(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 437 678**

(51) Int. CI.:

H04N 21/418 (2011.01)
H04N 21/266 (2011.01)
H04L 29/06 (2006.01)
H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.11.2010 E 10191981 (9)**

(97) Fecha y número de publicación de la concesión europea: **11.09.2013 EP 2328316**

(54) Título: **Control de acceso a un contenido digital**

(30) Prioridad:

20.11.2009 FR 0958243

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.01.2014

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

GUIONNET, CHANTAL y
FEVRIER, PIERRE

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Control de acceso a un contenido digital

La invención se refiere al campo de la transmisión de contenidos multimedia en redes de transmisión y, más particularmente, al control de acceso a estos contenidos multimedia.

En este tipo de redes de transmisión, se transmiten unos contenidos multimedia de manera codificada, y no pueden restituirse en el receptor más que en ciertas condiciones. Las redes de transmisión de contenidos multimedia se pueden utilizar particularmente para aplicaciones de televisión de pago con el fin de controlar el acceso al contenido digital, se prevé difundirlas bajo una forma codificada. Para acceder a ellas, un receptor de este contenido digital codificado debe recuperar la clave de codificación (o CW por 'Control Word') o las claves de codificación que están asociadas con ella con el fin de poder decodificar el contenido digital recibido.

Son conocidos dichos sistemas de control de acceso en los que estos mensajes de control de acceso se difunden de manera repetida y de manera sincronizada con el contenido digital. Estos mensajes de control son del tipo ECM (por 'Entitlement Control Message') e indican, en una forma codificada, la o las claves de codificación a utilizar para decodificar el contenido digital. Este tipo de mensaje de control de acceso indica la vez la clave de codificación en una forma codificada e igualmente unos criterios de acceso que están asociados con el contenido digital. Por otro lado, se vinculan respectivamente unos derechos de acceso a los receptores. Estos derechos de acceso se puedan recibir mediante unos mensajes individualizados del tipo EMM (por 'Entitlement Management Message'). Este tipo de mensaje es un mensaje personalizado o no que se puede emitir con destino en un único abonado o incluso con destino en un grupo de abonados.

En este contexto, con la recepción del mensaje de control de acceso ECM, el receptor controla si sus derechos de acceso cumplen con los criterios de acceso asociados al contenido digital. Si ese es el caso, la clave de codificación transportada en una forma codificada en el mensaje de control de acceso puede ser decodificada y utilizada entonces para acceder al contenido digital.

La decodificación de la clave de codificación se puede realizar si el receptor dispone previamente de una clave de explotación. Esta clave de explotación está comprendida generalmente en los derechos que receptor ha recibido a través de un mensaje del tipo EMM. En consecuencia, si los derechos del receptor son compatibles con los criterios de acceso del ECM, y si el receptor posee la clave de explotación asociada al ECM, el receptor está autorizado a decodificar la clave de codificación recibida en asociación con el contenido digital, y entonces está en situación de decodificar el contenido digital.

En estas condiciones, el control de acceso se efectúa sobre la base de los derechos de acceso atribuidos a cada receptor. De ese modo, sólo un usuario que disponga derechos de acceso correspondientes a los criterios de acceso puede decodificar a continuación la o las claves de codificación requeridas y acceder al contenido digital difundido.

El documento US 2009/190757 A1 se refiere particularmente a los sistemas y métodos de difusión de mensajes de gestión de derechos (EMM) que utilizan una ventana de envío planificada. D1 divulga la recepción de una ventana de difusión de mensajes EMM desde un sistema de distribución, la escucha de los mensajes EMM durante la ventana de difusión de mensajes EMM y la recepción de los mensajes EMM desde el sistema de distribución durante la ventana de difusión de mensajes EMM.

El documento EP 1995933 A1 se relaciona con unos sistemas y métodos de gestión de distribución de contenidos tales como unos programas televisados que incluyen un sistema de gestión de difusión dispuesto para generar el envío de contenido, un sistema de gestión de cuentas dispuesto para generar las solicitudes de utilización de contenido y las comunicaciones de/hacia unos terminales de usuario, así como un sistema de tratamiento conectado al sistema de gestión de cuentas y dispuesto para analizar las solicitudes en relación con las informaciones disponibles al respecto de los usuarios con el fin de determinar si los recursos requeridos para el suministro de contenido a los terminales pueden estar compensados teniendo en cuenta una cantidad de recursos de utilización previamente asignados.

El documento EP 1947853 A1 se refiere particularmente a un servidor de contenidos dispuesto para añadir un identificador de clave de codificación durante la codificación del contenido con dicha clave, y para transmitir el contenido concatenado con dicho identificador a un dispositivo de restitución de contenidos, al mismo tiempo que transmite la clave de codificación a un servidor suministrador de mensajes comerciales. El servidor suministrador de los mensajes comerciales incorpora la clave de codificación en los datos de mensajes comerciales y envía los datos de mensajes comerciales en los que está incorporada la clave de codificación correspondiente al identificador recibido de parte del dispositivo de restitución de contenidos, al dispositivo de restitución de contenidos. El dispositivo de restitución de contenidos transmite el identificador de la clave de codificación al servidor suministrador de los mensajes comerciales y reproduce los datos de los mensajes comerciales recibidos de parte del servidor suministrador de mensajes comerciales para decodificar el contenido utilizando la clave de codificación incorporada

en los datos de los mensajes comerciales.

El documento EP 1968316 A1 tiene por objetivo particularmente impedir la pérdida de ganancias unida a los grabadores digitales dispuestos para no grabar los mensajes publicitarios. La solución se apoya en un procedimiento de control de acceso condicional a unos contenidos de audio/video que comprenden al menos una sección publicitaria. El procedimiento define una información de control asociada al contenido de audio/video y almacenada en un módulo de seguridad, y actualiza la información de control en el módulo de seguridad con ayuda de informaciones de condición incluidas en un mensaje de control que se relaciona con la sección publicitaria. El procedimiento comprende la recepción por parte del módulo de seguridad del mensaje de control que se refiere a la sección principal de contenido del contenido de audio/video y que contiene una información de condición ligada a la información de control almacenada. El procedimiento comprende la verificación de que la información de condición corresponde a la información de control y, si éste es el caso, el envío al grabador digital de una señal de autorización que permita el acceso a la sección principal de contenido del contenido de audio/video.

