(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 551 173**

(51) Int. CI.:

H04N 21/4405 (2011.01)
H04N 21/442 (2011.01)
H04N 21/4623 (2011.01)
G06F 21/34 (2013.01)
G06F 21/36 (2013.01)
H04L 29/06 (2006.01)
H04N 21/418 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.10.2011 E 11776147 (8)**

(97) Fecha y número de publicación de la concesión europea: **19.08.2015 EP 2633677**

(54) Título: **Procedimiento de recepción de un contenido multimedia codificado con la ayuda de palabras de control y captcha**

(30) Prioridad:

27.10.2010 FR 1058845

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.11.2015

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
92057 Paris La Défense, FR

(72) Inventor/es:

GADACHA, HAYTHEM

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCION

Procedimiento de recepción de un contenido multimedia codificado con la ayuda de palabras de control y captcha

La invención se refiere a un procedimiento de recepción de un contenido multimedia codificado con la ayuda de palabras de control. La invención se refiere igualmente a un procesador de seguridad, a un terminal así como a un soporte de registro de informaciones para la realización de este procedimiento.

La invención se aplica en particular al ámbito del control de acceso para el suministro de programas multimedia de pago tales como la televisión de pago.

Es conocido difundir varios contenidos multimedia el mismo tiempo. Para ello, cada contenido multimedia se difunde en su propio canal. El canal utilizado para transmitir un contenido multimedia es igualmente conocido bajo el término de «cadena». Un canal corresponde típicamente a una cadena de televisión. Eso permite a un usuario seleccionar simplemente el contenido multimedia que desea visualizar cambiando para ello de canal.

En esta descripción, se designa más específicamente por «contenido multimedia» un contenido audio y/o visual destinado para ser restituido bajo una forma directamente perceptible y comprensible por un ser humano. Típicamente, un contenido multimedia corresponde a una sucesión de imágenes que forman una película, una emisión de televisión o publicidad. Un contenido multimedia puede igualmente ser un contenido interactivo tal como un juego.

Para asegurar y someter la visualización de los contenidos multimedia con ciertas condiciones, como la suscripción de un abono de pago por ejemplo, los contenidos multimedia se difunden en forma codificada y no en claro. En esta descripción, el canal se dice «codificado» cuando el contenido multimedia difundido en este canal está codificado.

Más precisamente, cada contenido multimedia se divide en una sucesión de criptoperiodos. Durante todo el tiempo de duración de un criptoperiodo, las condiciones de acceso al contenido multimedia codificado permanecen inalteradas. En particular, durante todo el tiempo que dure un criptoperiodo, el contenido multimedia está codificado con la misma palabra de control. Generalmente, la palabra de control varía de un criptoperiodo a otro.

Además, la palabra de control es generalmente específica de un contenido multimedia, siendo este último aleatoriamente o pseudo aleatoriamente sacado. Así, si en un instante dado, **N** contenidos multimedia son simultáneamente difundidos en **N** canales, existen **N** palabras de control diferentes e independientes utilizadas cada una para codificar uno de estos contenidos multimedia.

Aquí, los términos «codificar» y «cifrar» se consideran como sinónimos. Sucede lo mismo para los términos «descodificar» y «descifrar».

El contenido multimedia en claro corresponde al contenido multimedia antes que éste sea codificado. Este puede hacerse directamente comprensible por un ser humano sin tener que recurrir a operaciones de descodificado y sin que su visualización sea sometida a ciertas condiciones.

Las palabras de control necesarias para descodificar los contenidos multimedia se transmiten de forma sincronizada con los contenidos multimedia. Por ejemplo, las palabras de control necesarias para descodificar el t-mo criptoperiodo se reciben por cada terminal durante el (t-1)-mo criptoperiodo. Para ello, por ejemplo, las palabras de control son multiplexadas con el contenido multimedia codificado.

Para asegurar la transmisión de las palabras de control, éstas se transmiten a los terminales en forma de criptogramas contenidos en mensajes ECM (Entitlement Control Message). Se designa aquí por «criptograma» una información insuficiente por si sola para recuperar la palabra de control en claro. Así, si la transmisión de la palabra de control es interceptada, el único conocimiento del criptograma de la palabra de control no permite recuperar la palabra de control que permite descodificar el contenido multimedia.

Para recuperar la palabra de control en claro, es decir la palabra de control que permite descodificar directamente el contenido multimedia, esta debe combinarse con una información secreta. Por ejemplo, el criptograma de la palabra de control se obtiene cifrando la palabra de control en claro con una clave criptográfica. En este caso, la información secreta es la clave criptográfica que permite descifrar este criptograma. El criptograma de la palabra de control puede también ser una referencia a una palabra de control almacenada en una tabla que contiene una multitud de palabras de control posibles. En este caso, la información secreta es la tabla que asocia con cada referencia una palabra de control en claro.

La información secreta debe guardarse en lugar seguro. Para ello, se ha propuesto ya almacenar la información secreta en procesadores de seguridad tales como tarjetas con microcircuito integrado directamente conectadas con cada uno de los terminales.

Por otro lado, los contenidos multimedia difundidos por los diferentes canales pueden ser coordenados temporalmente entre si. Por ejemplo, los instantes de difusión de los contenidos multimedia están regulados para respetar los horarios de difusión indicados en una parrilla de programas preestablecida. Cada terminal en un canal dado recibe por consiguiente sustancialmente al mismo tiempo el mismo contenido multimedia. Se dice que estos contenidos multimedia son flujos «live» (en directo) o «linéarisés» (linealizados) pues el usuario no controla su momento de transmisión.

En este contexto, se han producido ataques para permitir a usuarios descodificar contenidos multimedia para los cuales no han adquirido lícitamente derechos de acceso.

Uno de estos ataques es conocido bajo el término de «partage de carte» (partición de tarjeta) («card sharing» en inglés). Este ataque consiste en adquirir de forma lícita un procesador de seguridad para disponer de los derechos de acceso necesarios para descodificar varios canales. Seguidamente, este procesador de seguridad «lícito» se introduce en un servidor pirata que recibe mensajes ECM de una multitud de terminales satélites piratas. Así, cuando un terminal satélite pirata desea descodificar ilícitamente un contenido multimedia difundido, recibe este contenido multimedia y transmite los mensajes ECM correspondientes al servidor pirata. El servidor pirata transmite estos mensajes ECM al procesador de seguridad lícito. En respuesta, el procesador de seguridad lícito descifra las palabras de control contenidas en estos mensajes ECM y reenvía las palabras de control en claro al servidor pirata. El servidor pirata transmite entonces estas palabras de control en claro al terminal satélite pirata que puede entonces descodificar el contenido multimedia deseado.

En este ataque, el procesador de seguridad se utiliza normalmente salvo que trate los mensajes ECM de una multitud de terminales satélites mientras que en una utilización lícita, solo trata los mensajes ECM de un solo terminal.

