(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 993**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.06.2007 PCT/FR2007/000984**

(87) Fecha y número de publicación internacional: **21.12.2007 WO07144510**

(96) Fecha de presentación y número de la solicitud europea: **13.06.2007 E 07788889 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2019 EP 2027667**

(54) Título: **Procedimientos de difusión y recepción de un programa multimedia codificado, cabezal de red, terminal, receptor y procesador de seguridad para dichos procedimientos**

(30) Prioridad:

14.06.2006 FR 0605296

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.06.2020

(73) Titular/es:

VIACCESS (100.0%)
LES COLLINES DE L'ARCHE, TOUR OPERA C
92057 PARIS LA DEFENSE CEDEX, FR

(72) Inventor/es:

CARLES, PHILIPPE;
CHEVALLIER, ANTHONY;
DUBROEUCQ, GILLES y
LANFRANCHI, STÉPHANE

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimientos de difusión y recepción de un programa multimedia codificado, cabezal de red, terminal, receptor y procesador de seguridad para dichos procedimientos

[0001] La presente invención consiste en procedimientos de difusión y recepción de un programa multimedia codificado, un cabezal de red, un terminal, un receptor y un procesador de seguridad para dichos procedimientos.

[0002] Existen procedimientos de difusión de programas multimedia a través de redes de banda ancha con los cuales:

- una información puede enrutarse a una dirección de multidifusión, de modo que solo un grupo de varios terminales correspondientes a dicha dirección reciba la información y no otros terminales conectados a la misma red, y
- una información puede enrutarse a una dirección de unidifusión de modo que solo el terminal correspondiente a dicha dirección reciba la información y no otros terminales conectados a la misma red.

[0003] Por ejemplo, una red de este tipo es una red basada en el protocolo de Internet (IP), como la red de Internet, también conocida como «World Wide Web».

[0004] Según los procedimientos existentes, un cabezal de red:

- codifica el programa multimedia con una palabra de control,
- cifra la palabra de control para obtener un primer criptograma,
- cifra el primer criptograma para obtener un segundo criptograma; el primero y el segundo criptograma se realizan utilizando diferentes claves de cifrado seleccionadas del grupo formado por una clave operativa y una clave de licencia,
- multiplexa el segundo criptograma con el programa multimedia codificado para obtener contenido multiplexado,
- difunde contenido multiplexado a una dirección de multidifusión de difusión para establecer una conexión punto a multipunto entre el cabezal y varios receptores del contenido multiplexado, y
- en una conexión punto a punto establecida con un terminal que utilice la dirección de unidifusión de dicho terminal, transmite la clave de licencia individualmente a dicho terminal a través de dicha conexión punto a punto.

[0005] Paralelamente, los terminales conectados a la misma red ejecutan un procedimiento de recepción de los programas multimedia codificados difundidos. Según los procedimientos de recepción existentes, el terminal:

- escucha la dirección de multidifusión de difusión y recibe el contenido multiplexado,
- demultiplexa el contenido multiplexado recibido para obtener el segundo criptograma y el programa multimedia codificado,
- descifra el segundo criptograma para obtener el primer criptograma,
- descifra el primer criptograma para obtener la palabra de control; el primer y segundo descifrado se realizan utilizando diferentes claves de cifrado seleccionadas del grupo formado por la clave operativa y la clave de licencia, y
- descodifica el programa multimedia codificado con la palabra de control.

[0006] En la parte restante de esta descripción, la clave de licencia se denomina K_{Term}.

[0007] Con criptograma de la clave K_{Term}, nos referimos aquí a un contenido cifrado creado cifrando el resultado de la concatenación de la clave K_{Term} con, posiblemente, otros datos. Así, cifrando solo la clave K_{Term} se obtiene, como mínimo, un criptograma de la clave K_{Term}. En otros casos, este criptograma se obtiene cifrando el resultado de la concatenación de la clave K_{Term} con otros datos.

[0008] Según los procedimientos existentes, y a diferencia de otros procedimientos actuales de difusión y recepción de programas multimedia codificados por satélite, la palabra de control se codifica al menos dos veces y el cifrado de la palabra de control por cada terminal utiliza, además de una clave operativa K_{Proc}, la clave de licencia K_{Term} obtenida a través de una conexión punto a punto.

[0009] Si bien estos procedimientos resultan plenamente satisfactorios, hoy en día conviene seguir mejorando la seguridad de los procedimientos existentes para evitar la «piratería» de programas multimedia por parte de personas sin escrúpulos.

[0010] Así pues, la invención pretende satisfacer este deseo ofreciendo un procedimiento más seguro de difusión y recepción de programas multimedia codificados.

[0011] La finalidad de la invención es, por tanto, un procedimiento de difusión de programas multimedia codificados mediante el cual:

- el cabezal de red ejecuta una fase de autenticación del terminal, y
- si el terminal se ha autenticado correctamente, el cabezal de red envía un mensaje de transmisión de licencia al terminal que contiene la clave de licencia o un criptograma de la clave de licencia, a través de la conexión punto a punto establecida, y
- si el terminal no se autentica correctamente, el cabezal actúa para evitar que este terminal descifre completamente el programa multimedia codificado difundido.

[0012] La invención consiste asimismo en un procedimiento de recepción del programa multimedia codificado difundido utilizando el procedimiento anterior, mediante el cual el terminal opera conjuntamente con el cabezal de red durante la fase de autenticación para autenticarse.

[0013] En los procedimientos anteriores, la clave K_{Term}, o su criptograma, solo se transmite al terminal si ha sido correctamente autenticada de antemano por el cabezal de red. Así aumenta la seguridad del procedimiento, al dificultar la creación de terminales «piratas».

[0014] Los modos de realización de este procedimiento pueden constar de una o varias de las características siguientes:

- si el terminal se ha autenticado correctamente, el cabezal pasa a una fase de establecimiento de un túnel seguro en la conexión punto a punto creada, durante la cual establece, de manera aleatoria, una clave de sesión común al terminal y al cabezal, y luego envía al terminal el mensaje de transmisión de licencia cifrado con esta clave de sesión;
- el cabezal determina una clave única apta para identificar el terminal entre todos los terminales conectados a la red, a partir de:

  • datos previamente registrados conocidos por el cabezal de red que no le hayan sido transmitidos por el terminal, y
  • datos transmitidos por el terminal al cabezal, siendo los datos previamente registrados y datos transmitidos insuficientes por sí solos para determinar la clave única utilizada por dicho terminal; después, verifica que el terminal es capaz de cifrar o descifrar correctamente los datos con la clave única que ha determinado sin que el cabezal tenga que transmitir primero los datos previamente registrados o la clave única determinada a dicho terminal y, en caso afirmativo, que el terminal está autenticado;

- para verificar que el terminal es capaz de descifrar correctamente los datos cifrados con la clave única determinada, el cabezal de red envía un mensaje ECM («Entitlement Control Message») al terminal en el que el campo destinado a contener un criptograma de una palabra de control contiene un criptograma obtenido cifrando un dato desconocido del terminal utilizando la clave única determinada y, a continuación, comprueba que los datos desconocidos del terminal han sido descifrados correctamente por este terminal;
- el cabezal de red cifra la clave de licencia al menos utilizando la clave del procesador de seguridad del terminal para obtener un criptograma de la clave de licencia, e incorpora este criptograma de la clave de licencia en el mensaje de transmisión de licencia;
- el cabezal de red realiza sucesivamente en el tiempo el primer y segundo cifrado de la clave de licencia para obtener un criptograma de la clave de licencia; el primer y segundo cifrado se realizan utilizando diferentes claves de cifrado seleccionadas del grupo formado por la clave del procesador y la clave de cifrado de la clave de licencia, e incorpora únicamente dicho criptograma que contiene la clave de licencia cifrada dos veces en el mensaje de transmisión de licencia.

[0015] Los modos de realización del procedimiento de recepción pueden constar de una o varias de las características siguientes:

- durante la fase de establecimiento del túnel de seguridad:

  a) si el terminal se ha autenticado correctamente, este terminal operará conjuntamente con el cabezal para establecer la clave de sesión común y descifrar el mensaje de transmisión de licencia recibido utilizando la clave de sesión común, y
  b) si el terminal no se ha autenticado correctamente, se evitará el descifrado del programa multimedia por este;

- el terminal también procede a una fase de autenticación del cabezal de red y, si este se ha autenticado correctamente, el terminal obtiene la clave de licencia del mensaje de transmisión de licencia, mientras que si el cabezal no se ha autenticado correctamente, se impide el descifrado del programa multimedia por este terminal;
- durante el paso de autenticación del cabezal, el terminal comprueba que el cabezal es capaz de cifrar o descifrar correctamente los datos con la clave única determinada por el cabezal a partir de:

  • datos previamente registrados conocidos por el cabezal de red que no le hayan sido transmitidos por el

terminal, y
• de los datos transmitidos por el terminal al cabezal de red, siendo los datos previamente registrados y datos transmitidos insuficientes por sí solos para permitir determinar la clave única de dicho terminal;

- el procesador de seguridad descifra el criptograma de la clave de licencia utilizando la clave de procesador;
- el procesador de seguridad y el receptor realizan sucesivamente el primer y segundo descifrado de un criptograma de la clave de licencia; el primer y segundo descifrado se realizan utilizando, respectivamente, una primera y una segunda clave de descifrado diferentes seleccionadas del grupo formado por la clave del procesador y la clave de cifrado de la clave de licencia.