La presente invención tiene por objetivo mejorar la situación.

Un primer aspecto de la presente invención propone un procedimiento de gestión de acceso del receptor a un contenido digital transmitido en una red de comunicación en una forma codificada; comprendiendo dicho procedimiento de gestión de acceso las etapas siguientes en el receptor:

/a/ recibir un mensaje de control de acceso,

/b/ obtener un mensaje de control de acceso completo añadiendo una información complementaria a dicho mensaje de control de acceso,

/c/ obtener una clave de decodificación del contenido en base al mensaje de control de acceso completado, y

/d/ decodificar el contenido digital transmitido con ayuda de la clave de decodificación obtenida;

en el que dicha información complementaria es suministrada por un usuario.

Se entiende por el término ‘receptor’ todo tipo de receptor de contenido digital transmitido en una red de comunicación sin que se vincule ninguna limitación ni al tipo de red de comunicación ni tampoco al protocolo de transmisión utilizado para esta transmisión. Un contenido puede corresponder a cualquier tipo de datos transmitidos, como por ejemplo unos datos de video, audio, unas imágenes, sonido, todo tipo de documentos, etc.

No se vincula ninguna limitación en cuanto a la transmisión del contenido digital, en la forma de un flujo de datos, a la presente invención de ninguna forma. Se puede concebir por ejemplo una difusión general del contenido digital.

Se entiende por la expresión ‘mensaje de control de acceso’ todo tipo de mensaje emitido que permita efectuar un control del acceso del receptor a este contenido digital. Un mensaje de este tipo de control de acceso puede ser un mensaje del tipo ECM o incluso un mensaje del tipo EMM. En el caso en que mensaje de control es un mensaje del tipo ECM, contiene por sí mismo la clave de decodificación, en el caso en que mensaje de control sea un mensaje del tipo EMM, contiene unas informaciones previas (como unos derechos de acceso o incluso unas claves de acceso) para el tratamiento del mensaje posterior de tipo ECM. De ese modo, tanto si es de manera directa a través del mensaje ECM como incluso si es de manera indirecta a través de un mensaje EMM seguido de un mensaje de tipo ECM, a continuación de la recepción de este mensaje de control de acceso de acuerdo con un modo de realización de la presente invención, el receptor está en condiciones de obtener la clave de decodificación del contenido digital.

El contenido digital se transmite en una forma codificada y puede ser decodificado con ayuda de una clave de decodificación que puede corresponder a la clave de codificación del contenido digital o que puede igualmente ser diferente. Esta clave de decodificación no puede obtenerse más que si el usuario ha suministrado una información complementaria para completar el mensaje de control de acceso recibido.

De manera general, se prevé en este caso transmitir un mensaje de control de acceso al que no se puede aplicar un tratamiento para obtener la clave de decodificación, tanto si es de manera directa, es decir en el caso en que el mensaje recibido contiene en sí mismo la clave de decodificación, como por ejemplo un mensaje del tipo ECM, o bien de manera indirecta, es decir en el caso en que el mensaje recibido permite obtener la clave de decodificación contenida en un mensaje recibido posteriormente, como por ejemplo un mensaje del tipo EMM. Más precisamente, en un modo de realización, el mensaje de control de acceso transmitido es incompleto. Faltan ciertos datos para permitir su tratamiento.

En efecto, en un modo de realización, el receptor espera un mensaje de control de acceso de acuerdo con un cierto formato para permitir un tratamiento correcto. Particularmente, en el caso de que el mensaje de control de acceso recibido sea un mensaje del tipo ECM, el formato esperado en el receptor comprende unos criterios de acceso, una

clave de decodificación del contenido digital, y una firma digital del conjunto de estos datos. En el caso de que se trate de un mensaje del tipo EMM, el formato esperado comprende unos derechos de acceso o incluso unas claves de acceso, y una firma digital. Al ser incompleto el mensaje de control de acceso recibido, conviene completarlo con una información complementaria para permitir su tratamiento en la recepción.

Se entiende por la expresión 'información complementaria' cualquier información que permita completar el mensaje de control de acceso recibido con el fin de obtener la clave de decodificación en claro del contenido digital difundido.

No se vincula ninguna limitación a la presente invención en relación al mecanismo implementado para que el receptor y una entidad de transmisión a cargo de la transmisión del mensaje de control de acceso estén en cualquier forma sincronizados con la información complementaria requerida para el mensaje de control de acceso transmitido. Se puede prever particularmente que el mensaje de control de acceso indique por sí mismo el tipo de información complementaria que el usuario debe suministrar o bien se pueden concebir igualmente que el receptor conozca previamente el tipo de información complementaria que falta en el mensaje de control de acceso recibido. De ese modo, el usuario puede ser requerido por un medio cualquiera para que suministre esta información complementaria. No se vincula ninguna limitación a la presente invención con relación al mecanismo utilizado para que el usuario ponga de una información complementaria de ese tipo. Se puede prever hacerle adivinarla o también transmitirla a través de la red de comunicación, por ejemplo, o incluso mostrar este dato durante la difusión de un programa publicitario.

Se puede prever igualmente que el usuario suministre una información complementaria que no corresponda a los datos necesarios para completar el mensaje de control de acceso. De este modo, la información complementaria puede representar particularmente menos datos que los necesarios para completar el mensaje de control de acceso recibido. El receptor puede entonces adaptarse para completar correctamente el mensaje de control de acceso.

En un modo de realización, el mensaje de control de acceso completado complementario puede corresponder entonces al menos a una parte de la clave de decodificación bajo forma codificada. En este caso, el mensaje de control de acceso recibido es incompleto en el sentido en el que no contiene, completamente o al menos parcialmente, la clave de decodificación a utilizar para decodificar el contenido digital.

Se puede prever igualmente que el mensaje de control de acceso a completar indique las claves de decodificación en forma codificada y al menos un criterio de acceso, y la información complementaria puede corresponder entonces al menos a uno de entre una parte de la clave de decodificación en forma codificada y a una parte de dicho criterio de acceso. De ese modo, el mensaje de control de acceso a completar puede estar incompleto en el sentido de que no indique al menos uno de los criterios de acceso previstos inicialmente. No podrá ser tratado correctamente en el receptor más que en el caso de que se concrete mediante el al menos un criterio de acceso faltante. Se puede prever igualmente que los datos faltantes en el mensaje de control sean relativos a su firma digital. De manera más general, se puede prever retirar del mensaje de control de acceso cualquier tipo de dato que contenga de acuerdo con un formato conocido por el receptor.

