(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 621 785**

(51) Int. CI.:

H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.05.2011 E 11165950 (4)**

(97) Fecha y número de publicación de la concesión europea: **25.01.2017 EP 2391126**

(54) Título: **Método de seguridad para prevenir el uso no autorizado de contenido multimedia**

(30) Prioridad:

26.05.2010 EP 10163979

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.07.2017

(73) Titular/es:

NAGRA FRANCE SAS (100.0%)
86, rue Henri Farman
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

TRAN, MINH SON;
SARDA, PIERRE-SERNIN DOMINIQUE y
BAUDIN, GEOFFROY VIRGILE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de seguridad para prevenir el uso no autorizado de contenido multimedia

Campo de la invención

[0001] La invención generalmente se refiere al acceso condicional de contenido multimedia.
En particular, la presente invención se refiere a un método para insertar el seguimiento de datos secretos en el contenido multimedia entregado a usuarios particulares.

Antecedentes de la invención

[0002] Los proveedores de contenido digital buscan limitar el uso por la implementación de acceso condicional.
Un escenario como este son los aspectos de seguridad de radiodifusión de vídeo digital vía satélite (DVB-S).
Ha habido un historial de ataques en esta tecnología para eludir cualquier medida de seguridad y algunas técnicas han sido contrarrestadas por el despliegue de receptores específicos personalizados/de proveedor.
Sin embargo, esto lleva a una elección fija definitivamente del proveedor, por lo tanto una pluralidad de equipamientos se necesitan a nivel de cliente para el multiacceso de proveedores.
Receptores de satélite abiertos se han introducido para permitir a un usuario único el acceso a diferentes proveedores de servicios/contenido a partir de una pieza única de equipo de receptor.

[0003] Estas cajas proporcionan un ambiente altamente configurable con emulaciones de software de sistemas de acceso condicionales que desafortunadamente están abiertas al abuso.
El factor clave del espacio de seguridad es que cuando un receptor abierto (incluso el propietario) cae en posesión del usuario, no se puede considerar de confianza.
El dominio de usuario es de no confianza y podría estar sujeto a ataques independientes o de usuario conspirado.
La introducción de tarjetas inteligentes con un procesador incorporado en tal receptor pretende proporcionar una confianza en un ambiente inseguro.
Se cree que la respuesta está en la tarjeta inteligente: esta es la única entidad de confianza en el extremo de cliente.

[0004] Cabe observar que la introducción de la tarjeta inteligente no resuelve automáticamente / absolutamente todas las amenazas de seguridad.
Gracias a la estructura flexible, bien modularizada de los receptores abiertos, el usuario fraudulento puede todavía comprometer el sistema con la unidad de seguridad "inquebrantable" como sigue.
Usuarios fraudulentos con la tarjeta suscrita legítimamente operan un servidor de tarjeta en su receptor abierto reconfigurado/hackeado y escuchas para la comunicación de clientes (ilegales) en un puerto dado.
En el servidor de tarjeta, el acceso condicional se realiza como de costumbre para un cliente autorizado gracias a la tarjeta legítima.
Es decir, que los mensajes de gestión de derecho de acceso (EMMs) y mensajes de control de derecho de acceso (ECMs) se procesan por la famosa unidad de seguridad "inquebrantable" (todavia queda intacta) que desencripta sucesivamente y devuelve las palabras de control al decodificador para desencriptar el contenido.
Por el espionaje de la comunicación entre el decodificador y la unidad de seguridad, el servidor puede además realizar una distribución de masa de la palabra de control a sus propios clientes, que permite a los clientes (sin suscripción al proveedor de contenido real) acceder a programas DVB codificados.
Se cree que este ataque, es decir "ataque de tarjeta de distribución" o "distribución de palabras de control", será fundamental para el uso de los receptores abiertos en el presente al igual que en el futuro.
Afectará a la industria a largo plazo por la captación a un índice estable del ingreso en la industria y clientes potenciales.

[0005] Dado que se admite que el acceso condicional nunca proporciona una seguridad absoluta, los proveedores de contenido digital tratan de desplegar la técnica de toma de huella genética para insertar automáticamente una identificación única del usuario de demanda en el contenido final siempre que se consuma.
Con la suposición de que el proceso de toma de huella genética fue realizado exitosamente, la característica de tractabilidad de la técnica podría desalentar la distribución ilegal del contenido cuando el acceso condicional es derrotado.
Aquí, el receptor abierto puede nuevamente desafiar la implementación de la técnica.
El proceso de inserción se puede circunvenir de manera que el contenido distribuido no contiene ninguna identificación en absoluto.
Resulta interesante destacar que la técnica de toma de huella genética puede confundir el proceso de trazado si no está diseñado cuidadosamente.
Por ejemplo, el usuario con la tarjeta inteligente que dirige el servidor de tarjeta - el fraude primario, es decir, la fuente de filtración inicial - puede no dejar rastro en el trabajo de control que ella/él radiotransmite.
Por el contrario, los clientes que asumen las ventajas de la transmisión ilegal - estos son en realidad los fraudes (inexpertos) secundarios, es decir las víctimas - pueden ocasionalmente dejar en el proceso de toma de huella

genética insertar su identificación en el contenido consumible final.
El fraude primario nunca se detecta en tal escenario.

[0006] El documento WO 2008/023023 describe una solución para rastrear los módulos de seguridad al incrustar un comando de trazado en el flujo de palabras de control.
En la solicitud, el módulo de seguridad emitirá este valor de seguimiento en vez de la palabra de control a la unidad de decodificación.
Este valor puede utilizarse para determinar qué módulo de seguridad ha emitido el valor de seguimiento y así detecta módulos de seguridad forjados.

[0007] El documento US 2006/153377 describe una función matemática que se implementa de una manera única en cada módulo de seguridad.
El resultado producido por cada función matemática es el mismo y es congruente con la función maestra ejecutada para encriptar la palabra de control.
El análisis de la función matemática de un módulo de seguridad falsificado puede después usarse para detectar qué módulo de seguridad auténtico fue usado para producir este falsificado.

Resumen de la invención

[0008] La presente invención propone un método para resolver las desventajas/deficiencias mencionadas anteriormente.

[0009] En el lado de cabecera, las operaciones siguientes serán realizadas:

1. Análisis del fichero multimedia/secuencia de bits originales,
2. Extracción de algunos elementos binarios pertinentes que sobre todo afectan a la representación visual y/o audible de los medios dados, aquellos elementos se llaman los valores originales
3. Generar señuelos de datos llamados simulados o datos alternos (AD) y reemplazar los valores originales extraídos mencionados en la etapa 2 por estos datos alternos.
Este proceso degrada seriamente la calidad de los medios originales.
Los medios resultantes se refieren al flujo modificado.
Hay que señalar que el proceso descrito representa una técnica alternativa "encriptada" en un sentido amplio.
Por lo tanto, el flujo modificado es también referido como un flujo codificado.
4. Almacenamiento del valor original y su ubicación de los elementos mencionados en la etapa 2 en la denominada estructura de objeto de control (CO), que será más tarde reutilizada en el proceso de recuperación de los medios dados.

