

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 754 376**

51 Int. Cl.:

G01S 19/09 (2010.01)

G01S 19/14 (2010.01)

G01S 19/21 (2010.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **21.03.2014 PCT/NL2014/050179**

87 Fecha y número de publicación internacional: **04.12.2014 WO14193221**

96 Fecha de presentación y número de la solicitud europea: **21.03.2014 E 14716036 (0)**

97 Fecha y número de publicación de la concesión europea: **14.08.2019 EP 3004913**

54 Título: **Procedimiento y sistema para recuperar datos de localización de un objeto a lo largo del tiempo utilizando un receptor GNSS para anti falsificación, y receptor y lector de señales en el espacio para dicho procedimiento y sistema**

30 Prioridad:
29.05.2013 NL 2010886

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
17.04.2020

73 Titular/es:
**FOLKERS, WILLEM (100.0%)
4, Mezenhof
1933 Sterrebeek, BE**

72 Inventor/es:
FOLKERS, WILLEM

74 Agente/Representante:
CONTRERAS PÉREZ, Yahel

ES 2 754 376 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

5 Procedimiento y sistema para recuperar datos de localización de un objeto a lo largo del tiempo utilizando un receptor GNSS para anti falsificación, y receptor y lector de señales en el espacio para dicho procedimiento y sistema

10 La invención se refiere a un procedimiento para reducir un riesgo de manipulación (tampering) y/o falsificación (spoofing) de datos de localización de un objeto a lo largo del tiempo. La invención se refiere además a usar un receptor y lector de señales en el espacio (signals-in-space) en dicho procedimiento.

15 Cuando se transportan objetos, en particular cuando el objeto es una embarcación o un contenedor, a menudo se desea conocer la trayectoria del objeto, es decir, dónde se ubicó el objeto en un período de tiempo determinado. La trayectoria es, por lo tanto, la ubicación de dicho objeto a lo largo del tiempo, por ejemplo, múltiples ubicaciones a lo largo del tiempo. Por ejemplo, una entidad gubernamental quiere asegurarse de que una embarcación, tal como un barco, no entre en una región determinada. Por ejemplo, a un barco de pesca sólo se le permite pescar en una región determinada.

20 Se sabe que estos barcos pesqueros disponen de receptores GPS que almacenan datos de localización a lo largo del tiempo en el receptor GPS. Cuando una embarcación de este tipo entra en un puerto, se comprueban los datos de localización almacenados en el receptor GPS y se comparan con la región prohibida predefinida. Los datos de localización, por ejemplo, están compuestos de varias posiciones para varios momentos en el tiempo. Las posiciones se pueden expresar, por ejemplo, en longitud y latitud.

25 Una desventaja de este procedimiento y sistema conocidos es que estos receptores GPS pueden ser fácilmente falsificados (tampered) y/o manipulados (spoofed). Es decir, los datos de localización almacenados en el receptor GPS pueden ser manipulados y/o falsificados y modificados, de tal forma que parece que el barco de pesca ha estado en una localización en un determinado período de tiempo que es diferente al de las ubicaciones reales en las que ha estado el barco de pesca.

Otro inconveniente es que estos receptores GPS necesitan procesar las señales recibidas y almacenar los datos de localización en una unidad de memoria que requiere energía.

35 WO 2012/007720 A1 divulga un mecanismo para verificar en un sitio remoto una determinación de geolocalización realizada en un receptor, aprovechando elementos de señales de localización recibidos por ese receptor no detectables o decodificables alternativamente por el receptor. Los elementos son al menos detectables por medios de verificación en la ubicación remota y desde los cuales se puede verificar una determinación de ubicación del receptor.

40 Es un objeto de la invención proporcionar un procedimiento que elimine al menos parcialmente los inconvenientes mencionados anteriormente o, en todo caso, proporcione una alternativa.

45 En particular, el objetivo de la invención es proporcionar un procedimiento para recuperar datos de localización de un objeto a lo largo del tiempo en el que se reduce el riesgo de falsificación (spoofing) no deseado.

Este objeto es conseguido por la invención por medio de un procedimiento según la reivindicación 1.

50 En un primer aspecto de la presente invención, se proporciona un procedimiento para reducir un riesgo de manipulación (tampering) y/o falsificación (spoofing) de datos de localización de un objeto a lo largo del tiempo. Los datos de localización son representativos de al menos una posición del objeto a lo largo del tiempo, pero también pueden ser representativos de una velocidad y un tiempo del objeto. En particular, los datos de localización son representativos de la denominada Posición, Velocidad, Tiempo (PVT).

55 El procedimiento comprende la etapa de proporcionar al objeto un receptor de señales en el espacio.

60 El receptor de señales en el espacio comprende una antena para recibir una señal de navegación encriptada y un convertidor A/D para discretizar la señal de navegación encriptada.

65 La antena recibe señales de navegación encriptadas procedentes de uno o más satélites del Sistema Mundial de Navegación por Satélite (GNSS: Global Navigation Satellite System) y/o de satélites de navegación basados en el espacio. Ejemplos de estos satélites que originan señales en el espacio son el Sistema de Posicionamiento Global (GPS: Global Positioning System), Galileo, el Sistema Globalnaya Navigatsionnaya Sputnikovaya (GLONASS) y/o el Sistema de Navegación por Satélite BeiDou (BDS).

La señal de navegación procedente del satélite de navegación basado en el espacio está encriptada. Es

decir, sin conocer una clave o un algoritmo de descifrado, la señal de navegación no se puede utilizar para recuperar datos de localización.

5 Por ejemplo, el sistema de posicionamiento Galileo proporciona dos servicios encriptados, que son el Servicio de Navegación Comercial (CNS: Commercial Navigation Service) y el Servicio Público de Navegación Regulada (PRS: Public Regulated Navigation Service). Ambos servicios se corresponden con una señal de navegación encriptada procedente de un satélite Galileo. Se tratan respectivamente de una señal de navegación CNS y una señal de navegación PRS. Pagando un precio, la señal de navegación CNS puede ser descifrada. El servicio PRS será utilizado principalmente por entidades gubernamentales. Por ejemplo, las claves de descifrado sólo están disponibles con el consentimiento de las entidades gubernamentales.

15 Por lo tanto, el receptor está adaptado para recibir señales de navegación encriptadas procedentes del espacio y discretizarlas en forma de datos de navegación encriptados. En particular, el receptor está adaptado para recibir, a través de la antena, todas las señales de navegación encriptadas que están a la vista de la antena. El convertidor A/D proporciona la discretización, es decir, la conversión de la señal de navegación encriptada analógica en forma de datos de navegación encriptados digitales.

20 La antena está diseñada para recibir una señal en el espacio particular, por ejemplo, una o más señales de navegación encriptadas al mismo tiempo. En otras palabras, la antena está diseñada para recibir todas las señales en el espacio particular, por ejemplo, todas las señales de navegación encriptadas particulares que están a la vista de la antena. Por ejemplo, en el caso del sistema de satélites Galileo, cuatro o más satélites Galileo están a la vista de la antena y cada uno de los satélites Galileo está transmitiendo una señal de navegación PRS. Todas esas señales de navegación PRS, que corresponden a y proceden de estos satélites Galileo a la vista, son recibidas por la antena al mismo tiempo y discretizadas, por ejemplo convertidas, por el convertidor A/D en datos de navegación encriptados.

