(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 479 790**

(51) Int. CI.:

G06F 21/10 (2013.01)
G06F 21/77 (2013.01)
H04N 7/16 (2011.01)
H04N 21/258 (2011.01)
H04N 21/418 (2011.01)
H04N 21/426 (2011.01)
H04N 21/482 (2011.01)
H04N 21/61 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.02.2003 E 03004319 (4)**

(97) Fecha y número de publicación de la concesión europea: **25.06.2014 EP 1345436**

(54) Título: **Identificación oculta**

(30) Prioridad:

28.02.2002 US 85346

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.07.2014

(73) Titular/es:

THE DIRECTV GROUP, INC. (100.0%)
2230 E. Imperial Highway
El Segundo, CA 90245, US

(72) Inventor/es:

COCCHI, RONALD P.;
CURREN, CHRISTOPHER P. y
KAHN, RAYMOND M.

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

Identificación oculta

Referencia cruzada a solicitudes relacionadas

Esta solicitud se refiere a las siguientes solicitudes de patente en tramitación junto con la presente y de titularidad compartida, solicitudes a las que se hace referencia en el presente documento:

solicitud de patente estadounidense con n.º de serie xx/xxx.xxx, titulada "MULTIPLE NONVOLATILE MEMORIES", de Ronald Cocchi, *et al.*, n.º de expediente del agente PD-200335, presentada en la misma fecha con el presente documento;

solicitud de patente estadounidense con n.º de serie xx/xxx.xxx, titulada "DEDICATED NONVOLATILE MEMORY", de Ronald Cocchi, *et al.*, n.º de expediente del agente PD-200337, presentada en la misma fecha con el presente documento; y

solicitud de patente estadounidense con n.º de serie xx/xxx.xxx, titulada "ASYNCHRONOUS CONFIGURATION", de Ronald Cocchi, *et al.*, n.º de expediente del agente PD-201161, presentada en la misma fecha con el presente documento.

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere a sistemas y a métodos para impedir/limitar el acceso no autorizado a servicios digitales y en particular a un método y a un sistema para identificar de manera unívoca una memoria no volátil de modo que la identidad de la memoria esté oculta.

2. Descripción de la técnica relacionada

Los servicios digitales tales como programas de televisión e información concerniente a esos programas (por ejemplo, una guía de programas) se distribuyen a usuarios mediante una variedad de métodos de difusión. Tales servicios pueden ser propietarios y estar disponibles bajo un abono. Para impedir el acceso no autorizado a los servicios se utilizan una plétora de mecanismos de seguridad. Tales mecanismos pueden almacenar información en una memoria, usándose la información para validar a un usuario o proporcionar acceso. Sin embargo, las personas a menudo intentan obtener acceso no autorizado/ilegal a los servicios alterando o accediendo al contenido de la memoria. Lo que se necesita es la capacidad de impedir o aumentar la dificultad para obtener acceso ilegal a la información y servicios digitales. Estos problemas pueden entenderse mejor mediante una descripción de métodos de difusión actuales, mecanismos de seguridad y métodos para obtener acceso no autorizado a tales servicios.

Tal como se describió anteriormente, los programas de televisión y servicios digitales se distribuyen a espectadores mediante una variedad de métodos de difusión. Estos métodos incluyen la televisión de difusión analógica tradicional (norma del Comité Nacional de Sistemas de Televisión o "NTSC"), la televisión de difusión digital que se requerirá pronto (norma del Comité de Sistemas de Televisión Avanzados o "ATSC"), la televisión por cable (tanto analógica como digital), la difusión por satélite (tanto analógica como digital), así como otros métodos. Estos métodos permiten que se multiplexen canales de contenido de televisión y se transmitan por un medio de transmisión común.

Para ver la programación de televisión y tener acceso a los servicios digitales, los usuarios tienen comúnmente un *set top box* (STB) (también denominado receptor/decodificador integrado [IRD]). Dentro del sistema o STB puede utilizarse un microcircuito/componente de seguridad conocido como tarjeta inteligente para impedir el acceso no autorizado a los programas de televisión y servicios digitales. El microcircuito de tarjeta inteligente puede contener un microprocesador, componentes de memoria volátil, un componente de memoria no volátil y un módulo de entrada/salida de sistema.

La memoria no volátil se ha usado ampliamente en toda la industria electrónica. Por ejemplo, en el IRD, el microprocesador utiliza una memoria no volátil para contener información de estado (por ejemplo, información de estatus) usada para proporcionar la funcionalidad deseada y ejecutar políticas de seguridad previstas por los diseñadores. El microprocesador y/o una unidad de control de acceso a la memoria utilizada por el microprocesador restringen el acceso a los componentes de memoria.

Sin embargo ha habido numerosos intentos por parte de individuos o compañías (es decir, piratas informáticos o atacantes) de atacar, usar inapropiadamente o modificar la memoria no volátil a través de medios externos de reprogramación o alterando de otra manera el contenido de la memoria cuando el componente de memoria ha estado disponible para el procesador central o de otra manera en el bus de sistema. Por ejemplo, los ataques que usan métodos imprevistos o que subvierten defensas mal implementadas pueden usarse para lograr un acceso no autorizado al contenido de la memoria y/o hacer que se reprograme el contenido de la memoria. La reprogramación o el acceso no autorizado al contenido de la memoria puede hacer que se vean completamente comprometidas las características de seguridad previstas en el dispositivo.

La forma más simple y más prevalente de ataque contra los componentes de memoria usa medios externos no invasivos que usan un módulo de entrada/salida de un sistema debido al bajo coste del equipo requerido para implementar esta forma de ataque. La mayoría de los ataques se producen mediante la manipulación inapropiada de un microprocesador o una unidad de control de acceso a la memoria. Por ejemplo, se ha subvertido el contenido de la memoria cuando se ha visto comprometida una unidad de control de acceso a la memoria (que controla el acceso a un componente de memoria). Una vez que se ha vulnerado el componente de memoria individual, el atacante puede tener entonces la capacidad de acceder a todas las ubicaciones de dirección de memoria que residen en otros componentes de memoria.

Un ejemplo de acceso no autorizado a servicios digitales se produce cuando se clona una tarjeta inteligente o un componente de memoria. En un ataque de clonación de bajo coste de este tipo, la identidad de una tarjeta pirata se copia en una nueva tarjeta. Por consiguiente, las tarjetas inteligentes/componentes de memoria tienen una identidad/número de identificación. En la técnica anterior, el número de identificación puede establecerse como número de identificación implementado con lógica permanente en una memoria de sólo lectura (ROM). Sin embargo, el uso de una nueva máscara ROM con un número de identificación implementado con lógica permanente para cada chip producido es caro y requiere mucho tiempo. Además, los números de identificación en la técnica anterior son accesibles para el módulo de entrada/salida de sistema, el bus de sistema, el microprocesador o el entorno externo, permitiendo así ataques al sistema.

El documento EP 1 176 826 A2 describe un sistema de distribución de vídeo por satélite y un receptor con procesos de cifrado/descifrado para garantizar que sólo usuarios autorizados puedan ver los datos de vídeo.

Shigeru Araki: "The Memory Stick", IEEE Micro, ISSN: 0272-1732, vol. 20 n.º 4 julio-agosto de 2000, páginas 40-46, XP002257044 describió un lápiz de memoria para almacenar datos como imágenes fijas, imágenes en movimiento, voz o música. El lápiz incluye una interfaz como controlador para la autenticación basada en una ID de unidad y la protección para material de derechos de autor.

Sumario de la invención

Los sistemas de servicios digitales contienen a menudo un módulo de servicio conocido como tarjeta inteligente para impedir el acceso no autorizado a los servicios. El microcircuito de tarjeta inteligente contiene un microprocesador, componentes de memoria volátil, componentes de memoria no volátil, un bloque lógico personalizado y un módulo de entrada/salida de sistema. El sistema de seguridad puede verse comprometido si se usan o atacan componentes de memoria de modos inesperados.

Una o más realizaciones de la invención proporcionan un método, un aparato y un artículo de fabricación para incorporar un número de identificación oculto en alguna forma de memoria no volátil. El número de identificación se oculta del microprocesador situando el número en una ubicación de memoria que no es accesible para el módulo de entrada/salida de sistema, el bus de sistema, el microprocesador o el entorno externo. La memoria no volátil es sólo de lectura a través de un bloque lógico personalizado. El número de identificación está protegido porque no es accesible para el microprocesador y, por tanto, no puede alterarse por medios externos. Además, el número de identificación identifica de manera unívoca el dispositivo que contiene la memoria no volátil y se asocia con y usa para determinar derechos/privilegios de acceso a servicios digitales.

Breve descripción de los dibujos

Ahora se hace referencia a los dibujos en los que números de referencia similares representan partes correspondientes por todo el documento:

la figura 1 es un diagrama que muestra una visión general de un sistema de distribución de vídeo;

la figura 2 es un diagrama de bloques que muestra una configuración de enlace ascendente típica que muestra cómo se transmite material de programa de vídeo en enlace ascendente a un satélite para su transmisión a abonados usando un transpondedor individual;

la figura 3 es un diagrama de bloques de una realización del subsistema de guía de programas;

la figura 4A es un diagrama de un flujo de datos representativo recibido desde un satélite;

la figura 4B es un diagrama que ilustra la estructura de un paquete de datos;

la figura 5 es un diagrama de bloques de una realización de un receptor/decodificador integrado;

las figuras 6A y 6B ilustran arquitecturas de un módulo de acceso condicional según una o más realizaciones de la invención; y

la figura 7 es un diagrama de flujo que ilustra el uso de un número de identificación oculto para limitar el acceso no autorizado a servicios digitales según una o más realizaciones de la invención

Descripción detallada de realizaciones preferidas

En la siguiente descripción se hace referencia a los dibujos adjuntos que forman parte del presente documento y que muestran, a modo de ilustración, diversas realizaciones de la presente invención. Debe entenderse que pueden utilizarse otras realizaciones y pueden hacerse cambios estructurales sin apartarse del alcance de la presente invención.