El mensaje de control de acceso completo puede ser un mensaje previo que permita tratar un mensaje posterior que indique la clave de decodificación. Ese es el caso cuando el mensaje de control de acceso es un mensaje del tipo EMM.

El mensaje de control de acceso puede ser un mensaje individual, como por ejemplo un mensaje del tipo EMM, un mensaje de grupo, o un mensaje general, como por ejemplo un mensaje del tipo ECM. Se puede prever en efecto en un sistema de control de acceso existente retirar una información al menos de un mensaje del tipo EMM, como por ejemplo un derecho de acceso o una clave de explotación codificada puesto que este tipo de mensaje permite transmitir los derechos de acceso de un usuario.

Utilizando como mensaje de control de acceso un mensaje individual del tipo EMM, por ejemplo, se está en condiciones de personalizar la información complementaria a suministrar por el usuario para acceder al contenido digital. En el contexto de un juego de televisión, es posible igualmente limitar fácilmente el número de jugadores autorizados a participar en este juego y no transmitir más que a un número limitado de receptores los mensajes EMM que suministran los derechos de acceso a este juego.

En un modo de realización de la presente invención, el mensaje de control de acceso indica una pluralidad de informaciones complementarias y, en este caso, el usuario puede seleccionar una de entre la pluralidad para suministrarla como la información complementaria. Si el usuario realiza una buena elección, el receptor tiene entonces una clave de decodificación válida para decodificar el contenido digital. Si realiza una mala elección, el mensaje de control de acceso puede ser tratado eventualmente correctamente, pero la clave de decodificación obtenida no permite decodificar el contenido digital.

En un modo de realización de la presente invención, la información complementaria se recibe en otro contenido digital. Por ejemplo, se puede prever transmitir la información complementaria requerida para completar el mensaje de control de acceso transmitido en un contenido digital transmitido en claro, como en el curso de una secuencia

publicitaria. De ese modo, sólo un usuario atento al curso de esta secuencia puede recuperar la información complementaria que le permita a continuación acceder a un contenido digital que sigue, transmitido o difundido en una forma codificada.

En otro modo de realización, las etapas siguientes se pueden implementar además en el receptor:

/1/ recibir y restituir una pregunta, y

/2/ recibir de un usuario una respuesta a dicha pregunta;

en el que dicha respuesta corresponde a la información complementaria.

Estas etapas pueden ser implementadas ventajosamente, particularmente en el contexto de un juego de televisión. En efecto, es posible entonces no dar acceso, en el sentido de decodificar, a continuación de una pregunta más que si la respuesta a la pregunta anterior es correcta. O, si la respuesta a la pregunta anterior corresponde a una información complementaria en el sentido de la presente invención, puede fácilmente dar acceso a un contenido digital transmitido en una forma codificada como se ha expuesto anteriormente.

Se puede de ese modo añadir fácilmente un nivel de control de acceso basado en una información complementaria al mensaje de control de acceso recibido, a suministrar al receptor. Se pueden implementar entonces fácilmente nuevos servicios diferentes en este entorno.

Estas disposiciones permiten ventajosamente una gran flexibilidad en la realización de un control de acceso a un contenido digital transmitido en una red, quedando facilitada la realización de un control de este tipo, particularmente en el contexto de un sistema existente.

En efecto, en un modo de realización, es suficiente prever retirar una información del mensaje de control de acceso a enviar y prever un mecanismo para solicitar esta información en el receptor. Sin embargo, es posible conservar ventajosamente unos controles similares a aplicar al mensaje de control de acceso completado de ese modo.

Se puede prever o bien autorizar el acceso al contenido digital en base a la información complementaria, o bien incluso autorizar el acceso al contenido digital en base a la vez en la información complementaria y además en unos criterios de acceso asociados al contenido digital.

Puede ser procedente para ciertas aplicaciones, o en ciertos sistemas de control de acceso, controlar el acceso a un contenido digital a la vez en base a una información complementaria suministrada por un usuario en un receptor y en base a unos criterios de acceso requeridos en relación a los derechos de acceso que dispone el receptor considerado. Cumplir con unos criterios de acceso puede corresponder, por ejemplo, a verificar si un abonado específico está presente y válido, o incluso verificar si una cuenta de usuario del receptor está bastante llena para poder pagar el acceso a un contenido cuyo coste, o débito a efectuar, constituye el criterio de acceso.

Con el fin de no autorizar el acceso más que en base a la información complementaria, en un sistema existente, es fácil utilizar un mensaje del tipo ECM como mensaje de control de acceso de acuerdo con un modo de realización y prever que el número de criterios de acceso indicado en este mensaje sea 0. Se puede prever igualmente indicar un número de criterios no nulos pero precisando que no hay ningún control a efectuar.

Un segundo aspecto de la presente invención propone un procedimiento de gestión de acceso del receptor a un contenido digital transmitido en una red de comunicación en una forma codificada; comprendiendo dicho procedimiento de gestión de acceso las etapas siguientes en una entidad de transmisión:

/a/ componer un mensaje de control de acceso, comprendiendo dicho mensaje de control de acceso unas informaciones adaptadas para un tratamiento en el receptor,

/b/ obtener un mensaje de control de acceso a completar retirando al menos una de dichas informaciones de dicho mensaje de control de acceso, y

/c/ transmitir a dicho receptor el mensaje de control de acceso a completar, habiéndose de completar dicho mensaje transmitido mediante la información complementaria suministrada por un usuario.

Ventajosamente esta entidad de transmisión permite transmitir un mensaje de control de acceso incompleto de acuerdo con un modo de realización. No se vincula ninguna limitación a la presente invención en relación al mecanismo que permita que el receptor sea informado del tipo de información faltante en el mensaje de control de acceso recibido.

Un tercer aspecto de la presente invención propone un receptor adaptado para la realización de un procedimiento de gestión de acceso de acuerdo con el primer aspecto de la presente invención.

Un cuarto aspecto de la presente invención propone una entidad de transmisión adaptada para la realización de un procedimiento de control de acceso de acuerdo con el segundo aspecto de la presente invención.