30 Por lo tanto, el convertidor A/D está adaptado para discretizar la una o más señales de navegación encriptadas recibidas en forma de datos de navegación encriptados.

35 Preferiblemente, el convertidor A/D convierte la señal de navegación encriptada analógica con una frecuencia de muestreo predefinida en datos de navegación encriptados digitales. La frecuencia de muestreo depende de una duración esperada y/o deseada del tiempo durante el cual se deben registrar los datos de localización del objeto, es decir, del tiempo de registro esperado y/o deseado. En caso de que el tiempo de registro esperado y/o deseado sea relativamente grande, en contraste, la frecuencia de muestreo es relativamente pequeña. En caso de que el tiempo de registro esperado y/o deseado sea relativamente bajo, en contraste, la frecuencia de muestreo es relativamente alta.

40 Por ejemplo, cuando el objeto tiene un tiempo de registro de un mes, la frecuencia de muestreo puede ser, por ejemplo, una muestra o una serie de muestras por día.

Por ejemplo, cuando el objeto tiene un tiempo de registro de una semana, la frecuencia de muestreo puede ser, por ejemplo, una muestra o una serie de muestras cada hora.

45 En particular, la frecuencia de muestreo también depende del tamaño, es decir, del almacenamiento disponible, de la unidad de memoria.

50 El receptor incluye además una unidad de memoria para almacenar los datos de navegación encriptados. Los datos de navegación encriptados incluyen datos representativos de una o más, preferiblemente cuatro señales de navegación encriptadas.

55 La unidad de memoria es un registrador de datos que almacena y/o registra los datos de navegación encriptados a lo largo del tiempo. Cuando la unidad de memoria es relativamente grande, se puede seleccionar una frecuencia de muestreo alta. Cuando la unidad de memoria es relativamente pequeña, se puede seleccionar una frecuencia de muestreo baja. Además, cuando la unidad de memoria es relativamente grande, se puede implementar un tiempo de registro relativamente grande. Cuando la unidad de memoria es relativamente pequeña, se puede implementar un tiempo de registro relativamente bajo. Una unidad de memoria relativamente pequeña es una unidad de memoria con una capacidad de almacenamiento relativamente pequeña. Una unidad de memoria relativamente grande es una unidad de memoria con una capacidad de almacenamiento relativamente grande.

60 Preferiblemente, la unidad de memoria almacena y/o registra la señal de navegación encriptada durante una duración predefinida, en la que la duración predefinida es representativa de una duración durante la cual se desean conocer los datos de localización del objeto. Esto puede ser, por ejemplo, de una magnitud del orden de días, semanas, meses y/o años.

El receptor incluye una interfaz para conectar un lector a la unidad de memoria. El lector es conectable de forma extraíble con el receptor a través de la interfaz.

5 El procedimiento comprende además la etapa de recibir la señal de navegación encriptada a lo largo del tiempo por parte de la antena y discretizar la señal de navegación encriptada a lo largo del tiempo por parte del convertidor A/D en forma de datos de navegación encriptados.

10 El procedimiento comprende la etapa de almacenar la señal de navegación encriptada a lo largo del tiempo en la unidad de memoria.

El procedimiento comprende la etapa de conectar el lector con la unidad de memoria para transferir la señal de navegación encriptada a lo largo del tiempo desde la unidad de memoria al lector.

15 Por ejemplo, el lector puede ser conectado a la unidad de memoria por un usuario del lector que es representante de una entidad gubernamental. El representante, por ejemplo, desea verificar dónde ha estado el objeto y cuándo.

20 El procedimiento comprende la etapa de descryptar en el lector la señal de navegación encriptada a lo largo del tiempo y recuperar los datos de localización del objeto a lo largo del tiempo.

25 La ventaja de descryptar la señal de navegación encriptada a lo largo del tiempo en el lector es que no es obligatorio para el receptor descryptar la señal de navegación encriptada. La descryptación se realiza en el lector y no en el receptor. Por lo tanto, el receptor no requiere una unidad de procesamiento que, a través de una clave de descryptación, esté configurada para descryptar la señal en el espacio encriptado. Esto reduce en gran medida el riesgo de manipulación (tampering) y/o falsificación (spoofing) de los datos de localización, ya que el receptor no contiene ningún dato de localización.

30 En una forma de realización, la energía suministrada al receptor es suministrada por una fuente externa de suministro de energía (o de alimentación) y/o una fuente interna de suministro de energía (o de alimentación). El procedimiento comprende entonces la etapa de suministrar energía al receptor por medio de la fuente de suministro de energía (o fuente de alimentación).

35 Por ejemplo, la fuente de suministro de energía está localizada externamente con respecto al receptor, en el que la fuente de suministro de energía está localizada en o cerca del objeto.

En otro ejemplo, la fuente de suministro de energía se encuentra internamente con respecto al receptor.

40 En una forma de realización preferida del procedimiento según la invención, la antena es adecuada para recibir más de una, preferiblemente más de tres señales de navegación encriptadas al mismo tiempo, en el que el convertidor A/D es adecuado para discretizar las señales de navegación encriptadas recibidas al mismo tiempo en forma de datos de navegación encriptados.

45 La una o más señales de navegación encriptadas proceden de más de un satélite, es decir, de satélites diferentes y diversos. En particular, se tratan de satélites GNSS que están a la vista de la antena. Sin embargo, la una o más señales de navegación encriptadas son recibidas y discretizadas al mismo tiempo en forma de datos de navegación encriptados. Por lo tanto, los datos de navegación encriptados incluyen datos representativos de una o más señales de navegación encriptadas.

50 El procedimiento comprende además las etapas de recibir las señales de navegación encriptadas a lo largo del tiempo por parte de la antena y discretizar las señales de navegación encriptadas a lo largo del tiempo por parte del convertidor A/D.

55 Esto tiene la ventaja de que es más difícil manipular y/o falsificar la una o más señales de navegación encriptadas recibidas. A fin de manipular y/o falsificar la recuperación de datos de localización a partir de una o más señales de navegación encriptadas se requiere una clave de descryptación que no se proporciona en el receptor. La manipulación y/o falsificación de la una o más señales de navegación encriptadas es mucho más difícil. Cuantas más señales de navegación encriptadas se discretizan y almacenan como datos de navegación encriptados en la unidad de memoria, mayor puede ser la reducción del riesgo de manipulación y/o falsificación. Es más difícil manipular o falsificar múltiples señales de navegación encriptadas en comparación con una señal de navegación encriptada.

65 Por lo tanto, la etapa de recuperar datos de localización a partir de los datos de navegación encriptados se realiza de forma independiente del almacenamiento de los datos de navegación encriptados. No sólo las etapas se realizan de forma independiente en el tiempo, sino que preferiblemente, las etapas se realizan en unidades físicas independientes. Preferiblemente, la etapa de recibir, discretizar y almacenar

se realiza en el receptor y la etapa de descifrar y recuperar se realiza en el lector. El receptor y el lector pueden ser conectables entre sí de forma extraíble.

5 En una forma de realización, la interfaz del receptor está configurada para transferir datos de navegación encriptados al lector de forma inalámbrica y/o por medio de un cable.