Visión general

Un número de identificación protegido/oculto no modificable se incrusta en un componente de memoria no volátil. El número de identificación oculto no es accesible a través de un módulo de entrada/salida de sistema, un bus de sistema, un microprocesador o un entorno externo. La identificación oculta se programa tras la fabricación y hace que el componente de memoria no volátil (y, por tanto, el chip que contiene el componente de memoria) sea único.

Sistema de distribución de vídeo

La figura 1 es un diagrama que ilustra una visión general de un sistema de distribución de vídeo por satélite individual 100. El sistema de distribución de vídeo 100 comprende un centro de control 102 en comunicación con un centro de enlace ascendente 104 mediante un enlace de tierra u otro enlace 114 y con una estación receptora de abonado 110 mediante una red telefónica pública conmutada (PSTN) u otro enlace 120. El centro de control 102 proporciona material de programa (por ejemplo servicios digitales, programas de vídeo, programas de audio y datos) al centro de enlace ascendente 104 y coordina con las estaciones receptoras de abonado 110 para ofrecer, por ejemplo, servicios de programa de pago por visión (PPV), que incluyen la facturación y el descifrado asociado de programas de vídeo.

El centro de enlace ascendente 104 recibe material de programa e información de control de programa desde el centro de control 102 y, usando una antena de enlace ascendente 106 y un transmisor 105, transmite el material de programa y la información de control de programa al satélite 108 mediante un enlace ascendente 116. El satélite recibe y procesa esta información, y transmite los programas de vídeo y la información de control a la estación receptora de abonado 110 mediante un enlace descendente 118 usando un transmisor 107. La estación de recepción de abonado 110 recibe esta información usando la unidad exterior (ODU) 112, que incluye una antena de abonado y un convertidor de bloque de bajo ruido (LNB).

La estación de recepción de abonado 110 permite el uso/la visión de la información por parte de un abonado 122. Por ejemplo, la información puede usarse/verse en un televisor 124 u otro dispositivo de visualización. Para controlar el acceso a la información, la estación de recepción de abonado 110 incluye un receptor/decodificador integrado (IRD) 126. En realizaciones de la invención, el IRD 126 está acoplado en comunicación a un componente de seguridad conocido como módulo de acceso condicional o tarjeta inteligente que controla el acceso a la información/servicios digitales.

En una realización, la antena de estación de recepción de abonado es una antena de banda Ku ligeramente ovalada de 18 pulgadas. La forma ligeramente ovalada se debe a la alimentación excéntrica de 22,5 grados del LNB (convertidor de bloque de bajo ruido) que se usa para recibir señales reflejadas desde la antena de abonado. La alimentación excéntrica posiciona el LNB fuera del paso de manera que no bloquea ningún área de superficie de la antena minimizando la atenuación de la señal de microondas entrante.

El sistema de distribución de vídeo 100 puede comprender una pluralidad de satélites 108 para proporcionar una cobertura terrestre más amplia, para proporcionar canales adicionales o para proporcionar un ancho de banda adicional por canal. En una realización de la invención, cada satélite comprende 16 transpondedores para recibir y transmitir material de programa y otros datos de control desde el centro de enlace ascendente 104 y proporcionarlos a las estaciones de recepción de abonado 110. Usando técnicas de compresión y multiplexación de datos para las capacidades de canal, dos satélites 108 que trabajan juntos pueden recibir y difundir más de 150 canales de audio y vídeo convencionales (no HDTV) mediante 32 transpondedores.

Aunque la invención dada a conocer en el presente documento se describirá con referencia a un sistema de distribución de vídeo por satélite 100, la presente invención también puede ejecutarse con transmisión terrestre de información de programa, ya sea mediante medios de difusión, cable u otros medios. Además, las diferentes funciones asignadas colectivamente entre el centro de control 102 y el centro de enlace ascendente 104 tal como se describió anteriormente pueden reasignarse tal como se desee sin apartarse del alcance previsto de la presente invención.

Aunque lo anterior se ha descrito con respecto a una realización en la que el material de programa emitido al abonado 122 es material de programa de vídeo (y audio) tal como una película, el método anterior también puede usarse para emitir material de programa que comprende puramente información de audio u otros datos.

Configuración de enlace ascendente

La figura 2 es un diagrama de bloques que muestra una configuración de enlace ascendente típica para un

transpondedor de satélite 108 individual, que muestra cómo se transmite material de programa de vídeo en enlace ascendente al satélite 108 mediante el centro de control 102 y el centro de enlace ascendente 104. La figura 2 muestra tres canales de vídeo (que pueden aumentarse respectivamente con uno o más canales de audio para música de alta fidelidad, información de banda sonora o un programa de audio secundario para transmitir lenguas extranjeras), un canal de datos desde un subsistema de guía de programas 206 e información de datos informáticos desde una fuente de datos informáticos 208.

Los canales de vídeo se proporcionan por una fuente de programa de material de vídeo 200A-200C (denominada colectivamente a continuación en el presente documento fuente(s) de vídeo 200). Los datos de cada fuente de programa de vídeo 200 se proporcionan a un codificador 202A-202C (denominado colectivamente a continuación en el presente documento codificador(es) 202). Cada uno de los codificadores admite un sello de fecha y hora de programa (PTS) desde el controlador 216. El PTS es un sello de fecha y hora binario de bucle cíclico que se usa para garantizar que la información de vídeo se sincroniza apropiadamente con la información de audio tras la codificación y la decodificación. Un sello de fecha y hora PTS se envía con cada trama I de los datos codificados por MPEG.

En una realización de la presente invención, cada codificador 202 es un codificador de grupo de expertos de imágenes en movimiento de segunda generación (MPEG-2), pero también pueden usarse otros decodificadores que implementan otras técnicas de codificación. El canal de datos puede someterse a un esquema de compresión similar mediante un codificador (no mostrado), pero tal compresión es habitualmente o bien innecesaria o bien se realiza por programas informáticos en la fuente de datos informáticos (por ejemplo, los datos fotográficos se comprimen normalmente en archivos *.TIF o archivos *.JPG antes de su transmisión). Tras la codificación mediante los codificadores 202, las señales se convierten en paquetes de datos por un paquetizador 204A-204F (denominado colectivamente a continuación en el presente documento paquetizador(es) 204) asociado con cada fuente 200.

Los paquetes de datos se ensamblan usando una referencia del reloj de sistema 214 (SCR), y del gestor de acceso condicional 210, que proporciona la SCID a los paquetizadores 204 para su uso en la generación de los paquetes de datos. Estos paquetes de datos se multiplexan entonces en datos en serie y se transmiten.

Subsistema de guía de programas

La figura 3 es un diagrama de bloques de una realización del subsistema de guía de programas 206. El sistema que transmite datos de guía de programas 206 incluye una base de datos de guía de programas 302, un compilador 304, subbases de datos 306A-306C (denominados colectivamente subbases de datos 306) y cicladores 308A-308C (denominados colectivamente cicladores 308).

Alimentaciones de planificación 310 proporcionan información de planificación electrónica sobre el horario y el contenido de diversos canales de televisión, tales como los que se encuentran en las planificaciones de televisión contenidas en periódicos y guías de televisión. Las alimentaciones de planificación 310 incluyen preferiblemente información de una o más compañías que se especializan en proporcionar información de planificación, tales como TRIBUNE MEDIA SERVICES™ y T.V. DATA™. Los datos proporcionados por compañías tales como TRIBUNE MEDIA SERVICES™ y T.V. DATA™ se transmiten normalmente por líneas de teléfono a una base de datos de guía de programas 302. Estas compañías proporcionan datos de planificación de televisión para todas las estaciones de televisión en la nación además de los canales nacionales, tales como SHOWTIME™, HBO™ y DISNEY CHANNEL™. El formato específico de los datos proporcionados por estas compañías varía de compañía en compañía. La base de datos de guía de programas 302 incluye preferiblemente datos de planificación para canales de televisión por toda la nación que incluyen todos los canales nacionales y canales locales, independientemente de si los canales se transmiten mediante la estación de transmisión.

La base de datos de guía de programas 302 es un sistema informatizado que recibe datos de alimentaciones de planificación 310 y organiza los datos en un formato estándar. El compilador 304 lee los datos de formato estándar de la base de datos de guía de programas 302, identifica partes de planificación comunes, convierte los datos de guía de programas al formato apropiado para la transmisión a usuarios (específicamente, los datos de guía de programas se convierten en objetos tal como se discute a continuación) y emite los datos de guía de programas a una o más de subbases de datos 306.

Los datos de guía de programas también pueden introducirse manualmente en una base de datos de guía de programas 302 a través de una estación de introducción de datos 312. La estación de introducción de datos 312 permite que un operador introduzca información de planificación adicional, así como combinar y organizar datos suministrados por las compañías de planificación. Tal como con los datos organizados por ordenador, los datos introducidos manualmente se convierten mediante el compilador en objetos separados y se envían a una o más subbases de datos 306.

Los objetos de guía de programas se almacenan temporalmente en subbases de datos 306 hasta que cicladores 308 solicitan la información. Cada uno de los cicladores 308 puede transmitir objetos a una tasa diferente de los otros cicladores 308. Por ejemplo, el ciclador 308A puede transmitir objetos cada segundo, mientras que los cicladores 308B y 308C pueden transmitir objetos cada 5 segundos y cada 10 segundos, respectivamente.