[0010] Tales medios encriptados se transmiten a un receptor abierto sin alguna otra protección.
Al contrario, el flujo de CO debe ser enviado a la unidad de seguridad de este receptor exclusivamente a través de un canal fijado.
En la condición de tener todos los derechos necesarios, el receptor ejecuta las operaciones siguientes:

- Recepción del flujo codificado donde una pluralidad de valores originales del flujo de vídeo original a una pluralidad de ubicaciones ha sido modificada por valores alternos como la realización en la cabecera,
- recepción por la unidad de seguridad de un objeto de control que comprende un conjunto de datos de control, cada conjunto comprende datos que permiten determinar al menos el original, el valor alterno al igual que la ubicación donde valores alternos han sido introducidos en el primer flujo codificado,
- para cada conjunto de datos de control, calcular un parámetro de clave asociado a una operación matemática, esta operación y el parámetro de clave asociado están seleccionados entre una pluralidad de diferentes operaciones, dichas operaciones matemáticas permiten obtener un valor reconstruido desde el valor alterno gracias al parámetro de clave,
- variación del proceso de selección de dicha operación matemática basada en un primer parámetro interno de la unidad de seguridad para cada conjunto de datos de control
- transmisión a la unidad de decodificación de un conjunto de datos de corrección que corresponde con la designación de la operación matemática, el parámetro de clave y la ubicación del valor alterno,
- recepción de los datos de corrección por la unidad de decodificación y,
- cálculo del valor reconstruido que corresponde con los datos de corrección y los valores alternos recuperados desde el primer flujo de codificación
- reemplazar el valor alterno por el valor reconstruido en el primer flujo codificado para obtener el flujo de vídeo reconstruido.

[0011] Según una forma de realización, el vídeo reconstruido es idéntico al vídeo original.
Aún según otra forma de realización, el vídeo reconstruido es un vídeo personalizado, que es diferente ligeramente del vídeo original, pero tal modificación es imperceptible para el humano espectador.

[0012] Se puede observar que los datos de corrección (CD) juegan el papel de la palabra de control - los datos

circulados entre la unidad de seguridad y de decodificación - en el acceso condicional clásico.
Gracias a los CD marcados, la fuente (fraudes primarios) de su distribución ilegal puede ser ahora detectada fácilmente.

[0013] Una característica clave de la presente invención es producir por la unidad de seguridad un conjunto de CD que es individual a dicha unidad de seguridad aunque el resultado final en el flujo de vídeo - el vídeo reconstruido obtenido gracias a estos datos de corrección personal - es el mismo que para otros CD originados de otras unidades de seguridad.

[0014] Esto es posible usando presentaciones equivalentes diferentes de los datos de corrección.
Es decir, que cada CD comprenden al menos dos componentes: una operación matemática y un parámetro de clave.
Existe una pluralidad de diferentes operaciones matemáticas, cada operación permite la obtención del valor (original) idéntico desde el valor alterno gracias a su propio parámetro de clave.
Por ejemplo, para obtener el resultado final idéntico, el parámetro de clave por supuesto no será el mismo si la operación seleccionada es una adición o una sustracción.
Por tanto, la adición como sustracción con sus propios parámetros clave apropiados todavía pueden producir el mismo resultado.

[0015] Consecuentemente, una marca se puede introducir directamente en las presentaciones equivalentes de CD (de aquí en adelante la marca insertada en tal manera es referida como marca primaria PM) como sigue.
Una marca es únicamente aplicada a una secuencia de operaciones matemáticas, que se asocia a un conjunto de CD.
Para cada CD, el parámetro de clave es luego deducido con una operación matemática dada de modo que el valor reconstruido forzado para estos CD se puede obtener.

[0016] La relación mutua entre el operador matemático y su parámetro de clave mejora la seguridad del PM.
El pirata informático no puede sencillamente atacar los operadores matemáticos, el portador directo del PM, porque cualquier operador (comprometido) diferente no está armonizado en absoluto con el parámetro de clave dado.
Como resultado, los CD no pueden crear correctamente el valor reconstruido asignado, que afecta seriamente a la calidad de vídeo.
Luego el pirata informático tiene que cambiar el parámetro de clave correspondientemente.
Hay que señalar que hasta esta fase en el receptor, los valores reconstruidos no están disponibles.
Por lo tanto, derivar un parámetro de clave apropiado para un operador comprometido es casi imposible.

[0017] Además, la presente invención incluye un método para detectar/corregir la integración/validez del PM insertado en los CD, especialmente para los CD supervivientes al ataque de colusión.

[0018] Otra característica clave de la presente invención es producir por la unidad de seguridad un conjunto de CD que es individual a dicha unidad de seguridad de modo que el resultado final en el vídeo - los datos reconstruidos (por lo tanto, el vídeo reconstruido) obtenidos gracias a estos CD personales - es también individual para cada unidad de seguridad desde el punto de vista de la detección base de ordenador.
Desde el punto de vista de percepción humana, el vídeo reconstruido se puede considerar idéntico, es decir, su impacto en la calidad es distorsión imperceptible para todas las unidades de seguridad.
De aquí en adelante, la marca insertada en los datos reconstruidos es referida como marca secundaria (SM).

[0019] Una marca ahora no (sólo) se inserta en la presentación equivalente de los CD, sino en los valores reconstruidos derivados, que persisten en el vídeo reconstruido.
Por lo tanto, la infracción de uso del vídeo puede ser por sí misma también identificada.
Tales marcas (SMS) son útiles para identificar los fraudes secundarios.

[0020] Según una forma de realización, la SM se basa en la estructura orientada al cliente.
En la cabecera, los valores alternos se generan en tantas posiciones como sea posible.
Los valores reconstruidos para estas ubicaciones serán en realidad calculados en la unidad de seguridad en la función del SM.
El proceso en la unidad de seguridad comprende:

- extraer el valor original desde el objeto de control,
- calcular el valor personalizado basado en el valor original y la SM,
- utilizar el valor personalizado en vez del valor original para calcular el operador y el parámetro de clave de los CD.

[0021] Según otra forma de realización, la inserción de la SM se basa en la estructura distribuida, incluyendo pre-señalización y proceso de post-señalización.
El proceso de pre-señalización selecciona las posiciones en los medios, así como la preparación de todos los valores posibles - referida como valores dedicados - en cada posición.

El post-proceso ocurre finalmente en la unidad de seguridad que comprende:
- extraer el valor original y el conjunto de valores dedicados desde el objeto de control,
- seleccionar como valor personalizado entre el valor original y el conjunto de los valores dedicados basados en una SM asignada al decodificador,
- utilizar el valor personalizado en vez del valor original para calcular el operador y el parámetro de clave de los CD.