[0016] La invención consiste asimismo en un cabezal y un terminal capaces de implementar, respectivamente, los citados procedimientos de difusión y recepción.

[0017] La invención consiste asimismo en un receptor y un procesador de seguridad para el terminal mencionado anteriormente.

[0018] La invención se comprenderá mejor con la lectura de la descripción que aparece a continuación, la cual se facilita únicamente a modo ilustrativo pero no limitativo y haciendo referencia a planos en los cuales:

- la figura 1 es una ilustración esquemática de la arquitectura de un sistema de difusión y recepción de programas multimedia codificados,
- la figura 2 es un primer modo de realización de un procedimiento de difusión y recepción de programas multimedia codificados implementado en el sistema de la figura 1,
- las figuras 3 y 4 son un diagrama de flujo de un procedimiento de transmisión de una clave de licencia en el procedimiento de la figura 2, y
- la figura 5 es un diagrama de flujo de un segundo modo de realización de un procedimiento de difusión y recepción de programas multimedia codificados que puede implementarse en el sistema de la figura 1.

[0019] La figura 1 representa un sistema 2 de difusión y recepción de programas multimedia codificados. Este sistema 2 incluye uno o varios cabezales de red capaces de difundir programas multimedia de manera codificada y varios terminales capaces de recibir estos programas multimedia codificados con el fin de descodificarlos para poder utilizarlos. Por ejemplo, el terminal utiliza los programas multimedia recibidos para generar un flujo de vídeo que pueda visualizarse de forma clara en una pantalla.

[0020] Para simplificar la figura 1, solo se representan un cabezal 4 y tres terminales 6, 7 y 8.

[0021] El cabezal de red 4 incluye:

- un generador 10 de mensajes ECM («Entitlement Control Message»),
- un generador 12 de mensajes EMM («Entitlement Management Message»),
- un codificador 13 apto para codificar un programa multimedia con una palabra de control CW,
- un módulo 14 apto para la difusión a una o más direcciones de multidifusión para la difusión de contenidos multiplexados,
- un administrador 16 de derechos de acceso, denominado ORM («Online Rights Manager»), apto para comunicar una clave de licencia K_{Term} a los terminales para que puedan descifrar los programas multimedia codificados, y
- medios para almacenar información, como una memoria 18 que contiene datos secretos previamente registrados.

[0022] El generador 10 también contiene un módulo criptográfico 22 capaz de ejecutar algoritmos criptográficos para crear un criptograma de la palabra de control CW.

[0023] El generador 12 es capaz de generar claves criptográficas y, en particular, la clave de licencia K_{Term}, así como de transmitir las claves así generadas al generador 10 y al administrador 16.

[0024] El módulo 14 es capaz de multiplexar el programa multimedia codificado con mensajes ECM generados por el generador 10 y mensajes EMM generados por el generador 12 para obtener contenido multiplexado. Normalmente, los mensajes ECM multiplexados con el programa multimedia codificado contienen un criptograma de la palabra de control CW utilizada para codificar este programa multimedia. Los mensajes ECM también suelen contener condiciones de acceso asociadas con el programa multimedia codificado.

[0025] Los mensajes EMM generalmente contienen información, como claves o derechos, que permite o prohibir que un terminal descifre correctamente los programas multimedia codificados recibidos para poder utilizarlos.

[0026] El módulo 14 también es capaz de encapsular cada contenido multiplexado en tramas IP (protocolo de Internet).

[0027] Aquí, los programas multimedia son generados por diferentes operadores de servicios. Para simplificar la figura 1, solo se ha representado un operador 20.

[0028] El administrador 16 es capaz de comunicar la clave de licencia K_{Term} a través de una conexión punto a punto establecido con un terminal determinado utilizando su dirección de unidifusión. El administrador 16 también incluye un módulo criptográfico 24 capaz de desempeñar diferentes funciones criptográficas y, en particular, un algoritmo criptográfico A_{KS} y una función hash H_S.

[0029] Los mensajes generados por el administrador 16 que contienen la clave de licencia K_{Term} se denominan aquí mensajes ECM-U y tienen la misma estructura que los mensajes ECM convencionales. En particular, estos mensajes ECM-U incluyen un campo para recibir un criptograma y otro para recibir condiciones de acceso. Sin embargo, a diferencia de un mensaje ECM convencional que se dirige a todos los procesadores de seguridad de un operador, un mensaje ECM-U únicamente puede ser procesado por un solo procesador de seguridad para el cual se ha generado utilizando claves individualizadas para dicho procesador de seguridad. Se trata de un direccionamiento individual implícito. Téngase en cuenta que, de forma similar, un mensaje calificado como ECM-S puede dirigirse a un grupo de procesadores de seguridad que compartan el mismo identificador de grupo y las mismas claves.

[0030] A modo de ejemplo, los datos secretos incluidos en la memoria 18 son aquí:

- una clave raíz $K_{ROOTECMU}$,
- una lista de las claves de procesador de seguridad K_{ProcU} que asocian a cada identificador UA de un procesador de seguridad la clave K_{ProcU} previamente registrada en dicho procesador de seguridad,
- una lista de las claves de receptores K_r que asocian una clave K_r a cada identificador STBId de receptor, y
- una clave $K_{licence}$ para cifrar la clave de licencia K_{Term}.

[0031] La memoria 18 está conectada al generador 10 y al administrador 16.

[0032] La red utilizada para transmitir contenidos multiplexados y mensajes ECM-U a los distintos terminales es una red de banda ancha 30 que utiliza el protocolo de Internet (IP). Cabe recordar que este protocolo utiliza enrutadores capaces de enrutar una trama de información a una dirección específica. En el protocolo IP, se utiliza una dirección de multidifusión para establecer una conexión punto a multipunto. Una dirección de multidifusión de este tipo difiere de una dirección de difusión amplia («broadcast») en que las tramas de información solo se enrutan a un grupo limitado de varios terminales entre todos los terminales conectados a la red 30. La dirección de multidifusión también difiere de una dirección de unidifusión en que solo permite establecer una conexión punto a punto.

[0033] Se supone que los terminales 6, 7 y 8 son idénticos y solo se describirá detalladamente el 8.

[0034] El terminal 8 incluye un receptor 40 asociado con un procesador de seguridad extraíble 42.

[0035] El receptor 40 está equipado con un módem 44, un módulo 46 de demultiplexación, desaleatorización y decodificación y un módulo de software de control de acceso 48.

[0036] El receptor 40 también incluye una memoria 50 en la que se pueden almacenar los programas multimedia recibidos para su posterior visualización.

[0037] El módem 44 está conectado a la red 30 y permite, por ejemplo, recibir contenido multiplexado y mensajes ECM-U transmitidos por el cabezal de red 4.

[0038] El módulo 46 es especialmente adecuado para demultiplexar contenidos multiplexados recibidos, transmitir mensajes ECM y EMM al módulo 48, descodificar programas multimedia codificados de manera que se genere un flujo multimedia utilizable, por ejemplo, mostrándolo claramente en una pantalla 52 conectada al terminal 8.

[0039] El módulo 48 asegura la interconexión con el procesador 42. En particular, transmite los mensajes ECM y EMM al procesador 42 y recibe del procesador 42 la palabra de control descifrada que el módulo 46 utilizará para descodificar los programas multimedia recibidos.

[0040] Aquí el módulo 48 está equipado con un módulo criptográfico secundario 54 capaz de realizar operaciones criptográficas como el cifrado o descifrado correspondiente a las implementadas por el cabezal y la función hash H_S.

[0041] Con este fin, el submódulo 54 está asociado a medios de almacenamiento de información como una memoria 55 que también contiene las claves criptográficas secretas que le permiten llevar a cabo operaciones criptográficas. Por ejemplo, la memoria 55 incluye la clave $K_{licence}$ y la clave K_r. Estas claves, por ejemplo, se han cargado previamente en el terminal 40 durante su fabricación o han sido recibidas por la terminal 40 a través de un

mensaje EMM. La memoria 55 también incluye un identificador STBId que identifica de manera única el receptor 40 entre todos los receptores del sistema 2.