Puesto que los receptores del abonado pueden no estar siempre encendidos y recibiendo y guardando objetos, la información de guía de programas se retransmite continuamente. Los objetos de guía de programas para programas que se mostrarán en el siguiente par de horas se envían más frecuentemente que los objetos de guía de programas para programas que se mostrarán posteriormente. Por tanto, los objetos de guía de programas para los programas más actuales se envían a un ciclador 308 con una tasa de transmisión alta, mientras que los objetos de guía de programas para programas posteriores se envían a cicladores 308 con una tasa de transmisión menor. Una o más de las salidas de datos 314 de los cicladores 308 se reenvían al paquetizador de un transpondedor particular, tal como se representa en la figura 2.

Debe indicarse que la configuración de enlace ascendente representada en la figura 2 y el subsistema de guía de programas representado en la figura 3 pueden implementarse mediante uno o más módulos de hardware, uno o más módulos de software que definen instrucciones realizadas por un procesador, o una combinación de ambos.

Formato y protocolo de flujo de datos de difusión

La figura 4A es un diagrama de un flujo de datos representativo. El primer segmento de paquete 402 comprende información de un canal de vídeo 1 (datos procedentes de, por ejemplo, la primera fuente de programa de vídeo 200A). El siguiente segmento de paquete 404 comprende información de datos informáticos que se obtuvo, por ejemplo, de la fuente de datos informáticos 208. El siguiente segmento de paquete 406 comprende información de un canal de vídeo 5 (de una de las fuentes de programa de vídeo 200). El siguiente segmento de paquete 408 comprende información de guía de programas tal como la información proporcionada por el subsistema de guía de programas 206. Tal como se muestra en la figura 4A pueden insertarse paquetes nulos 410 creados por el módulo de paquete nulo 212 en el flujo de datos según se desee.

Por tanto, el flujo de datos comprende una serie de paquetes de una cualquiera de las fuentes de datos en un orden determinado por el controlador 216. El flujo de datos se cifra mediante el módulo de cifrado 218, se modula mediante el modulador 220 (usando normalmente un esquema de modulación QPSK) y se proporciona al transmisor 222, que difunde el flujo de datos modulado en un ancho de banda de frecuencia al satélite mediante la antena 106. El receptor 126 recibe estas señales y, usando la SCID, vuelve a ensamblar los paquetes para volver a generar el material de programa para cada uno de los canales.

La figura 4B es un diagrama de un paquete de datos. Cada paquete de datos (por ejemplo 402-416) tiene una longitud de 147 bytes y comprende varios segmentos de paquetes. El primer segmento de paquete 420 comprende dos bytes de información que contienen la SCID y banderas. La SCID es un único número de 12 bits que identifica de manera unívoca al canal de datos del paquete de datos. Las banderas incluyen 4 bits que se usan para controlar otras características. El segundo segmento de paquete 422 está constituido por un indicador de tipo de paquete de 4 bits y un contador de continuidad de 4 bits. El tipo de paquete identifica el paquete como uno de los cuatro tipos de datos (vídeo, audio, datos o nulo). Cuando se combina con la SCID, el tipo de paquete determina cómo se usará el paquete de datos. El contador de continuidad aumenta una vez para cada tipo de paquete y SCID. El siguiente segmento de paquete 424 comprende 127 bytes de datos de carga útil, que en los casos de paquetes 402 ó 406 es una parte del programa de vídeo proporcionado por la fuente de programa de vídeo 200. El segmento de paquete final 426 son datos requeridos para realizar una corrección de errores sin canal de retorno.

Receptor/decodificador integrado

La figura 5 es un diagrama de bloques de un receptor/decodificador integrado (IRD) 126 (también denominado a continuación en el presente documento alternativamente receptor 126 o STB). El receptor 126 comprende un sintonizador/demodulador 504 acoplado en comunicación a una ODU 112 que tiene uno o más LNB 502. El LNB 502 convierte la señal de enlace descendente 118 de 12,2 a 12,7 GHz de los satélites 108 en, por ejemplo, una señal de 950-1450 MHz requerida por el sintonizador/demodulador 504 del IRD 126. El LNB 502 puede proporcionar o bien una salida doble o bien una individual. El LNB de salida individual 502 tiene sólo un conector de RF, mientras que el LNB de salida doble 502 tiene dos conectores de salida de RF y pueden usarse para alimentar un segundo sintonizador 504, un segundo receptor 126 o alguna otra forma de sistema de distribución.

El sintonizador/demodulador 504 aísla un único transpondedor de 24 MHz modulado digitalmente y convierte los datos modulados en un flujo de datos digital. El flujo de datos digital se suministra entonces a un decodificador de corrección de errores sin canal de retorno (FEC) 506. Esto permite que el IRD 126 vuelva a ensamblar los datos transmitidos por el centro de enlace ascendente 104 (que aplicó la corrección de errores sin canal de retorno a la señal deseada antes de la transmisión a la estación de recepción de abonado 110) verificando que se recibió la señal de datos correcta y corrigiendo errores, si los hay. Los datos de error corregido pueden alimentarse desde el módulo decodificador de FEC 506 al módulo de transporte 508 mediante una interfaz paralela de 8 bits.

El módulo de transporte 508 realiza muchas de las funciones de procesamiento de datos realizadas por el IRD 126. El módulo de transporte 508 procesa datos recibidos desde el módulo decodificador de FEC 506 y proporciona los datos procesados al decodificador MPEG de vídeo 514 y al decodificador MPEG de audio 517. En una realización de la presente invención, el módulo de transporte, el decodificador MPEG de vídeo y el decodificador MPEG de audio están todos implementados en circuitos integrados. Este diseño promueve eficiencia tanto de espacio como

energética, y aumenta la seguridad de las funciones realizadas dentro del módulo de transporte 508. El módulo de transporte 508 también proporciona un paso para comunicaciones entre el microcontrolador 510 y los decodificadores MPEG de vídeo y de audio 514, 517. Tal como se expone de manera más completa a continuación en el presente documento, el módulo de transporte también trabaja con el módulo de acceso condicional (CAM) 512 para determinar si la estación de recepción de abonado 110 puede acceder a cierto material de programa. También pueden suministrarse datos desde el módulo de transporte a un módulo de comunicación externo 526.

El CAM 512 funciona en asociación con otros elementos para decodificar una señal cifrada del módulo de transporte 508. El CAM 512 también puede usarse para rastrear y facturar estos servicios. En una realización de la presente invención, el CAM 512 es una tarjeta inteligente, que tiene contactos que interaccionan de manera cooperativa con contactos en el IRD 126 para pasar información. Para implementar el procesamiento realizado en el CAM 512, el IRD 126 y específicamente el módulo de transporte 508 proporcionan una señal de reloj al CAM 512. A continuación se describen detalles de la arquitectura del CAM 512.

Los datos de vídeo se procesan mediante el decodificador de vídeo MPEG 514. Usando la memoria de acceso aleatorio (RAM) de vídeo 536, el decodificador de vídeo MPEG 514 decodifica los datos de vídeo comprimidos y los envía a un codificador o procesador de vídeo 516, que convierte la información de vídeo digital recibida desde el módulo MPEG de vídeo 514 en una señal de salida que puede usarse por una pantalla u otro dispositivo de salida. A modo de ejemplo, el procesador 516 puede comprender un codificador del Comité Nacional de Sistemas de Televisión (NTSC) o del Comité de Sistemas de Televisión Avanzados (ATSC). En una realización de la invención se proporcionan señales tanto de S-Video como de vídeo ordinario (NTSC o ATSC). También pueden utilizarse otras salidas y son ventajosas si se procesa programación de alta definición.

Los datos de audio se decodifican de la misma manera mediante el decodificador de audio MPEG 517. Los datos de audio decodificados pueden enviarse entonces a un convertidor digital-analógico (D/A) 518. En una realización de la presente invención, el convertidor D/A 518 es un convertidor D/A doble, uno para los canales derecho e izquierdo. Si se desea pueden añadirse canales adicionales puede para su uso en el procesamiento de sonido ambiente o programas de audio secundarios (SAP). En una realización de la invención, el propio convertidor D/A doble 518 separa la información de canal derecho e izquierdo, así como cualquier información de canal adicional. Pueden soportarse otros formatos de audio de manera similar. Por ejemplo pueden soportarse otros formatos de audio tales como DOLBY DIGITAL AC-3 multicanal.

Una descripción de los procesos realizados en la codificación y la decodificación de flujos de vídeo, particularmente con respecto a la codificación/decodificación MPEG y JPEG, puede encontrarse en el capítulo 8 de "Digital Television Fundamentals", de Michael Robin y Michel Poulin, McGraw-Hill, 1998, que se incorpora de esta manera al presente documento como referencia.

El microcontrolador 510 recibe y procesa señales de órdenes del control remoto 524, una interfaz de teclado de IRD 126 y/u otro dispositivo de entrada. El microcontrolador recibe órdenes para realizar sus operaciones desde una memoria de programación de procesador, que almacena de manera permanente tales instrucciones para realizar tales órdenes. La memoria de programación de procesador puede comprender una memoria de sólo lectura (ROM) 538, una memoria de sólo lectura programable y borrable eléctricamente (EEPROM) 522 o un dispositivo de memoria similar. El microcontrolador 510 también controla los otros dispositivos digitales del IRD 126 mediante líneas de dirección y datos (denominadas "A" y "D" respectivamente, en la figura 5).

El módem 540 se conecta a la línea de teléfono del cliente mediante el puerto PSTN 120. Éste llama, por ejemplo al proveedor de programa, y transmite la información de compra del cliente para fines de facturación, y/u otra información. El módem 540 se controla mediante el microprocesador 510. El módem 540 puede emitir datos a otros tipos de puerto de E/S incluyendo puertos de E/S informáticos en paralelo y en serie convencionales.

