(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 648 039**

(51) Int. CI.:

H04L 9/32 (2006.01)
G01S 1/00 (2006.01)
H04N 1/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.09.2008 PCT/EP2008/061780**

(87) Fecha y número de publicación internacional: **26.03.2009 WO09037133**

(96) Fecha de presentación y número de la solicitud europea: **05.09.2008 E 08803749 (4)**

(97) Fecha y número de publicación de la concesión europea: **23.08.2017 EP 2188943**

(54) Título: **Procedimiento que proporciona los medios para reconocer el origen y/o el contenido de una señal de RF**

(30) Prioridad:

21.09.2007 FR 0706643

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.12.2017

(73) Titular/es:

THALES (100.0%)
Tour Carpe Diem, Place des Corolles, Esplanade Nord
92400 Courbevoie, FR

(72) Inventor/es:

DAMIDAUX, JEAN-LOUIS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento que proporciona los medios para reconocer el origen y/o el contenido de una señal de RF

La presente invención se refiere a un procedimiento que proporciona los medios que permiten reconocer el origen y/o el contenido de una señal de RF.

Se conocen numerosas técnicas para combatir la interferencia de señales tales como las de los radares. En cambio, en un campo tal como en el de la recepción de señales de radiolocalización, es necesario disponer de las medidas (denominadas pseudo-medidas) proporcionadas por unos satélites y de datos de efemérides. Es relativamente fácil proteger los datos de efemérides para garantizar el origen y/o el contenido. En cambio, las características de las señales de medida son del dominio público, y por tanto no pueden protegerse. Es fácil entonces emular estas señales con el fin de que un usuario obtenga unas coordenadas de posición geográfica falseadas. Igualmente ocurre en otros dominios de transmisiones digitales tales como las telecomunicaciones o las difusiones de programas de televisión.

Se han llevado a cabo pocas investigaciones para permitir garantizar el origen de dichas señales de RF. En efecto, ahora es posible, si se implementan unos calculadores suficientemente potentes, producir de manera malintencionada unas señales que imitan las emitidas por los satélites de geolocalización. Estas técnicas de engaño se denominan en inglés "spoofing".

Se han descrito algunas indicaciones para tratar de autenticar las señales recibidas por ejemplo en un artículo de Logan SCOTT "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation systems" aparecido en la revista ION GPS/GNSS 2003, 9-12 de septiembre de 2003, Portland, OR. Sin embargo, la determinación del origen y/o del contenido de las señales recibidas necesita igualmente importantes medios de cálculo que consumen una energía no despreciable y no están por tanto al alcance de un simple usuario de un receptor de radionavegación o de un usuario ordinario abonado a unos programas de televisión digital. Se conocen por el estado de la técnica las siguientes técnicas.

El documento WO2004002160 describe un procedimiento de autenticación de una señal audiovisual. Se deduce una firma de todas las franjas de visualización, comprendidas en ellas los espacios que incluyen un contenido plano o no marcado. Combinando unos bits de firma asociados con todas las zonas de la señal audiovisual y ensanchándolas sobre el conjunto de la señal audiovisual o al menos sobre la mayor parte de esta, aplicando preferentemente una técnica de marcado por ensanchamiento del espectro se puede verificar la autenticidad de las franjas planas.

El documento EP1594122 describe un método de inserción de marcado de espectro ensanchado que puede utilizarse para la marca de agua de señales de audio. La señal que lleva la marca de agua puede modularse mediante una función de reparto o una función aleatoria. En el decodificador, la marca de agua que se inserta en la señal de audio se extrae por convolución.

El documento XP011026243 describe un algoritmo para realizar una marca de agua de imagen pero también de audio, video y multimedia, siendo dicho algoritmo de seguridad y "tamper resistant". Siendo la construcción de la marca de agua una construcción independiente e idénticamente distribuida (i.i.d.) de un vector aleatorio gaussiano que se inserta de manera imperceptible repartido sobre la parte más pertinente del espectro.

El documento US7194620 describe un método de autenticación en tiempo real que comprende la etapa de inserción de una firma en los datos.

El documento US7020555 describe un sistema de suscripción para un servicio GPS.

El documento US2002191809 describe un sistema de marca de agua asimétrico repartido sobre el espectro. La presente invención tiene por objeto un procedimiento que proporciona los medios que permiten reconocer el origen y/o el contenido de una señal de RF sin precisar de importantes medios de cálculo, no siendo estos medios de reconocimiento accesibles más que a unas personas autorizadas y siendo prácticamente no modificables y muy difícilmente detectables por unas personas no autorizadas, y esto en diversas aplicaciones que implementan unas señales de RF que transmiten unas informaciones ocultas al menos en parte.