Un quinto aspecto de la presente invención propone un sistema de control de acceso a un contenido digital, que comprende una entidad de transmisión de acuerdo con el cuarto aspecto de la presente invención, y al menos un receptor de acuerdo con el tercer aspecto de la presente invención.

Un sexto aspecto de la presente invención propone un programa de ordenador que comprende unas instrucciones para la realización del procedimiento de acuerdo con el primer aspecto de la presente invención, cuando se ejecuta este programa por un procesador.

Un séptimo aspecto de la presente invención propone un programa de ordenador que comprende unas instrucciones para la realización del procedimiento de acuerdo con el segundo aspecto de la presente invención, cuando se ejecuta este programa por un procesador.

Surgirán otras particularidades y ventajas de la presente invención en la descripción detallada a continuación, realizada con referencia a los dibujos adjuntos en los que:

- la figura 1 ilustra un sistema de control de acceso de acuerdo con un modo de realización de la presente invención;

- la figura 2 las principales etapas del procedimiento de gestión de acceso de acuerdo con un modo de realización de la presente invención;

- la figura 3 ilustra un sistema de control de acceso de acuerdo con un modo de realización de la presente invención;

- la figura 4 ilustra otro sistema de control de acceso de acuerdo con un modo de realización de la presente invención;

- la figura 5 ilustra un receptor de una entidad de transmisión de acuerdo con un modo de realización de la presente invención.

Referencias idénticas designan objetos idénticos o similares de una figura a otra.

La figura 1 ilustra un sistema de control de acceso de acuerdo con un modo de realización de la presente invención.

Este sistema de control de acceso comprende una entidad de transmisión 101 que está adaptada para transmitir un contenido digital codificado 102 en una red de comunicación 12. Este contenido digital puede ser cualquier contenido de tipo video, audio o visual o texto, o, de manera general, multimedia.

Este contenido digital codificado 102 transmitido en la red puede ser difundido por ejemplo, o multi-difundido en la red hacia uno o varios receptores 13. Cada receptor 13 está adaptado para restituir el contenido digital en claro en el caso de que el control de acceso le autorice el acceso a este contenido.

El receptor 13 puede contener un módulo de seguridad 14 que está más particularmente a cargo del tratamiento efectivo del mensaje de control de acceso y de obtener la clave de decodificación bajo forma clara en el caso en el que el acceso al contenido digital está autorizado.

La figura 2 ilustra las principales etapas de un procedimiento de gestión de acceso de acuerdo con un modo de realización de la presente invención.

En una etapa 21, se recibe un mensaje de control de acceso en el receptor. Este mensaje de control de acceso puede estar asociado de manera directa o indirecta al contenido digital transmitido. En efecto, cuando es del tipo ECM está asociado directamente al contenido digital en el sentido de que contiene la clave de decodificación de este contenido y en el caso en que es de tipo EMM está asociado de manera indirecta en el sentido de que la clave de decodificación correspondiente se puede recuperar en un mensaje posterior del tipo ECM, en base a las informaciones recibidas previamente en el mensaje de tipo EMM.

Posteriormente, en una etapa 22, se prevé obtener una información complementaria destinada a completar el mensaje de control de acceso recibido.

A continuación, en una etapa 23, se obtiene la clave de decodificación del contenido en base al mensaje de control de acceso completado con la información complementaria. Después, en una etapa 24, el contenido digital se decodifica con la ayuda de la clave obtenida en la etapa 23 y puede así ser restituido para un usuario del receptor.

Estas etapas principales permiten basar el control de acceso a un contenido digital en una información

complementaria suministrada por el usuario en el receptor.

Son fáciles de implementar estas etapas en el seno de un sistema de control de acceso existente que ya se base en unos criterios de acceso y unos derechos de acceso para decir autorizar o no a un receptor a restituir un contenido digital en claro para un usuario.

La figura 3 ilustra una realización de ese tipo en un sistema de control de acceso, basada a la vez en unos criterios de acceso transportados en unos mensajes de control y en una información complementaria de acuerdo con un modo de realización de la presente invención.

El sistema ilustrado comprende una entidad de transmisión 101 de contenido digital en la red 12.

No se vincula una limitación al tipo de derechos de acceso que se pueden tener en cuenta en el sistema ni al mecanismo que permite a un receptor o usuario recuperar sus derechos de acceso. Se puede prever particularmente con este fin una entidad de gestión de acceso 31 que transmite los derechos al receptor 13 a través de unos mensajes 301. Estos mensajes 301 pueden ser unos mensajes del tipo EMM. Posteriormente, estos derechos de acceso se almacenan en el módulo de seguridad del receptor. Cuando el mensaje de control de acceso de acuerdo con la presente invención corresponde a un mensaje del tipo EMM, la emisión de este mensaje de control de acceso incompleto puede realizarse por esta entidad de gestión de acceso.

Estos derechos de acceso pueden corresponder a un abonado de un tipo dado para un periodo dado, una reserva de sesión particular, o incluso un número de fichas que permitan a continuación una compra impulsiva local, una clave de explotación de ECM, etc.

En este contexto, el contenido digital se puede difundir en asociación con un mensaje que indique unos criterios de acceso 302 asociados a este contenido digital 102. Este tipo de mensaje que indica un criterio de acceso 302 puede ser por ejemplo un mensaje ECM.

De ese modo, el acceso al contenido digital es función entonces de unos criterios de acceso asociados al contenido digital y unos derechos de acceso vinculados al receptor.

Además, en este caso, se prevé que el receptor 13 disponga de una información complementaria asociada al contenido digital suministrado por el usuario. Una vez completado el mensaje de control de acceso con esta información complementaria, si se satisfacen los criterios de acceso por los derechos de acceso, entonces se decide autorizar el acceso al contenido digital. Se obtiene entonces la clave de decodificación en claro para decodificar el contenido digital protegido.

De ese modo, ventajosamente, es posible controlar el acceso al contenido digital a la vez en base a los derechos de acceso previamente registrados por el receptor y sobre la base de una información complementaria que se puede recuperar por no importa qué medio y particularmente de manera dinámica.

En este caso, el receptor está autorizado a restituir el contenido digital a un usuario solamente si dispone a la vez de unos derechos de acceso requeridos y de una formación complementaria asociada al contenido digital y suministrada por el usuario.

