caracterizado por que dicho módulo de pasarela (92) es adecuado para operar hacia un módulo de transmisión de datos radio de VHF montado a bordo de dichos uno o más barcos cooperantes (30).

15 12. Un sistema según cualquier reivindicación 8 a 10, caracterizado por que dicho módulo de pasarela (92) es adecuado para operar hacia un módulo de transmisión radio de U/VHF y por satélite, montado a bordo de cada uno de dichos uno o más barcos cooperantes (30) para el envío de datos a tierra (20).

20 13. Un sistema según cualquier reivindicación 8 a 12, caracterizado por que dicho módulo de pasarela (92) comprende un submódulo para la gestión de comandos y parámetros pertinentes a la comunicación radio, tales como por ejemplo el traspaso en la selección de las frecuencias y canales radio a ser utilizados en dicho sistema de comunicación.

14. Un sistema según la reivindicación 8 a 13, caracterizado por que cada uno de dichos uno o más dispositivos (90) comprende dos módulos (91, 93) de conexión a dichos sensores de vigilancia marítima (12', 11'):

- un módulo de conexión directa (91), que extrae los datos y los representa en un formato predefinido;

25 - un módulo de conexión indirecta de canal principal (93) (ETH), que es un olfateador para extracción de datos y representación de datos en un protocolo estándar.

30 15. Un sistema según cualquier reivindicación 1 a 14, caracterizado por que dicho sistema de identificación y autenticación (13, 70) utiliza indiferentemente o bien el mensaje N° 8 o bien el 6 del estándar de AIS, que proporciona medios de elaboración electrónica que añaden una información secreta a la cadena de los 24 mensajes de AIS y calculan una función de generación de claves de la cadena entera así obtenida, dicha función de generación de claves que se inserta o bien en dicho mensaje 8 o bien 6, la cadena de 24 mensajes así obtenida que es finalmente enviada a través de dicho sistema de comunicación.

16. Un sistema según la reivindicación 15, caracterizado por que dicha información secreta es una clave criptográfica.

35 17. Un sistema según cualquier reivindicación 1 a 16, caracterizado por que cada uno de dichos uno o más dispositivos (90) utiliza un GPS y un módulo de localización geográfica, que es adecuado para detectar cualquier desviación del barco cooperante correspondiente a ser protegido (30) desde los límites de un área segura predeterminada y/o el plan de navegación en caso de captura del barco cooperante (30) por piratas y también es adecuado para transmitir tal desviación a un sistema de control con base en tierra (10, 20, 40).

40 18. Un dispositivo (90) para extracción de datos de vigilancia marítima desde sensores de vigilancia marítima (12', 11') que incluyen sensores de radar, dispuesto dentro de un barco (30, 31) a ser protegido contra embarcaciones sospechosas (50) y configurado para vigilar el espacio alrededor del barco, dicho barco (30, 31) que incluye un módulo de transmisión de datos para enviar datos a un centro en tierra a través de un sistema de comunicación asociado, el dispositivo que se caracteriza por que comprende:

45 - un módulo de conexión (91, 93) para conectar dichos sensores de vigilancia marítima (12', 11'), que comprende:

- un módulo de conexión directa (91), que extrae los datos de dichos sensores de vigilancia marítima (12', 11') y calcula las trazas; y

- un módulo de conexión indirecta de canal principal (93) (ETH), que es un olfateador para extracción de datos que representan trazas;

50 que producen trazas elaboradas representando trazas en formatos predefinidos;

- un módulo de pasarela (92) conectado tanto a dicho módulo de conexión directa como indirecta de canal principal (91, 93) para conectar a dichos sensores de vigilancia marítima (12', 11') y configurado para ser conectado a dicho módulo de transmisión de datos;

5 de tal forma que, en uso, dichas trazas elaboradas se transmiten a tierra a través de dicho módulo de pasarela (92).