Para detectar este ataque, ha sido propuesto ya:

- contar los cambios de canales producidos en un periodo predeterminado de tiempo (ver la solicitud de patente EP 1 575 293),
- contar el número de canales diferentes descodificados por el procesador de seguridad en un periodo predeterminado de tiempo (ver la solicitud de patente EP 1 447 976), y
- contar el número de mensajes ECM recibidos por el procesador de seguridad en un periodo de tiempo predeterminado (ver la solicitud de patente WO 2008 049 882).

Estos procedimientos de detección aprovechan todos el hecho de que un ataque por partición de tarjeta se traduce por:

- un número de cambios de canales (igualmente conocido bajo el término «zapping») anormalmente elevado, y/o
- un número de mensajes ECM recibidos anormalmente elevado.

La detección de este ataque permite seguidamente tomar contra-medidas.

Existe igualmente otro ataque conocido bajo la expresión de «partage de mots de contrôle» («control word sharing» en inglés) que explota, también, un procesador de seguridad lícito para descodificar uno o varios canales. En este ataque, el procesador de seguridad lícito se introduce en un servidor de palabras de control. Este servidor recibe el contenido multimedia y extrae de él los mensajes ECM. Los mensajes ECM extraídos se transmiten al procesador de seguridad lícito que descifra entonces los criptogramas de las palabras de control y reenvía las palabras de control así descifradas al servidor. El servidor difunde entonces a un gran número de terminales satélites piratas estas palabras de control, lo que les permite descodificar ilícitamente los contenidos multimedia. Por ejemplo, en este ataque, los terminales satélites piratas se abonan simplemente al flujo de palabras de control en claro generado por el servidor y correspondiente al canal que desea descodificar.

Este último ataque difiere del ataque por partición de tarjeta por el hecho de que los terminales satélites piratas no tienen necesidad de transmitir al servidor los mensajes ECM del canal que desea descodificar. Por consiguiente, el número de mensajes ECM tratados por el procesador de seguridad en este ataque es mucho menos elevado que en un ataque por partición de tarjeta. Sin embargo, si para este ataque, se utiliza el mismo procesador de seguridad para tratar los mensajes ECM de diferentes canales, este ataque puede también detectarse con la ayuda de los procedimientos de detección conocidos presentados más arriba.

Por el estado de la técnica se conocen igualmente por:

. Francis et Al: «Countermeasures for attack on satellite TV cards using open receivers», Australasian Information Security Workshop: Digital Rights Management, 6 de Noviembre de 2004, páginas 1-6, XP002333719

. US2006/294547A1,

. EP2098971A1, y

. US2010/0373319A1.

Los ataques presentados permiten a un gran número de piratas acceder al contenido multimedia de una cadena de pago gratuitamente. Estos ataques representan en consecuencia un beneficio previsto no obtenido para un proveedor de este contenido multimedia.

Con el fin de paliar este inconveniente, la invención trata de hacer más difícil la puesta en práctica de estos ataques.

La invención se refiere a un procedimiento de recepción de un contenido multimedia codificado con la ayuda de palabras de control conforme a la reivindicación 1.

Un punto común a los ataques presentados más arriba es que el funcionamiento de los servidores piratas está totalmente automatizado con el fin de responder de forma continua y rápida a las solicitaciones de los piratas conectados con este servidor. En el procedimiento de la invención, la utilización de un captcha permite impedir esta automatización de los servidores piratas. En efecto, la respuesta correcta a un captcha solo puede ser encontrada fácilmente por un ser humano y no por una máquina. Así, la utilización de un captcha supone una intervención humana, por ejemplo, a nivel del servidor pirata lo cual hace más difícil la utilización de tales ataques.

Por otro lado, un servidor pirata no puede fácilmente salvar esta utilización. En efecto, la respuesta correcta asociada con el captcha está memorizada en el procesador lo cual impide la extracción de ésta respuesta por un servidor pirata. Además, la comparación entre una respuesta al captcha y la respuesta correcta se realiza por el procesador de seguridad y no por el terminal de recepción (servidor pirata). De este modo, la integridad del resultado de la comparación está garantizada.

Además, utilizando un captcha específico para un procesador pirata, se disuade al servidor pirata de transmitir este captcha a terminales piratas ya que la intercepción de un captcha de este tipo transmitido permitiría identificar el procesador de seguridad y por consiguiente obtener la identidad de un pirata.

Los modos de realización de este procedimiento pueden comprender una o varias de las características de las reivindicaciones dependientes de procedimiento.

Los modos de realización de este procedimiento pueden presentar además las ventajas siguientes:

■ dejando un tiempo de respuesta antes de limitar el descodificado, se obliga al usuario o al servidor pirata a responder a este captcha. Además, se limita la molestia causada al usuario durante la utilización del captcha y se limitan las posibilidades de éxito de un ataque por diccionario o por la fuerza bruta,

■ repitiendo la utilización del captcha, se perturba más aún la automatización de los ataques piratas,

■ limitando el número de respuestas que puede recibir el procesador a un captcha, se impide la realización de ataques mediante diccionario o por la fuerza bruta para responder correctamente al captcha,

■ al iniciar la utilización del captcha cuando se detecta una utilización potencialmente anormal, se aumenta la fiabilidad de la detección de una utilización anormal del procesador, y

■ al incluir en el captcha específico la marca que contiene la información indispensable para responder correctamente a este captcha, se hace difícil la ocultación de esta marca, y por consiguiente la ocultación del identificante del procesador de seguridad, antes de la transmisión del captcha a los usuarios.

La invención se refiere igualmente a un soporte de registro de informaciones, que comprenden instrucciones para la ejecución del procedimiento presentado, cuando estas instrucciones son realizadas por un calculador electrónico.

La invención se refiere por último a un procesador de seguridad para la realización del procedimiento presentado anteriormente, siendo este procesador conforme a la reivindicación 13.

La invención se refiere por último a un conjunto de procesadores de seguridad conforme a la reivindicación 10 o 12.

Otras características y ventajas de la invención se desprenderán claramente de la descripción que se da a continuación, a título indicativo y en modo alguno limitativo, haciendo referencia a los dibujos adjuntos, en los cuales:

. la figura 1 es una ilustración esquemática de un sistema de emisión y de recepción de contenidos multimedia codificados,

. la figura 2 es una ilustración esquemática de un captcha utilizado por el sistema de la figura 1,

. la figura 3 es un organigrama de construcción del captcha de la figura 2,

. la figura 4 es un organigrama de un procedimiento de recepción de un contenido multimedia en el sistema de la figura 1, y

. la figura 5 es un organigrama de una variante del procedimiento de la figura 4.

En estas figuras las mismas referencias se utilizan para designar los mismos elementos.

En lo que sigue de esta descripción, las características y funciones bien conocidas del experto en la materia no se describen con detalle. Además, la terminología utilizada es la de los sistemas de acceso condicionales a contenidos multimedia. Para más informaciones sobre esta terminología, el lector puede hacer referencia al documento siguiente:

> «Functional Model of Conditional Access System», EBU Review, Technical European Broadcasting Union, Brussels, BE, nº 266, 21 de Diciembre 1995.