[0022] SM se inserta en el valor reconstruido, que es un resultado deducido del operador y el parámetro de clave de los CD asociados.
Tal presencia implícita de SM en el flujo aumenta la seguridad de la marca.
Siempre que el significado de operador se mantenga en secreto (o se actualice periódicamente), el pirata informático controlará difícilmente el impacto de la modificación aplicada bien al operador o al parámetro de clave para comprometer la marca.
Es posible siempre que la calidad de vídeo ya se haya degradado pero la presencia de la marca sigue siendo detectable.
Aún el pirata informático puede sencillamente omitir estos CD (por lo tanto, el valor reconstruido resultante).
En tal caso, el valor alterno que ocurre en la ubicación en cuestión asegura introducir un efecto de distorsión suficiente, que haga el contenido inservible.

[0023] Similar a la PM, la SM se puede tratar por un pretratamiento de anti-colusión antes de ser insertada para aumentar su resistencia para atacar.

[0024] El método para la inserción de las PM y SM se puede usar independientemente.
La información de naturaleza/oculta de las dos marcas también se puede no-relacionar.

Breve descripción de los dibujos

[0025] El aspecto anterior de la presente invención se hará más aparente describiendo en detalle las formas de realización ejemplares del mismo con referencia a las figuras de dibujos anexos.
La Figura 1 muestra un diagrama de bloques de un sistema de transmisión (lado de proveedor de contenido) para facilitar la comunicación según una forma de realización de la presente invención.
La Figura 2 muestra un diagrama de bloques de un sistema de recepción para captar la comunicación para una forma de realización de la presente invención.
La Figura 3 ilustra los datos de entrada necesarios para detectar la marca según una forma de realización de la presente invención.

Descripción detallada de las formas de realización ejemplares

[0026] Ahora se hace referencia ahora en detalle a las formas de realización preferidas de la invención, ejemplos de los cuales se ilustran en los dibujos anexos.
Mientras la invención se describirá en conjunción con las formas de realización preferidas, se entiende que estos no se destinan a limitar la invención a estas formas de realización.
Al contrario, se pretende que la invención cubra alternativas, modificaciones y equivalentes, que se puedan incluir en el espíritu y ámbito de la invención tal y como se define por las reivindicaciones anexas.
Además, en la siguiente descripción detallada de la presente invención, se fijan detalles numerosos específicos en adelante para proporcionar una comprensión profunda de la presente invención.
Sin embargo, será obvio para un técnico en la materia que la presente invención puede tratarse de prácticas sin estos detalles específicos.
En otros casos, los métodos bien conocidos, procedimientos, componentes y circuitos no se han descrito en detalle para no ocultar innecesariamente aspectos de la presente invención.

[0027] El objetivo de la presente invención es cualquier decodificador (alternativamente receptor) que tenga una estructura denominada abierta.
Tal decodificador consiste en al menos un módulo de seguridad 2a y un módulo de descodificación 2b (figura 2).
En el escenario de un DRM convencional, el primero es responsable de la gestión de derechos al igual que la extracción de las claves de descodificación, mientras el último ejecuta la descodificación con la clave (palabra de control) suministrada desde el anterior.

[0028] Las unidades de seguridad, como se ha mencionado anteriormente, se pueden implementar en una variedad de maneras tales como en una tarjeta de microprocesador, en una tarjeta inteligente o cualquier unidad electrónica en forma de una identificación o clave.
Estas unidades son portátiles generalmente y separables del receptor/decodificador y se diseñan por ser a prueba de manipulaciones.
La forma usada más frecuentemente tiene contactos eléctricos pero versiones sin contacto de tipo ISO 14443 también existen.
Otra implementación de la unidad de seguridad existe donde esta está directamente soldada dentro del

receptor/decodificador, una variación de esta es un circuito en un hueco o conector tal como un módulo de SIM.
Otra implementación es tener la unidad de seguridad integrada en un chip que tiene otra función por ejemplo en el módulo de de-codificación o en el módulo de microprocesador del receptor/decodificador.
La unidad de seguridad puede también ser implementada en el software puro sin algún hardware dedicado.
Tal implementación basada en software de la unidad de seguridad expone evidentemente un espacio de seguridad severo.

[0029] La Figura 1 resume las funcionalidades de bloque y sus datos asociados en el lado de transmisión según una forma de realización de la presente invención.
El contenido de multimedia original 100 se alimenta al proceso 11, que reivindica para garantizar que la calidad del contenido modificado 111 sea significativamente baja - de hecho, inservible - para cualquier adversario.
Como otra emisión del proceso, se genera el denominado objeto de control (CO), que es necesario para la reconstrucción del contenido de multimedia de origen 100 más tarde.
Una implementación de tal proceso 11 está descrita en la patente francesa WO 03/063445 A1 (dispositivo para grabación de transmisión segura y visualización de programas audiovisuales).
De hecho, si uno considera la técnica en la WO 03/063445 A1 como una operación criptográfica, luego CO se puede considerar como su clave privada/palabra de control, que será usada por el decodificador del cliente 2b para "desencriptar" el contenido inducido 111.
El CO corresponde a un conjunto de datos modificados en 111, que comprenden el valor original, el valor alterno y la ubicación donde se hizo la sustitución.
Un mecanismo de acceso condicional se debe aplicar al CO.
Según la forma de realización ejemplar en la figura 1, el DVB-CA se despliega como sigue.
El multiplexor 14 introduce CO en los datos multiplexados 141 (en la actualidad, los datos CO se refieren a 112, 121 y 131 completamente.
Estos tipos detallados de CO serán explicados en la siguiente explicación).
Luego, los datos multiplexados se encriptan por la entidad 15, que transforma los datos 141 al encriptado CO 151 y el asociado ECM, las estructuras EMM 152 - una estructura estandarizada de DVB-CA para habilitar la desencriptación en el lado de cliente.
Los datos 152 pueden ser cualquiera de los otros datos suplementarios necesarios para el proceso en el receptor.
Desarrollaremos el alcance de 152 más abajo.
En un escenario dentro de banda como en la figura 1, todos los datos, con el contenido inducido 111, el encriptado CO 151 y los controles 152 serán multiplexados nuevamente con el multiplexor 16.
El flujo multiplexado resultante 161 es adecuado para ser transmitido al cliente.

[0030] Según otra forma de realización de la presente invención, solo el contenido inducido 111 se transmite al receptor vía un canal de radiodifusión tradicional (satélite-, canal de cable, canal terrestre, ...). El contenido 111 puede hacerse disponible para la descarga libre de Internet o cualquier red de pares.
Una versión almacenada del contenido 111 en cualquier tipo de equipamientos de almacenamiento digital tal como clave USB, CD, DVD, disco blue-ray,... puede estar ya preparado para ser reproducido en el receptor del cliente.
Claramente, el encriptado CO 151 y los controles 152 se deben enviar al receptor del cliente vía un enlace unidifusión dedicado vía ADSL, 3G o conexión a Internet.