La presente invención también comprende una unidad de almacenamiento local tal como el dispositivo de almacenamiento de vídeo 532 para almacenar datos de vídeo y/o audio obtenidos del módulo de transporte 508. El dispositivo de almacenamiento de vídeo 532 puede ser un disco duro, un disco compacto de lectura/escritura de DVD, una RAM de estado sólido o cualquier otro medio de almacenamiento. En una realización de la presente invención, el dispositivo de almacenamiento de vídeo 532 es un disco duro con capacidad de lectura/escritura paralela especializada de manera que pueden leerse datos desde el dispositivo de almacenamiento de vídeo 532 y escribirse en el dispositivo 532 al mismo tiempo. Para efectuar esta tarea, puede usarse una memoria intermedia adicional accesible por el almacenamiento de vídeo 532 o su controlador. Opcionalmente puede usarse un procesador de almacenamiento de vídeo 530 para gestionar el almacenamiento y la recuperación de los datos de vídeo desde el dispositivo de almacenamiento de vídeo 532. El procesador de almacenamiento de vídeo 530 también puede comprender una memoria para almacenar de manera intermedia datos que entran en y salen del dispositivo de almacenamiento de vídeo 532. Alternativamente o en combinación con lo anterior pueden usarse una pluralidad de dispositivos de almacenamiento de vídeo 532. También alternativamente o en combinación con lo anterior, el microcontrolador 510 también puede realizar las operaciones requeridas para almacenar y/o recuperar datos de vídeo y otros en el dispositivo de almacenamiento de vídeo 532.

La entrada del módulo de procesamiento de vídeo 516 puede suministrarse directamente como salida de vídeo a un

dispositivo de visualización tal como un monitor de vídeo u ordenador. Además, las salidas de vídeo y/o audio pueden suministrase a un modulador de RF 534 para producir una salida de RF y/o banda lateral residual (VSB)-8 adecuada como señal de entrada a un sintonizador de televisión convencional. Esto permite que el receptor 126 funcione con televisores sin una salida de vídeo.

Cada uno de los satélites 108 comprende un transpondedor, que admite información de programa del centro de enlace ascendente 104, y retransmite esta información a la estación de recepción de abonado 110. Se usan técnicas de multiplexación conocidas de manera que pueden proporcionarse múltiples canales al usuario. Estas técnicas de multiplexación incluyen, a modo de ejemplo, diversas técnicas de multiplexación estadísticas o de otro dominio de tiempo y multiplexación por polarización. En una realización de la invención, un transpondedor individual que funciona en una banda de frecuencia individual porta una pluralidad de canales identificados por una identificación de canal de servicio (SCID) respectiva.

Preferiblemente, el IRD 126 también recibe y almacena una guía de programas en una memoria disponible para el microcontrolador 510. Normalmente, la guía de programas se recibe en uno o más paquetes de datos en el flujo de datos procedente del satélite 108. Puede accederse a y realizarse búsquedas en la guía de programas mediante la ejecución de etapas de operación adecuadas implementadas por el microcontrolador 510 y almacenadas en el procesador ROM 538. La guía de programas puede incluir datos para mapear números de canal de espectador con transpondedores de satélite e identificaciones de canal de servicio (SCID), y también proporcionar información de listado de programas de televisión al abonado 122 que identifica eventos de programa.

La funcionalidad implementada en el IRD 126 representado en la figura 5 puede implementarse mediante uno o más módulos de hardware, uno o más módulos de software que definen instrucciones realizadas por un procesador, o una combinación de ambos.

Tarjeta de acceso

Un CAM 512 contiene a menudo un microprocesador, componentes de memoria (un componente volátil y un componente no volátil) y un módulo de entrada/salida (E/S) de sistema para comunicarse con el módulo de transporte 508. Los microprocesadores tradicionales dentro de un CAM 512 tienen una memoria no volátil para contener el estado que se usa para proporcionar la funcionalidad deseada y ejecutar políticas de seguridad previstas por los diseñadores. El microprocesador y/o una unidad de control de acceso a la memoria restringen el acceso a los componentes de memoria. Además, números de identificación pueden identificar un CAM 512. Sin embargo, en la técnica anterior no hay ningún intento de aislar el número de identificación del módulo de E/S de sistema, del bus de sistema, del microprocesador o del entorno externo.

Tal como se describió anteriormente, los ataques pueden usar métodos imprevistos o pueden subvertir defensas ,mal implementadas para lograr un acceso no autorizado al contenido de la memoria y/o hacer que se reprograme el contenido de la memoria. Por ejemplo, la mayoría de los ataques se producen mediante una manipulación inapropiada del microprocesador o de la unidad de control de acceso a la memoria. La reprogramación o el acceso no autorizado al contenido de la memoria puede hacer que se vean completamente comprometidas las características de seguridad previstas en el CAM 512. La forma más simple y más prevalente de ataque contra el componente de memoria usa medios externos que usan el módulo de E/S de sistema debido al bajo coste del equipo requerido para implementar esta forma de ataque. Por ejemplo, la identificación del CAM 512 puede obtenerse a través del módulo de E/S de sistema o del microprocesador y duplicarse para crear una tarjeta pirata.

La invención intenta específicamente asegurar el contenido de la memoria ocultándolo del entorno externo garantizando que no se sitúe en el bus de sistema y no esté disponible para el microprocesador o el módulo de E/S de sistema. Por consiguiente, para evitar los métodos de ataque descritos anteriormente, el acceso al número de identificación se oculta almacenando el número en un componente de memoria no volátil protegido conectado no directamente al módulo de E/S de sistema, al bus de sistema o al microprocesador. El bloque lógico personalizado se implementa en un hardware de estado sólido que implementa una máquina de estado simple y bien definida. Las funciones definidas en el bloque lógico personalizado especifican un puñado de operaciones bien definidas que pueden realizarse usando el número de identificación oculto. Al impedir que el módulo de E/S de sistema, el bus de sistema, el microprocesador o la unidad de control de acceso a la memoria acceda directamente al componente de memoria no volátil protegido (y, por tanto, al número de identificación y a la identidad del CAM 512) ya no son posibles ataques anteriormente exitosos.

Las figuras 6A y 6B ilustran dos arquitecturas de un CAM 512 según una o más realizaciones de la invención. El CAM 512 contiene un microprocesador 602, componentes de memoria volátiles 604 (por ejemplo, memoria de acceso aleatorio [RAM]), uno o más componentes de memoria no volátiles 606 (por ejemplo, memoria de sólo lectura programable y borrable eléctricamente [EEPROM], memoria de sólo lectura programable y borrable [EPROM] o RAM con respaldo de batería), un módulo de entrada/salida de sistema 608, un bloque lógico personalizado 612 y un número de identificación oculto 614 (que está almacenado dentro de un componente de memoria no volátil separado 606). Los diversos componentes del CAM 512 pueden estar acoplados en comunicación a un bus de sistema 610.

Garantizar que el número de identificación 614 esté protegido contra modificación conserva la unicidad del dispositivo (es decir, CAM 512) que es importante para muchos modelos de seguridad. El número de identificación oculto 614 puede incrustarse en el CAM 512 tras la fabricación.

En la figura 6A, el número de identificación oculto 614 se programa por el microprocesador 602 (a lo largo del bus de sistema 610) usando una memoria programable una sola vez protegida por un fusible de hardware 616 que aísla el número de identificación 614 (y el componente de memoria no volátil 606 que contiene el número de identificación 614) del microprocesador 602 tras haberse escrito el número de identificación 614. En otras palabras, tras haberse escrito el número de identificación oculto 614, el fusible 616 se funde.

En la figura 6B, el número de identificación oculto 614 se programa por el bloque lógico personalizado 612 usando una memoria programable una sola vez/conexión de una sola escritura 616. Por tanto, tras escribir el bloque lógico personalizado 612 el número de identificación oculto 614, la conexión 616 ya no existe (por ejemplo, se destruye). Tal como en la figura 6A, la conexión de una sola escritura 616 de la figura 6B puede ser un fusible de hardware que se funde tras haberse escrito el número oculto 614.

Por consiguiente, en la figura 6A y la figura 6B, tras haberse escrito el número de identificación oculto 614, el número de identificación 614 está protegido porque no es accesible por el microprocesador 602 y, por tanto, no puede alterarse por medios externos. Una vez aislado, el número de identificación oculto 614 sólo puede leerse (y no modificarse) por el bloque lógico personalizado 612 a través de la conexión de sólo lectura 618. El bloque lógico personalizado 612 se implementa en un hardware de estado sólido que implementa una máquina de estado simple y bien definida. Las funciones definidas en el bloque lógico personalizado 612 especifican un puñado de operaciones bien definidas que pueden realizarse usando el número de identificación oculto 614.

Además de lo anterior, el componente de memoria no volátil 606 del microprocesador 602 y el componente de memoria no volátil que contiene el número oculto 614 pueden usar los mismos intervalos de dirección física y lógica porque se controlan y programan por entidades separadas. Alternativamente, los dos componentes de memoria 606 (y el componente 606 que contiene el número oculto 614) pueden usar intervalos de dirección separados según considere conveniente el diseñador del sistema. Esto ayuda a obstaculizar el uso de la memoria que contiene el número oculto 614 por parte de atacantes potenciales haciendo más difícil determinar el mapa de memoria y el uso de segmentos de código dentro del CAM 512.

Adicionalmente, los dos componentes de memoria no volátiles 606 pueden compartir bombas de carga de programación y un control de programación. Si se comparten las bombas y/o el control de programación debe tenerse cuidado de garantizar que las líneas de datos y dirección del componente de memoria no volátil 606 que contienen el número oculto 614 estén direccionadas sólo hacia el bloque lógico personalizado 612. Esto ahorra área de chip y reduce el coste de chip. Por consiguiente, el microprocesador 602 no puede proporcionar información de control que puede llevar a un ataque sucesivo al componente de memoria protegido/dedicado 606 (es decir, el componente que contiene el número oculto 614). Puede preferirse compartir las bombas de carga para aliviar los requisitos de temporización y alta tensión de todo el chip dentro del CAM 512.