La figura 1 representa un sistema 2 de emisión y de recepción de contenidos multimedia codificados. Los contenidos multimedia emitidos son contenidos multimedia linealizados. Por ejemplo, un contenido multimedia corresponde a una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

Los contenidos multimedia en claro son generados por una o varias fuentes 4 y transmitidos a un dispositivo 6 de difusión. El dispositivo 6 difunde los contenidos multimedia simultáneamente a una multitud de terminales de recepción a través de una red 8 de transmisión de informaciones. Los contenidos multimedia difundidos se sincronizan temporalmente los unos con los otros para, por ejemplo, respetar una parrilla preestablecida de programas.

La red 8 es típicamente una red de gran distancia de transmisión de informaciones tal como la red Internet o una red satélite o cualquier otra red de difusión tal como la utilizada para la transmisión de la televisión digital terrestre (TNT).

Para simplificar la figura 1, solo se han representado tres terminales 10 a 12 de recepción.

El dispositivo 6 comprende un codificador 16 que comprime los contenidos multimedia que recibe. El codificador 16 trata contenidos multimedia digitales. Por ejemplo, este codificador funciona conforme a la norma MPEG2 (Moving Picture Expert Group – 2) o la norma UIT-T H264.

Los contenidos multimedia comprimidos son dirigidos hacia una entrada 20 de un codificador 22. El codificador 22 codifica cada contenido multimedia comprimido para condicionar su visualización en ciertas condiciones tales como la compra de un título de acceso por los usuarios de los terminales de recepción. Los contenidos multimedia codificados son restituidos en una salida 24 conectada con la entrada de un multiplexor 26.

El codificador 22 codifica cada contenido multimedia comprimido con la ayuda de una palabra de control $CW_{i,t}$ que le es proporcionada, así como a un sistema 28 de acceso condicional, por un generador 32 de claves. El sistema 28 es más conocido bajo el acrónimo CAS (Conditional Access System). El índice i es un identificador del canal en el cual se difunde el contenido multimedia codificado y el índice t es un número de orden que identifica el criptoperiodo codificado con esta palabra de control.

Típicamente, este codificado es conforme a una norma tal como la norma DVB-CSA (Digital Video Broadcasting – Common Scrambling Algorithm), ISMA Cryp (Internet Streaming Media Alliance Cryp), SRTP (Secure Real-time Transport Protocol), AES (Advanced Ecryption Standard),...etc.

Para cada canal i, el sistema 28 genera mensajes $ECM_{i,t}$ (Entitlement Control Message) que contienen al menos el criptograma $CW^*_{i,t}$ de la palabra de control $CW_{i,t}$ generada por el generador 32 y utilizada por el codificador 22 para codificar el criptoperiodo t del canal i. Estos mensajes y los contenidos multimedia codificados se multiplexan por el multiplexor 26, siendo estos últimos respectivamente proporcionados por el sistema 28 de acceso condicional y por el codificador 22, antes de ser transmitidos a la red 8.

El sistema 28 introduce igualmente en cada ECM:

. el identificador i del canal,

. los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ de las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$ que permiten descodificar los criptoperiodos t y t+1 inmediatamente consecutivos del canal i,

. etiquetas de tiempo TS_t y TS_{t+1}, o «timestamp» en inglés que señalan los instantes en los cuales deben jugarse los criptoperiodos t y t+1,

. condiciones de acceso CA destinadas para ser comparadas con títulos de acceso adquiridos por el usuario, y

. una firma o una redundancia criptográfica MAC que permite comprobar la integridad del mensaje ECM.

El mensaje ECM que contiene el par de palabras de control $CW_{i,t}/CW_{i,t+1}$ es indicado $ECM_{i,t}$ en lo que sigue de la descripción donde:

. el índice i identifica el canal, y

. el índice t es un número de orden que identifica la posición temporal de este mensaje ECM con relación a los demás mensajes ECM diferentes emitidos para descodificar el canal i.

Aquí, el índice t identifica igualmente el criptoperiodo $CP_{i,t}$ descodificable con la ayuda de la palabra de control $CW_{i,t}$ contenida en el mensaje $ECM_{i,t}$. El índice t es único para cada criptoperiodo $CP_{i,t}$.

Las etiquetas de tiempo están definidas con relación a un origen absoluto independiente del contenido multimedia difundido y del canal por el cual se difunde el contenido multimedia.

El mismo identificador i es introducido en todos los mensajes $ECM_{i,t}$ que contienen un criptograma $CW^*_{i,t}$ para el descodificado de los contenidos multimedia difundidos por este canal i. A título de ilustración, aquí, el codificado y el multiplexado de los contenidos multimedia son conformes al protocolo DVB-Simulcrypt (ETSI TS 103 197). En este caso, el identificador i puede corresponder a un par «cannel ID/stream ID» único por el cual son enviadas todas las peticiones de generación de mensaje ECM para este canal.

Cada mensaje $ECM_{i,t}$ comprende un par $CW^*_{i,t}/CW^*_{i,t+1}$ de criptogramas de palabras de control. Después del descifrado, este par $CW^*_{i,t}/CW^*_{i,t+1}$ de criptogramas permite obtener un par $CW_{i,t}/GW_{i,t+1}$ de palabras de control.

En el ejemplo, los terminales 10 a 12 son idénticos. También, en lo que sigue solo el terminal 10 se describe con más detalle.

El terminal 10 se describe aquí en el caso particular en que éste es capaz de descodificar simultáneamente un solo canal i. A este respecto, el terminal 10 comprende una sola línea 60 de descodificado que permite el descodificado del canal i. Por ejemplo, la línea 60 descodifica el canal i para presentarlo visualmente en un visualizador 84.

Por ejemplo, el visualizador 84 es una televisión, un ordenador o también un teléfono fijo o móvil. Aquí, el visualizador es una televisión.

La línea 60 comprende un receptor 70 de contenidos multimedia difundidos. Este receptor 70 está conectado con la entrada de un desmultiplexor 72 que transmite por un lado el contenido multimedia a un descodificador 74 y por otro lado los mensajes $ECM_{i,t}$ y EMM (Entitlement Management Message) a un procesador de seguridad 76.

Típicamente, el acoplamiento mutuo entre el terminal 10 con el procesador 76 es gestionado por un módulo de control de acceso 85. En particular, el módulo 85 gestiona la visualización en el visualizador 84 de datos transmitidos por el procesador 76 al terminal 10 y la transmisión al procesador 76 de informaciones adquiridas por mediación de una interfaz hombre-máquina. Por ejemplo, la interfaz hombre-maquina está compuesta por la pantalla 84 y un mando a distancia.