El procedimiento de acuerdo con la invención se caracteriza porque se ensancha una información a ocultar con ayuda de un código oculto, porque se reparte esta información, con ayuda de una función XOR (O exclusiva), en unos códigos conocidos con la ayuda de un algoritmo de reparto oculto, porque durante la recepción se implementa el algoritmo inverso de aquel que haya servido para el reparto para acceder al código ensanchado, porque se correlaciona este código ensanchado con el código oculto para encontrar la información oculta. De manera ventajosa, el código oculto se desfasa en el momento de la emisión, con el fin que durante la recepción, durante la correlación de este código ensanchado con el código oculto no desfasado, se detecte el desfase. El valor de este desfase puede permitir transmitir información.

La presente invención se comprenderá mejor con la lectura de la descripción detallada de un modo de realización, considerado a título de ejemplo no limitativo e ilustrado por el dibujo adjunto, en el que:

- la figura única es un diagrama de bloques simplificado de un dispositivo de implementación del procedimiento de la invención.

La invención se describe en el presente documento a continuación con referencia a la verificación del origen y/o del contenido de señales de radiolocalización (GNSS), pero se sobrentiende que no está limitada a esta única aplicación, y que puede implementarse para diferentes señales de RF, tales como otros tipos de señales de localización (terrestres por ejemplo) o unas señales de televisión digital terrestre (TDT), en particular de televisión de pago, o incluso unas señales de telefonía de pago.

Una característica esencial del procedimiento de la invención es ocultar en la secuencia de ensanchamiento una firma digital que se puede calificar como marca de agua ("watermark" en inglés). Esta marca de agua se oculta de manera que no se pueda detectar directamente o con la ayuda de métodos estadísticos en la secuencia de ensanchamiento. Por supuesto, un usuario autorizado puede extraer fácilmente esta marca de agua de la secuencia de ensanchamiento y servir para determinar el origen de la señal recibida.

En el diagrama de bloques de la figura única del dibujo, que muestra un satélite 1 y uno de los receptores correspondientes 2, no se han representado más que los elementos relacionados con la invención.

Los circuitos apropiados del satélite 1 reciben una información 3 de firma oculta que pueden almacenarse a bordo o transmitirse desde tierra. Esta firma es una información oculta conocida únicamente por el organismo que controla el satélite y por unos usuarios habilitados para conocerla (por ejemplo los abonados a un servicio de pago transmitido por el satélite 1). La firma 3 incluye una larga secuencia, preferentemente de un centenar de bits al menos, que permite reconocer el origen y/o el contenido de las señales de radiolocalización y es ventajosamente modificable dinámicamente desde tierra con ayuda de mensajes cifrados enviando o bien una nueva secuencia, o bien una nueva semilla para generar una nueva secuencia, o bien una orden de cambio de firma entre las almacenadas a bordo. Se "modula" (5) por esta firma (3) un código oculto de ensanchamiento (marca de agua) 4. Esta modulación consiste en ensanchar la marca de agua a todo lo largo de la secuencia de la firma 3. Se obtiene de ese modo una marca de agua modulada 6. Este código 4 de ensanchamiento es un código privado que puede modificarse también dinámicamente desde tierra tal como se ha descrito anteriormente para la firma 3.

Se modifica a continuación (de manera difícilmente detectable, como se precisa en el presente documento a continuación) una parte de un código público 7, que en este caso es un código de ensanchamiento de navegación clásico, con ayuda de una técnica que recurre a una marca de agua modulada 6 y a una función "O exclusiva" 8 (igualmente denominada "XOR"). Esta modificación consiste en invertir dinámicamente ciertos de los elementos ("chips" en inglés) del código 7, es decir que esta modificación se efectúa a medida que se desarrolla el código 6, estando presente el código 7 en las diferentes células de la función 8 en cada secuencia de la marca de agua modulada 6, siendo determinado el emplazamiento de estos elementos en el seno del código público mediante un algoritmo 9 que utiliza unas claves privadas. Estos elementos se eligen por el algoritmo de manera pseudo-aleatoria y constituyen una reducida parte del código público 7, ventajosamente algunos pocos porcentajes de este código, con el fin de hacer más difícil la detección de las modificaciones de este código 7 y degradar de una manera mínima la correlación del código público 7. Teniendo el código modulado 6 una longitud superior a la del código 7 y no modificando más que una reducida parte de este, la función XOR 8 emplea varias células que realizan cada una en tiempo real la operación XOR sobre el código 7 que se presenta en cada una de ellas.

El código de navegación así oculto se difunde (11) por el emisor (no representado) del satélite 1. Se procesa según unas operaciones inversas a aquellas que se han practicado en la emisión en un receptor de radionavegación 2, de la manera siguiente. Los circuitos de recepción (no representados) del receptor 2 transmiten las señales recibidas del satélite 1 a una entidad 12 que selecciona dinámicamente con la ayuda de la clave pública 13 el emplazamiento de los chips en los que se ha realizado la operación 8 de "O exclusiva" (XOR).