10 Por ejemplo, los datos de navegación encriptados se transfieren de forma inalámbrica, a través de Internet, al lector. En este caso, el lector puede ser, por ejemplo, también un servidor. En otro ejemplo, los datos de navegación encriptados se transfieren por cable al lector. También en este caso, el lector puede ser, por ejemplo, un servidor. Alternativamente, el lector es una unidad dedicada a descifrar los datos de navegación encriptados y recuperar los datos de localización del objeto a lo largo del tiempo.

15 En una forma de realización del procedimiento según la invención, el procedimiento comprende además la etapa de proporcionar al lector una clave de descifrado para descifrar los datos de navegación encriptados a lo largo del tiempo.

20 Esto es ventajoso ya que la clave de descifrado se proporciona en el lector y no en el receptor, lo que reduce el riesgo de manipulación (tampering) y/o falsificación (spoofing) en el receptor. La clave de descifrado es proporcionada, por ejemplo, por una entidad gubernamental cuando se almacena una señal de servicio público regulado (PRS: Public Regulated Service) como datos de navegación encriptados.

25 En una forma de realización del procedimiento según la invención, el procedimiento comprende además la etapa de comparar los datos de localización del objeto a lo largo del tiempo con una región predefinida.

30 El lector recupera los datos de localización a lo largo del tiempo a partir de los datos de navegación encriptados almacenados en la unidad de memoria del receptor. Los datos de localización a lo largo del tiempo son comparados con una región predefinida. Esto es ventajoso ya que permite a un usuario del lector, por ejemplo un representante de una entidad gubernamental, recuperar si un objeto ha estado o no ha estado en la región predefinida.

En otra forma de realización del procedimiento según la invención, el procedimiento comprende además la etapa de comparar los datos de localización recuperados con los datos de navegación no encriptados.

35 Estos datos de navegación no encriptados se adquieren recibiendo señales de navegación no encriptadas por parte de la antena y discretizando estas señales de navegación no encriptadas por el convertidor A/D en forma de datos de navegación no encriptados.

40 En una forma de realización del procedimiento según la invención, la señal de navegación encriptada es una señal encriptada del Sistema Mundial de Navegación por Satélite (GNSS: Global Navigation Satellite System).

45 En una forma de realización del procedimiento según la invención, el objeto es una embarcación, preferiblemente un barco de pesca. Esto le permite saber a un usuario del lector cuándo y dónde ha estado un barco.

50 En una forma de realización del procedimiento según la invención, el objeto es un contenedor, preferiblemente en una embarcación. Esto le permite saber a un usuario del lector cuándo y dónde ha estado un contenedor.

55 En una forma de realización del procedimiento según la invención, el objeto es un cuerpo humano. Esto le permite saber a un usuario del lector cuándo y dónde ha estado un cuerpo humano. Por ejemplo, el usuario del lector es un representante de una entidad encargada de hacer cumplir la ley y/o de la administración de justicia. El cuerpo humano, por ejemplo, es un convicto que está bajo arresto domiciliario. En este ejemplo, este representante puede comprobar dónde ha estado el condenado y dónde cuando el representante conecta el lector con el receptor y el lector recupera los datos de localización del receptor.

60 En una forma de realización del procedimiento según la invención, el objeto es un contenedor en un camión de carretera.

65 En una forma de realización del procedimiento según la invención, el objeto es cualquier vehículo de alquiler, tal como por ejemplo un coche de alquiler, un barco de alquiler, una bicicleta de alquiler y/o un avión de alquiler.

Esto es ventajoso ya que un propietario del vehículo de alquiler puede comprobar fácilmente si el vehículo de alquiler ha estado dentro de una determinada área predefinida en un determinado momento.

5 En una forma de realización del procedimiento según la invención, el objeto es cualquier vehículo, tal como por ejemplo, pero no limitado a vehículos terrestres, vehículos marítimos, vehículos aéreos y/o vehículos espaciales. Otros ejemplos son aviones, helicópteros, cohetes, barcos, embarcaciones, coches, botes, camiones y/o bicicletas.

En una forma de realización del procedimiento según la invención, la señal de navegación encriptada es una señal del servicio público regulado (PRS: Public Regulated Service).

10 En una forma de realización del procedimiento según la invención, la señal de navegación encriptada es una señal del Servicio de Navegación Comercial (CNS: Commercial Navigation Service).

15 El procedimiento comprende la etapa de transferir los datos de navegación encriptados a lo largo del tiempo desde la unidad de memoria al lector.

El procedimiento también comprende la etapa de desencriptar en el lector los datos de navegación encriptados a lo largo del tiempo y recuperar los datos de localización del objeto a lo largo del tiempo.

20 Esto es ventajoso ya que proporciona al usuario del lector la posibilidad de recuperar del receptor datos de localización del objeto con un riesgo reducido de manipulación (tampering) y/o falsificación (spoofing). El lector no recibe datos de localización procedentes del receptor, sino que se transfieren al lector datos de navegación encriptados en bruto (o sin procesar) almacenados en la unidad de memoria. La desencriptación, es decir, la desencriptación de los datos de navegación encriptados, se realiza en el lector. Los datos de navegación desencriptados se utilizan posteriormente para recuperar los datos de localización del objeto.

30 En una forma de realización del procedimiento según la invención, el procedimiento comprende además etapas de proporcionar al objeto el receptor de señales en el espacio, recibir la señal de navegación encriptada a lo largo del tiempo por parte de la antena, discretizar la señal de navegación encriptada a lo largo del tiempo por parte del convertidor A/D en forma de datos de navegación encriptados, y almacenar los datos de navegación encriptados a lo largo del tiempo en la unidad de memoria.

35 Esto es ventajoso ya que el almacenamiento y la adquisición de los datos de navegación encriptados en el receptor se realiza de forma independiente de la desencriptación de los datos de navegación encriptados y de la recuperación de los datos de localización del objeto en el lector. Esto reduce el riesgo de manipulación y/o falsificación. En otras palabras, dificulta la manipulación y la falsificación de los datos de localización.

40 El receptor comprende una antena para recibir una señal de navegación encriptada, un convertidor A/D para discretizar la señal de navegación encriptada en forma de datos de navegación encriptados, una unidad de memoria para almacenar los datos de navegación encriptados a lo largo del tiempo y una interfaz para conectar un lector a la unidad de memoria.

45 El procedimiento comprende las etapas de recibir la señal de navegación encriptada a lo largo del tiempo por parte de la antena y discretizar la señal de navegación encriptada a lo largo del tiempo por parte del convertidor A/D en forma de datos de navegación encriptados.

50 El procedimiento comprende la etapa de almacenar los datos de navegación encriptados a lo largo del tiempo en la unidad de memoria, en el que los datos de navegación encriptados a lo largo del tiempo son representativos de los datos de localización del objeto a lo largo del tiempo.

55 Esto es ventajoso ya que el receptor registra las señales de navegación encriptadas recibidas a lo largo del tiempo como datos de navegación encriptados en la unidad de memoria, sin desencriptar la señal de navegación. Los datos de localización no se recuperan ni se registran en el receptor. En su lugar, se almacenan datos de navegación encriptados en bruto. Esto permite al receptor no desencriptar datos de navegación encriptados y recuperar datos de localización. Por lo tanto, no es posible manipular y/o falsificar datos de localización en el receptor, ya que no se requieren datos de localización en el receptor. La manipulación y/o la falsificación de los datos de navegación encriptados es mucho más difícil, de modo que se reduce el riesgo de manipulación y/o falsificación.