El descodificador 74 descodifica contenido multimedia codificado a partir de la palabra de control transmitida por el procesador 76. El contenido multimedia descodificado es transmitido a un decodificador 80 que lo descodifica. El contenido multimedia descomprimido o descodificado es transmitido a una tarjeta gráfica 82 que pilota la representación visual de este contenido multimedia en el visualizador 84 equipado con una pantalla 86.

El visualizador 84 visualiza en claro el contenido multimedia en la pantalla 86.

El procesador 76 trata informaciones confidenciales tales como claves criptográficas. Para preservar la confidencialidad de estas informaciones, se ha concebido para que sea lo más robusto posible respecto a tentativas de ataques llevadas por piratas informáticos. Es por consiguiente más robusto respecto a estos ataques que los demás componentes del terminal 10. Por ejemplo, a este respecto, el procesador 76 es una tarjeta con microcircuito electrónico.

Por ejemplo, el procesador 76 está realizado con la ayuda de un calculador 77 electrónico programable apto para ejecutar instrucciones registradas en un soporte de registro de informaciones. A este respecto, el procesador 76 comprende una memoria 78 que contiene las instrucciones necesarias para la ejecución del procedimiento de la figura 4.

La memoria 78 contiene igualmente una base de datos 79 que comprende captchas pre-registrados (Completely

Automated Public Turing test to tell Computers and Humans Apart).

En esta descripción, se designa por «captcha» toda prueba que permita diferenciar un hombre de una máquina. Así, en esta descripción los captchas no están limitados al caso en que una imagen de una cadena de caracteres tenga que ser copiada de nuevo en un campo previsto a este efecto. Un captcha comprende por ejemplo una secuencia audio, una imagen, un enigma, o incluso un juego. Un enigma es por ejemplo una operación matemática sencilla tal como una multiplicación o una pregunta con elecciones múltiples. Un juego es por ejemplo un laberinto que comprende una entrada y varias salidas de las cuales una sola está asociada con la entrada. Cada salida está asociada con una cadena de caracteres no trivial que el usuario debe escoger como respuesta al captcha. Por el contrario, se excluyen aquí captchas tales como el visualizado de un mensaje que pida a un usuario cambiar de canal antes de volver a un canal inicial.

Cada captcha de la base de datos 79 está asociado con una respuesta correcta. Esta respuesta correcta está igualmente memorizada en la base 79, asociada con el captcha correspondiente. El registro de las respuestas correctas en el procesador 79 garantiza que la comprobación de la respuesta se realiza en el interior del procesador 79 lo cual hace la recuperación de estas respuestas correctas por medio de un logicial espía más difícil.

Los captchas de la base 79 son específicos al procesador 76. Por «específico» se designa el hecho de que existe una relación predefinida que asocia un identificador del procesador 76 únicamente en los captchas de la base 79. En estas condiciones, a partir de un captcha de la base 79 y de la relación predefinida, es posible identificar, entre el conjunto de procesadores de seguridad del sistema 2, el procesador 76.

Un captcha 87 pre-registrado en la base 79 se describirá ahora con referencia a la figura 2.

El captcha 87 comprende una prueba 872. Se designa por «challenge» de un captcha el conjunto de informaciones del captcha indispensable para que un ser humano sea apto para encontrar sistemáticamente la respuesta correcta a este captcha en un solo ataque.

En este ejemplo, la prueba 872 es una imagen de una cadena de caracteres que un usuario debe copiar de nuevo en un campo 874 previsto a este efecto. De forma conocida en sí, los caracteres de la cadena de caracteres de la prueba 872 comprenden un orden, un tamaño, una distorsión que varia de un carácter a otro. En estas condiciones, el reconocimiento automático de esta cadena de caracteres por un ordenador se hace más difícil.

Para simplificar la figura 2, la totalidad de los caracteres de la cadena de caracteres no ha sido representada.

El captcha 87 comprende por otro lado un contexto 876. Por «contexto de un captcha» se designa el conjunto de informaciones que no pertenecen a la prueba 872. El contexto 876 comprende una frase explicativa 879 que invita a un usuario a copiar de nuevo en el campo 874 la cadena de caracteres ilustrada en la prueba 872.

El captcha 87 comprende por otro lado una marca 878 para identificar el procesador 76. Aquí, la marca 878 es una cadena de caracteres. Esta marca 878 es la imagen del identificador del procesador 76 por una función F. Típicamente, el identificador del procesador 76 es un número de fabricación o un número de serie del procesador 76 que permite identificar sin ambigüedad este procesador 76 entre el conjunto de procesadores del sistema 2.

La función F es aquí una función inversible. En este caso, para identificar el procesador 76 que contiene la respuesta correcta al captcha 87, basta con aplicar la función inversa de la función F al captcha 87.

De preferencia, la función F es una función de cifrado tal como una función con clave secreta. Por ejemplo las funciones DES (Data Encryption Standard) o AES (Advanced Encryption Standard) pueden ser utilizadas para cifrar el identificador del procesador 76 con el fin de obtener la marca 878.

Siempre de forma preferencial, la función F toma por parámetro de entrada una incertidumbre r sacada pseudoaleatoriamente por el procesador 76, además del identificador. Así, aunque el identificador del procesador 76 sea constante, en cada construcción de un captcha, las marcas (imagen del identificador por la función F) incluidas en los captchas específicos son diferentes las unas de las otras. Aquí, la incertidumbre r está igualmente incluida en la imagen de la cadena de caracteres en un emplazamiento predeterminado con el fin de permitir la identificación del procesador 76 a partir, solamente, del captcha específico y de la inversa de la función F. Por ejemplo, la incertidumbre r se encuentra aquí incluida en la prueba 872 en un emplazamiento 880. En la figura 2, el emplazamiento 880 está formado por los cuatro primeros caracteres de la imagen de la cadena de caracteres.

En este ejemplo, la marca 878 está ventajosamente incluida en la prueba 872. En estas condiciones, la marca 878, y por consiguiente el identificador del procesador 76, no puede suprimirse fácilmente del captcha 87. Típicamente, si esta marca 878 se suprime, es imposible para un ser humano responder correctamente al captcha en un solo ataque. En efecto, en este caso la prueba 872 está incompleta. La marca 878 está también situada en un lugar predeterminado en el interior de la prueba 872. Por ejemplo, aquí, la marca 878 está constituida por los dos últimos caracteres de la prueba 872.

Un procedimiento de construcción del captcha 87 se describirá ahora con referencia a la figura 3. En este caso particular, la construcción del captcha 87 se realiza por un servidor conectado con cada procesador del sistema 2 por mediación de una red de transmisión de informaciones tal como la red 8.

Durante una etapa 90, el servidor obtiene una incertidumbre r pseudo-aleatoriamente.

Durante una etapa 92, el servidor genera un criptograma Id* del identificador del procesador 76 aplicando la función F a la incertidumbre r y al identificador del procesador 76. Para ello, el identificador del procesador 76 se memoriza, antes, en el servidor.