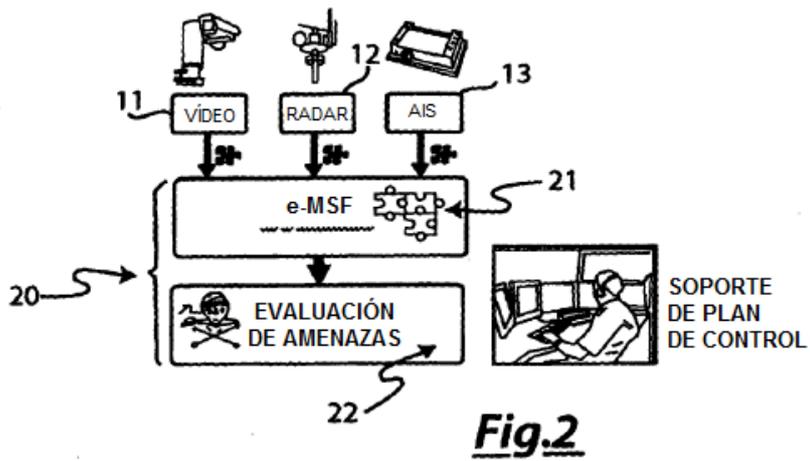
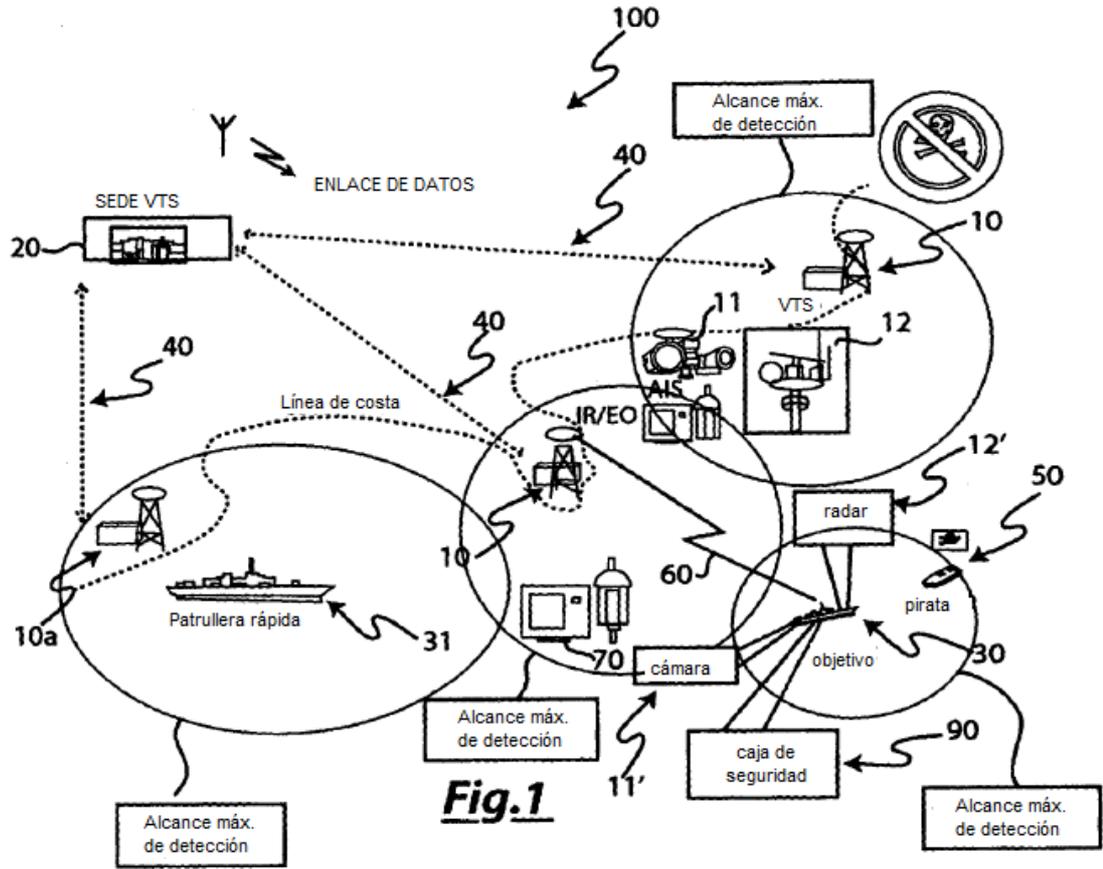
19. Un dispositivo según la reivindicación 18, caracterizado por que dicho módulo de conexión directa (91) calcula trazas para datos de sensores de radar y/o sensores de vídeo.

10 20. Un dispositivo según cualquier reivindicación 18 a 19, caracterizado por que además comprende un módulo de localización geográfica, que usa información GPS desde el barco o desde un GPS integrado y comprende todos los mapas para detectar cualquier desviación de los límites de un área segura y/o un plan de navegación, los datos de desviación que se transmiten a tierra a través de dicho módulo de pasarela.

15 21. Un dispositivo según cualquier reivindicación 18 a 20, caracterizado por que dicho módulo de pasarela (92) es adecuado para operar hacia un módulo de transmisión por satélite y/o radio U/VHF, montado a bordo de dichos barcos (30) para el envío de datos a tierra, en particular hacia un módulo de transmisión de datos radio de VHF dentro de un dispositivo de AIS (70) montado a bordo de dicho barco (30).

22. Un dispositivo según cualquier reivindicación 18 a 21, caracterizado por que dicho módulo de pasarela (92) comprende un submódulo para la gestión de comandos y parámetros pertinentes a la comunicación radio, tales como por ejemplo el traspaso en la selección de las frecuencias y canales radio a ser utilizados en la comunicación a tierra.

20 23. Un dispositivo según cualquier reivindicación 18 a 22, caracterizado por que el dispositivo se usa en el sistema según cualquier reivindicación 1-17.