Hay muchas ventajas por utilizar un número de identificación oculto 614. Por ejemplo, el número de identificación oculto 614 puede resistir ataques externos sustanciales sin modificar inapropiadamente el contenido del componente de memoria no volátil 606 que contiene el número de identificación. Además, al impedir que el módulo de E/S de sistema 608, el bus de sistema 610, el microprocesador 602 o la unidad de control de acceso a la memoria acceda directamente al número de identificación oculto 614 contenido en un componente de memoria no volátil aislado 606, ya no es posible comprometer la seguridad de manera tradicionalmente exitosa.

Además, la integridad de información se mejora significativamente a través del aislamiento de su componente de almacenamiento del módulo de E/S de sistema 608, del bus de sistema 610 y/o del microprocesador 602. Proteger la integridad del número oculto 614 es importante porque impide/limita los ataques de clonación de bajo coste en los que se copia la identidad de una tarjeta pirata a una nueva tarjeta. Este ataque se limita a través del número de identificación oculto 614.

Puesto que el número de identificación oculto 614 sólo puede leerse por un bloque lógico personalizado 612 y no puede reprogramarse por el microprocesador 602, la identidad del CAM 512 no puede transferirse a un segundo CAM 512, impidiendo así un ataque de clonación exitoso de bajo coste. Por tanto, la identidad del dispositivo (es decir, el CAM 512) está protegida para su uso en operaciones con el CAM 512, el IRD 126 y la cabecera. Por ejemplo, el CAM 512 proporciona una unicidad no modificable (es decir, se almacena en una memoria protegida 614) que puede usarse para impedir la clonación del CAM 512 para obtener acceso no autorizado. Además, el CAM 512 puede proporcionar un IRD 126 para un emparejamiento y una lista negra no modificables, y puede proporcionar una cabecera que controla derechos de acceso y la lista negra. Un lista negra se utiliza para impedir que se usen/clonen CAM 512 con una identificación particular. Con una lista negra, la cabecera puede proporcionar una lista de tarjetas en lista negra/no autorizadas a un IRD 126. El IRD 126 se niega entonces a conceder derechos de acceso si el CAM 512 que se utiliza está en la lista negra. Por consiguiente pueden utilizarse CAM 512 identificados de manera unívoca con una identificación única que es sólo accesible a través de un bloque lógico personalizado 612 para impedir el acceso no autorizado y la clonación.

Impedir ataques de bajo coste obliga a que los atacantes usen ataques invasivos caros que no están disponibles para la vasta mayoría de piratas. Inhibir esta forma simple de ataque impide que intrusos usen ataques que requieren sólo un ordenador personal y un lector de tarjeta de 10$. En cambio se obliga a que los piratas utilicen ataques invasivos sofisticados, costosos y que requieren mucho tiempo en los que se modifica el hardware real. Adicionalmente, comprometer adicionalmente un dispositivo a través de un ataque invasivo interno no lleva a un ataque exitoso a través de un ataque externo de bajo coste.

La figura 7 es un diagrama de flujo que ilustra el uso del número de identificación oculto 614 para limitar el acceso no autorizado a servicios digitales según una o más realizaciones de la invención. En la etapa 700, el número de identificación oculto no modificable 614 se incrusta (por ejemplo, por un microprocesador 602 o un bloque lógico personalizado 612) en un componente de memoria no volátil 606. El número 614 identifica de manera unívoca un dispositivo (por ejemplo, CAM 512) que contiene el componente de memoria no volátil 606 (que contiene el número 614). Tal incrustación se produce tras fabricar el CAM 512. Tal como se describió anteriormente, el componente de memoria no volátil 606 se usa para contener información de estado para proporcionar la funcionalidad deseada y ejecutar una o más políticas de seguridad para acceder a servicios digitales.

En la etapa 702, el acceso al componente de memoria no volátil 606 está aislado de modo que el número de identificación 614 (y el componente de memoria no volátil que contiene el número oculto 614) está protegido contra modificación de modo que se lee sólo el componente de memoria no volátil 606. El componente de memoria 606 puede aislarse impidiendo que un módulo de E/S de sistema 608, un bus de sistema 610, un microprocesador 602 o un entorno externo acceda directamente al número de identificación 614. Por ejemplo, tal como se describió anteriormente, el número de identificación 614 puede incrustarse usando una memoria programable una sola vez que está protegida por un fusible de hardware que aísla el número de identificación 614 y el componente 606 del microprocesador 602 tras haberse escrito el número de identificación 614.

En la etapa 704, el número de identificación 614 se lee por un bloque lógico personalizado 612. El número de identificación 614 puede leerse para su uso en una función definida en el bloque lógico personalizado 612, en el que la función especifica una operación que va a realizarse usando el número de identificación 614. Por ejemplo, para activar o garantizar que un usuario está autorizado para recibir/usar servicios digitales de difusión, el número de identificación 614 puede leerse por el bloque lógico personalizado 612 conforme a una política de seguridad ejecutada por la memoria no volátil 606 dentro del CAM 512. Por tanto, el acceso a los servicios digitales se basa en derechos de acceso asociados con el número de identificación oculto no modificable 614. Por ejemplo, si el número oculto 614 existe en una lista negra (es decir, una lista de números no autorizados 614 tal como se describió anteriormente) puede rechazarse el acceso a los servicios digitales.

Por tanto, tal como se describe, el número de identificación 614 se incrusta en una memoria no volátil 606 (en la etapa 700) y la memoria no volátil 606 se aísla (ocultando así el acceso a y la modificación del número de identificación 614) (en la etapa 702). Una vez que el número de identificación 614 se ha incrustado en la memoria 606, la tarjeta mantiene una identidad no modificable que puede usarse entonces para ejecutar una política de seguridad (por ejemplo, leyendo la identificación 614 en la etapa 704) basándose en esa identidad única.

El uso de un número de identificación 614 de esta manera mejora significativamente la integridad de información a través del aislamiento del componente de almacenamiento de la información (por ejemplo, memoria no volátil 606) del módulo de E/S de sistema 608, del bus de sistema 610 y/o del microprocesador 602. También se reduce la manipulación de contenido almacenado a través de la conexión directa de una máquina de bloque lógico personalizado de estado fijo de sólo lectura 612. Por tanto puede escribirse información (por ejemplo, el número de identificación 614 u otra información) una vez y ocultarse del módulo de E/S de sistema 608, del bus de sistema 610, y/o del microprocesador 602. Además puede usarse el bloque lógico personalizado 612 para ocultar información de estos otros componentes.

Conclusión

Esto concluye la descripción de una o más realizaciones de la presente invención. Se ha presentado la descripción anterior de la invención para fines de ilustración y descripción. No se pretende que sea exhaustiva o que limite la invención a la forma precisa dada a conocer. Son posibles muchas modificaciones y variaciones a la luz de la enseñanza anterior. Por consiguiente, aunque la invención puede proteger la recepción de servicios de vídeo, audio, banda ancha y datos usando un microcircuito que reside en una tarjeta inteligente y un STB, la invención no se limita a aplicaciones de tarjeta inteligente o a un sistema de servicio digital particular.

REIVINDICACIONES

1. Sistema para controlar el acceso a servicios digitales que comprende:

(a) un centro de control (102) configurado para coordinar y proporcionar servicios digitales;

(b) un centro de enlace ascendente (104) configurado para recibir los servicios digitales desde el centro de control (102) y transmitir los servicios digitales a un satélite (108);

(c) el satélite (108) configurado para:

(i) recibir los servicios digitales desde el centro de enlace ascendente (104);

(ii) procesar los servicios digitales; y

(iii) transmitir los servicios digitales a una estación receptora de abonado (110);

(d) la estación receptora de abonado (110) configurada para:

(i) recibir los servicios digitales desde el satélite (108);

(ii) controlar el acceso a los servicios digitales a través de un receptor/decodificador integrado (IRD) (126);

(e) un módulo de acceso condicional (CAM) (512) acoplado en comunicación al IRD (126), en el que el CAM (512) comprende:

(i) un componente de memoria no volátil protegido (606), caracterizado porque:

(1) el componente de memoria no volátil protegido (606) está adaptado para contener información de estado para ejecutar una o más políticas de seguridad para acceder a los servicios digitales; y

(2) el componente de memoria no volátil protegido (606) está protegido contra modificación de modo que el componente de memoria no volátil (606) es sólo de lectura; y

(3) el acceso al componente de memoria no volátil protegido (606) está aislado;

(ii) un componente de memoria no volátil de un microprocesador en el que el componente de memoria no volátil del microprocesador y el componente de memoria no volátil protegido usan intervalos de dirección física y lógica que son los mismos;

(iii) un número de identificación oculto no modificable (614) incrustado en el componente de memoria no volátil protegido (606), en el que el número de identificación (614) identifica de manera unívoca el CAM (512), no pudiendo leerse el número de identificación oculto no modificable desde ninguno del microprocesador, un módulo de E/S de sistema, un bus de sistema y una unidad de control de acceso a la memoria del CAM; y en el que el acceso a dichos servicios digitales se basa en derechos de acceso asociados con el número de identificación oculto no modificable; y

(iv) un bloque lógico personalizado de estado fijo (612), en el que el componente de memoria no volátil protegido (606) no es accesible mediante el bus de sistema (610) y el acceso al componente de memoria no volátil protegido (606) está limitado al bloque lógico personalizado (612), y en el que las líneas de datos y dirección del componente de memoria no volátil protegido están direccionadas sólo hacia el bloque lógico personalizado de estado fijo; estando adaptado el bloque lógico personalizado para leer el número de identificación oculto no modificable para realizar una operación usando el número de identificación oculto no modificable, incluyendo dicha operación dicho acceso a dichos servicios digitales.