Durante una etapa 94, la respuesta correcta a la prueba se obtiene concatenando la incertidumbre r y el criptograma Id* en la misma cadena de caracteres.

Durante una etapa 96 el servidor construye la prueba 872 aplicando a cada carácter de la cadena construida durante la etapa 94, una transformación geométrica para deformarla y hacerla difícilmente identificable por un ordenador. Por «transformación geométrica» se designa por ejemplo la elección de un conjunto y de un factor de distorsión para cada uno de estos caracteres. La marca 878 es la imagen del criptograma Id* por la transformación geométrica.

La aplicación de tales transformaciones para generar la prueba 872 se describen por ejemplo en la solicitud de patente US2008/0072293.

Durante una etapa 98, el captcha y la respuesta correcta asociada con este captcha se memorizan por el servidor.

Seguidamente, durante una etapa 99, el captcha 87 y la respuesta correcta se registran en la base 79 del procesador 76 durante la fabricación del procesador 76 en fábrica o se transmite durante la utilización del procesador 76 por medio de un mensaje EMM. En respuesta al mensaje EMM, el procesador registra el captcha 87 en la base 79.

Un procedimiento de recepción de un contenido multimedia con la ayuda del sistema 2 se describirá ahora con referencia a la figura 4.

Durante una fase 100 de utilización, un usuario visiona un contenido multimedia en claro en la pantalla 86 del visualizador 84. Por ejemplo, el usuario está viendo una película.

A este respecto, durante una etapa 101a, el terminal 10 recibe un contenido multimedia multiplexado por mediación del receptor 70. Este contenido es desmultiplexado por el desmultiplexor 72 y los mensajes ECM son transmitidos al procesador 76 por mediación del módulo 85. Por ejemplo, el módulo 85 solo transmite los mensajes $EGM_{i,t}$ relativos al canal i en el cual se difunde la película visionada por el usuario. Estos mensajes $ECM_{i,t}$ contienen un criptograma $CW^*_{i,t}$ de una palabra de control $CW_{i,t}$ que permite descodificar el contenido multimedia difundido por el canal i así como los derechos de acceso para autorizar o no el descifrado del criptograma $CW^*_{i,t}$.

Durante una etapa 101b, el procesador 76 comprueba si el usuario tiene títulos de acceso correspondientes a los derechos de acceso contenido en el mensaje $ECM_{i,t}$ recibido.

En caso negativo, el procesador 76 no descifra el criptograma $CW^*_{i,t}$ y no transmite la palabra de control $CW_{i,t}$ al descodificador 74. El procedimiento retorna entonces a la etapa 101a. El descodificado del contenido multimedia se interrumpe.

Si el usuario tiene los títulos de acceso correspondientes a los derechos de acceso recibidos, entonces el procesador 76 procede a una etapa 102.

Durante la etapa 102, el procesador 76 detecta una utilización potencialmente anormal.

En esta descripción, se considera que la utilización del procesador 76 es potencialmente anormal cuando el procesador 76 parece ser utilizado dentro del marco de uno de los ataques presentado con anterioridad. Aquí, se considera más particularmente que la utilización del procesador 76 es potencialmente anormal si el procesador 76 parece ser utilizado dentro del marco de un ataque por partición de la tarjeta o de un ataque por partición de palabras de control.

En el ejemplo, durante una operación 106, el procesador 76 calcula un número N_{ECM} de mensajes ECM recibidos por el procesador 76 por unidad de tiempo. A este respecto, el procedimiento de detección descrito en la solicitud de patente WO2008049882 es por ejemplo utilizado.

Durante una operación 108, el procesador 76 determina si la utilización del procesador es normal, potencialmente anormal o anormal comparando el número N_{ECM} con umbrales S_{1ECM} y S_{2ECM}. Si el número N_{ECM} es inferior al umbral S_{1ECM} entonces la utilización es normal. Si el número N_{ECM} es superior al umbral S_{2ECM}, entonces la utilización es

anormal. Si el número N_{ECM} está comprendido entre los umbrales S_{1ECM} y S_{2ECM}, entonces la utilización es potencialmente anormal. Una utilización potencialmente anormal corresponde a una zona de incertidumbre donde las mediciones realizadas por el procesador 76 no permiten resolver con certeza entre una utilización normal y una utilización anormal. Esta zona de incertidumbre debe reducirse todo lo posible para evitar sancionar una utilización normal o evitar no sancionar una utilización anormal.

Si el procesador 76 detecta que su utilización es normal entonces, durante una etapa 110, el procesador 76 descifra el criptograma $CW^*_{i,t}$. Seguidamente, el procesador 76 transmite la palabra de control $CW_{i,t}$ al terminal 10 para descodificar el flujo multimedia y el usuario continua el visionado de la película en claro.

Si el procesador 76 detecta que su utilización es anormal, durante una etapa 111, el procesador 76 no descifra el criptograma $CW^*_{i,t}$. El terminal 10 es por consiguiente incapaz de descodificar el contenido multimedia y el usuario no visiona ya la película en claro.

Si el procesador 76 detecta que su utilización es potencialmente anormal, entonces procede a una etapa 112 durante la cual se realiza una prueba suplementaria para reducir la zona de incertidumbre.

Durante una operación 114, el procesador selecciona un captcha entre los captchas pre-registrados en la base de datos 79. Por ejemplo, el procesador 76 selecciona pseudo-aleatoriamente un captcha en la base de datos 79. En lo que sigue de la descripción, se supone que el procesador 76 ha seleccionado el captcha 87.

Durante esta operación 114, el procesador 76 transmite el captcha 87 al módulo 85 que controla el terminal 10 para visualizar el captcha 87 en la pantalla 86. Simultáneamente, el procesador 76 inicia un contador que deduce un intervalo de tiempo predeterminado DR. Por ejemplo, un contador CD_{DR} se inicia durante la selección del captcha por el procesador 76 y luego se pone en funcionamiento. Típicamente, el intervalo DR es superior a 2 minutos y, de preferencia, superior a 5 minutos. Aquí, el intervalo DR es de 15 minutos.

Por otro lado, durante esta operación 114, un contador CR_{MR} para contar las respuestas incorrectas recibidas por el procesador 76 se inicia igualmente.

Un usuario es entonces invitado a responder al captcha visualizado: Aquí, el usuario es invitado a copiar de nuevo la prueba 872 en el campo 874. En el ejemplo, el usuario tiene el intervalo de tiempo predeterminado DR para proporcionar una respuesta correcta al captcha seleccionado.

Durante una operación 116, el usuario responde al captcha por mediación de una interfaz hombre-máquina (por ejemplo un teclado de mando a distancia) conectado con el terminal 10. La respuesta se transmite entonces por el terminal 10 y el módulo 85 al procesador 76.

Ventajosamente, si durante la operación 116 el usuario no comprende el captcha visualizado, éste tiene la posibilidad de solicitar la selección de un nuevo captcha por el procesador 76. En este caso, el contador CD_{DR} no se reinicializa.