Alternativamente, en un modo de realización de la presente invención, se prevé controlar el acceso a un contenido digital o bien en base a unos derechos de acceso almacenados en el receptor, o bien en base a un valor suministrado por el usuario del receptor. De ese modo, en lugar de asociar estos dos tipos de controles de acceso, se puede generarlos de manera alternativa. Por un lado, un receptor que dispone de los derechos de acceso requeridos para tener un contenido digital es autorizado entonces a acceder a este contenido digital. Por otro lado, un receptor que no disponga de estos derechos de acceso, puede acceder igualmente al contenido digital considerado si está en condiciones de obtener la información complementaria requerida para completar el mensaje de control de acceso recibido de acuerdo con un modo de realización de la presente invención.

Este modo de realización se ilustra en la figura 4 y se describe a continuación en el presente documento en su aplicación al servicio de difusión de televisión. El sistema ilustrado en la figura 4 comprende dos entidades de difusión 401 y 402 que difunden respectivamente unos contenidos digitales 412 y 400, así como unos receptores 13-1, 13-2 y 13-3.

En lo que sigue, únicamente a título ilustrativo y no limitativo, la clave de decodificación correspondiente a la clave de decodificación y el mensaje de control de acceso recibido es un mensaje del tipo ECM.

El contenido digital 400 se difunde en una forma codificada 411 con la ayuda de la clave de codificación CW 404. Esta clave de codificación CW está a su vez codificada para ser transmitida de manera segura a través de uno o varios mensajes ECM asociados al contenido digital 411.

La entidad de difusión 402 transmite la clave de codificación CW en una forma codificada en asociación con unos criterios de acceso en un mensaje 407 del tipo ECM. La entidad de difusión 402 transmite igualmente otro mensaje de control de acceso 410 del tipo ECM en el que la clave de codificación en una forma codificada ha sido retirada, sólo se indica una referencia a esta clave de codificación y, en este ejemplo, no está presente ningún criterio de acceso. El mensaje de control de acceso es por lo tanto un mensaje de control de acceso a completar de acuerdo con un modo de realización de la presente invención.

En un modo de realización, el primer contenido digital 412 indica la clave de codificación CW, utilizada para codificar el segundo contenido digital 400. Esta clave de codificación CW, en una forma codificada, se puede insertar en el contenido digital en forma de imagen con el fin de poder restituir en imagen su valor a un usuario del receptor. Este primer contenido digital 412 se transmite antes que el segundo contenido digital 400.

La entidad de difusión 401 transmite por lo tanto un flujo de datos 413 que comprende el primer contenido digital 412 con la imagen de la clave de codificación codificada.

Un multiplexor 403 está a cargo de recibir estos diferentes flujos de datos y de difundirlos en una forma multiplexada en la red hacia los receptores. Este multiplexor 403 recibe por lo tanto en su entrada:

- un flujo de datos 413 que comprende el contenido digital 412 y la imagen del valor de la clave de codificación en forma codificada utilizada para la codificación del segundo contenido 400;

- un flujo de datos 411 que comprende el contenido digital 400 en una forma codificada con la ayuda de la clave de codificación;

- un mensaje de control de acceso 407 asociado al flujo 411 y que contiene unos criterios de acceso 406 asociados al contenido digital 400 y la clave de codificación CW en una forma codificada;

- un mensaje de control de acceso 410 incompleto asociado al flujo 411 y que no contiene ni la clave de codificación en forma codificada, ni criterios de acceso.

El flujo de datos 413 puede difundirse en claro sin estar codificado. Durante la restitución de este flujo de datos 413 por el receptor, el usuario puede visualizar entonces el valor de la clave de codificación CW en forma codificada, indicada aquí como 456 y que puede utilizarse en el mensaje del tipo ECM 410 asociado al segundo flujo 411.

Se puede prever que el contenido digital 400 difundido en una forma codificada corresponde a una película y que el contenido digital 412 difundido en claro corresponde a una secuencia de anuncios.

Los receptores 13-1 a 13-3 reciben todas esas informaciones en forma multiplexada.

El receptor 13-1 dispone de derechos de acceso que cumplen los criterios de acceso presentes en el mensaje de control de acceso ECM 407 y asociados al contenido digital 400 difundido en forma codificada. En consecuencia, puede tratar correctamente el mensaje de control de acceso 407. O, este mensaje de control de acceso 407 indica la clave de codificación en una forma codificada. Se puede entonces decodificar la clave de codificación CW codificada y se puede entonces acceder al contenido digital 400 y restituirlo en el receptor 13-1.

El receptor 13-2, de la misma forma que el receptor 13-3, no dispone de derechos de acceso al segundo contenido 400. De ese modo, ni el uno ni el otro pueden tratar correctamente el mensaje de control de acceso ECM 407. Recuperan entonces el mensaje de control de acceso 410 cuyo acceso no está sometido al control de derechos de acceso en relación a los criterios de acceso requeridos, puesto que no contiene criterios de acceso restrictivos. Sin embargo, este mensaje no contiene la clave de codificación en forma codificada en su integridad.

De este modo, con la recepción de este mensaje de control de acceso 410, el receptor 13-3 recibe del usuario correspondiente la clave de codificación en una forma codificada 456 y completa el mensaje de control de acceso 410 de manera que recupera la clave de codificación en claro.

En el ejemplo de la aplicación ilustrado en este caso, la clave de codificación en forma codificada se recupera a partir del mensaje de control de acceso 413. En consecuencia, en este caso, si el usuario de uno de los receptores 13-2 ó 13-3 está atento en el curso de la difusión previa de publicidad, memoriza la clave de codificación codificada que se le suministra durante los anuncios. Puede completar a continuación el mensaje de control de acceso 410 con esta clave de codificación codificada y recibir de vuelta la clave de codificación en claro para acceder al contenido digital 400. El usuario del receptor 13-2 que no haya memorizado la clave de codificación codificada 450 no puede obtener la clave de codificación decodificada para acceder al contenido digital 400.

De ese modo, en este sistema, o bien el receptor dispone de los derechos de acceso que le permiten utilizar un mensaje del tipo ECM clásico para obtener la clave de codificación que permite acceder al contenido digital, o bien el receptor no dispone de estos derechos de acceso, en este caso se puede utilizar otro mensaje de control de acceso

‘incompleto’ de alguna forma, completándolo con una información obtenida por otro lado. El control de acceso se realiza entonces a través de un control de la acción, como en este caso por ejemplo, la visualización de una publicidad.