[0031] Según una forma de realización de la presente invención, el mensaje de control 152 puede contener la descripción de las condiciones de acceso del receptor.
Una vez recibido por la unidad de seguridad del receptor, el mensaje de control se desencripta y las condiciones de acceso se comparan con los derechos contenidos en la unidad de seguridad.
Si las condiciones de acceso vinculan con los derechos, el CO pueden ser después procesado.

[0032] Para reducir la calidad de un contenido multimedia, la técnica en la WO 03/063445 A1 según una forma de realización de la invención analiza el contenido de los medios dados.
Diferentes elementos de sintaxis cruciales serán luego extraídos: sus valores de origen se guardan en CO; datos alternos (AD) se generan en su ubicación.
La introducción de los AD genera el flujo inducido 111, que tiene la misma sintaxis que el flujo original 100.
Sin embargo, el contenido del flujo 111 es diferente completamente/degradado en comparación con el contenido 100 desde el punto de vista de percepción humano.
Las estructuras de 3-tuplas - incluyendo ubicaciones, los tamaños y los valores de origen de los elementos de sintaxis extraídos - se registran en CO de modo que más adelante, con un operador de sustitución simple, los valores originales de los elementos de sintaxis asociados y, por lo tanto, la calidad del contenido se pueden recuperar correctamente.

[0033] Según otra forma de realización de la presente invención, los AD también están registrados en CO para ser capaces de producir el PM.
Cada elemento de sintaxis extraído ahora se guarda como una estructura de 4-tuplas (valor de origen, AD, ubicación y tamaño) en CO.

[0034] La estructura de 3 o 4-tuplas se refiere como unidad de señuelo (LU) 112 de aquí en adelante.

[0035] La Figura 2 resume las funcionalidades de bloque y sus datos asociados en el lado de recepción según una forma de realización de la presente invención.
El flujo multiplexado 161 construido como en la figura 1 es ahora manejado en un modelo de receptor abierto.
El demultiplexor 21 separa los datos 161 en medios modificados 211, encriptado CO 212 y si EMM es aplicable, los datos ECM 213.

[0036] Según otra forma de realización de la invención, el encriptado CO 212 y los datos de control 213 se reciben directamente a partir de un enlace de unidifusión dedicado.

[0037] En la unidad de seguridad, los COs se descifran con claves que pertenecen al sistema de acceso condicional y en el caso de que las condiciones de acceso se incluyan en 213, las condiciones de acceso se controlan frente a las correctas almacenadas en la unidad de seguridad para autorizar el otro tratamiento del COs.

[0038] Cuando las condiciones de acceso se encuentran, el CO es luego procesado en vistas al equipamiento del decodificador del receptor con los datos de corrección marcados primarios PMCD 231 para decodificar el flujo modificado.

Insertación de la marca primaria

[0039] Según el primer aspecto de la invención, el CO contiene un conjunto de datos modificados, cada dato modificado comprende al menos el valor original, el valor alterno y la ubicación donde la modificación se hizo en el flujo original.

[0040] También según el primer aspecto de la invención, desde el CO, uno puede derivar solo las LUs (112,221) para calcular los datos de corrección, que a su vez consisten en datos solo de tipo PMCDs 231.
Detallaremos otro tipo de CD más adelante.

[0041] Según una forma de realización de la presente invención, el tratamiento de los datos 212 y 213 ocurre completamente dentro de la unidad de seguridad, que se puede considerar como la única entidad de confianza en el lado de cliente.
El proceso 22 desencripta LUs 221, luego las pasa a través de la entidad 23 antes de entregar a la unidad de desaleatorización 2b una forma nueva de datos: datos de corrección primarios marcados PMCDs 231.
El papel de PMCD debe ser combinado con los señuelos 211 en el recorrector 26 para producir los datos reconstruidos, que son en realidad los datos originales para cada uno de los elementos de sintaxis extraídos.
Tal contenido comprimido reconstruido 261 (idéntico al contenido original comprimido 100) es luego decodificado por la entidad 27 para hacerse un contenido significativo 271, que es utilizable para clientes.

[0042] Según una forma de realización de la presente invención, la funcionalidad principal del proceso 23 es convertir CO a CD.
En el alcance del primer aspecto de la invención, el proceso 23 transforma un LU 221 a un MPCD 231, con los pasos siguientes:

- copiar la compensación y tamaño de LU a PMCD
- seleccionar de forma arbitraria un valor a un operador matemático
- basándose en el operador elegido, los valores alternos (si existen) y el valor original almacenado en LU, el parámetro de clave puede ser derivado.

[0043] Según una forma de realización de la presente invención, el proceso se realiza en la unidad de decodificación del receptor estructurado abierto.
El tráfico de PMCD entre la unidad de seguridad y unidad de decodificación es el objetivo del ataque de palabra de control.

[0044] Según una forma de realización de la presente invención, los dos primeros campos de PMCD identifican la posición inicial al igual que la longitud de la corrección que se debe realizar en el recorrector 26.
Los últimos dos campos especifican cómo, es decir qué tipo de operador matemático, el proceso 26 debe aplicar el parámetro de clave a los señuelos para reproducir el valor de origen en la posición dada.

Tabla 1: el papel de los operadores matemáticos

Operador	Designación	Original	Alterno	Decodificador de ejecución 26	Par de clave.
Sobrescribir (O)	0			A □ B	A
Añadir (D)	1			B+(A-B) □ B	A-B

Sub (S)	2	A	B	B-(B+A) □ B	B+A
XOR (X)	3			B xor (AxorB) □ B	(A xor B)
1 desvío de bit a la izquierda y Delta (L)	4			B<<1+(A-B<<1) □ B	A-B<<1
1 desvío derecho de bit y Delta (R)	5			B>>1+(A-B>>1) □ B	A-B>>1

[0045] Según una forma de realización de la presente invención, siempre que el recorrector 26 recibe un PMCD con compensación X, tamaño I, operador matemático L y el parámetro de clave de valor A-B<<1, las operaciones siguientes deben ser realizadas:

- ir a la posición X en la unidad de acceso corriente de los señuelos 211
- extraer de esta posición I bits. Llamar a la cantidad extraída B.
- realizar el desvío binario de 1 bit a la izquierda en B, añadir el resultado a A-B<<1. Esta es la operación matemática designada para el operador L (ver tabla 1)
- la cantidad resultante (valor reconstruido) se fija de nuevo a los I bits empezando de la posición X.

[0046] En el supuesto de que los datos originales en el flujo original se denominen A, los datos simulados (valor alterno) en el flujo modificado se denomina B. Tabla 1 muestra varias operaciones matemáticas y el parámetro de clave asociado.
Podemos imaginar muchas de estas operaciones/operaciones concatenadas con todo tipo de manipulación de datos.
Cabe señalar que el modo en que la unidad de seguridad calcula el parámetro de clave es diferente de la operación ejecutada en el decodificador 26.
Por ejemplo, la unidad de seguridad, mientras se selecciona la adición D debería de hecho calcularse una sustracción ya que el parámetro de clave será k = A-B.
A consecuencia, el decodificador puede ejecutar una adición con el parámetro de clave y recuperar el valor A.