Durante una operación 118, el procesador 76 recibe la respuesta y la compara con la respuesta correcta para este captcha contenido en la base de datos 79. A cada respuesta incorrecta recibida por el procesador 76, el contador CR_{MR} se incrementa un paso predeterminado.

Si el número de respuestas incorrectas recibidas por el procesador 76 para un captcha seleccionado es superior a un umbral MR_{max} predefinido o si el usuario solicita cambiar de captcha, el procesador 76 vuelve a la etapa 114 para seleccionar un nuevo captcha entre los captchas pre-registrados en la base 79. Sin embargo, en este caso el procesador 76 reinicializa el contador CR_{MR} pero el contador CD_{DR} no se reinicializa. Típicamente, el umbral MR_{max} es superior o igual a uno e inferior o igual a cinco. Aquí, el umbral MR_{max} es superior a dos. Es igual a tres. Cada nuevo captcha es de preferencia seleccionado por el procesador 76 de forma que la respuesta correcta a este nuevo captcha seleccionado sea distinta de la respuesta correcta del precedente captcha seleccionado. Así, un ataque por diccionario, es decir un ataque consistente en ensayar combinaciones de respuestas registradas procedentes de captchas sometidos en el pasado, no puede ser utilizado por un servidor pirata para responder correctamente a un captcha seleccionado. Un ataque por diccionario difiere de un ataque por la fuerza bruta en la cual una a una, se ensayan todas las respuestas posibles.

Durante la operación 118, si el procesador 76 recibe una respuesta correcta al captcha seleccionado antes de la expiración del intervalo de tiempo DR, entonces el procesador 76 concluye que la utilización es normal y procede a la etapa 110.

Siempre durante la operación 118, si el intervalo de tiempo DR expira y ninguna respuesta correcta a un captcha seleccionado ha sido recibida por el procesador 76, el procesador 76 concluye que se trata de una utilización anormal.

En consecuencia, durante una operación 122, el procesador 76 selecciona pseudo-aleatoriamente un nuevo captcha en la base de datos 79 y controla el módulo 85 para visualizar este captcha en la pantalla 86.

A continuación, en una operación 124, el procesador 76 inicia la puesta en práctica de una contramedida. Por ejemplo, aquí, el procesador 76 limita el descifrado de los criptogramas CW*. Por «limitar el descifrado de los criptogramas» se designa aquí la suspensión del descifrado de los criptogramas $CW^*_{i,t}$ del canal i actualmente visualizado únicamente o de los criptogramas CW* de todos los canales durante un tiempo predeterminado.

Además, mientras el procesador 76 no reciba la respuesta correcta al captcha visualizado durante la operación 122, el procedimiento permanece en la operación 124. En estas condiciones, el terminal 10 no puede descodificar el contenido multimedia y el usuario no puede continuar el visionado de la película en claro.

Si el procesador recibe la respuesta correcta al captcha visualizado durante la operación 122, entonces procede a la etapa 110. El descodificado de los contenidos multimedia es por consiguiente desbloqueado.

Por ejemplo, la puesta en práctica de este captcha durante la etapa 124 es idéntica a la que ha sido descrita con referencia a las etapas 114, 116 y 118. En particular, un intervalo de tiempo DR limitado para responder al captcha y un número máximo de falsas respuestas son utilizados.

El procedimiento de la figura 4 permite luchar eficazmente contra la realización de ataques piratas mediante partición de tarjeta o partición de palabras de control. En efecto, supongamos que el procesador 76 se utiliza por un servidor pirata. En este caso, un conjunto de usuarios piratas visionan ilícitamente un contenido multimedia de pago por medio de máquinas, por ejemplo, contactadas con el servidor pirata por mediación de la red 8.

En este contexto, cuando el procesador 76 detecta (etapa 102) una utilización potencialmente anormal, el procesador 76 selecciona y controla (etapa 114) el visualizado de un captcha por el servidor pirata (aquí el servidor pirata ocupa la función del terminal 10) en un visualizador.

Si el servidor pirata es poco avanzado (caso trivial), este no está en condiciones de tratar el comando generado por el procesador 76 y el servidor no visualiza el captcha en un visualizador. Por lo tanto, el intervalo de tiempo DR expira sin que ninguna respuesta correcta sea recibida por el procesador 76. Por consiguiente, el procesador 76 limita el descifrado de los criptogramas CW* (etapa 122). En estas condiciones, el servidor pirata no puede ya transmitir a piratas las palabras de control descifradas. Los piratas no pueden ya ver el contenido multimedia en claro.

Si el servidor pirata es avanzado (caso no trivial), cuando el servidor pirata recibe la petición del procesador 76 para visualizar un captcha, el servidor pirata trata de desbaratar la realización de este captcha. Dos estrategias se pueden considerar.

En una primera estrategia, el servidor visualiza el captcha seleccionado por el procesador 76 en una pantalla conectada localmente con el servidor pirata. En estas condiciones, uno o varios operadores pirata deben estar presentes permanentemente delante de la pantalla de esta máquina para responder correctamente a los captchas que se visualizan con el fin de impedir la limitación del descifrado de los criptogramas CW* por el procesador 76. Una estrategia de este tipo presenta el inconveniente de impedir la automatización del servidor pirata.

En una segunda estrategia, el servidor redirige el captcha seleccionado por el procesador 76 hacia un terminal de un pirata conectado con la red 8 de forma que el usuario ilícito puede proporcionar una respuesta correcta para este captcha. Típicamente, el usuario ilícito introduce la respuesta correcta en su terminal y reenvía esta respuesta al procesador 76 por medio del servidor pirata. En estas condiciones, el procesador 76 no limita el descodificado de los criptogramas CW* y el conjunto de piratas de la red puede continuar visionando el contenido multimedia en claro.

Desde el punto de vista de los piratas esta estrategia presenta la ventaja de poder automatizar el funcionamiento del servidor pirata. Sin embargo, el operador de televisión de pago puede en adelante identificar el procesador 76. En efecto, los captchas al ser seleccionados en la base de datos 79, estos son específicos al procesador 76 y permiten así identificar el procesador 76.

Más precisamente, basta con interceptar un captcha transmitido en la red 8 procedente del servidor pirata para identificar el procesador 76. Eso puede fácilmente ser hecho conectándose directamente con el servidor pirata para visionar un contenido multimedia en claro de forma ilícita. Seguidamente, el operador puede identificar el procesador 76 a partir de la marca 878 y de la incertidumbre 880 comprendida en el captcha interceptado.

Por otro lado, una vez el procesador 76 identificado con certeza, el operador puede sancionar al usuario del procesador 76. Por ejemplo, el operador cesa de enviar al procesador 76 las claves secretas para descifrar los criptogramas CW*. En estas condiciones, el servidor pirata no puede ya ser utilizado para descodificar el flujo multimedia.