Por otro lado, la clave 13 permite generar el código oculto 14 de ensanchamiento de la marca de agua (idéntico al código 4). Este código 14 se envía a un correlador 15 que recibe de la entidad 12 unas secuencias de códigos en las que los chips del código 7 modificados en la emisión se han restablecido a sus valores de origen. A la salida del correlador 15, si el código de ensanchamiento 14 está efectivamente presente en la señal recibida, se obtienen los símbolos (16) que deben permitir reconstruir la firma 17 después de la decodificación, que debe ser idéntica a la firma 3 si las informaciones recibidas desde el satélite 1 son correctamente aquellas emitidas por el organismo que controla el satélite, y no un engaño.

En conclusión, la implementación del procedimiento de la invención es "transparente" para el usuario que no tiene necesidad de servicios (en general de pago) protegidos por este procedimiento. El marcado efectuado por este procedimiento es muy difícilmente detectable debido a que el código transmitido (10) así modificado no se altera casi y porque el código público de ensanchamiento de navegación (7) no se modifica.

Además, Incluso si unas personas malintencionadas implementaran unos medios muy importantes para simular este marcado, estarían obligadas a utilizar una antena de muy alta ganancia para detectar los chips modificados, porque sin ellos, es imposible modular las señales de navegación con los chips modificados. No sería posible más que diferir la emisión de los engaños para tener el tiempo de extraer cada chip y analizarlo, pero entonces, puede

efectuarse fácilmente la verificación de la coherencia Doppler de estas señales. Un usuario advertido puede verificar la coherencia de las señales recibidas (en Doppler y en distancia, y los valores de efemérides). Debido a que el valor de los chips modificados depende igualmente de los datos emitidos, incluso si fuera posible para unas personas malintencionadas detectar unos chips modificados, les sería imposible introducir unos engaños porque no pueden determinar en cuáles emplazamientos deben modificar los chips ya que si desean transmitir el valor opuesto al valor transmitido por el sistema real, no conocen más que el emplazamiento de los chips a no modificar.

REIVINDICACIONES

1. Procedimiento que permite reconocer el origen y/o el contenido de una señal de RF, que comprende las siguientes etapas:

- ensanchar una firma digital (3) en un código oculto (4), aplicándose un desfase de tiempo para dicho código oculto, para obtener un código oculto modulado (6),
- repartir el código oculto modulado (6) en un código público de ensanchamiento de navegación (7) aplicando un algoritmo de clave privada (9) con una función "O exclusiva" (8), para obtener unas secuencias de códigos modulados (10);
- transmitir (11) las secuencias de códigos modulados (10);
- en la recepción, aplicar un algoritmo de clave pública (13) para seleccionar unas secuencias de códigos modulados (12) y para generar un código oculto de ensanchamiento (14); y
- correlacionar las secuencias de código seleccionadas (12) con el código de ensanchamiento (14) para encontrar la firma digital oculta (17).

2. Procedimiento según la reivindicación 1, **caracterizado porque** el desfase se detecta durante la correlación del código de ensanchamiento con las secuencias de código seleccionadas.

3. Procedimiento según la reivindicación 1 o 2, **caracterizado porque** el desfase se utiliza para transmitir información.

4. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** la señal de RF es una señal de radiolocalización de una constelación de satélites.

5. Procedimiento según la reivindicación 4, **caracterizado porque** la firma digital a ocultar (3) se almacena a bordo de los satélites.

6. Procedimiento según la reivindicación 4, **caracterizado porque** la firma digital a ocultar se transmite desde tierra a los satélites.

7. Procedimiento según una de las reivindicaciones anteriores, **caracterizado porque** la firma digital a ocultar se modifica dinámicamente desde tierra con la ayuda de mensajes cifrados.

8. Procedimiento según la reivindicación 7, **caracterizado porque** la firma digital a ocultar se modifica mediante el envío de una nueva secuencia.

9. Procedimiento según la reivindicación 7, **caracterizado porque** la firma digital a ocultar se modifica mediante el envío de una nueva semilla para generar una nueva secuencia.