60 En una forma de realización del procedimiento, el procedimiento comprende las etapas de conectar el lector con la unidad de memoria para transferir los datos de navegación encriptados a lo largo del tiempo desde la unidad de memoria al lector y desencriptar en el lector los datos de navegación encriptados a lo largo del tiempo y recuperar los datos de localización del objeto a lo largo del tiempo.

65 Esto es ventajoso ya que la recuperación de los datos de localización no se realiza en el receptor sino que se realiza en el lector. El lector es conectable de forma extraíble con el receptor, por lo tanto, la

manipulación y/o la falsificación de los datos de localización es mucho más difícil cuando el lector y el receptor son independientes.

5 En un segundo aspecto, la presente invención proporciona un uso de un receptor de señales en el espacio en el procedimiento de la invención.

10 Este receptor de señales en el espacio comprende una antena para recibir una señal de navegación encriptada a lo largo del tiempo, un convertidor A/D para discretizar la señal de navegación encriptada a lo largo del tiempo en forma de datos de navegación encriptados a lo largo del tiempo, una unidad de memoria para almacenar los datos de navegación encriptados a lo largo del tiempo y una interfaz para conexión con un lector y transferir los datos de navegación encriptados a lo largo del tiempo al lector.

15 Esto es ventajoso ya que los datos de navegación encriptados no se descifran en el receptor de señales en el espacio. No se recuperan datos de localización en el receptor. En lugar de registrar los datos de localización en el receptor, se almacenan datos de navegación encriptados en bruto (o sin procesar) en la unidad de memoria. Por lo tanto, no es posible manipular o falsificar datos de localización, ya que no se almacenan ni registran datos de localización en el receptor.

20 En un tercer aspecto, la presente invención proporciona un uso de un lector en el procedimiento de la invención.

25 Este lector se refiere a recuperar datos de localización de un objeto a lo largo del tiempo y comprende una interfaz para conexión con un receptor de señales en el espacio y transferencia de datos de navegación encriptados a lo largo del tiempo almacenados en el receptor desde el receptor al lector y una unidad de descifrado configurada para descifrar los datos de navegación encriptados a lo largo del tiempo y recuperar los datos de localización del objeto a lo largo del tiempo.

30 Un sistema comprende un receptor de señales en el espacio, en particular un receptor de señales en el espacio según una de las formas de realización anteriores.

35 El receptor comprende una antena para recibir una señal de navegación encriptada a lo largo del tiempo y un convertidor A/D para discretizar la señal de navegación encriptada a lo largo del tiempo en forma de datos de navegación encriptados a lo largo del tiempo. El receptor comprende una unidad de memoria para almacenar los datos de navegación encriptados a lo largo del tiempo y una interfaz de lector para conexión con un lector y para transferir los datos de navegación encriptados a lo largo del tiempo al lector.

El sistema comprende además el lector, en particular un lector de acuerdo con una de las formas de realización anteriores, para recuperar los datos de localización del objeto a lo largo del tiempo.

40 El lector comprende una interfaz de receptor para conexión con el receptor de señales en el espacio y para transferencia de los datos de navegación encriptados a lo largo del tiempo almacenados en el receptor desde el receptor al lector. El lector incluye además una unidad de descifrado configurada para descifrar los datos de navegación encriptados a lo largo del tiempo y para recuperar los datos de localización del objeto a lo largo del tiempo.

45 Una ventaja de este sistema es que el lector y el receptor son conectables de forma extraíble, de modo que permite recuperar datos de localización a partir de datos de navegación encriptados de forma independiente del almacenamiento de los datos de navegación encriptados.

50 Esto tiene la ventaja de que es más difícil manipular y/o falsificar la una o más señales de navegación encriptadas recibidas. A fin de manipular y/o falsificar la recuperación de datos de localización a partir de la una o más señales de navegación encriptadas, se requiere una clave de descifrado que no se proporciona en el receptor. La manipulación y/o la falsificación de la una o más señales de navegación encriptadas es mucho más difícil. Cuantas más señales de navegación encriptadas se discretizan y almacenan como datos de navegación encriptados en la unidad de memoria, mayor puede ser la reducción del riesgo de manipulación y/o falsificación. Es más difícil manipular o falsificar múltiples señales de navegación encriptadas en comparación con una señal de navegación encriptada.

60 En una forma de realización preferida, el sistema está diseñado para realizar al menos algunas de las etapas de un procedimiento de la invención de acuerdo con una o más de las formas de realización anteriores.

65 Estos y otros aspectos de la invención se apreciarán más fácilmente a medida que se entiendan mejor en referencia a la siguiente descripción detallada y se consideren en conexión con los dibujos adjuntos en los cuales símbolos de referencia similares designan partes similares.

ES 2 754 376 T3

La figura 1 muestra un receptor de señales en el espacio acoplado a un barco y un lector para el procedimiento según la invención.

La figura 2 muestra una visión general detallada del receptor de señales en el espacio y del lector.

La figura 3 muestra una visión general detallada de un sistema.

La figura 1 muestra un receptor de señales en el espacio 2 acoplado a un objeto 4. En este caso, el objeto 4 es un barco, por ejemplo un barco de pesca. El receptor 2 es suministrado al objeto 4 de manera que datos de localización 5 del receptor 2 corresponden a datos de localización 5 del objeto 4. En otras palabras, el objeto 4 se corresponde con ciertos datos de localización 5, por ejemplo, el barco tiene una posición y una velocidad determinadas en un momento determinado (PVT). Como el receptor 2 está acoplado y/o es suministrado al objeto 4, sus datos de localización corresponden.

Además se muestra un lector 6. El lector 6 es adecuado para su conexión con el receptor 2. Para este fin, el receptor comprende una interfaz 7. Cuando el lector 6 es conectado, se pueden transferir datos entre el receptor 2 y el lector 6. En particular, se transfieren datos desde el receptor 2 al lector 6. El lector 6 es adecuado para recuperar datos de localización 5 que corresponden al lector 6 y, por lo tanto, al objeto 4.

Para ilustrar la invención, se describe con más detalle un procedimiento para recuperar datos de localización 5 del objeto 4.

Una primera etapa es que el receptor de señales en el espacio 2 es proporcionado o acoplado al objeto 4. Por ejemplo, esto se hace por medio de imanes u otros medios de fijación. Después de proporcionar el receptor 2 al objeto 4, los datos de localización 5 del receptor 2 corresponden a los datos de localización 5 del objeto 4 y viceversa.

El receptor 2 comprende una antena 8 para recibir señales de navegación encriptadas 10a, 10b, 10c, 10d. Esto se puede ver en la Figura 2.

Las señales de navegación encriptadas 10a, 10b, 10c, 10d proceden de satélites del Sistema Mundial de Navegación por Satélite (GNSS). En este caso, un total de cuatro satélites GNSS 11a, 11b, 11c, 11d están a la vista y cada uno de ellos transmite respectivamente una señal de navegación encriptada 10a, 10b, 10c, 10d.

Las señales de navegación encriptadas 10a, 10b, 10c, 10d son recibidas por la antena 8 al mismo tiempo y son convertidas en datos de navegación encriptados 12 por parte de un convertidor A/D 15. La conversión de señales de navegación analógicas en datos de navegación digitales significa que se discretizan las señales de navegación encriptadas 10a, 10b, 10c, 10d en forma de datos de navegación encriptados 12. Después de la discretización, los datos de navegación encriptados 12 son adecuados para su procesamiento digital, por ejemplo, para su almacenamiento en una unidad de memoria 16.