[0047] El PMCD por lo tanto comprende la designación de la operación matemática (ver designación en la tabla 1) y el parámetro de clave al igual que la ubicación de los datos simulados.
Una vez el decodificador recibe el PMCD, extrae los datos simulados B desde el flujo modificado y selecciona la operación matemática correcta (a partir de una biblioteca de todas las operaciones matemáticas) gracias a la designación de la operación matemática.
Los datos simulados B y el parámetro de clave k se usan por la operación matemática seleccionada para calcular los datos originales A.

[0048] El decodificador luego reemplaza los datos simulados B por el valor original recién calculado A.
Para cada dato de corrección, se ejecuta el mismo procedimiento para obtener los datos originales.

[0049] Ahora de nuevo al comportamiento de la unidad de seguridad.
Como hemos visto antes, todas las operaciones matemáticas permiten recuperar los datos originales A.
Un aspecto importante de la presente invención es el hecho de que la unidad de seguridad puede libremente seleccionar la misma operación.
Aprovechando esta virtud, la selección no es aleatoria para nada, sino que se dicta por al menos un parámetro interno de la unidad de seguridad, es decir, la marca primaria PM.

[0050] Un ejemplo simple de tal parámetro interno es la dirección única de la unidad de seguridad.
Imaginemos que tenemos una selección de 16 operaciones matemáticas y la dirección única UA contiene 32 bits.
Podemos luego dividir la UA en 8 bloques de 4 bits, cada bloque de datos sirve para apuntar a la operación matemática seleccionada.
Cada vez que se producen unos datos de corrección por la unidad de seguridad, otro bloque de datos de la UA se utiliza para seleccionar la operación.
Siempre que los datos de corrección 8 se haya generado por la unidad de seguridad, la UA completa se puede saber leyendo la designación de la operación matemática contenida en los datos de corrección sucesivos enviados al decodificador.
Un contador de barrido se utiliza para barrer los 8 bloques y se incrementa a cada producción de los datos de corrección.
Este contador de barrido girará de 1 a 8.

[0051] Según una forma de realización de la presente invención, la combinación de los valores operadores en un número predefinido de PMCDs se puede aprovechar para codificar/insertar el ID de la tarjeta inteligente como el parámetro interno del receptor.
Forzado por el ID, el valor operador de PMCD ya no es un factor libre.
Aún, la recorrección del contenido comprimido 261 sigue siendo posible gracias a la sintonización apropiada del

relativo parámetro de clave.
Tabla 2 ilustra la codificación de los IDs vía los valores operadores de 5 PMCDs.
Los valores posibles de un PMCD se toman de la tabla 1.

[0052] Según una forma de realización de la invención, los datos de control 152 pueden además contener alguna información sincronizada que permita definir qué bloque debería usarse.
La vía más simple es añadir un bit único en el PMCD para resincronizar el contador de barrido.
Otra resincronización se puede decidir en el lado de transmisión por ejemplo para cada grupo de dibujos GOP.

[0053] Otra vía para seleccionar el bloque del parámetro interno que influirá la selección de la operación matemática se basa en el uso de la información de ubicación.
Como previamente se ha explicado, la ubicación es parte del objeto de control.
Luego es posible usar los últimos 5 bits de la ubicación para dirigir el bit (o bits) del parámetro interno que decide la selección.
Alternativamente, una función control de la ubicación puede utilizarse para crear una mejor entropía.
El valor de control luego seleccionará el primer bit, participando a la selección de la operación matemática.

[0054] El ejemplo de arriba del parámetro interno se da para la dirección única de la unidad de seguridad.
Cabe destacar que, según otra forma de realización, la función de la UA se puede usar antes que la misma UA.
Esta función puede ser una función criptográfica con una clave conocida por la unidad de seguridad y el centro de gestión.
Esta clave es común para todas las unidades de seguridad.

[0055] El parámetro interno usado para la etapa de selección puede ser una dirección de grupo, es decir, común a un grupo de unidades de seguridad.

[0056] Un comando se puede añadir al objeto de control CO para activar o desactivar esta función.
En caso de desactivación, la misma operación matemática será usada para todos los CD.

Tabla 2: inserción de ID implica la combinación de operador de CDs

	PMCD 1	PMCD 2	PMCD 3	PMCD 4	PMCD 5	ID
Combinación 0	O	O	O	O	O	0
Combinación 1	O	O	O	O	D	1
....						
Combinación 4^5-1	R	R	R	R	R	4^5- 1

[0057] Según otra forma de realización de la presente invención, los CDs afectados por la desactivación de la función UA se consideran como un CD libre 232, es decir, su operador matemático se puede seleccionar de forma arbitraria sin ninguna restricción.
Su papel es únicamente para la reconstrucción de los valores originales.

[0058] Además del soporte de un ID, algunos PMCDs pueden ser también aprovechados para codificar algún control/corrección de algoritmos como la codificación Reed-Salomon, codificación Hamming, etc, que se calculan sobre el mismo ID.
Gracias a estos algoritmos, el proceso de detección ID más adelante puede recuperar incluso el valor adecuado del parámetro interno en el caso de diferentes PMCDs dañados, lo que es útil en el caso de ataque de colusión.

Inserción de la marca secundaria:

[0059] Según el segundo aspecto de la invención, los COs pueden además contener MUs 121, 222.
En los datos de corrección CD, los datos de corrección secundarios de marca SMCD 241 también se pueden encontrar.

[0060] Según una forma de realización de la presente invención, un proceso denominado de pre-señalización 12 se añade como en la figura 1.
Se suele insertar la denominada segunda marca (SM).
En realidad, esto puede ser un proceso convencional de marca de agua/toma de huella genética, que analiza el contenido de entrada 100 para insertar un número determinado de identificaciones ID en una manera imperceptiva.
La identificación de la unidad de seguridad es un caso del parámetro interno, como se ha discutido en detalle en el proceso de inserción del PM.

[0061] Una restricción debe tenerse en cuenta mientras se ejecuta el proceso de toma de huella genética.
Esa inserción de cada ID modificará como mucho, números fijados, bien localizados de elementos sintácticos en

el medio (de aquí en adelante estos elementos son referidos como Mark Hookers MHs).
Por ejemplo, en el caso de un vídeo de bastidor, la inserción de N número de IDs modificará los valores de como mucho 5 píxeles, con las ubicaciones fijas { (x_{-1},y_1), (x_2,y_2),..., (x_5,y_5)}.
Según una forma de realización de la presente invención, cada uno de estos píxeles puede coger uno de 2 valores de (luminancia) dedicados a insertar todos los IDs (esto implica N <= 2^5=31).
En otras palabras, existe un conjunto de 10 valores para estos 5 píxeles como sigue: {(V_{11},V_{12}), (V_{21},V_{22}),...,(V_{51},V_{52})}, donde V_{ij} con j {1,2} y i {1,2, ...5}. Estos valores V_{ij} son seleccionados de modo que la inserción de un ID se puede definir únicamente como una combinación de los valores posibles sobre estos 5 píxeles.
Tal aplicación se ilustra en la tabla 3.