[0042] El procesador 42 es, por ejemplo, una tarjeta inteligente. Este procesador 42 está diseñado para realizar todas las operaciones de seguridad, así como el control de acceso a programas multimedia. Con este fin, incluye, en particular, un módulo 56 de cifrado y descifrado, así como una memoria no volátil 58.

[0043] El módulo 56 es, en particular, capaz de ejecutar algoritmos de descifrado y cifrado correspondientes a los implementados por el cabezal de red 4.

[0044] La memoria 58 contiene, entre otros elementos:

- derechos de acceso y claves 60,
- un identificador UA que identifica de forma única este procesador de seguridad entre todos los procesadores de seguridad utilizados en el sistema 2,
- dos claves únicas previamente registradas K_{ECMU} y K_{ProcU} para identificar este procesador de seguridad entre todos los procesadores de seguridad utilizados en el sistema 2,
- una clave operativa K_{Proc}.

[0045] Las dos claves K_{ECMU} y K_{ProcU} se individualizan en este procesador de seguridad en relación con el identificador UA. Estas dos claves K_{ECMU} y K_{ProcU}, así como el identificador UA, se cargan normalmente en la memoria 58 cuando el procesador de seguridad se fabrica, configura o utiliza mediante mensajes EMM.

[0046] La clave K_{Proc} es la clave utilizada por el cabezal de red para producir el criptograma de la palabra de control insertada en los mensajes ECM difundidos a cada uno de los terminales del sistema 2. Esta clave, común a todos los terminales del operador, se carga normalmente en la memoria 58 a través de un mensaje EMM transmitido por el cabezal de red. Normalmente, este mensaje EMM se difunde en una dirección de multidifusión de difusión. Por ejemplo, este mensaje EMM se multiplexa con el programa multimedia codificado y luego se transmite a los terminales.

[0047] El funcionamiento del sistema 2 se describirá ahora con respecto al procedimiento de las figuras de la 2 a la 4.

[0048] Durante el funcionamiento del sistema 2, el cabezal de red 4 ejecuta un procedimiento 80 de difusión de programas multimedia codificados y cada uno de los terminales ejecuta paralelamente un procedimiento 82 de recepción de los programas multimedia difundidos por el cabezal de red 4.

[0049] Inicialmente, al comienzo del procedimiento 80, en un paso 90, el generador 12 genera una clave de licencia K_{Term}. Luego, en un paso 92, el generador 12 transmite esta clave K_{Term} al generador 10 y al administrador 16.

[0050] Después, en un paso 94, el cabezal de red genera una palabra de control CW y, en un paso 96, el codificador 13 codifica el programa multimedia con esta palabra de control.

[0051] En este punto, en un paso 98, el generador 10 cifra la palabra de control CW mediante el módulo 22 usando un algoritmo de cifrado A_{Term} y la clave K_{Term} generada por el generador 12. Al final de la fase 98, se obtiene un primer criptograma $CW*_{KTerm}$ de la palabra de control CW mediante la clave K_{Term}.

[0052] Luego, en un paso 100, el generador 10 cifra el criptograma $CW*_{KTerm}$ mediante el módulo 22 usando la clave K_{Proc} y un algoritmo de cifrado A_{Proc}. Al final de la fase 100, se obtiene un criptograma $(CW*K_{Term})*K_{Proc}$ del criptograma $CW*K_{Term}$ anterior.

[0053] En una fase 102, el generador 10 crea un mensaje ECM que contiene el criptograma $(CW*K_{Term})*_{KProc}$ y las condiciones de acceso.

[0054] Luego, en una fase 104, el mensaje ECM creado, posibles mensajes EMM, así como el programa multimedia codificado, se multiplexan juntos para formar un contenido multiplexado. En un paso 106, este contenido multiplexado se encapsula en tramas IP (protocolo de Internet). El contenido multiplexado encapsulado en tramas IP se transmite entonces, en un paso 108, a una o varias direcciones de multidifusión de difusión.

[0055] Los pasos del 94 al 108 se repiten cada vez que un programa multimedia se codifica con una nueva palabra de control. Los pasos del 90 al 108 se repiten cada vez que se cambia la clave K_{Term}.

[0056] El procedimiento de recepción 82 es ejecutado de forma idéntica por cada uno de los terminales del sistema 2. Para simplificar la descripción, este procedimiento se describirá aquí solo en el caso del terminal 8.

[0057] Inicialmente, en un paso 120, la terminal 8 escucha la dirección de multidifusión de difusión donde se

difunden los programas multimedia. Luego, en un paso 122, el contenido multiplexado de difusión se recibe y, después, se demultiplexa.

[0058] En un paso 124, los mensajes ECM y EMM extraídos del contenido multiplexado se transmiten a través del módulo 48 al procesador de seguridad 42. En un paso 126, el procesador de seguridad 42 compara las condiciones de acceso incluidas en el mensaje de ECM con los derechos de acceso 60.

[0059] Si los derechos de acceso almacenados en la memoria 58 no se corresponden con las condiciones de acceso recibidas, el procesador de seguridad actúa, en un paso 128, para impedir la descodificación del programa multimedia codificado recibido. Por ejemplo, el procesador de seguridad no descifra la palabra de control incluida en el mensaje ECM ni transmite la palabra de control descifrada al receptor 40. En el paso 128, el procesador 42 también puede transmitir una palabra de control incorrecta al receptor 40 en lugar de la palabra de control correcta.

[0060] Si los derechos de acceso se corresponden con las condiciones de acceso recibidas, en un paso 130, el módulo 56 descifra el criptograma $(CW^*K_{Term})^*_{KProc}$ utilizando la clave operativa K_{Proc} incluida en la memoria 58. Así, al final del paso 130, se obtiene el criptograma CW^*_{KTerm}.

[0061] Luego, el procesador 42 transmite el criptograma CW^*_{KTerm} al receptor 40 en un paso 132.

[0062] En un paso 134, el módulo 48 y, más concretamente, el submódulo 54 descifra el criptograma CW^*_{KTerm} con la clave K_{Term}, previamente recibida, para obtener la palabra de control CW sin cifrar. La palabra de control CW obtenida de este modo se utiliza, en un paso 136, para descodificar el programa multimedia codificado recibido.

[0063] Por lo tanto, se entiende que en este modo de realización, la palabra de control CW se cifra previamente utilizando la clave K_{Term}, de modo que la descodificación de los programas multimedia recibidos solo es posible si el cabezal ha transmitido previamente la clave K_{Term} al terminal. La forma en que el cabezal transmite la clave K_{Term} a cada uno de los terminales se describirá ahora junto a las figuras 3 y 4 en el caso particular del terminal 8.

[0064] Para que el terminal 8 pueda descodificar los programas multimedia codificados recibidos según el procedimiento de la figura 2, se establece una conexión punto a punto, en un paso 150, entre este terminal y el administrador 16, normalmente por iniciativa del terminal. Por ejemplo, el terminal 8 activa esta conexión punto a punto cuando este se enciende o se activa. Para establecer esta conexión punto a punto, el terminal 8 utiliza la dirección de unidifusión del administrador 16.

[0065] Luego, el cabezal de red y el terminal 8 proceden a un paso 152 de establecimiento de un túnel seguro en esta conexión punto a punto.

[0066] Más concretamente, en el paso 154, el módulo 48 envía a través de la conexión punto a punto una petición de una licencia para descodificar programas multimedia. Esta petición contiene un identificador de sesión $ID_{session}$, un identificador STBId, un identificador SOID del operador, así como el identificador UA. El identificador $ID_{session}$ se genera aleatoriamente cada vez que se establece un túnel seguro.

[0067] En el paso 156, el administrador 16 recibe esta petición.

[0068] En respuesta a esta petición, el administrador 16:

- genera un número aleatorio $AleaA_{uth}$ y una clave de sesión K_s aleatoria, en un paso 158,
- determina a partir del identificador UA recibido una clave K_{ECMU} única que coincide con la clave K_{ECMU} incluida en la memoria 58 del terminal 8, en un paso 160,
- concatena el identificador $ID_{session}$, el número de $AleaA_{uth}$ y la clave de sesión K_s y luego cifra el resultado de esta concatenación utilizando la clave K_r correspondiente al identificador STBId recibido para obtener un primer criptograma, en un paso 162,
- cifra este primer criptograma con la clave K_{ECMU} determinada en el paso 160 para obtener un segundo criptograma, en un paso 164,
- encapsula este segundo criptograma en un mensaje ECM-U insertando el segundo criptograma en el campo previsto para recibir un criptograma de una palabra de control en un mensaje ECM, en un paso 166, y luego
- envía este mensaje ECM-U al terminal 8 a través de la conexión punto a punto del paso 168.

[0069] En el paso 160, la clave K_{ECM} se determina a partir del identificador UA recibido y de los datos previamente registrados en la memoria 18. Por ejemplo, aquí, la clave K_{ECMU} se genera diversificando la clave raíz de $K_{RootECMU}$ con el identificador UA recibido.