La segunda etapa del procedimiento es, por lo tanto, la recepción de las señales de navegación encriptadas 10a, 10b, 10c, 10d por parte de la antena 8. A continuación, el procedimiento comprende la etapa de discretizar las señales de navegación encriptadas 10a, 10b, 10c, 10d en forma de datos de navegación encriptados 12 por parte del convertidor A/D 15.

Una etapa siguiente es que los datos de navegación encriptados 12 son almacenados en la unidad de memoria 16. La unidad de memoria 16 está comprendida en el receptor 2.

Por ejemplo, la unidad de memoria 16 es una Unidad de Estado Sólido (SSD: Solid State Drive) también conocida como Almacenamiento de Estado Sólido (Solid State Storage) y/o Disco de Estado Sólido (Solid State Disk) y/o Disco Electrónico (Electronic Disk). Estas unidades SSD realmente no comprenden un disco sino que se componen de circuitos integrados como almacenamiento de memoria.

En otro ejemplo, la unidad de memoria 16 es una tarjeta de memoria no volátil, tal como una tarjeta Digital Segura (SD: Secure Digital).

El receptor 2 registra ahora todas las señales de navegación encriptadas 10a, 10b, 10c, 10d a lo largo del tiempo y las almacena como datos de navegación encriptados 12 en la unidad de memoria 16.

El almacenamiento, es decir, el registro, se puede realizar a una frecuencia de muestreo predefinida y durante un tiempo predefinido.

Por ejemplo, después de acoplar el receptor 2 al objeto 4, por ejemplo, un barco, el objeto 4 estará en el mar durante 2 semanas. El receptor 2 discretiza, por ejemplo, muestrea/registra, las señales de navegación encriptadas 10a, 10b, 10c, 10d durante 2 semanas a una frecuencia de muestreo de dos

ES 2 754 376 T3

muestras por día. En total se almacenan 14 o 28 muestras de datos de navegación encriptados 12 en la unidad de memoria 16.

5 En general, la frecuencia de muestreo y la duración del muestreo dependen de la duración total de los datos de localización que se requieren y del tipo de objeto.

10 Durante la recepción de las señales de navegación encriptadas 10a, 10b, 10c, 10d no se procesan los datos de navegación encriptados 12 en forma de datos de localización reales 5. Dado que el receptor 2 no incluye una clave de descryptación 20, es mucho más difícil falsificar y/o manipular el receptor para generar datos de localización falsos 5. Esto reduce el riesgo de manipulación y/o falsificación del receptor.

15 Cuando el objeto 4, en este caso el barco, vuelve a puerto, una entidad gubernamental puede recuperar los datos de localización 5 en base a los datos de navegación encriptados 12 almacenados en el receptor 2.

Por lo tanto, en otra forma de realización, el procedimiento comprende la etapa de conectar el lector 6 con la unidad de memoria 16 para transferir los datos de navegación encriptados 12 a lo largo del tiempo desde la unidad de memoria 16 al lector 6.

20 Ahora, los datos de navegación encriptados 12 están disponibles para el lector 6.

La etapa siguiente es descryptar, en el lector 6, los datos de navegación encriptados 12 a lo largo del tiempo.

25 Para este propósito, el lector 6 comprende una unidad de descryptación 21 que descrypta los datos de navegación encriptados 12 en forma de datos de navegación descryptados 22. La clave de descryptación 20 puede ser suministrada al lector 6 o puede estar ya programada en la unidad de descryptación 21. Por ejemplo, la unidad de descryptación 21 es un denominado módulo de seguridad que ya contiene la clave de descryptación 20.

30 La etapa siguiente es recuperar los datos de localización 5 a lo largo del tiempo a partir de los datos de navegación descryptados 22 por parte del lector 6. En la Figura 2 se muestra que el lector 6 incluye una unidad de recuperación 23 para recuperar los datos de localización 5 a partir de los datos de navegación descryptados 22.

35 Separar la etapa de descryptar los datos de navegación encriptados 12 y recuperar los datos de localización 5 con respecto a registrar/almacenar los datos de navegación encriptados 12 tiene la ventaja de que la falsificación y/o manipulación de los datos de localización 5 es mucho más difícil.

40 La invención también está relacionada con el uso del receptor de señales en el espacio 2, según se describe y se muestra en las Figuras 1 y 2.

45 En este caso, el receptor de señales en el espacio 2 comprende la antena 8 para recibir la señal de navegación encriptada 10a, 10b, 10c, 10d a lo largo del tiempo. El receptor comprende el convertidor A/D 15 para discretizar la señal de navegación encriptada 10a, 10b, 10c, 10d en forma de datos de navegación encriptados 12 a lo largo del tiempo. Comprende la unidad de memoria 16 para almacenar los datos de navegación encriptados 12 a lo largo del tiempo. Y el receptor 2 comprende la interfaz 7 para su conexión con el lector 6 y para transferencia de datos de navegación encriptados 12 a lo largo del tiempo al lector 6.

50 La invención también está relacionada con el uso del lector según se describe en las Figuras 1 y 2. El lector comprende una interfaz, que es una interfaz de receptor 27, para su conexión con el receptor de señales en el espacio 2 y para transferencia de datos de navegación encriptados 12 a lo largo del tiempo almacenados en el receptor 2 desde el receptor 2 al lector 6. El receptor 2 comprende una interfaz 7, que es una interfaz de lector, para su conexión con el lector 6. Preferentemente, la interfaz de receptor 27 es conectable de forma extraíble con la interfaz de lector 7 para comunicación entre el lector 6 y el receptor 2 respectivamente.

60 El lector 6 comprende además la unidad de descryptación 21 configurada para descryptar los datos de navegación encriptados 12 a lo largo del tiempo. El lector 6 comprende la unidad de recuperación 23 para recuperar los datos de localización 5 del objeto 4 a lo largo del tiempo.

65 Un procedimiento para recuperar los datos de localización 5 del objeto 4 del receptor de señales en el espacio 2, según se describe en las Figuras 1 y 2, comprende las etapas de conectar el lector 6 con el receptor de señales en el espacio 2, transferir los datos de navegación encriptados 12 a lo largo del tiempo desde la unidad de memoria 16 al lector 6 y descryptar en el lector 6 los datos de navegación

encriptados 12 a lo largo del tiempo y recuperar los datos de localización 5 del objeto 4 a lo largo del tiempo.

5 Un procedimiento para almacenar los datos de localización 5 del objeto 4 en el receptor 2, según se describe en las Figuras 1 y 2, comprende las etapas de proporcionar el receptor de señales en el espacio 2 al objeto 4, recibir la señal de navegación encriptada 10a, 10b, 10c, 10d a lo largo del tiempo por parte de la antena 8, discretizar la señal de navegación encriptada 10a, 10b, 10c, 10d a lo largo del tiempo por parte del convertidor A/D 15 en forma de datos de navegación encriptados 12 y almacenar los datos de navegación encriptados 12 a lo largo del tiempo en la unidad de memoria 16. Los datos de navegación encriptados 12 a lo largo del tiempo son representativos de datos de localización 5 del objeto 4 a lo largo del tiempo.