Tabla 3: la inserción ID implica los valores alternos de cada píxel

	Píxel 1	Píxel 2	Píxel 3	Píxel 4	Píxel 5	Derivado ID
Combinación 0	V_{11}	V_{21}	V_{31}	V_{41}	V_{51}	0
Combinación 1	V_{11}	V_{21}	V_{31}	V_{41}	V_{52}	1
....						
Combinación 31	V_{12}	V_{22}	V_{32}	V_{42}	V_{52}	31

[0062] Correspondientemente, se crea el componente nuevo de CO, es decir, la unidad de señalización (MU) 121, que contiene la posición, el tamaño y los dos valores V_{ij} de cada MH.
Es decir, que cada MH se registra como una estructura 4-tupla (valor dedicado 1, valor dedicado 2, ubicación y tamaño) en MU.
En el caso de no binario MU, la estructura de MU será extendida con tantos valores como sean posibles los valores en cada ubicación de píxel.

[0063] Según una forma de realización de la invención, el mapeo en la tabla 3 se incorpora con algún control/algoritmos de corrección como codificación Reed-Salomon, codificación Hamming, etc, que se calcula sobre el mismo ID.
Gracias a estos algoritmos, el ID proceso de detección más adelante puede incluso recuperar el valor correcto incluso si resultan diferentes SMCDs dañados, que es útil en el caso de ataque de colusión.

[0064] El proceso 24 toma la responsabilidad de convertir cualquier MUs a SMCDs como sigue:
- copiar la compensación y tamaño de MU a SMCD,
- determinar el valor apropiado V_{ij} como en la tabla 3 según SM,
- seleccionar de forma arbitraria un valor para el operador (por lo tanto, no es un PMCO)
- basándose en el operador seleccionado y el V_{ij}, el parámetro de clave puede ser derivado.

[0065] Según otra forma de realización de la presente invención, el post marcado 24 puede activamente generar el V_{ij} por sí mismo.
En este caso, la estructura de MU necesariamente no contiene los valores dedicados V_{ij}, lo que puede drásticamente salvar el ancho de banda del canal dedicado desplegado para la transmisión del CO 151 y datos de control 152.
Gracias a la información 152, el proceso 24 puede realizar la marca de agua idéntica/toma de huella genética como en 12.
Por lo tanto, el V_{ij} se puede derivar directamente en la unidad de seguridad en el receptor.

[0066] Según una forma de realización de la presente invención, cualquier SMCD se puede considerar como un CD libre 232, es decir, su operador matemático se puede seleccionar libremente sin ninguna restricción.

[0067] Cabe destacar que las sintaxis de LUs (112,221) y MUs (121,222) son diferentes, pero aquellas de PMCD, (231) SMCD (241) y CD libre (232) son idénticas, lo que mejora la seguridad de las marcas.
Estos tres tipos de CD: PMCD, SMCD y CD libres son responsables de derivar los datos reconstruidos para recorregir el contenido correctamente.
Además, el PMCD y SMCD llevan la marca primaria introducida en el operador y la segunda marca oculta en los datos reconstruidos respectivamente.
Los CDs libres son menos importantes relativamente desde el punto de vista del trazado del uso no autorizado.
Intuitivamente, los piratas informáticos deberían tratar de abandonar el PMCD y SMCD - estos pueden tener menos impacto en la reconstrucción del vídeo - mientras dejan intactos todos los CDs libres para reconstruir tantos elementos sintácticos extraídos/modificados como sea posible.
Tal manipulación excluye cualquier impermeabilización para el trazado implicado en PM y SM.
Inspeccionando el tráfico de CDs, los piratas informáticos difícilmente distinguen un tipo de otro gracias a la estructura de los datos similar del CDs.
Por lo tanto, la eliminación de todos los PMCD y SMCD y el mantenimiento solo de CD libres en la unidad de descodificación 2b no son para nada baladíes.

Escenario combinado del PM y SM

[0068] Según una forma de realización de la presente invención, un CO (CD) puede jugar un papel doble: este puede ser LU y MU (PMCD y SMCD) al mismo tiempo.
Dos procesos independientes 11 y 12 pueden producir un elemento sintáctico extraído y un MH en la misma ubicación.

[0069] Si la unidad sincronizada 13 detecta una coincidencia en MHs extraídos y elementos sintácticos, el correspondiente LU y el MU será sustituido por un componente nuevo de CO, es decir, unidad combinada (CU) 131.

[0070] Según una forma de realización de la presente invención, CU es un dato de 5-tuplas, incluyendo la posición y el tamaño de elemento sintáctico extraído/MH, 2 valores V_{ij} y ADs.

[0071] Según una forma de realización de la presente invención, CU tiene la misma estructura que LU.
En este caso, el proceso 24 mismo generará los valores dedicados V_{ij} dentro de la unidad de seguridad.

[0072] Para crear el CD de este tipo de CO, los CUs son primero tratados como MUs.
Es decir, que serán en primer lugar alimentados al proceso 24 para insertar una marca secundaria, es decir, determinar el V_{ij} 242.
Después, el SMCD resultante será dirigido de nuevo al proceso 23 para añadir la marca primaria, es decir, determinar el operador (y el parámetro clave asociado).

[0073] La Figura 3 describe los datos de entrada necesarios para detectar la marca según una forma de realización de la presente invención.
Los principios para detectar las marcas primarias o secundarias son similares.
Para el anterior, los datos 301 son los CDs.
Para localizar los PMCDs desde los CDs libres posibles, el proceso 31 requiere el PMC 132 como los datos de control 302 adicionales.
Para el caso de marcas secundarias, los datos consumibles 271 se convierten en los datos 301, mientras los datos de control 302 corresponden al SMC 133.

REIVINDICACIONES

1. Método para la decodificación de un primer flujo de vídeo codificado para obtener un flujo de vídeo reconstruido que corresponde a un flujo de vídeo original por un decodificador que comprende al menos una unidad de seguridad y una unidad de decodificación, este método incluye las etapas de:

• recepción por el decodificador del primer flujo codificado donde una pluralidad de valores originales del flujo de vídeo original en una pluralidad de ubicaciones han sido modificados por valores alternos,

• recepción por la unidad de seguridad de un objeto de control que comprende un conjunto de datos de control, cada conjunto comprende datos que permiten determinar al menos el original, el valor alterno al igual que la ubicación donde valores alternos han sido introducidos en el primer flujo codificado,

• para cada conjunto de datos de control, cálculo de un parámetro de clave asociado a una operación matemática, esta operación y el parámetro de clave asociado están seleccionados entre una pluralidad de diferentes operaciones, dichas operaciones matemáticas permiten obtener un valor reconstruido del valor alterno gracias al parámetro de clave,

• variación del proceso de selección de dicha operación matemática basada en un primer parámetro interno de la unidad de seguridad para cada conjunto de datos de control

• transmisión a la unidad de decodificación de un conjunto de datos de corrección que corresponde con la designación de la operación matemática, el parámetro de clave y la ubicación del valor alterno,

• recepción de los datos de corrección por la unidad de decodificación y,

• cálculo del valor reconstruido que corresponde con los datos de corrección y los valores alternos recuperados del primer flujo codificado

• reemplazo del valor alterno por el valor reconstruido en el primer flujo codificado para obtener el flujo de vídeo reconstruido.