Este tipo de sistema puede utilizarse ventajosamente para realizar una aplicación relativa a unos juegos de televisión. En efecto se puede prever un juego que se base en una sucesión de preguntas. Cada pregunta requiere una respuesta que corresponde a una clave de codificación o a una parte de la clave de codificación que permite acceder a la próxima pregunta. De este modo, cada pregunta se transmite de manera codificada con una clave de codificación que corresponde, en su forma codificada, a la respuesta a la cuestión anterior.

Sólo se han descrito anteriormente explícitamente algunos ejemplos. Sin embargo, se permite una gran flexibilidad de ofertas y de combinaciones de ofertas gracias a las características de la presente invención.

La figura 5 ilustra un receptor y una entidad de transmisión de acuerdo con un modo de realización de la presente invención.

El receptor 12 comprende:

- una unidad de recepción 51 adaptada para recibir un mensaje de control de acceso;

- una unidad de entrada 52 adaptada para recibir una información complementaria de un usuario;

- una primera unidad de obtención 53 adaptada para obtener un mensaje de control de acceso completado añadiendo una información complementaria a dicho mensaje de control de acceso;

- una segunda unidad de obtención 54 adaptada para obtener una clave de decodificación del contenido digital en base al mensaje de control de acceso completado; y

- una unidad de decodificación 55 adaptada para decodificar el contenido digital transmitido con ayuda de la clave de decodificación.

La unidad de entrada 52 puede corresponder a un teclado, como el teclado de un mando a distancia, por ejemplo, sobre el que el usuario puede introducir la información complementaria de acuerdo con un modo de realización.

Una entidad de transmisión 402 de acuerdo con un modo de realización de la presente invención comprende:

- una unidad de construcción 56 adaptada para componer un mensaje de control de acceso, comprendido dicho mensaje de control de acceso unas informaciones adaptadas para un tratamiento en el receptor;

- una unidad de obtención 57 adaptada para obtener un mensaje de control de acceso a completar retirando una información de dicho mensaje de control de acceso; y

- una unidad de transmisión 58 adaptada para transmitir a dicho receptor el mensaje de control de acceso a completar, siendo a completar dicho mensaje transmitido, mediante una información complementaria suministrada por un usuario.

REIVINDICACIONES

1. Procedimiento de gestión de acceso de un receptor (13) a un contenido digital (400) transmitido en una red de comunicación (12) en una forma codificada (CW); comprendiendo dicho procedimiento de gestión de acceso las etapas siguientes en el receptor:

/a/ recibir (21) un mensaje de control de acceso (410),

/b/ obtener (22) un mensaje de control de acceso completo añadiendo una información complementaria a dicho mensaje de control de acceso a completar (410),

/c/ obtener (23) una clave de decodificación del contenido en base al mensaje de control de acceso completado, y

/d/ decodificar (24) el contenido digital transmitido con ayuda de la clave de decodificación obtenida;

en el que dicha información complementaria es suministrada por un usuario.

2. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, en el que el mensaje de control de acceso completado indica la clave de decodificación (CW) en una forma codificada y en el que la información complementaria corresponde a al menos una parte de la clave de decodificación en forma codificada.

3. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, en el que el mensaje a completar indica la clave de decodificación en forma codificada y al menos un criterio de acceso y en el que la información complementaria corresponde a una al menos que entre una parte de la clave de decodificación en forma codificada y una parte de dicho criterio de acceso.

4. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, en el que el mensaje de control de acceso completado es un mensaje previo que permite tratar un mensaje posterior que indica la clave de decodificación.

5. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, en el que el mensaje de control de acceso a completar (410) es un mensaje individual, un mensaje de grupo o un mensaje general.

6. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, en el que el mensaje de control de acceso a completar (410) indica una pluralidad de informaciones complementarias y en el que un usuario suministra información complementaria seleccionándola de entre dicha pluralidad.

7. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, en el que la información complementaria se recibe en otro contenido digital (413).

8. Procedimiento de gestión de acceso de acuerdo con la reivindicación 1, que comprende además las etapas siguientes en el receptor:

/1/ recibir y restituir una pregunta, y

/2/ recibir de un usuario una respuesta a dicha pregunta;

en el que dicha respuesta corresponde a la información complementaria.

9. Procedimiento de gestión de acceso de un receptor (13) a un contenido digital (400) transmitido en una red de comunicaciones en una forma codificada; comprendiendo dicho procedimiento de gestión de acceso las etapas siguientes en una entidad de transmisión:

/a/ componer un mensaje de control de acceso, comprendiendo dicho mensaje de control de acceso unas informaciones adaptadas para un tratamiento en el receptor,

/b/ obtener un mensaje de control de acceso a completar retirando al menos una de dichas informaciones de dicho mensaje de control de acceso, y

/c/ transmitir a dicho receptor el mensaje de control de acceso a completar (410), habiéndose de completar dicho mensaje transmitido mediante la información complementaria suministrada por un usuario para obtener una clave de decodificación del contenido digital.

10. Receptor adaptado para recibir un contenido digital transmitido en una red de comunicación en una forma codificada; comprendiendo dicho receptor:

- una unidad de recepción (51) adaptada para recibir un mensaje de control de acceso a completar (410);

- una unidad de entrada (52) adaptada para recibir una información complementaria de un usuario;

- una primera unidad de obtención (53) adaptada para obtener un mensaje de control de acceso completado añadiendo una información complementaria a dicho mensaje de control de acceso a completar (410);

- una segunda unidad de obtención (54) adaptada para obtener una clave de decodificación del contenido digital en base al mensaje de control de acceso completado; y

- una unidad de decodificación (55) adaptada para decodificar el contenido digital transmitido con ayuda de la clave de decodificación.

11. Entidad de transmisión (402) adaptada para generar un acceso de un receptor a un contenido digital transmitido en una red de comunicación en una forma codificada; comprendiendo dicha entidad de transmisión:

- una unidad de construcción (56) adaptada para componer un mensaje de control de acceso asociado al contenido digital transmE-7R0472 francésitido, comprendido dicho mensaje de control de acceso unas informaciones adaptadas para un tratamiento en el receptor;

- una unidad de obtención (57) adaptada para obtener un mensaje de control de acceso a completar retirando una información de dicho mensaje de control de acceso; y

- una unidad de transmisión (58) adaptada para transmitir a dicho receptor el mensaje de control de acceso a completar, siendo a completar dicho mensaje transmitido, mediante una información complementaria suministrada por un usuario para obtener una clave de decodificación del contenido digital.