15 Un sistema 1 para recuperar datos de localización 5 de un objeto 4, mostrado en la Figura 3, comprende el receptor 2 y el lector 6 de acuerdo con una de las formas de realización anteriores.

20 El procedimiento para recuperar datos de localización 5 de un objeto 4 a lo largo del tiempo, el procedimiento para recuperar datos de localización 5 de un objeto 4 a lo largo del tiempo a partir de un receptor de señales en el espacio 2, el receptor de señales en el espacio 2, el lector 6 para recuperar datos de localización 5 de un objeto 4 a lo largo del tiempo, el procedimiento para almacenar datos de localización 5 de un objeto 4 a lo largo del tiempo en un receptor de señales en el espacio 2, el sistema 1 para recuperar datos de localización 5 de un objeto 4 a lo largo del tiempo no se limitan a las formas de realización descritas. Cualquier combinación de las formas de realización descritas es posible y está prevista.

25 En particular, un receptor 2 y/o lector 6 descritos en una forma de realización se pueden aplicar en otra forma de realización con las ventajas correspondientes.

30 Según se requiere, en el presente documento se divulgan formas de realización detalladas de la presente invención; sin embargo, se debe entender que las formas de realización divulgadas son meramente de ejemplos de la invención, que pueden ser realizadas de varias formas. Por tanto, los detalles estructurales y funcionales específicos divulgados en el presente documento no se deben interpretar como limitantes, sino simplemente como una base para las reivindicaciones y como una base representativa para enseñar a un experto en la materia a utilizar la presente invención de diversas maneras en prácticamente cualquier estructura detallada apropiada. Además, los términos y frases utilizadas en el presente documento no pretenden ser limitantes, sino más bien, proporcionar una descripción comprensible de la invención.

35 Los términos "un" o "una", según se utilizan en el presente documento, se definen como uno o más de uno. El término "múltiple", según se utiliza en el presente documento, se define como dos o más de dos. El término "otro", según se utiliza en el presente documento, se define como al menos un segundo o más. Los términos "incluye" y/o "tiene", según se utilizan en el presente documento, se definen como comprende (es decir, lenguaje abierto, sin excluir otros elementos o etapas). Cualesquiera signos de referencia en las reivindicaciones no se deben interpretar como una limitación del alcance de las reivindicaciones de la invención.

45 El mero hecho de que se reciten ciertas medidas en reivindicaciones dependientes diferentes entre sí no indica que no pueda aprovecharse una combinación de estas medidas.

50 En resumen, se adquiere un procedimiento según la invención y el uso de un lector y receptor según la invención que resultan en una menor manipulación y/o falsificación de datos de localización. Con la separación del almacenamiento de datos de navegación encriptados y la descryptación de los datos de navegación encriptados para recuperar los datos de localización en términos de etapas y dónde se realizan estas etapas, resultan en una gran reducción de los riesgos de manipulación/falsificación.

55 La invención no se limita a las formas de realización descritas.

Los datos de localización comprenden posición, velocidad y tiempo.

60 El receptor no requiere y/o no tiene un módulo de seguridad, es decir, una unidad de descryptación para descryptar la señal de navegación encriptada.

En una forma de realización, la unidad de memoria es una memoria interna, por ejemplo, una tarjeta SSD o SD.

65 El lector está configurado para descryptar los datos de navegación encriptados y recuperar los datos de localización, tales como posición, velocidad y tiempo, por marca de tiempo (o time stamp).

El lector puede estar configurado además para transmitir (o hacer streaming de) los datos de localización,

ES 2 754 376 T3

preferiblemente por marca de tiempo(o time stamp) directamente en un mapa digital o un archivo de datos.

- 5 En otra forma de realización, el procedimiento comprende además la etapa de comparar los datos de localización recuperados con datos de navegación no encriptados. Estos datos de navegación no encriptados se adquieren recibiendo señales de navegación no encriptadas por parte de la antena y discretizando estas señales de navegación no encriptadas por parte del convertidor A/D en forma de datos de navegación no encriptados. Por ejemplo, los datos de navegación no encriptados son GPS civil o Galileo OS.
- 10 El procedimiento puede comprender además la etapa de acoplar el receptor a un objeto por medio de imanes.
- 15 El procedimiento puede comprender además la etapa de suministrar energía al receptor acoplado al objeto a partir de una fuente de energía dentro del objeto.

REIVINDICACIONES

1. Procedimiento para reducir un riesgo de manipulación y/o falsificación de datos de localización (5) de un objeto (4) a lo largo del tiempo, comprendiendo el procedimiento las etapas de:
- 5 - proporcionar un receptor de señales en el espacio (2) al objeto (4), comprendiendo el receptor de señales en el espacio (2) una antena (8) para recibir una señal de navegación encriptada (10a, 10b, 10c, 10d), un convertidor A/D (15) para discretizar la señal de navegación encriptada (10a, 10b, 10c, 10d) en forma de datos de navegación encriptados (12), una unidad de memoria (16) para almacenar los datos de navegación encriptados (12) y una interfaz (7) para conectar un lector (6) a la unidad de memoria (16), en
- 10 el que no se proporciona en el receptor de señales en el espacio (2) una clave de descryptación para descryptar los datos de navegación encriptados (12);
- recibir la señal de navegación encriptada (10a, 10b, 10c, 10d) a lo largo del tiempo por parte del receptor de señales en el espacio (2) a través de su antena (8);
- 15 - discretizar la señal de navegación encriptada (10a, 10b, 10c, 10d) a lo largo del tiempo por parte del convertidor A/D (15) en forma de datos de navegación encriptados (12);
- almacenar los datos de navegación encriptados (12) a lo largo del tiempo en la unidad de memoria (16);
- conectar el lector (6) con la unidad de memoria (16) del receptor de señales en el espacio (2);
- transferir los datos de navegación encriptados (12) a lo largo del tiempo desde la unidad de memoria (16) al lector (6);
- 20 - descryptar en el lector (6) los datos de navegación encriptados (12) a lo largo del tiempo y recuperar los datos de localización (5) del objeto (4) a lo largo del tiempo,
- caracterizado por**
- comprobar a partir de los datos de localización (5) a lo largo del tiempo recuperados dónde ha estado el objeto (4).
- 25
2. Procedimiento según la reivindicación anterior, en el que la antena (8) es adecuada para recibir más de una, preferiblemente más de tres señales de navegación encriptadas (10a, 10b, 10c, 10d) al mismo tiempo, en el que el convertidor A/D (15) es adecuado para discretizar las señales de navegación encriptadas recibidas (10a, 10b, 10c, 10d) al mismo tiempo en forma de datos de navegación encriptados (12), y el procedimiento comprende las etapas de:
- 30 - recibir las señales de navegación encriptadas (10a, 10b, 10c, 10d) a lo largo del tiempo por parte de la antena (8);
- discretizar las señales de navegación encriptadas (10a, 10b, 10c, 10d) a lo largo del tiempo por parte del convertidor A/D (15).
- 35
3. Procedimiento según una de las reivindicaciones anteriores, en el que el procedimiento comprende además la etapa de proporcionar al lector (6) una clave de descryptación para descryptar los datos de navegación encriptados (12) a lo largo del tiempo.
- 40
4. Procedimiento según una de las reivindicaciones anteriores, en el que el procedimiento comprende además la etapa de comparar los datos de localización (5) del objeto (4) a lo largo del tiempo con una región predefinida.
- 45
5. Procedimiento según una de las reivindicaciones anteriores, en el que el procedimiento comprende además la etapa de comparar los datos de localización recuperados con datos de navegación no encriptados.
- 50
6. Procedimiento según una de las reivindicaciones anteriores, en el que la señal de navegación encriptada (10a, 10b, 10c, 10d) es una señal encriptada del Sistema Mundial de Navegación por Satélite (GNSS: Global Navigation Satellite System).
7. Procedimiento según una de las reivindicaciones anteriores, en el que el objeto (4) es:
- 55 - una embarcación, en particular el objeto (4) es un barco de pesca, o
- un contenedor, en particular en una embarcación o en un camión de carretera, o
- un vehículo, o
- un cuerpo humano.
8. Procedimiento según una de las reivindicaciones anteriores, en el que la señal de navegación encriptada (10a, 10b, 10c, 10d) es una señal de servicio público regulado (PRS: Public Regulated Service) y/o una señal de servicio de navegación comercial (CNS: Commercial Navigation Service).
- 60
9. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el receptor de señales en el espacio (2) incluye además una interfaz de suministro de energía conectable a una fuente externa de suministro de energía, y el procedimiento comprende además la etapa de suministrar energía de la fuente externa de suministro de energía al receptor de señales en el espacio (2), en el que la fuente externa de suministro de energía es externa al receptor de señales en el espacio (2).
- 65