La figura 5 ilustra un procedimiento de recepción de un contenido multimedia codificado con la ayuda de palabras de control. Este procedimiento es idéntico al procedimiento de la figura 2 a excepción del hecho de que la etapa 102 es sustituida por una etapa 140 y la etapa 111 es omitida.

Durante la etapa 140, el procesador cuenta el número de mensajes ECM recibidos. Si este número sobrepasa un umbral Smax, entonces procede automáticamente a la etapa 112. En caso contrario, procede a la etapa 110. Así, la etapa 112 es sistemáticamente regularmente utilizada. En cada nueva utilización de la etapa 112, se selecciona un nuevo captcha.

Numerosos modos de realización son posibles.

Por ejemplo, los captchas pre-registrados en la base de datos 79 pueden ser actualizados periódicamente por el operador de televisión de pago por medio de mensajes ECM o EMM.

Por captcha específico no se designa únicamente el caso donde solo un procesador contiene la respuesta correcta a un captcha. Dos captchas, específicos a dos procesadores diferentes, pueden tener la misma respuesta. En este caso, por ejemplo, el identificador del procesador está codificado por las transformaciones aplicadas a cada uno de los caracteres y no por los caracteres seleccionados.

La base de datos 79 no contiene necesariamente captchas pre-registrados. Por ejemplo, la base de datos 79 contiene direcciones para permitir al procesador 76 telecargar captchas desde un servidor del operador de televisión de pago. En este caso, las respuestas correctas respectivas a los captchas asociados con estas direcciones se pre-registran en la memoria 78. Típicamente, las direcciones son URLs (Uniform Ressource Locator). Por ejemplo, la memoria 78 contiene una tabla que asocia cada URL con una respuesta pre-registrada respectiva. Cuando el procesador desea iniciar la visualización de un captcha, transmite la URL al módulo 85 que se encarga de telecargarlo y de utilizar el captcha telecargado en esta dirección URL. En este modo de realización cada terminal está conectado con un servidor de captcha del operador por Internet.

La marca para identificar el procesador 76 no está necesariamente incluida en la prueba del captcha. La misma puede estar incluida en el contexto de este captcha. En este caso, de preferencia el emplazamiento de la marca en el contexto varía de un captcha a otro para hacer más difícil la automatización de su ocultación.

La marca no es necesariamente una cadena de caracteres. Puede tratarse de un motivo, de una cadena de caracteres o también de un sonido.

La función F puede ser la función identidad. En este caso, el identificador del procesador 76 se incluye en el captcha.

La función F puede ser una función no inversible. Por ejemplo, la función F es una función de entrecortado de tipo SHA1 (Secure Hash Algorithm 1). En este caso, para identificar el procesador que contiene la respuesta correcta a un captcha, es necesario comparar el resultado de la función F tomando por parámetro el identificador del procesador 76 con el conjunto de resultados de la función F que toma por parámetro los identificadores de cada uno de los procesadores del sistema 2. En la práctica, el operador de televisión de pago conoce los identificadores de cada uno de los procesadores del sistema 2. También, en este caso este operador es apto para identificar el procesador 76 a partir de un captcha.

En un modo de realización previsto por la invención, los captchas son específicos al procesador 76 pero no lleva marca u otro elemento construido a partir de la función F. Por ejemplo, la relación predefinida es una base de datos del operador que asocia con cada captcha específico el identificador del procesador de seguridad que cuenta la respuesta correcta a este captcha. Así, a partir de un captcha interceptado y de esta base de datos, el operador puede encontrar el identificador del procesador utilizado.

Los captchas utilizados no son necesariamente específicos de un procesador.

En el procedimiento de la figura 4, el captcha no es necesariamente seleccionado por el procesador 76. Por ejemplo, el captcha es seleccionado por el operador de televisión de pago por mediación de un mensaje EMM o ECM.

El intervalo de tiempo DR no es necesariamente un tiempo predefinido. Puede por ejemplo tratarse de un número predefinido de mensajes ECM recibidos por el procesador 76 desde la selección del captcha. El intervalo DR es de preferencia sacado de forma aleatoria o pseudoaleatoria dentro de un margen predeterminado de valores.

Cuando el procesador 76 controla la visualización de un captcha seleccionado, éste no es necesariamente visualizado en la pantalla 86. En variante, el terminal está equipado con su propia pantalla de control y el captcha es directamente visualizado en la pantalla de control del terminal de forma que no moleste al usuario en la realización de la etapa 112.

El captcha no se visualiza necesariamente. Por ejemplo, en el caso donde el captcha comprende únicamente una secuencia audio, el captcha puede ser realizado por mediación de un altavoz.

La operación 106 de detección de una utilización potencialmente anormal del procesador 76 puede ser realizada de forma diferente. Por ejemplo, el procesador 76 puede contar los cambios de canales durante un periodo de observación predefinido. Este recuento de los cambios de canales se realiza a partir del identificador i de canal contenido en los mensajes ECM recibidos por el procesador 76. En otro modo de realización, el identificador i del canal visto es obtenido de modo diferente.

Si la detección de una utilización potencialmente anormal no utiliza el identificador i de canal contenido en el mensaje ECM, entonces este puede ser omitido en mensajes ECM.

La etapa 140 de iniciación sistemática y a intervalos regulares de la visualización de un captcha puede también ser realizada contando el número de mensajes EMM recibidos o de criptogramas descifrados. En otra variante, durante la etapa 140, el procesador mide un tiempo DP transcurrido desde la ejecución de una etapa precedente 112 y, únicamente si este tiempo DP pasa un umbral predeterminado, el procesador 76 ejecuta la etapa 112. En el caso contrario, la etapa 112 no se ejecuta y el procesador 76 ejecuta la etapa 110.

En los procedimientos de las figuras 4 y 5, el procesador 76 mantiene el descifrado de los criptogramas CW* en la utilización del captcha y el descodificado se limita únicamente si el procesador 76 no recibe ninguna respuesta al captcha correspondiente con una respuesta correcta antes de la expiración del intervalo de tiempo DR. En una variante, el descifrado de los criptogramas CW* está limitado desde la selección del captcha por el procesador 76. El descifrado de los criptogramas CW* es seguidamente restablecido únicamente cuando el procesador 76 recibe una respuesta correcta al captcha visualizado.

Durante la operación 122, la limitación del descifrado de los criptogramas CW* puede también ser obtenida modificando los títulos de acceso registrados en la memoria 78.

Es posible prever una suspensión momentánea de la ejecución de la etapa 102 o 140. Cuando estas etapas son suspendidas, la realización del captcha se desactiva. Eso puede ser útil cuando el usuario es un niño.

Los parámetros de los procedimientos de las figuras 4 y 5 y de sus variantes (intervalo DR, tiempo DP, umbrales MR_{max}, S_{max},...) pueden ser pre-registrados de forma definitiva en la memoria 78 durante la fabricación del procesador 76. En variante, pueden ser cambiados dinámicamente por el operador, por ejemplo por mediación de mensajes EMM.