[0070] En un paso 170, el terminal 8 recibe el mensaje ECM-U y el módulo 48 transmite este mensaje ECM-U al procesador 42.

[0071] Luego, en un paso 172, el procesador 42 descifra el segundo criptograma usando la clave K_{ECMU} incluida en su memoria 58 para obtener el primer criptograma.

[0072] En un paso 174, el primer criptograma obtenido de esta manera se transmite al receptor 40 y, en un paso 176, el módulo 48 y, más concretamente, el submódulo 54 descifra este primer criptograma utilizando la clave K_r incluida en su memoria 52.

[0073] Luego, en el paso 178, el módulo 48 compara el identificador $ID_{session}$ descifrado en el paso 176 con el enviado en el paso 154.

[0074] Si los identificadores $ID_{session}$ coinciden, entonces el módulo 58 aplica, en un paso 180, la función hash H_s al número de $AleaA_{uth}$ para obtener un resultado R_h. La función hash H_s es una función hash unidireccional.

[0075] Después, en el paso 182, el módulo 48 cifra el resultado R_h utilizando la clave de sesión K_s descifrada en el paso 176 para obtener un criptograma $(R_h)*K_s$.

[0076] En un paso 184, el terminal 8 transmite el criptograma $(R_h)*_{Ks}$ al cabezal de red 4 mediante la conexión punto a punto.

[0077] En un paso 190, el administrador 16 recibe el criptograma $(R_h)*_{Ks}$ y luego, en el paso 192, descifra este criptograma utilizando la clave K_s generada en el paso 158, para encontrar el resultado R_h.

[0078] En un paso 194, el administrador 16 aplica al número $AleaA_{uth}$ generado en el paso 158 la misma función hash H_s que debería haber utilizado la terminal 8 para crear el resultado R_h.

[0079] En el paso 196, se comparan los resultados R_h obtenidos al final de los pasos 192 y 194. Si los resultados coinciden, el administrador 16 establece, en un paso 198, que el terminal 8 es auténtico y que todos los demás mensajes intercambiados a través de la conexión punto a punto están cifrados con la clave de sesión K_s.

[0080] En el caso de que los identificadores $ID_{session}$ comparados en el paso 178 o los resultados del R_h comparados en el paso 196 no coincidan, entonces la autenticación mutua del terminal 8 y el cabezal de red 4 ha fallado y no se ha establecido ningún túnel seguro de transmisión de información entre los mismos. Además, en un paso 200, el administrador 16 o el terminal 8 actúan para impedir la descodificación de los programas multimedia codificados recibidos. Por ejemplo, en el paso 200, el administrador 16 impide la transmisión de la clave K_{Term} al terminal 8. Normalmente, el administrador 16 interrumpe la conexión punto a punto establecida antes de que se pueda realizar la transmisión de la clave K_{Term}.

[0081] En el caso de que la autenticación mutua del terminal 8 y del cabezal de red se haya realizado correctamente, en un paso 210, el administrador 16 cifra la clave K_{Term} con la clave $K_{licence}$ para obtener un criptograma $(K_{Term})\ K_{licence}$.

[0082] En un paso 212, este criptograma $(K_{Term})*K_{License}$ se cifra utilizando la clave K_{ProcU} para obtener un criptograma $((K_{Term})*K_{licence})*K_{ProcU}$. Luego, en un paso 214, este criptograma $((K_{Term})*K_{licence})*K_{ProcU}$ se inserta en un mensaje ECM-U asociado con las condiciones de acceso a dicha clave K_{Term}.

[0083] En un paso 216, este mensaje ECM-U se transmite a través del túnel seguro establecido entre el terminal 8 y el administrador 16. Así, en el paso 216, este mensaje es cifrado por el administrador 16 usando la clave K_s.

[0084] En un paso 218, el terminal 8 recibe este mensaje ECM-U; luego, en el paso 220, descifra el mensaje ECM-U usando la clave K_s.

[0085] En un paso 222, el módulo 48 transmite el mensaje ECM-U descifrado al procesador de seguridad.

[0086] En un paso 224, el procesador 42 compara las condiciones de acceso incluidas en este mensaje ECM-U con el derecho de acceso 60.

[0087] Si las condiciones de acceso no coinciden con el derecho de acceso incluido en la memoria 58, en un paso 226, el procesador 42 actúa para evitar que las palabras de control CW se descifren utilizando la clave K_{Term} incluida en dicho mensaje ECM-U. Por ejemplo, el procesador 42 no descifra criptogramas de la clave K_{Term}.

[0088] De lo contrario, es decir, si los derechos de acceso corresponden a las condiciones de acceso, en un paso 228, el módulo 56 descifra el criptograma $((K_{Term})*K_{licence})*K_{ProcU}$ utilizando la clave almacenada K_{ProcU} incluida en la memoria 58 para encontrar el criptograma $(K_{Term})*K_{license}$.

[0089] El criptograma $(K_{Term})*K_{license}$ se transmite entonces, en un paso 230, al receptor 40. En un paso 232, el

módulo 48 y, más concretamente, el módulo secundario 54 descifra el criptograma $(K_{Term})*K_{license}$ usando la clave $K_{licence}$ incluida en la memoria 52 para obtener la clave K_{Term} sin cifrar.

[0090] En un paso 234, la clave K_{Term} sin cifrar se almacena, por ejemplo, en la memoria 55 para usarla con el fin de descifrar las palabras de control CW previamente cifradas usando la misma clave K_{Term}.

[0091] Téngase en cuenta que los pasos del 154 al 178 constituyen un paso de autenticación del cabezal de red por el terminal. Por su parte, los pasos del 158 al 196 constituyen una fase de autenticación del terminal por el cabezal.

[0092] La figura 5 representa otro procedimiento, el 240, para la difusión de programas multimedia codificados que pueden ser implementados por el cabezal 4, y otro procedimiento, el 242, para la recepción de estos programas multimedia codificados que pueden ser implementados por los terminales del 6 al 8.

[0093] Los pasos 244, 246, 248 y 250 del procedimiento 240 son idénticos a los pasos 90, 92, 94 y 96 del procedimiento 80, respectivamente.

[0094] Luego, en el paso 252, el generador 10 cifra la palabra de control usando la clave K_{Proc} para obtener un criptograma CW*.

[0095] En un paso 254, este criptograma CW* y las condiciones de acceso se incorporan a un mensaje ECM.

[0096] Luego, en un paso 256, al menos la parte del mensaje ECM que contiene el criptograma CW* se sobrecifra con la clave K_{Term} para obtener un criptograma ECM*.

[0097] En un paso 258, el criptograma ECM*, los posibles mensajes EMM y el programa multimedia codificado son multiplexados por el multiplexor 14 para obtener contenido multiplexado.

[0098] A continuación, en los pasos 260 y 262, este contenido multiplexado se encapsula y difunde en la red 30 del mismo modo que en los pasos 106 y 108.

[0099] Los pasos del 248 al 262 se repiten para cada nueva palabra de control, mientras que los pasos del 244 al 262 se repiten cada vez que se modifica la clave K_{Term}.

[0100] El procedimiento 242 comienza con los pasos 270 y 272 idénticos a los pasos 120 y 122, respectivamente, del procedimiento 82.

[0101] Luego, en un paso 274, el módulo 48 y, más concretamente, el módulo secundario 54 descifra el criptograma ECM* usando la clave K_{Term} para encontrar el mensaje ECM sin cifrar.

[0102] El mensaje ECM sin cifrar y los posibles mensajes EMM incluidos en el contenido multiplexado se transmiten al procesador de seguridad 42, en un paso 276.

[0103] En un paso 280, el procesador 42 compara las condiciones de acceso incluidas en el mensaje ECM con los derechos de acceso 60. Si estos derechos de acceso no coinciden con las condiciones de acceso, en un paso 282, el procesador 42 actúa para impedir la descodificación completa de los programas multimedia codificados recibidos.

[0104] De lo contrario, en un paso 284, el módulo 56 descifra el criptograma CW* utilizando la clave K_{Proc} para encontrar la palabra de control CW sin cifrar.

[0105] A continuación, en un paso 286, la palabra de control CW descifrada se transmite al receptor 40.

[0106] Luego, en un paso 288, el receptor 40 descodifica el programa multimedia codificado recibido usando la palabra de control CW transmitida en el paso 286.

[0107] Los pasos del 270 al 288 se repiten al menos para cada nueva palabra de control CW.

[0108] En este segundo modo de realización, la palabra de control CW se sobrecifra utilizando la clave K_{Term} en lugar de cifrarse previamente. Sin embargo, como en el modo de realización de la figura 2, la descodificación de programas multimedia codificados recibidos solo es posible si el terminal ha recibido previamente la clave K_{Term}. Para ello se implementa, por ejemplo, el procedimiento de transmisión de esta clave K_{Term} ya descrito en las figuras 3 y 4.