ES 2 754 376 T3

10. Uso de un receptor de señales en el espacio (2) en el procedimiento según una cualquiera de las reivindicaciones 1 – 9,comprendiendo el receptor de señales en el espacio (2) una antena (8) para recibir una señal de navegación encriptada (10a, 10b, 10c, 10d), un convertidor A/D (15) para discretizar la señal de navegación encriptada (10a, 10b, 10c, 10c, 10d) en forma de datos de navegación encriptados (12), una unidad de memoria (16) para almacenar los datos de navegación encriptados (12), y una interfaz (7) para conectar un lector (6) a la unidad de memoria (16), en el que no se proporciona en el receptor de señales en el espacio (2) una clave de desencriptación para desencriptar los datos de navegación encriptados (12).
- 5
- 10 11. Uso de un lector (6) en el procedimiento según una cualquiera de las reivindicaciones 1 – 9,comprendiendo el lector (6) una interfaz de receptor (27) para su conexión con una unidad de memoria (16) de un receptor de señales en el espacio (2) y transferencia al lector (6) de datos de navegación encriptados (12) a lo largo del tiempo almacenados en la unidad de memoria (16), una unidad de desencriptación para desencriptar los datos de navegación encriptados (12) en forma de datos de navegación desencriptados (22), y una unidad de recuperación (23) para recuperar datos de localización
- 15 (5) del objeto (4) a lo largo del tiempo a partir de los datos de navegación desencriptados.

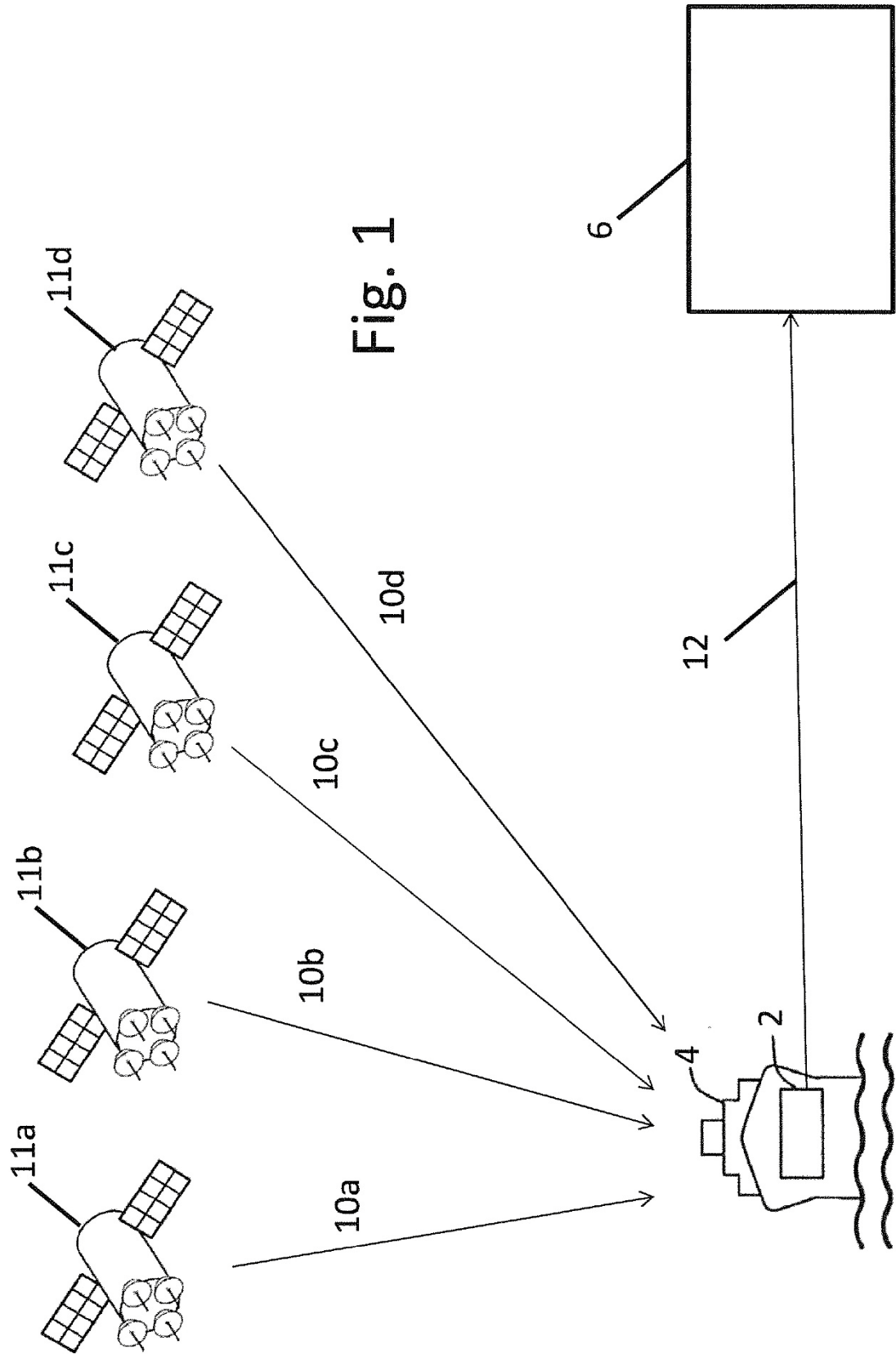
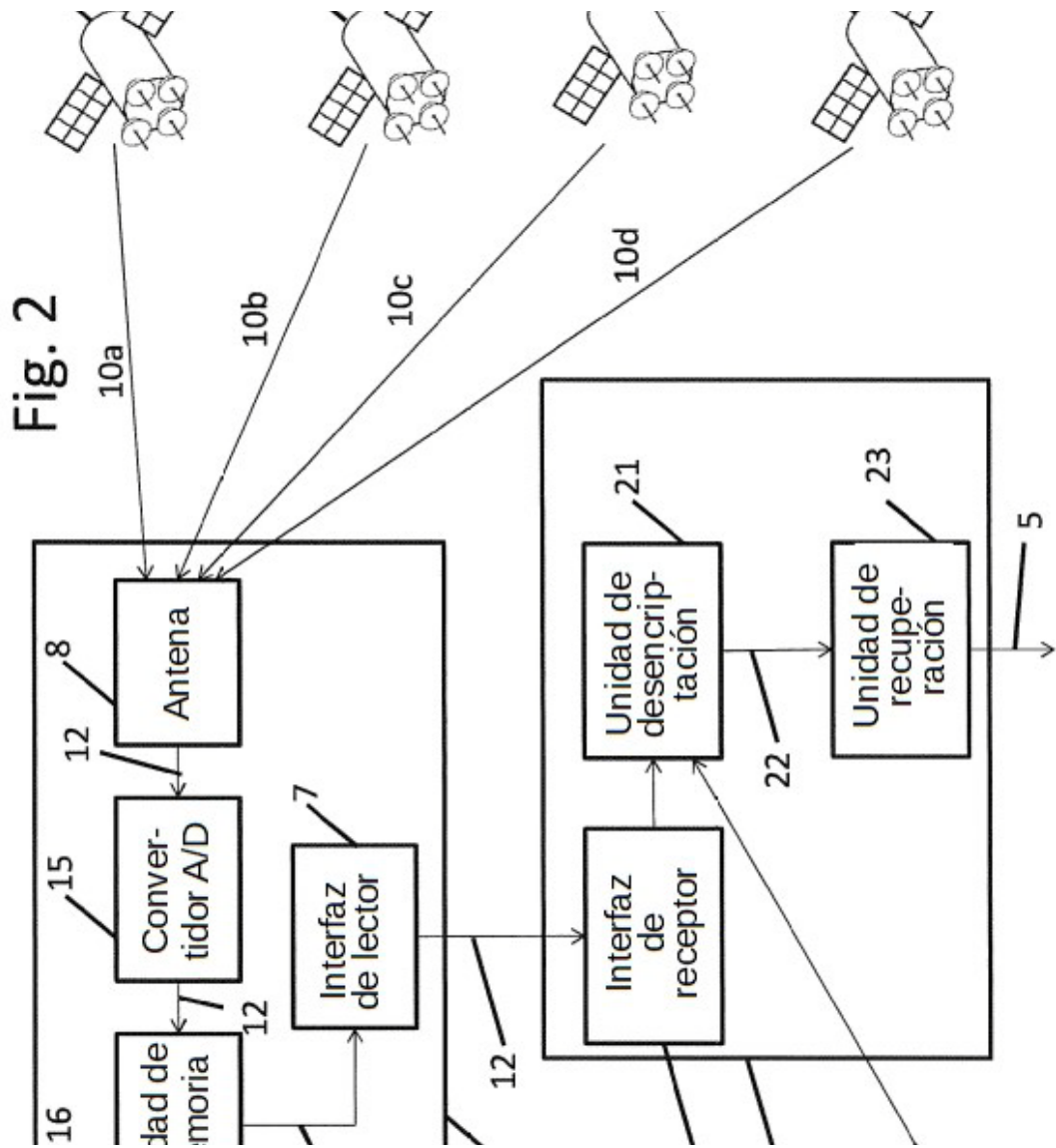