2. Sistema según la reivindicación 1, en el que el componente de memoria no volátil (606) está aislado de modo que se impide que un módulo de entrada/salida de sistema (608), un microprocesador (602) o un entorno externo acceda directamente al número de identificación (614).

3. Sistema según la reivindicación 1, en el que se permite al bloque lógico personalizado (612) leer el número de identificación (614).

4. Sistema según la reivindicación 1, que comprende además una memoria programable una sola vez protegida por un fusible de hardware que aísla el número de identificación (614) del microprocesador (602) tras haberse escrito el número de identificación (614).

5. Método para limitar el acceso no autorizado a servicios digitales que comprende:

(a) incrustar un número de identificación oculto no modificable (614) en un componente de memoria no volátil protegido (606), en el que:

(i) el componente de memoria no volátil protegido (606) se usa para contener información de estado para ejecutar una o más políticas de seguridad para acceder a los servicios digitales;

(ii) el número de identificación oculto no modificable (614) identifica de manera unívoca un dispositivo que contiene el componente de memoria no volátil protegido (606), no pudiendo leerse el número de identificación oculto no modificable desde ninguno del microprocesador, un módulo de E/S de sistema, un bus de sistema y una unidad de control de acceso a la memoria del CAM; y en el que el acceso a dichos servicios digitales se basa en derechos de acceso asociados con el número de identificación oculto no modificable; y

(b) aislar el acceso al componente de memoria no volátil protegido (606), en el que:

(i) el acceso al componente de memoria no volátil protegido (606) está limitado a un bloque lógico personalizado de estado fijo (612), estando adaptado el bloque lógico personalizado para leer el número de identificación oculto no modificable para realizar una operación usando el número de identificación oculto no modificable, incluyendo dicha operación dicho acceso a dichos servicios digitales;

(ii) el componente de memoria no volátil protegido (606) está protegido de modo que el componente de memoria no volátil (606) es sólo de lectura;

(iii) el componente de memoria no volátil protegido (606) no es accesible mediante el bus de sistema;

(iv) las líneas de datos y dirección del componente de memoria no volátil protegido están direccionadas sólo hacia el bloque lógico personalizado de estado fijo; y

(v) el componente de memoria no volátil de un microprocesador y el componente de memoria no volátil protegido usan intervalos de dirección física y lógica que son los mismos.

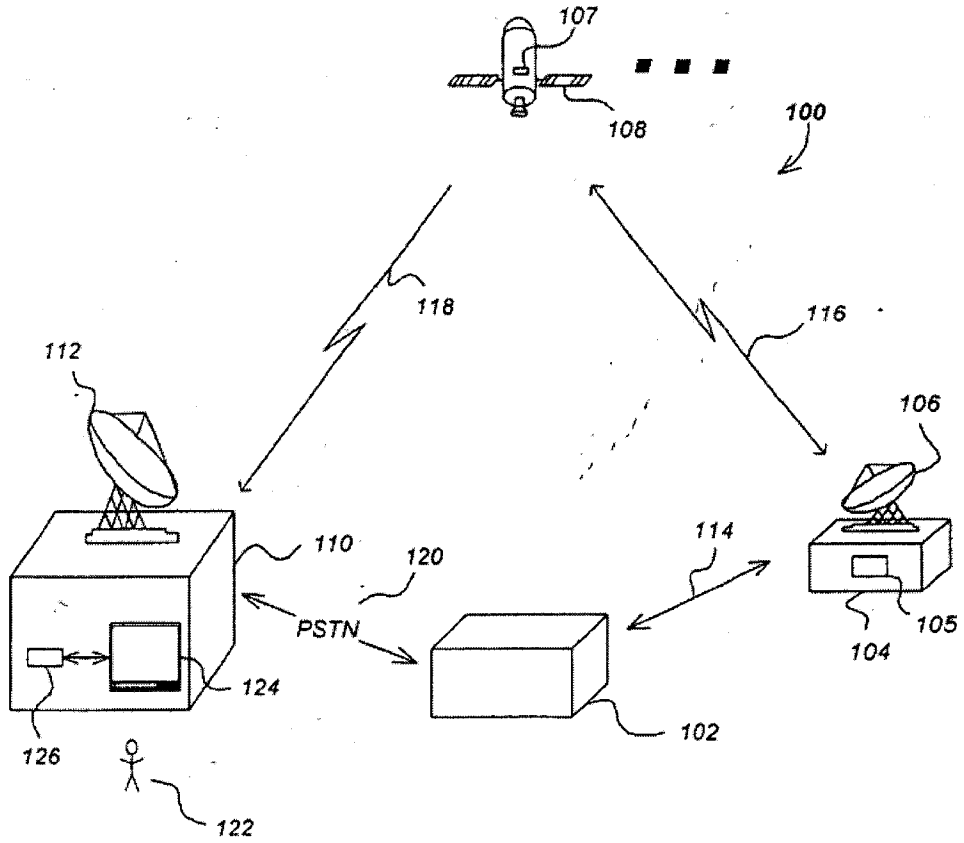
107
108
100
118
116
112
106
110
120
114
PSTN
105
104
124
126
102
122

FIG. 1

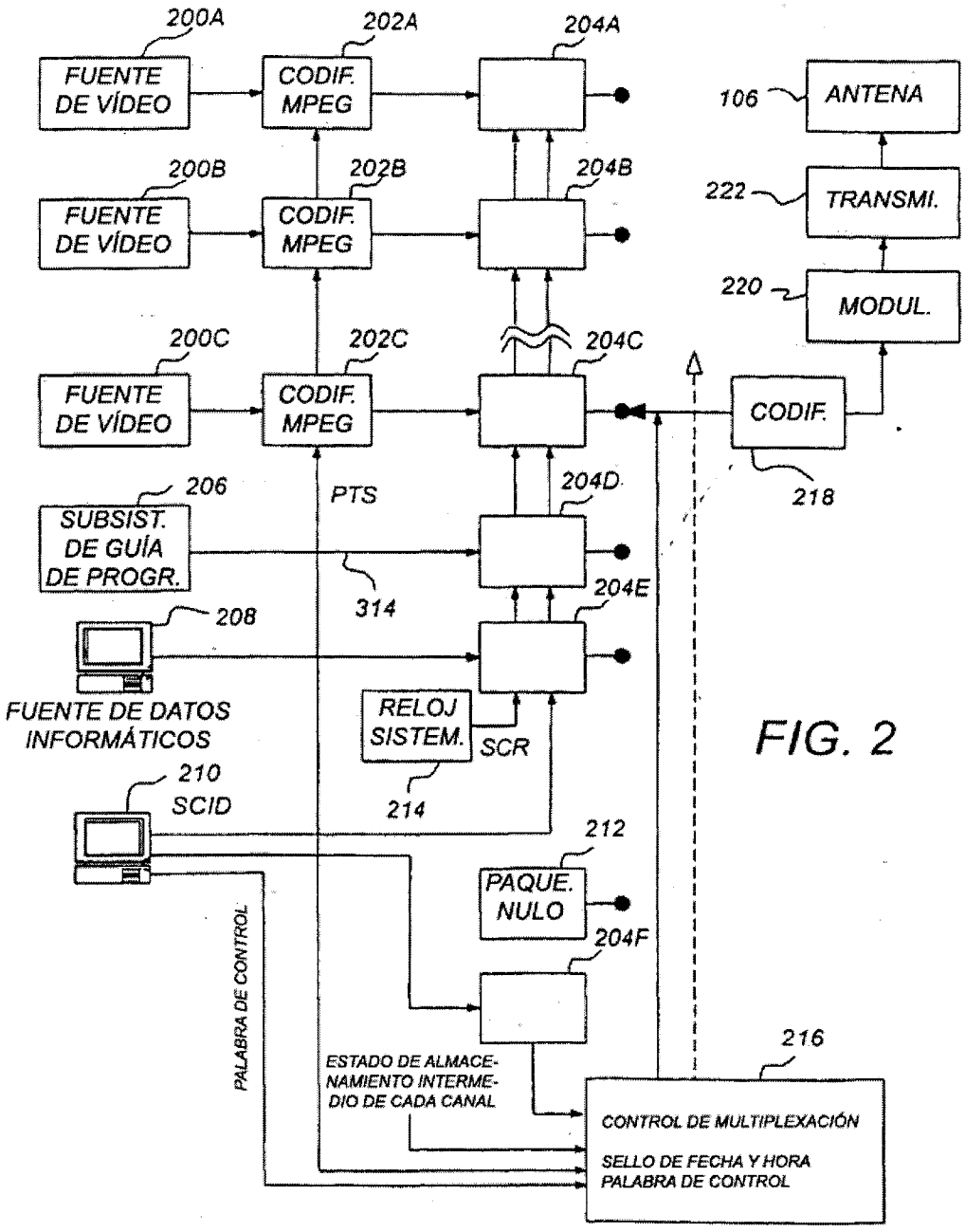
200A
FUENTE DE VÍDEO
202A
CODIF. MPEG
204A
106
ANTENA
200B
FUENTE DE VÍDEO
202B
CODIF. MPEG
204B
222
TRANSMI.
220
MODUL.
200C
FUENTE DE VÍDEO
202C
CODIF. MPEG
204C
CODIF.
218
206
SUBSIST. DE GUÍA DE PROGR.
PTS
204D
314
204E
208
FUENTE DE DATOS INFORMÁTICOS
RELOJ SISTEM.
SCR
214
210
SCID
212
PAQUE. NULO
204F
PALABRA DE CONTROL
ESTADO DE ALMACE-NAMIENTO INTERME-DIO DE CADA CANAL
216
CONTROL DE MULTIPLEXACIÓN
SELLO DE FECHA Y HORA
PALABRA DE CONTROL