[0109] Hay muchos otros modos de realización posibles. Por ejemplo, en lugar de una red 30 pueden utilizarse redes distintas de las basadas en IP, siempre que permitan el uso de direcciones de multidifusión y unidifusión de forma similar al que permite el protocolo IP.

[0110] El procesador de seguridad 42 se puede integrar en el receptor 40. Como alternativa, los módulos 46 y 48 se pueden implementar en un módulo extraíble.

[0111] Las diferentes funcionalidades del terminal 8 pueden distribuirse entre diferentes dispositivos conectados entre sí por una red local. Por ejemplo, estas diferentes funcionalidades pueden dividirse entre una pasarela local denominada «Home Gateway» y un decodificador local, cualquiera de los cuales puede recibir el procesador de seguridad 42. La pasarela es, pues, el elemento conectado a la red 30 que escucha direcciones de multidifusión o unidifusión. A continuación, la información recibida de la red 30 se transmite al decodificador local a través de la red local. En una arquitectura de este tipo, la pasarela puede, por ejemplo, encargarse del procesamiento de mensajes ECM para extraer las palabras de control necesarias para descodificar programas multimedia codificados. Evidentemente, hay otras arquitecturas posibles para el terminal 8.

[0112] El módem 44 puede integrarse en el receptor 40 o colocarse en el exterior.

[0113] El procedimiento de las figuras 3 y 4 se ha descrito en el caso concreto en que el mensaje ECM-U contiene una condición de acceso. Como alternativa, dicha condición no se implementa de modo que el terminal pueda descifrar la clave K_{Term} independientemente de los derechos de acceso 60 almacenados en su memoria 58.

[0114] Los modos de implementación de las figuras 2 y 5 pueden combinarse de manera que se aplique tanto el cifrado previo como el «sobrecifrado» de la palabra de control. En estas condiciones, para descifrar la palabra de control CW es necesario utilizar dos claves de licencia K_{Term}, una para realizar la cifrado previo y la otra para realizar el «sobrecifrado».

[0115] Las claves K_{Term}, $K_{license}$ y K_{ProcU} son únicas para cada terminal del sistema 2 o comunes a un grupo de terminales del sistema 2 o bien comunes a todos los terminales del sistema 2.

[0116] Aquí se ha descrito el sistema 2 en el caso concreto en que la clave K_{Term} se transmite en un mensaje ECM-U con una estructura idéntica a la de un mensaje ECM. Como alternativa, la clave K_{Term} es transmitida por el administrador 16 a la terminal 8 usando un mensaje EMM y, preferiblemente, un mensaje EMM-U.

[0117] Dependiendo del identificador UA, las claves individualizadas K_{ECMU} y K_{ProcU} se pueden obtener mediante la diversificación de una clave raíz utilizando el identificador UA o a partir de una base de datos que asocia las claves K_{ECMU} y K_{ProcU} únicas con cada identificador UA. Del mismo modo, la clave K_r del receptor se puede obtener diversificando una clave raíz del identificador STBId o una base de datos que asocia una clave K_r a cada identificador STBId.

[0118] El sistema 2 y los procedimientos que se describen en el presente documento se aplican tanto a los programas multimedia difundidos en directo, como, por ejemplo, un programa de televisión difundido en directo, como a los programas multimedia previamente grabados y descargables a petición de un usuario del terminal, por ejemplo, como parte de un servicio de vídeo a la carta (VOD, por sus siglas en inglés).

[0119] El sistema 2 y los procedimientos que se describen en el presente documento se aplican también a un servicio de explotación PVR («Personal Video Recorder») que permite grabar y reproducir contenidos multimedia desde la memoria 50, como se describe, por ejemplo, en la solicitud de patente FR 2 835 178. Para dicho servicio PVR, los mensajes ECM asociados con los contenidos recibidos por el terminal incluyen:

a) una parte dedicada a la visualización directa del contenido, y
b) una parte dedicada a la grabación y reproducción del programa multimedia recibido.

[0120] La parte a) contiene los elementos habituales de un mensaje ECM, en particular, el criptograma de la palabra de control CW.

[0121] La parte b) también contiene elementos habituales de un mensaje ECM, tales como las condiciones de acceso y un criptograma de la palabra de control, pero estos están destinados a extraerse y luego, tras su procesamiento local en el terminal, grabarse con el programa multimedia almacenado en la memoria 50. Estos mensajes de ECM registrados permiten la reproducción del programa multimedia grabado. El sistema y el procedimiento que se describen en el presente documento también se aplican a los ECM registrados.

[0122] Los modos de realización del sistema y los procedimientos descritos en el presente documento presentan las siguientes ventajas:

- el uso de un túnel seguro para transmitir la clave K_{Term} al terminal aumenta la seguridad del sistema,
- el hecho de que el cabezal de red verifique que el terminal es capaz de cifrar o descifrar correctamente los datos con la clave K_{ECMU} determinada en el paso 160 permite que el terminal se autentifique de forma fiable, ya que solo

el cabezal de red 4 puede determinar la clave K_{ECMU} asociada con el identificador UA único del terminal, de modo que solo un terminal auténtico puede tener una clave en su memoria K_{ECMU} correspondiente a la determinada por el cabezal,

- el uso de la estructura de un mensaje ECM para presentar una impugnación de autenticación al terminal en el paso 168 simplifica la realización del sistema porque no es necesario desarrollar una nueva estructura de mensajes para presentar esta impugnación de autenticación,
- la intervención de la clave K_{ProcU} en el cifrado de la clave K_{Term} hace que sea más difícil violar la seguridad del procedimiento, ya que en este interviene necesariamente el procesador de seguridad 42, que es un elemento que difícil de falsificar,
- la realización de un doble cifrado de la clave K_{Term} transmitida al terminal utilizando, por una parte, una clave de receptor (aquí, la clave $K_{licence}$) y, por otra, una clave del procesador de seguridad (aquí, la clave K_{ProcU}) que permite crear una sincronización entre dicho procesador de seguridad y dicho receptor,
- la autenticación del cabezal de red por el terminal también aumenta la seguridad de este sistema,
- verificar que el cabezal de red es capaz de cifrar o descifrar correctamente los datos con la clave K_{ECMU} que ha determinado permite autenticar de forma fiable dicho cabezal, ya que solo el cabezal de red auténtico puede determinar la clave K_{ECMU} utilizada por el terminal y asociada a su identificador UA único,
- el cifrado previo de la palabra de control con la clave K_{Term} ofrece la ventaja de que esta palabra de control solo se transmite en el lado del terminal de forma cifrada entre el procesador 42 y el receptor 40, lo que protege la interfaz entre dicho procesador y dicho receptor.

REIVINDICACIONES

1. Procedimiento de difusión, a través de una red de banda ancha, de un programa multimedia codificado en el que:

- una información puede enrutarse a una dirección de multidifusión, de modo que solo un grupo de varios terminales correspondientes a dicha dirección reciba la información y no otros terminales conectados a la misma red, y
- una información puede enrutarse a una dirección de unidifusión de modo que solo el terminal correspondiente a dicha dirección reciba la información y no otros terminales conectados a la misma red;

y en el que un cabezal de red (4):

- codifica (en 96; 250) el programa multimedia con una palabra de control,
- cifra (en 98; 252) la palabra de control para obtener un primer criptograma,
- cifra (en 100; 256) el primer criptograma para obtener un segundo criptograma; el primero y el segundo criptograma se realizan utilizando diferentes claves de cifrado seleccionadas del grupo formado por una clave operativa (K_{Proc}) y una clave de licencia (K_{Term}),
- multiplexa (en 104; 258) el segundo criptograma con el programa multimedia codificado para obtener contenido multiplexado,
- difunde (en 108; 262) el contenido multiplexado a una dirección de multidifusión de difusión para establecer una conexión punto a multipunto entre el cabezal y varios receptores del contenido multiplexado, y
- en una conexión punto a punto establecida (en 150) con un terminal que utilice la dirección de unidifusión de dicho terminal, transmite la clave de licencia individualmente a dicho terminal a través de dicha conexión punto a punto,

caracterizado porque dicha clave operativa es común a todos los terminales de un operador y **porque** antes de la transmisión de la clave de licencia:

- el cabezal de red ejecuta una fase de autenticación del terminal en el que dicho cabezal:

  - - determina (en 160) una clave única (K_{ECMU}) apta para identificar el terminal entre todos los terminales conectados a la red, a partir de:

    datos previamente registrados conocidos por el cabezal de red que no le hayan sido transmitidos por el terminal, y
    datos transmitidos (UA) por el terminal al cabezal de red, siendo los datos previamente registrados y datos transmitidos insuficientes por sí solos para permitir determinar la clave única (K_{ECMU}) utilizada por dicho terminal,

  - - verifica (en 196) que el terminal es capaz de cifrar o descifrar correctamente los datos con la clave única que ha determinado sin que el cabezal tenga que transmitir de antemano los datos previamente registrados ni la clave única (K_{ECMU}) determinada en dicho terminal; dicha verificación incluye:

    el envío, por el cabezal de red (en 168), de un mensaje ECM («Entitlement Control Message») al terminal en el que el campo destinado a contener un criptograma de una palabra de control contiene un criptograma obtenido mediante el cifrado de un dato desconocido ($AleaA_{uth}$) del terminal utilizando la clave única (K_{ECMU}) determinada,
    luego, la verificación (en 196) de que los datos desconocidos del terminal han sido descifrados correctamente por este terminal,

  - y si es así, determina (en 198) que el terminal está autenticado,
  - y
  - si el terminal se ha autenticado correctamente, el cabezal de red envía (en 216) un mensaje de transmisión de licencia al terminal que contiene la clave de licencia o un criptograma de la clave de licencia, a través de la conexión punto a punto establecida, y
  - si el terminal no se autentica correctamente, el cabezal de red actúa (en 200) para impedir que este terminal descodifique por completo el programa multimedia codificado difundido.