Fig. 1



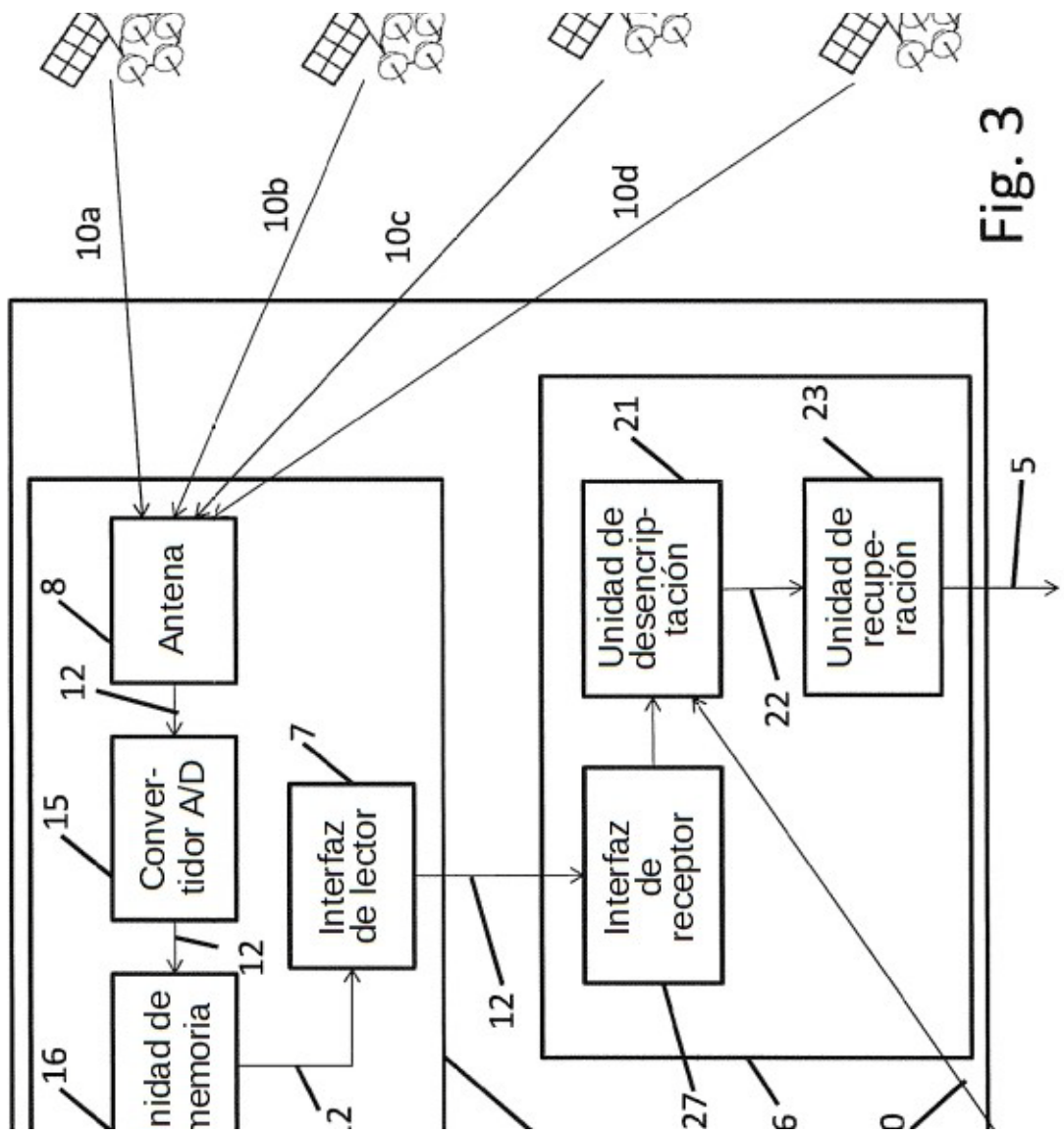


Fig. 3