FIG. 2

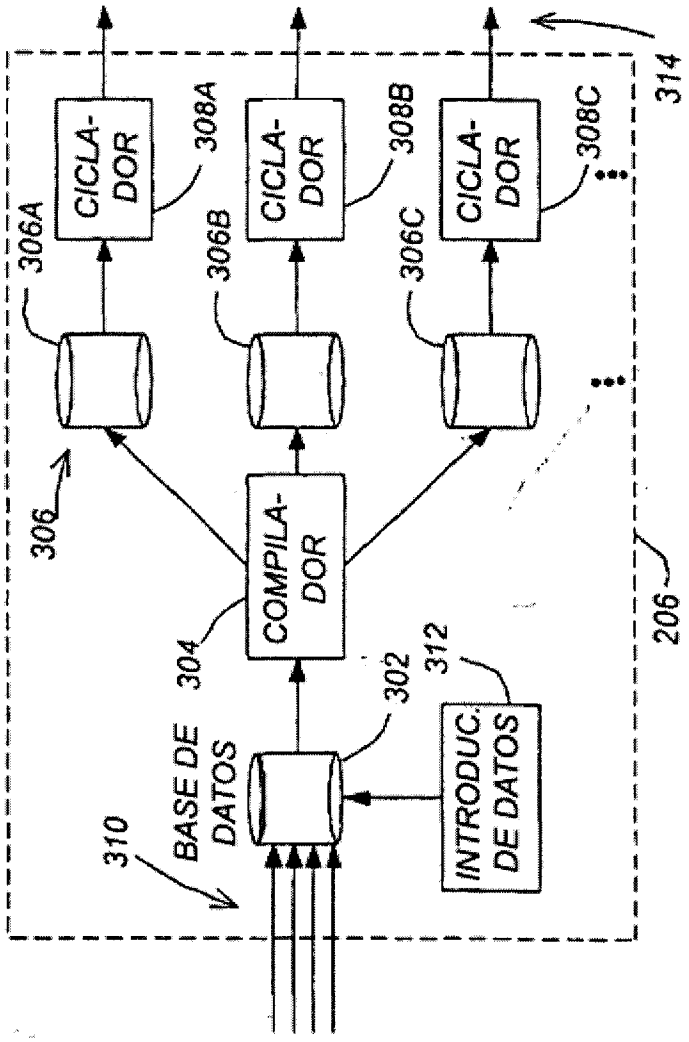
CICLA-DOR
308A
CICLA-DOR
308B
CICLA-DOR
308C
314
306A
306B
306C
306
COMPILA-DOR
304
206
302
312
BASE DE DATOS
310
INTRODUC. DE DATOS

FIG. 3

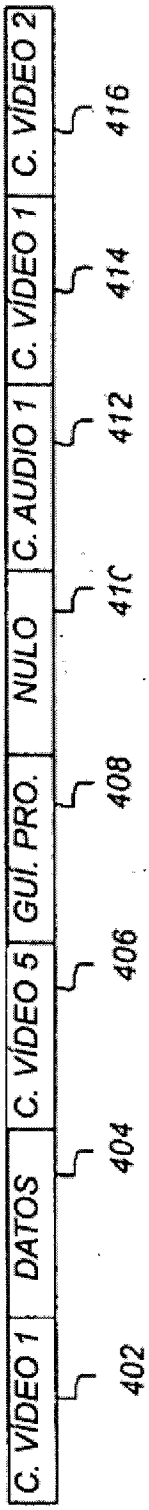
C. VÍDEO 1
DATOS
C. VÍDEO 5
GUI. PRO.
NULO
C. AUDIO 1
C. VÍDEO 1
C. VÍDEO 2
402
404
406
408
410
412
414
416

FIG. 4A

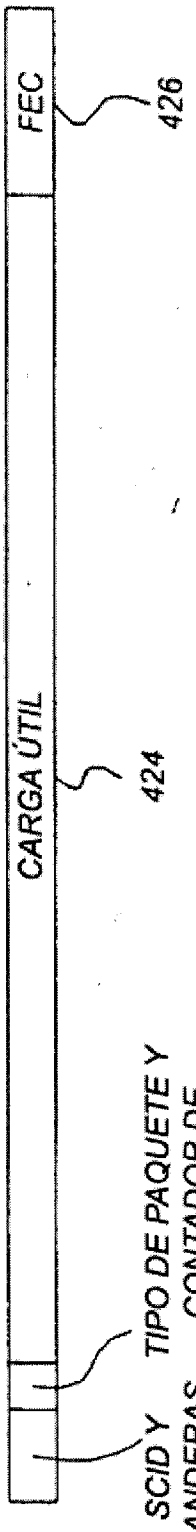
CARGA ÚTIL
FEC
424
426
SCID Y BANDERAS 420
TIPO DE PAQUETE Y CONTADOR DE CONTINUIDAD 422

FIG. 4B

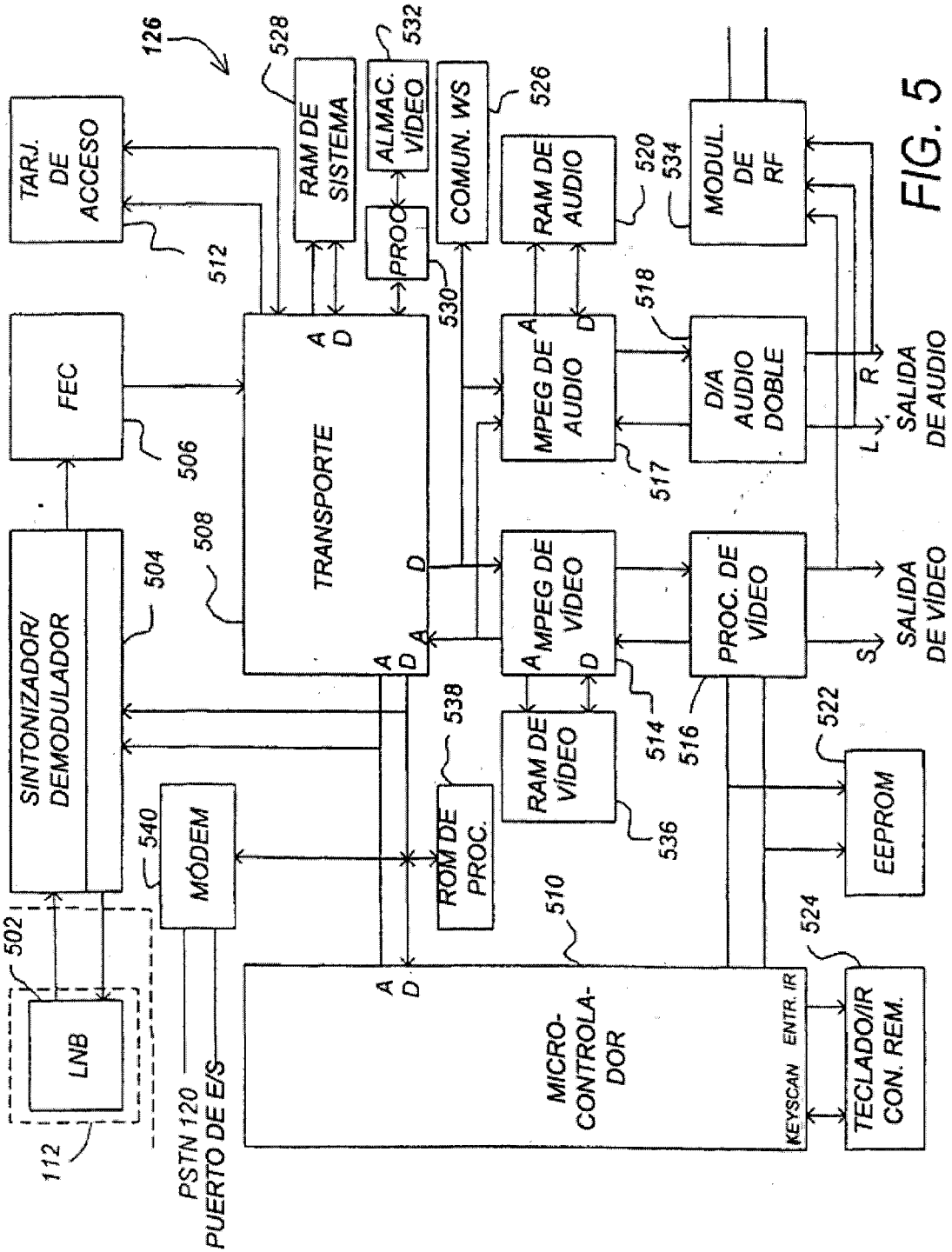
126
528
532
526
520
534
TARJ. DE ACCESO
RAM DE SISTEMA
ALMAC. VÍDEO
COMUN. WS
RAM DE AUDIO
MODUL. DE RF
512
PROC
530
FEC
TRANSPORTE
MPEG DE AUDIO
D/A AUDIO DOBLE
518
506
508
517
L
R
SALIDA DE AUDIO
SINTONIZADOR/ DEMODULADOR
504
MPEG DE VÍDEO
PROC. DE VÍDEO
S
SALIDA DE VÍDEO
538
522
514
516
RAM DE VÍDEO
ROM DE PROC.
EEPROM
536
540
MÓDEM
502
510
524
LNB
MICRO-CONTROLA-DOR
KEYSCAN
ENTR. IR
TECLADO/IR CON. REM.
112
PSTN 120
PUERTO DE E/S
A
D