2. Procedimiento según la reivindicación 1, en el que el cabezal de red lleva a cabo una fase de establecimiento de un túnel seguro en la conexión punto a punto establecida, durante la cual, si la terminal se ha autenticado con éxito:

- el cabezal de red establece, de manera aleatoria, una clave de sesión común al terminal y al cabezal, y luego
- envía al terminal el mensaje de transmisión de licencia cifrado con esta clave de sesión.

3. Procedimiento según cualquiera de las reivindicaciones anteriores para un terminal equipado con un

procesador de seguridad que contiene una clave de procesador de seguridad (K_{ProcU}), en el que el cabezal de red cifra (en 212) la clave de licencia (K_{Term}) utilizando, como mínimo, la clave del procesador de seguridad del terminal (K_{ProcU}) para obtener un criptograma de la clave de licencia (K_{Term}), e incorpora este criptograma de la clave de licencia (K_{Term}) al mensaje de transmisión de licencia.

4. Procedimiento según cualquiera de las reivindicaciones anteriores para un terminal equipado con un receptor que contiene una clave de cifrado de clave de licencia ($K_{licence}$) y con un procesador de seguridad extraíble que contiene una clave de procesador de seguridad (K_{ProcU}), siendo la clave del procesador inicialmente conocida solo por el procesador de seguridad y la clave de cifrado de clave de licencia inicialmente conocida por el receptor, en el cual el cabezal de red:

- realiza sucesivamente en el tiempo el primer y segundo cifrado (210, 212) de la clave de licencia (K_{Term}) para obtener un criptograma de la clave de licencia (K_{Term}); el primer y segundo cifrado se realiza utilizando diferentes claves de cifrado seleccionadas del grupo formado por la clave del procesador (K_{ProcU}) y la clave de cifrado de la clave de licencia ($K_{licence}$), e
- incorpora este segundo criptograma de la clave de licencia en el mensaje de transmisión de licencia.

5. Procedimiento de recepción de un programa multimedia codificado difundido mediante un procedimiento de difusión conforme a cualquiera de las reivindicaciones anteriores, en el cual el terminal:

- escucha (en 120; 270) la dirección de multidifusión para la difusión y recibe el contenido multiplexado,
- demultiplexa (en 122; 272) el contenido multiplexado recibido para obtener el segundo criptograma y el programa multimedia codificado,
- descifra (en 130; 274) el segundo criptograma para obtener el primer criptograma,
- descifra (en 134; 284) el primer criptograma para obtener la palabra de control, realizándose el primer y segundo descifrado utilizando diferentes claves de cifrado seleccionadas del grupo formado por la clave operativa (K_{Proc}) y la clave de licencia (K_{Term}),

y

- descodifica (en 136; 288) el programa multimedia codificado con la palabra de control, **caracterizado porque** durante el paso de autenticación, el terminal opera conjuntamente con el cabezal de red para autenticarse a sí mismo,

en el cual el terminal también ejecuta una fase de autenticación del cabezal de red y, si este se ha autenticado correctamente, el terminal obtiene (en 232) la clave de licencia del mensaje de transmisión de licencia,
mientras que si el cabezal no se ha autenticado correctamente, se impide el descifrado del programa multimedia por este terminal (en 200),
y en el cual, para un terminal capaz de cifrar o descifrar criptogramas utilizando una clave única predeterminada (K_{ECMU}), la cual identifica este terminal de forma única entre todos los terminales conectados a la red,
durante el paso de autenticación del cabezal, el terminal comprueba (en 178) que el cabezal de red es capaz de cifrar o descifrar correctamente los datos con la clave única (K_{ECMU}) determinada por el cabezal de red a partir de:

- datos previamente registrados conocidos por el cabezal de red que no le hayan sido transmitidos por el terminal, y
- de los datos (UA) transmitidos por el terminal al cabezal de red, siendo los datos previamente registrados y datos transmitidos insuficientes por sí solos para permitir determinar la clave única (K_{ECMU}) de dicho terminal.

6. Procedimiento según la reivindicación 5 para recibir un programa multimedia difundido según un procedimiento basado en la reivindicación 2, en el cual, durante la fase de establecimiento del túnel seguro:

a) si el terminal se ha autenticado correctamente, este terminal opera conjuntamente con el cabezal para establecer la clave de sesión común (K_s) y descifra (en 220) el mensaje de transmisión de licencia recibido utilizando la clave de sesión común, y
b) si el terminal no se autentica correctamente, se impide el descifrado del programa multimedia por dicho terminal (en 200).

7. Procedimiento de recepción de un programa multimedia difundido utilizando un procedimiento de difusión según la reivindicación 3 y un terminal equipado con un procesador de seguridad que contiene una clave de procesador (K_{ProcU}), en el cual el procesador de seguridad descifra (en 228) el criptograma de la clave de licencia (K_{Term}) utilizando la clave de procesador (K_{ProcU}).

8. Procedimiento según cualquiera de las reivindicaciones de la 5 a la 7 para un terminal equipado con un receptor que contiene una clave de cifrado de clave de licencia ($K_{licence}$) y un procesador de seguridad extraíble que contiene una clave de procesador (K_{ProcU}), siendo la clave del procesador inicialmente conocida solo por el procesador de seguridad y la clave de cifrado de clave de licencia inicialmente conocida por el receptor, en el cual el procesador de seguridad y el receptor realizan sucesivamente un primer y un segundo descifrado (en 228, 232) de un criptograma

de la clave de licencia (K_{Term}), realizándose el primer y el segundo descifrado utilizando, respectivamente, una primera y una segunda clave de descifrado diferentes seleccionadas del grupo formado por la clave de procesador (K_{ProcU}) y la clave de licencia ($K_{licence}$).

9. Cabezal de red (4), **caracterizado por** ser capaz de implementar un procedimiento de difusión de programas multimedia codificados según cualquiera de las reivindicaciones de la 1 a la 4.

10. Terminal (8) para la recepción de programas multimedia codificados, **caracterizado por** ser capaz de implementar un procedimiento de recepción según cualquiera de las reivindicaciones de la 5 a la 8.

11. Receptor (40) para programas multimedia codificados, **caracterizado porque** puede asociarse con un procesador de seguridad extraíble para formar un terminal de recepción según la reivindicación 10.

12. Procesador de seguridad extraíble (42), **caracterizado porque** puede asociarse con un receptor de programas multimedia codificados para formar un terminal de recepción según la reivindicación 10.