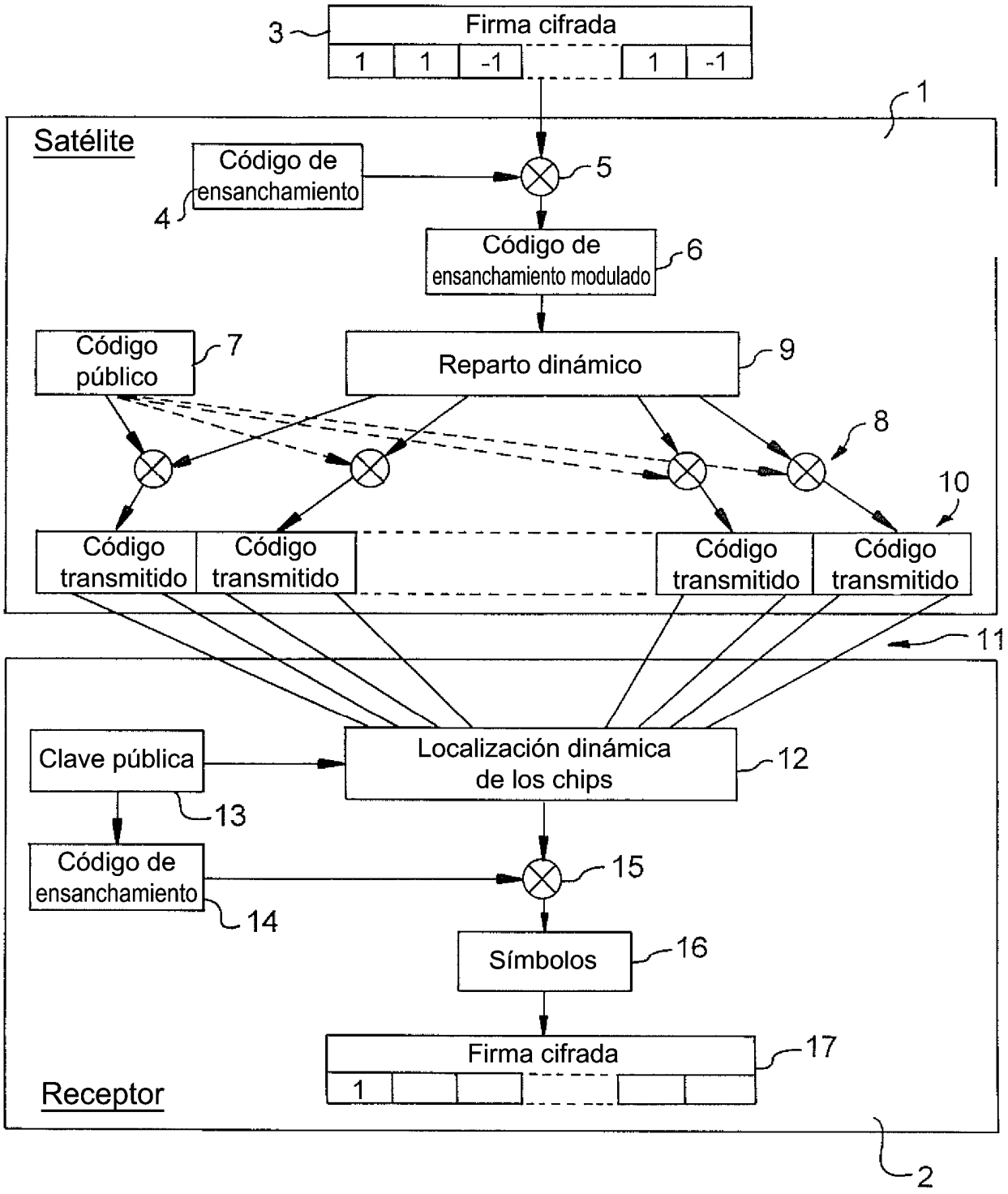
10. Procedimiento según la reivindicación 5, **caracterizado porque** se almacenan a bordo varias firmas digitales a ocultar y porque se envía una orden de cambio para seleccionar una de aquellas almacenadas a bordo.

11. Procedimiento según una de las reivindicaciones 4 a 10, **caracterizado porque** el código oculto de ensanchamiento (14) se modifica dinámicamente desde tierra con la ayuda de mensajes cifrados.

12. Procedimiento según la reivindicación 11, **caracterizado porque** el código oculto, que es una larga secuencia de bits, se modifica mediante el envío de una nueva secuencia.

13. Procedimiento según la reivindicación 11, **caracterizado porque** el código oculto se modifica mediante el envío de una nueva semilla para generar una nueva secuencia.

14. Procedimiento según la reivindicación 11, **caracterizado porque** se almacenan a bordo varios códigos ocultos y porque se envía una orden de cambio para seleccionar uno de aquellos almacenados a bordo.


3
Firma cifrada
1
1
-1
1
-1
1
Satélite
Código de ensanchamiento
4
5
Código de ensanchamiento modulado
6
Código público
7
Reparto dinámico
9
8
10
Código transmitido
Código transmitido
Código transmitido
Código transmitido
11
Clave pública
Localización dinámica de los chips
12
13
Código de ensanchamiento
14
15
Símbolos
16
Firma cifrada
17
1
Receptor
2