FIG. 5

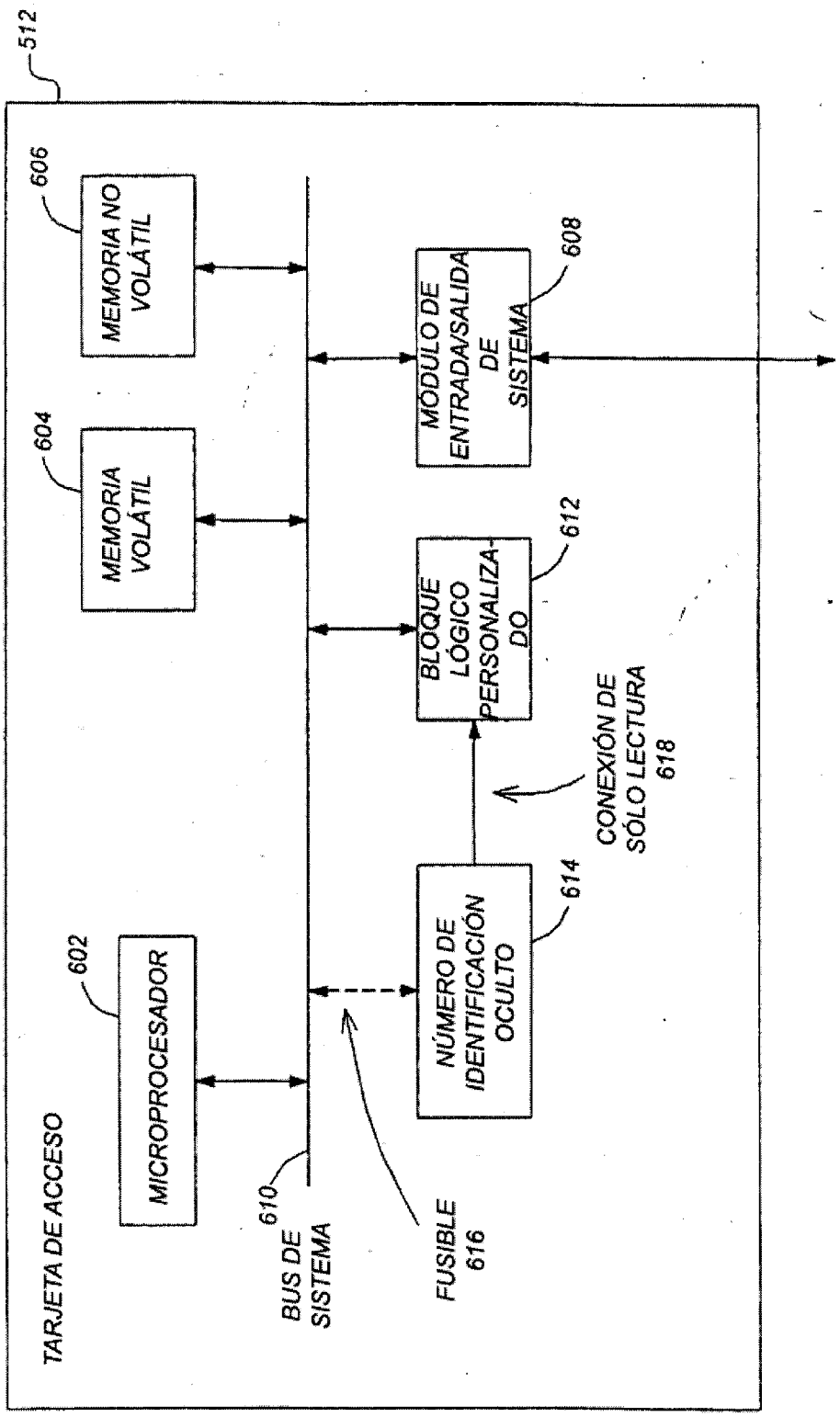
512
TARJETA DE ACCESO
606
MEMORIA NO VOLÁTIL
604
MEMORIA VOLÁTIL
608
MÓDULO DE ENTRADA/SALIDA DE SISTEMA
612
BLOQUE LÓGICO PERSONALIZADO
602
MICROPROCESADOR
614
NÚMERO DE IDENTIFICACIÓN OCULTO
CONEXIÓN DE SÓLO LECTURA 618
610
BUS DE SISTEMA
FUSIBLE 616

FIG. 6A

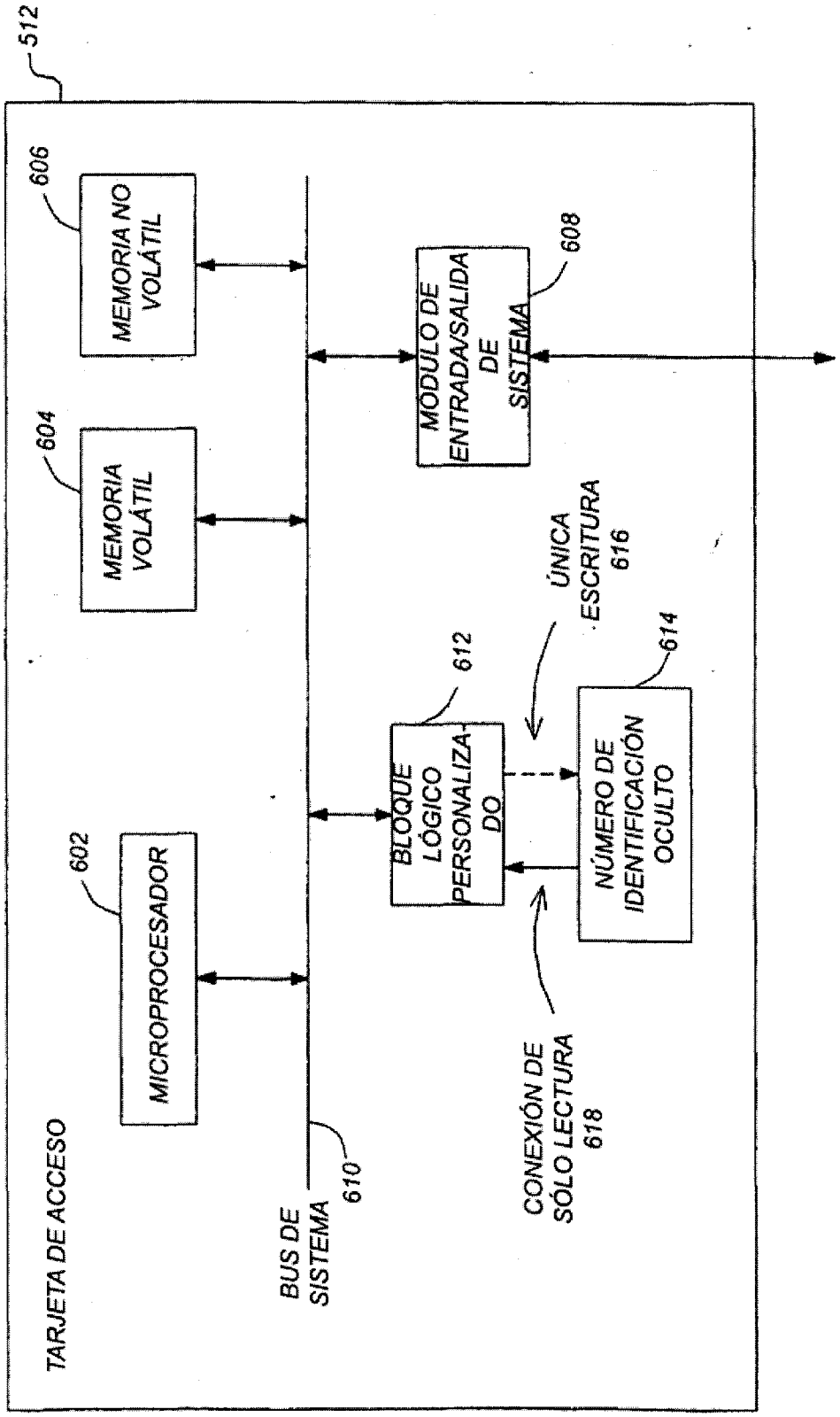
512
TARJETA DE ACCESO
606
MEMORIA NO VOLÁTIL
604
MEMORIA VOLÁTIL
602
MICROPROCESADOR
608
MÓDULO DE ENTRADA/SALIDA DE SISTEMA
612
BLOQUE LÓGICO PERSONALIZADO
614
NÚMERO DE IDENTIFICACIÓN OCULTO
ÚNICA ESCRITURA 616
CONEXIÓN DE SÓLO LECTURA 618
BUS DE SISTEMA 610

FIG. 6B

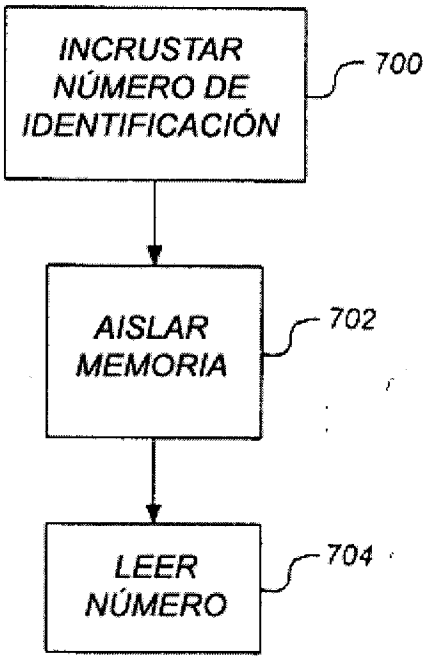
INCRUSTAR NÚMERO DE IDENTIFICACIÓN
700
AISLAR MEMORIA
702
LEER NÚMERO
704

FIG. 7