12. Sistema de control de acceso a un contenido digital que comprende una entidad de transmisión (402) de acuerdo con la reivindicación 11, y al menos un receptor (13) de acuerdo con la reivindicación 10.

13. Programa de ordenador que comprende unas instrucciones para la realización del procedimiento de acuerdo con la reivindicación 1, cuando este programa se ejecuta por un procesador.

14. Programa de ordenador que comprende unas instrucciones para la realización del procedimiento de acuerdo con la reivindicación 9, cuando este programa se ejecuta por un procesador

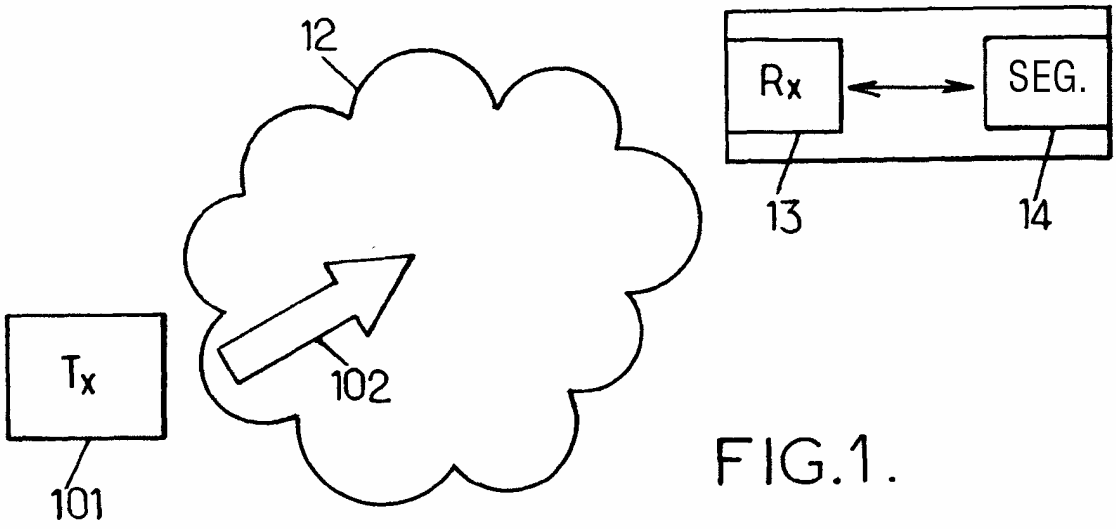

12
Rx
SEG.
13
14
Tx
102
101

FIG.1.

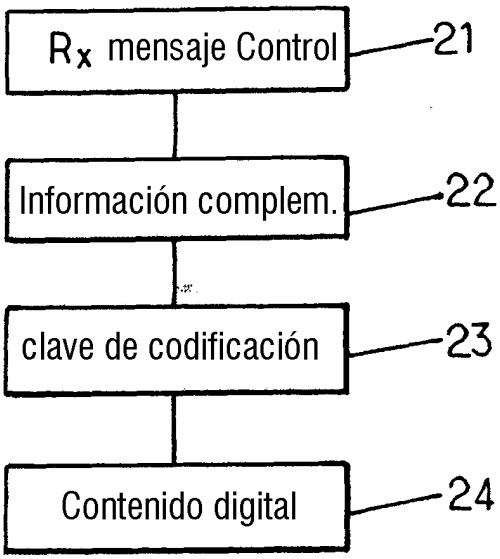

Rx mensaje Control
21
Información complem.
22
clave de codificación
23
Contenido digital
24

FIG.2.

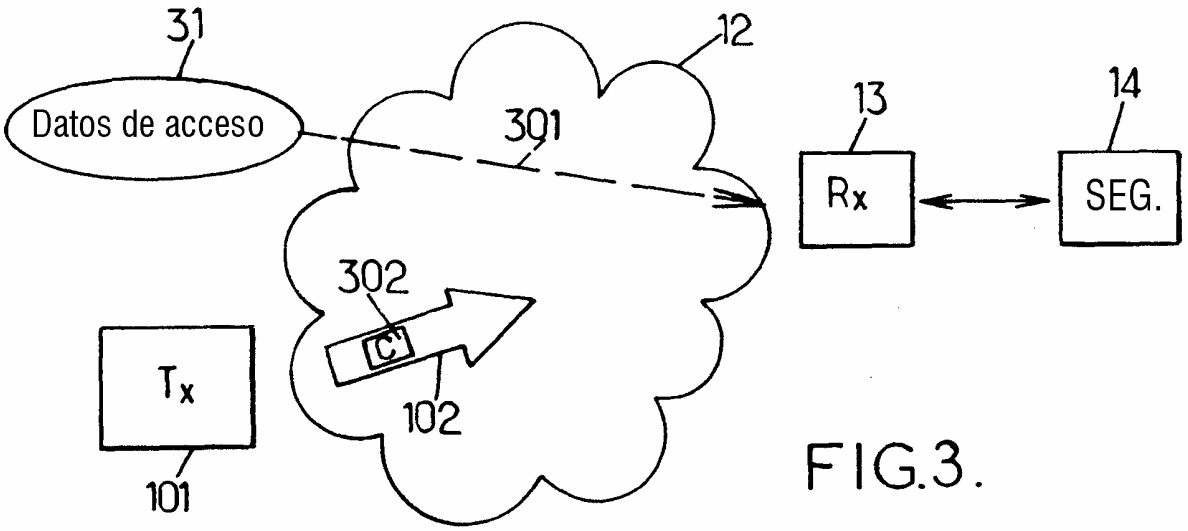

31
Datos de acceso
12
301
13
14
Rx
SEG.
302
C'
Tx
102
101

FIG.3.