2. Método, según la reivindicación 1, donde dicho valor reconstruido es igual al valor original para obtener el flujo de vídeo original.

3. Método, según la reivindicación 1 o 2, donde el primer parámetro interno se divide en una pluralidad de bloques de datos, el proceso de selección está basado en un bloque de datos, cada bloque de datos se usa consecutivamente para este proceso de selección.

4. Método, según las reivindicaciones 1 a 3, donde el primer parámetro interno representa la dirección única del decodificador, el primer parámetro interno es la dirección única o es una función de la dirección única.

5. Método, según la reivindicación 1, donde dicho valor reconstruido es un valor personalizado, dicho valor personalizado se determina según las etapas siguientes:

- extraer el valor original del objeto de control,
- calcular el valor personalizado basado en el valor original y un segundo parámetro interno del decodificador,
- utilizar el valor personalizado para calcular el parámetro de clave.

6. Método, según la reivindicación 1, donde dicho objeto de control comprende además un conjunto de valores dedicados asociados al valor original en los datos modificados, dicho valor reconstruido es un valor personalizado, dicho valor personalizado se determina según las etapas siguientes:

- extraer el valor original y el conjunto de valores dedicados del objeto de control,
- seleccionar como valor personalizado entre el valor original y el conjunto de los valores dedicados basados en un segundo parámetro interno del decodificador,
- utilizar el valor personalizado en vez del valor original para calcular el parámetro de clave.

7. Método, según la reivindicación 5 o 6, donde el segundo parámetro interno se divide en una pluralidad de bloques de datos, el proceso de selección está basado en un bloque de datos, cada bloque de datos se usa consecutivamente para este proceso de selección.

8. Método, según cualquiera de las reivindicaciones 5 a 7, donde el segundo parámetro interno representa la dirección única del decodificador, el segundo parámetro interno es igual que la dirección única o es una función de la dirección única.

9. Método, según cualquiera de las reivindicaciones 5 a 8, donde el valor personalizado produce una distorsión imperceptible para la percepción humana en comparación con el flujo de vídeo original.

10. Método, según cualquiera de las reivindicaciones 1 a 8, donde el valor alterno introduce una distorsión severa en el primer flujo de vídeo codificado en comparación con el flujo de vídeo original.

11. Método, según cualquiera de las reivindicaciones 1 a 8, donde la introducción del valor alterno en el primer flujo codificado preserva la misma sintaxis que el flujo de vídeo original.

12. Método, según cualquiera de las reivindicaciones anteriores, donde la unidad de seguridad es un módulo de tarjeta inteligente.

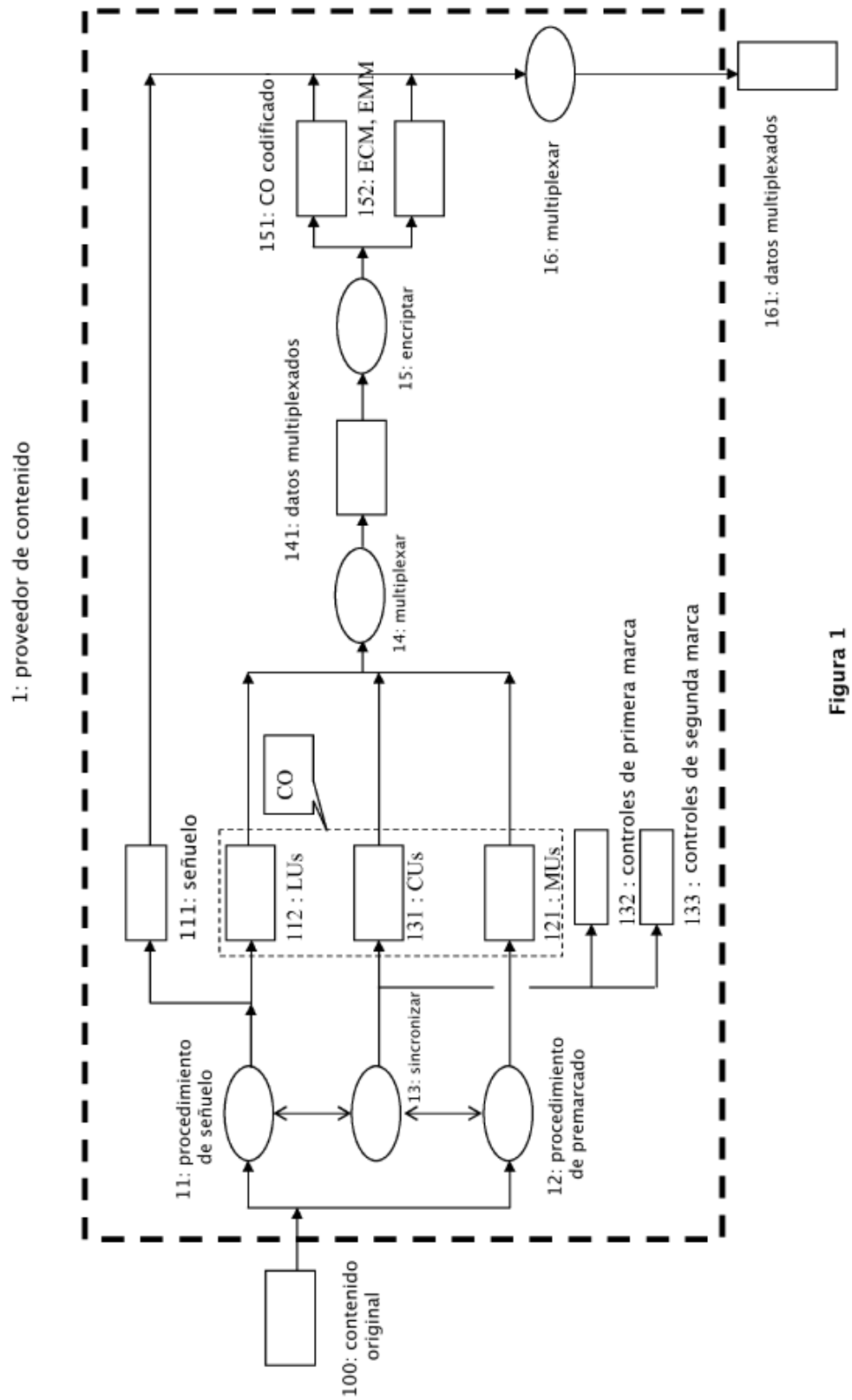
1: proveedor de contenido
100: contenido original
11: procedimiento de señuelo
12: procedimiento de premarcado
13: sincronizar
111: señuelo
112 : LUs
131 : CUs
121 : MUs
CO
132 : controles de primera marca
133 : controles de segunda marca
14: multiplexar
141: datos multiplexados
15: encriptar
151: CO codificado
152: ECM, EMM
16: multiplexar
161: datos multiplexados