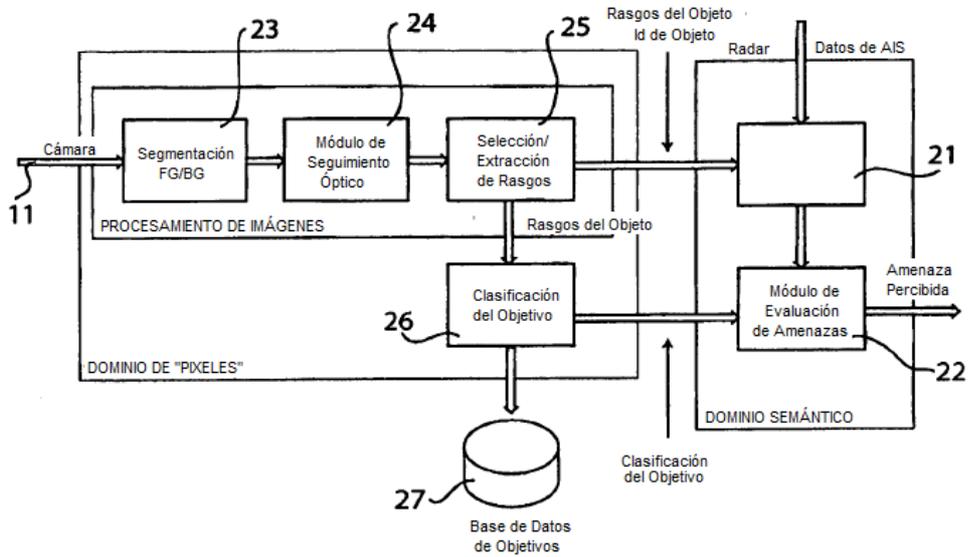


Fig.3

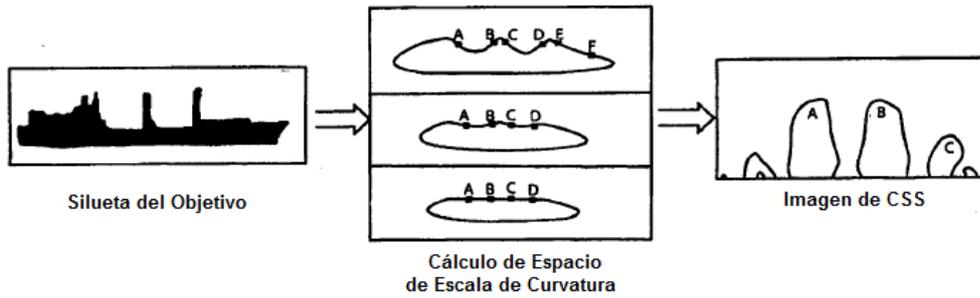


Fig.4

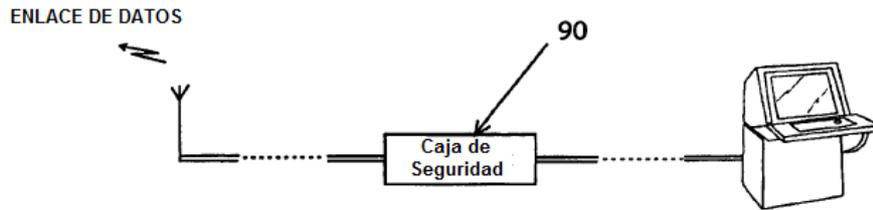


Fig.5

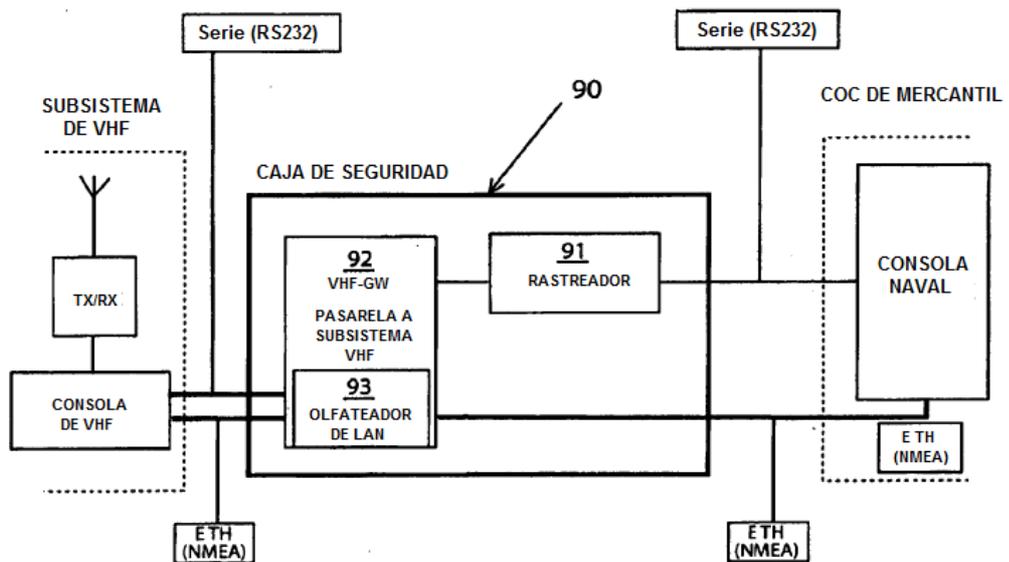


Fig.6