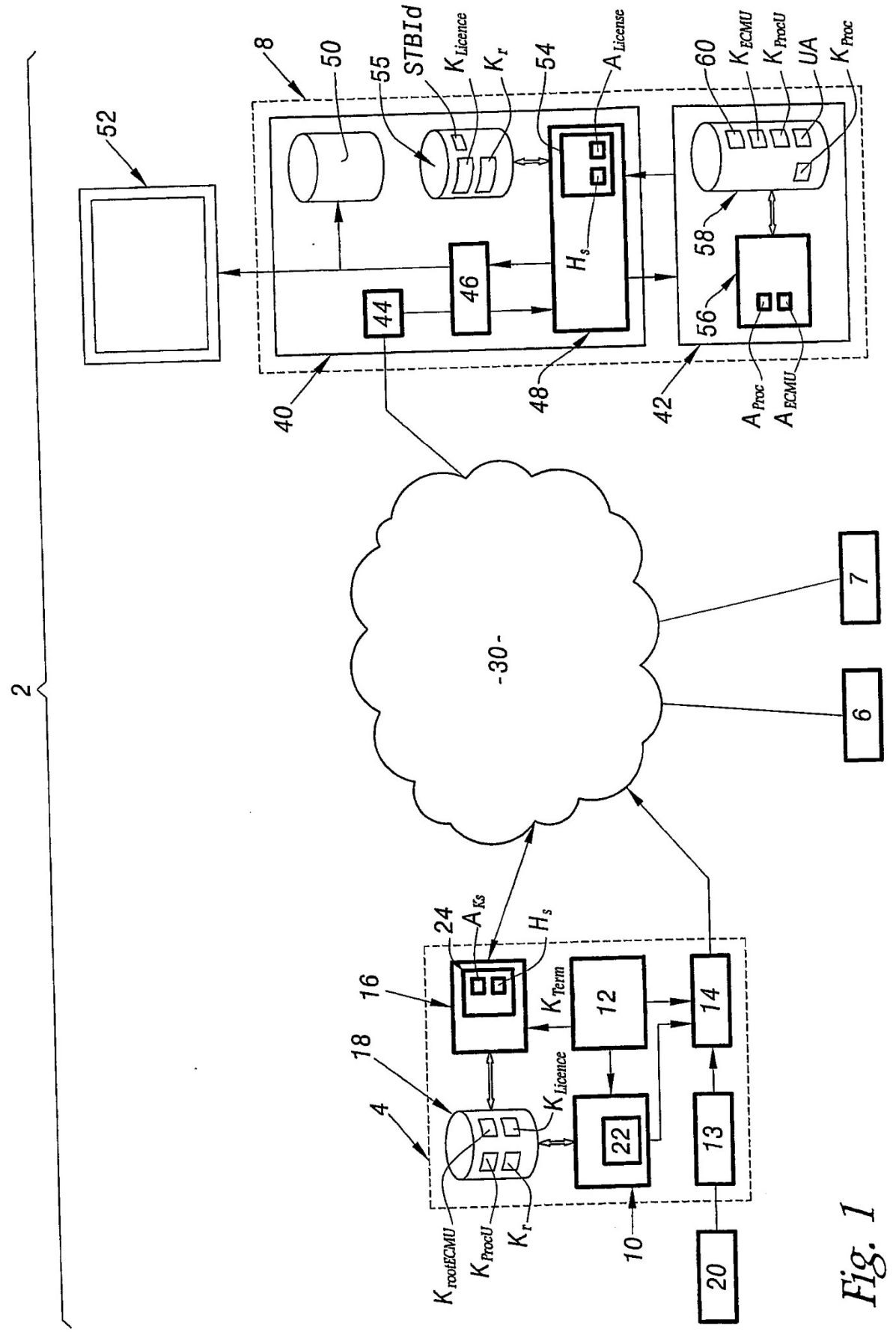
2
52
8
50
55
STBId
K Licence
K r
54
A License
60
K ECMU
K ProcU
UA
K Proc
58
H s
46
44
56
40
48
42
A Proc
A ECMU
-30-
7
6
24
A KS
H s
16
K Term
12
14
18
K Licence
4
22
13
K rootECMU
K ProcU
K r
10
20

Fig. 1

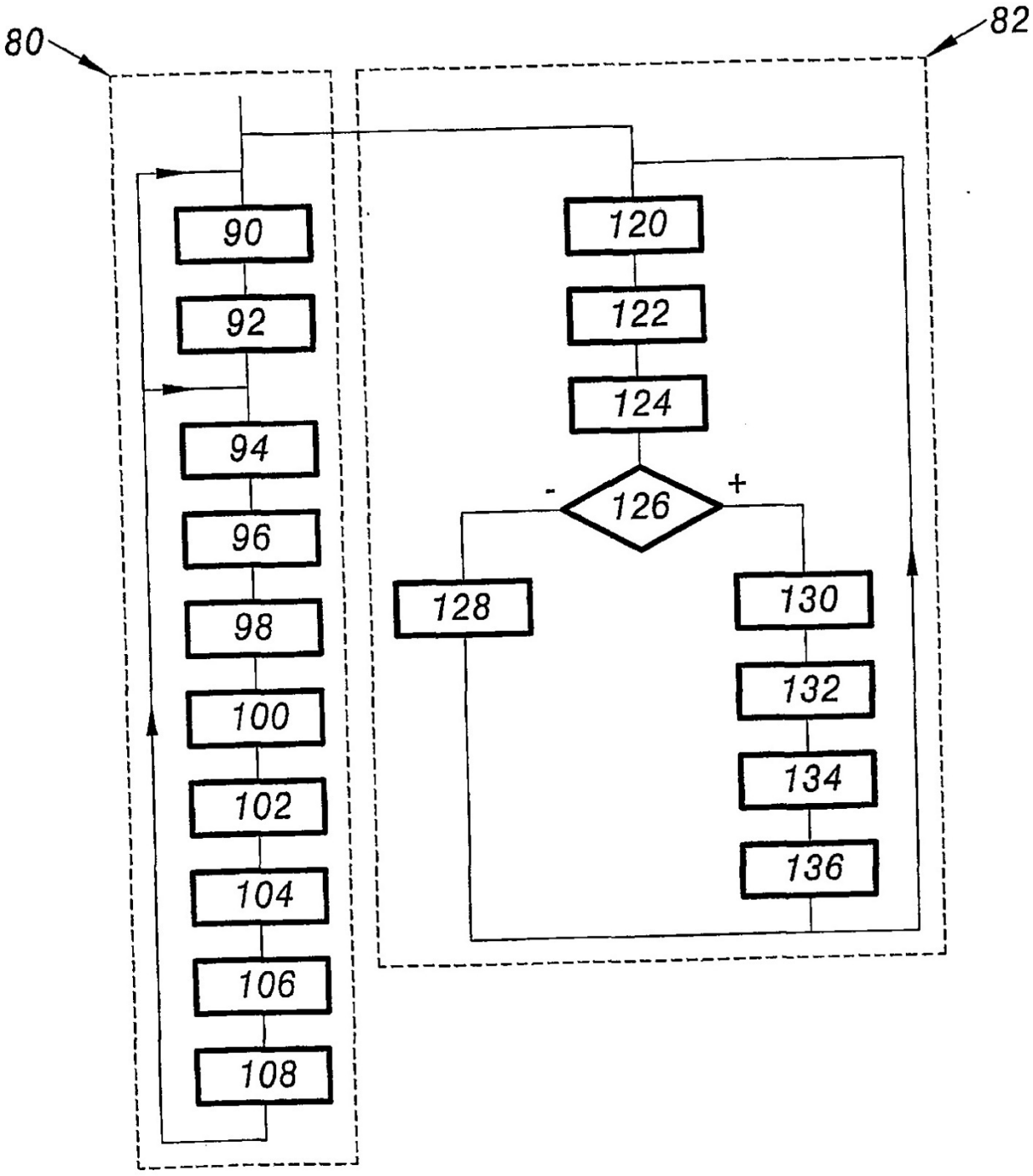
80
82
90
92
94
96
98
100
102
104
106
108
120
122
124
126
-
+
128
130
132
134
136

Fig. 2

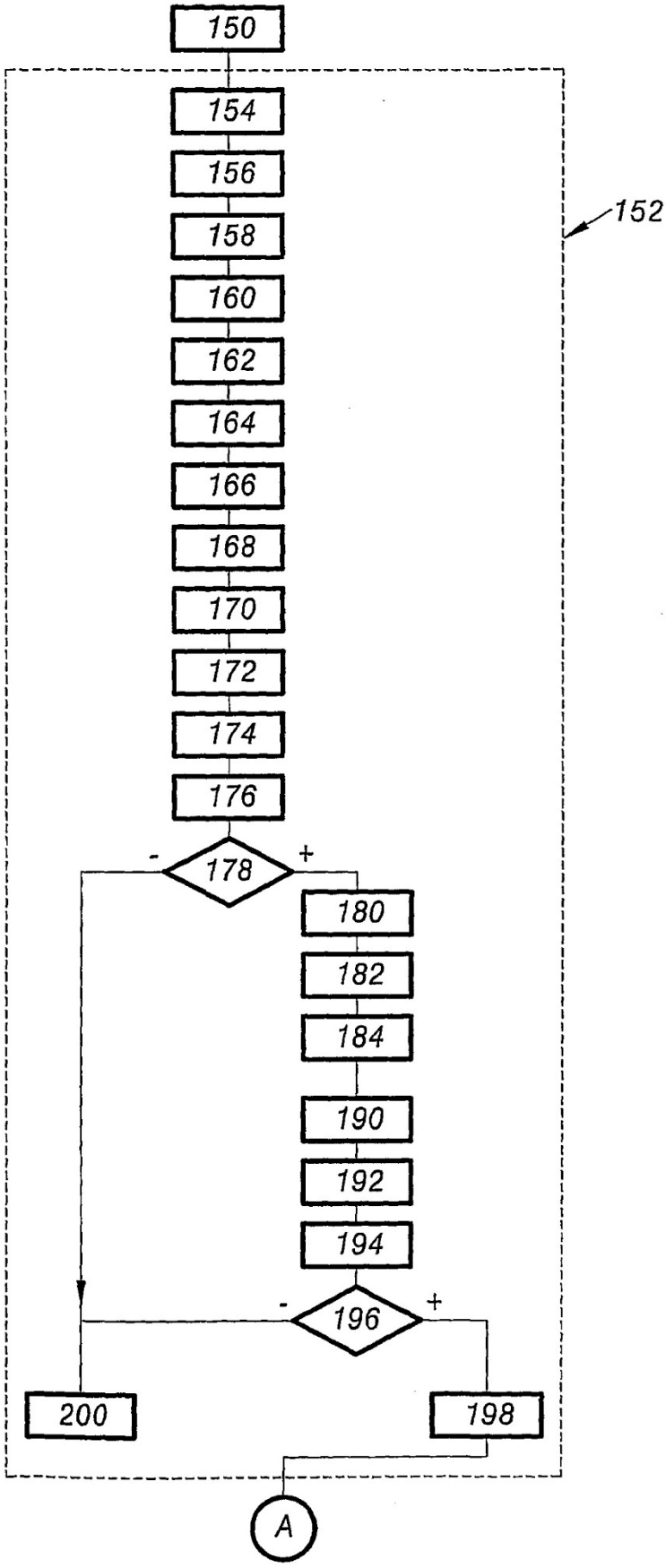
150
154
156
158
160
162
164
166
168
170
172
174
176
178
-
+
180
182
184
190
192
194
196
-
+
200
198
A
152