Figura 1

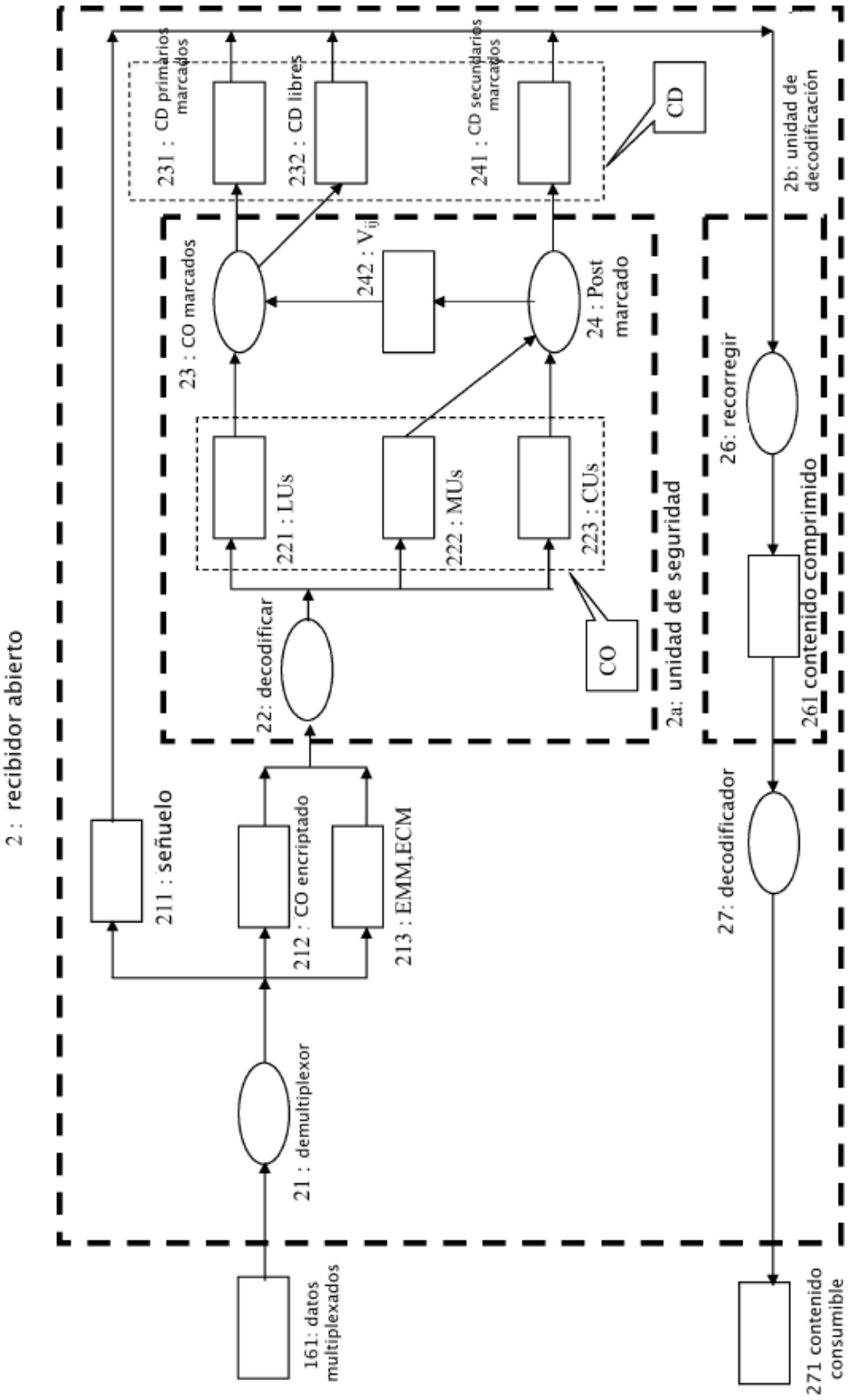
2 : recibidor abierto
161: datos multiplexados
21 : demultiplexor
211 : señuelo
212 : CO encriptado
213 : EMM,ECM
22: decodificar
2a: unidad de seguridad
23 : CO marcados
221 : LUs
222 : MUs
223 : CUs
CO
242 : Vij
24 : Post marcado
231 : CD primarios marcados
232 : CD libres
241 : CD secundarios marcados
CD
2b: unidad de decodificación
26: recorregir
261 contenido comprimido
27: decodificador
271 contenido consumible

Figura 2

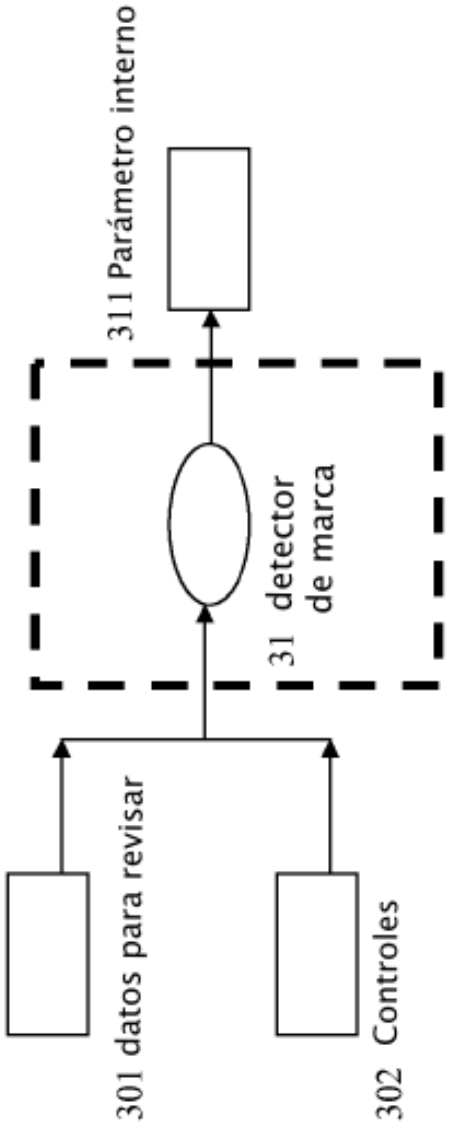
311 Parámetro interno
31 detector de marca
301 datos para revisar
302 Controles

Figura 3