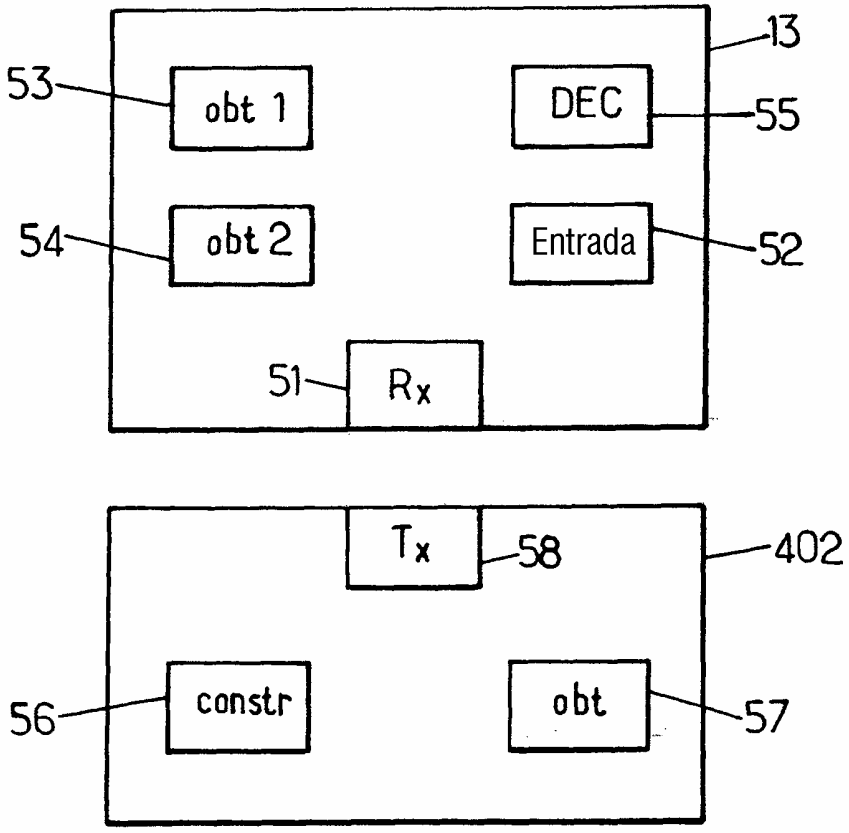
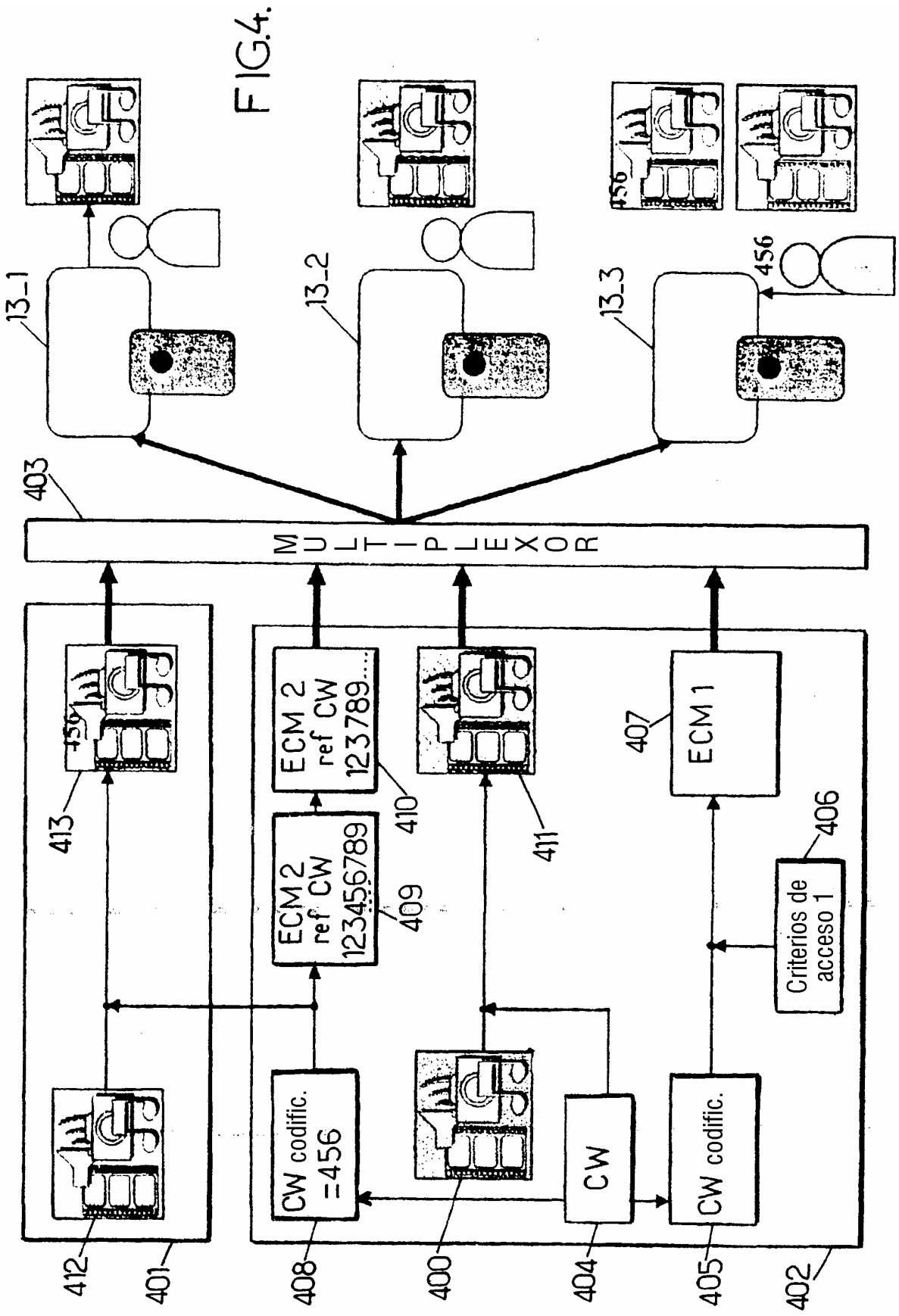

13
53
obt 1
DEC
55
54
obt 2
Entrada
52
51
Rx
Tx
58
402
56
constr
obt
57

FIG.5.

FIG.4.


13_1
13_2
13_3
456
403
MULTIPLEXOR
ECM 2 ref CW 123789....
410
ECM2 ref CW 123456789
409
411
407
ECM 1
406
Criterios de acceso 1
413
412
401
408
CW codific. =456
400
404
CW
405
CW codific.
402