Fig. 3

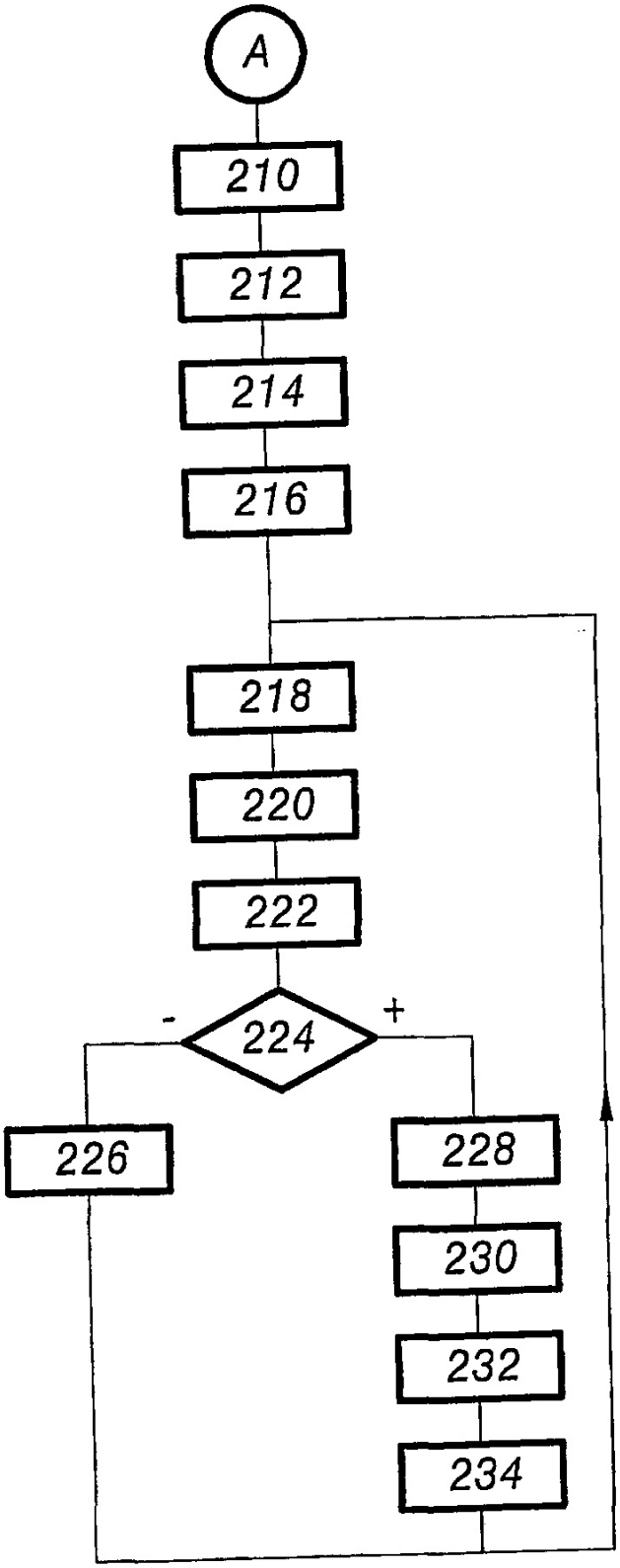

Fig. 4

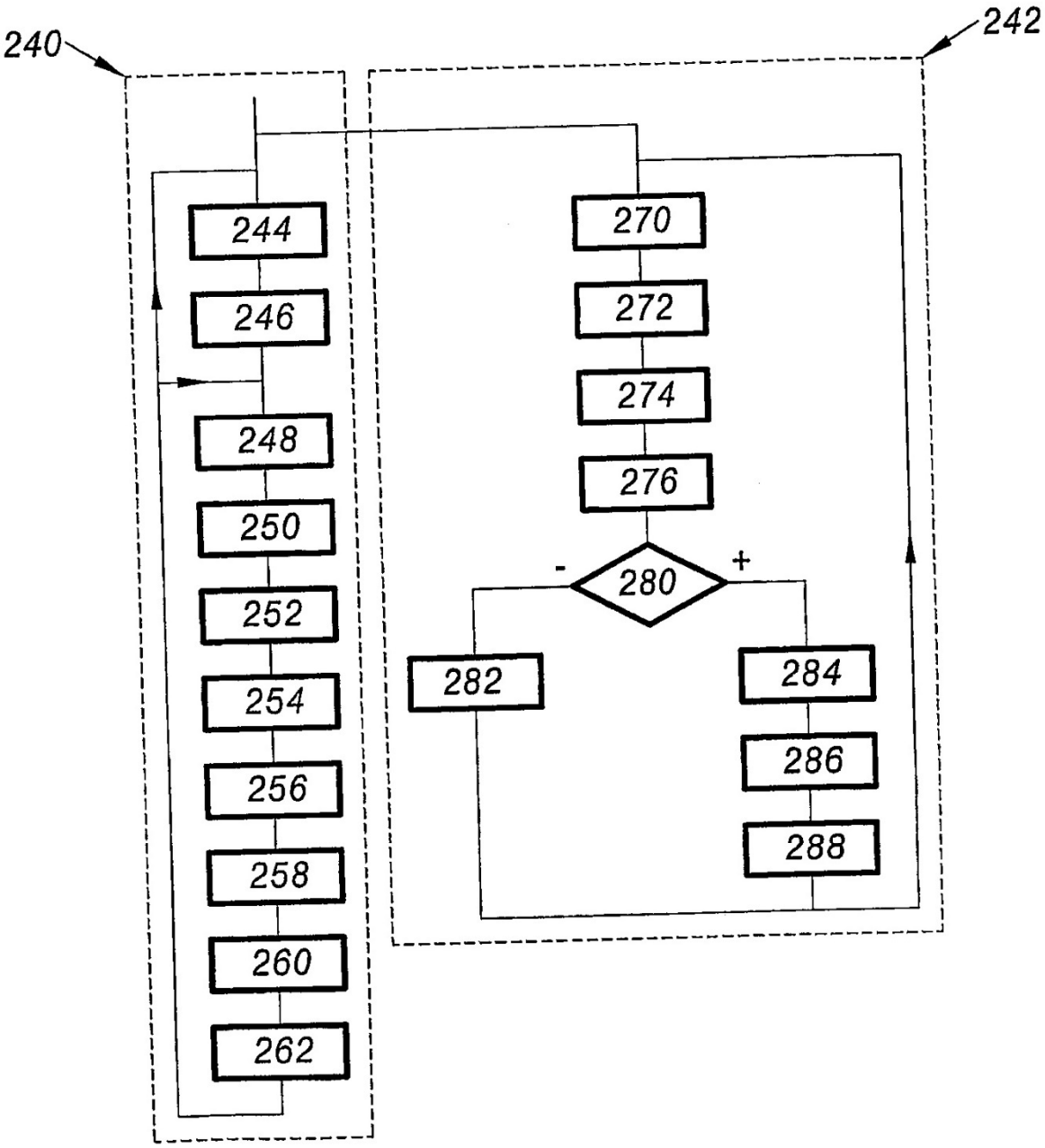
240
242
244
246
248
250
252
254
256
258
260
262
270
272
274
276
280
-
+
282
284
286
288

Fig. 5