Las etiquetas de tiempo pueden ser utilizadas para medir el intervalo DR por ejemplo. En otra variante, las etiquetas de tiempo son omitidas por los mensajes ECM.

Los captchas de la base 79 no son necesariamente construidos por un servidor del operador de televisión de pago. Estos pueden ser directamente construidos por el procesador 76.

En variante, las marcas 878 introducidas en los captchas codifican únicamente una parte respectiva del identificador del procesador. Así, es preciso interceptar varios captchas para obtener el identificador completo del procesador 76.

La utilización de captchas que comprenden una marca específica de un procesador puede ser puesta en práctica en otros ámbitos técnicos e independientemente de un procedimiento de recepción de un contenido multimedia codificado.

REIVINDICACIONES

1. Procedimiento de recepción de un contenido multimedia codificado con la ayuda de palabras de control, comprendiendo este procedimiento:

- la recepción (101a) por un procesador de seguridad de mensajes ECM (Entitlement Control Message) que contiene al menos un criptograma CW* de una palabra de control CW que permite descodificar un contenido multimedia,

- el descifrado (110) por el procesador de seguridad de este criptograma CW*, y

- el descodificado (110) del contenido multimedia codificado a partir de la palabra de control CW descifrada,

caracterizado por que el procedimiento comprende igualmente las etapas siguientes:

- al menos una utilización (114) de un captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) específico al procesador de seguridad, desde un terminal de recepción, cuya respuesta correcta está contenida en una memoria del procesador de seguridad y varía de una utilización a otra, comprendiendo esta utilización la transmisión del captcha hacia este terminal de recepción con el fin de iniciar su representación visual en una pantalla, estando este captcha específico asociado por mediación de una relación predefinida con un identificador de este procesador de seguridad que contiene la respuesta correcta a este captcha con el fin de permitir la identificación de este procesador de seguridad a partir de este captcha entre un conjunto de procesadores de seguridad,
- el procesador de seguridad obtiene (116) al menos una respuesta a este captcha y compara (118) esta respuesta con la respuesta correcta contenida en su memoria, y
- el procesador de seguridad limita (122) el descifrado de los criptogramas CW* si ninguna respuesta a este captcha corresponde a la respuesta correcta contenida en la memoria, y
- la intercepción del captcha transmitido y la identificación del procesador de seguridad a partir del captcha interceptado.

2. Procedimiento según la reivindicación 1, en el cual:

- el descifrado de los criptogramas CW* se mantiene durante la utilización del captcha (114), y

- si ninguna respuesta al captcha correspondiente a la respuesta correcta contenida en la memoria es recibida en un intervalo de tiempo predeterminado DR, el procesador limita (122) el descifrado de los criptogramas CW*.

3. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual el procedimiento comprende la utilización automática por el procesador de un nuevo captcha cada vez que el valor de un contador CR que cuenta el número de mensajes ECM o EMM recibidos por el procesador alcanza un umbral predefinido o cada vez que un tiempo DP predefinido ha transcurrido desde la utilización de un captcha precedente.

4. Procedimiento según una cualquiera de las reivindicaciones 2 a 3, en el cual si el intervalo de tiempo DR no ha terminado desde la utilización de un captcha anterior y cuando el número de respuesta incorrectas a este captcha anterior, recibidas por el procesador, es superior a un umbral MR_{max} predefinido, el procedimiento comprende la utilización de un nuevo captcha cuya respuesta correcta, igualmente contenida en la memoria del procesador, es distinta de la respuesta correcta del captcha anterior, debiendo la respuesta correcta ser recibida por el procesador antes de la expiración del intervalo de tiempo DR, no siendo reinicializado el intervalo de tiempo DR durante la utilización del nuevo captcha.

5. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual el procedimiento comprende:

- la detección (102) de una utilización potencialmente anormal del procesador de seguridad en función de mensajes ECM o EMM recibidos por este procesador de seguridad, y

-el inicio (112) de la utilización del captcha en respuesta a esta detección de una utilización potencialmente anormal.

6. Procedimiento según la reivindicación 5, en el cual la detección de la utilización potencialmente anormal del procesador de seguridad se realiza a partir de un recuento de los cambios de canales durante un periodo de observación o de un recuento de los mensajes ECM recibidos durante un periodo de observación.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual el procedimiento comprende la inclusión de un marca en el captcha específico, estando esta marca asociada por mediación de la relación predefinida con el identificador del procesador de seguridad y comprendiendo esta marca una información

indispensable que, si se suprime, hace imposible el descubrimiento de la respuesta correcta a este captcha en un solo ataque por un ser humano.

8. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual la relación predefinida es una base de datos que asocia con cada captcha específico el identificador del procesador de seguridad que contiene la respuesta correcta a este captcha o una función predefinida que permite construir el captcha en función del identificador del procesador de seguridad.

9. Soporte de registro de informaciones, **caracterizado por que** comprende instrucciones para la ejecución de un procedimiento conforme a una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por un calculador electrónico.

10. Conjunto de varios procesadores electrónicos (76) de seguridad para la puesta en práctica del procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8, estando cada procesador programado para:

- recibir mensajes ECM (Entitlement Control Message) que contienen al menos un criptograma CW* de una palabra de control CW que permite descodificar un contenido multimedia,

- descifrar este criptograma CW*, y

- transmitir la palabra de control descifrada a un descodificador para descodificar el contenido multimedia codificado a partir de esta palabra de control CW descifrada,

caracterizado por que

- cada procesador comprende una memoria (78) que contiene:
  . una base de datos (79) que contiene direcciones para permitir a este procesador (76) de seguridad telecargar captchas (Completely Automated Public Turing test to tell Computers and Humans Apart) específicos desde un servidor de un operador de televisión de pago, y
  . respuestas correctas pre-registradas respectivas a los captchas específicos asociados con estas direcciones,
  estando cada captcha específico asociado por mediación de una relación predefinida con un identificador de este procesador de seguridad que contiene la respuesta correcta a este captcha con el fin de permitir la identificación de este procesador de seguridad a partir de este captcha entre el indicado conjunto de varios procesadores de seguridad, y
- cada procesador está igualmente programado para:
  . transmitir una dirección contenida en su base de datos a un terminal de recepción que se encarga de telecargar y de utilizar el captcha telecargado en esta dirección, y
  . en respuesta a al menos una utilización de este captcha (Completely Automated Public Turing test to tell Computers and Humans Apart), desde el terminal de recepción,:

    - obtener al menos una respuesta a este captcha y comparar esta respuesta con la respuesta correcta pre-registrada contenida en su memoria, y
    - limitar (122) el descifrado de los criptogramas CW*si ninguna respuesta a este captcha corresponde a la respuesta correcta pre-registrada contenida en su memoria.

11. Conjunto según la reivindicación 10, en el cual las direcciones son URLs (Unform Ressources Locator).

12. Conjunto de varios procesadores electrónicos (76) de seguridad para la realización de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8, estando cada procesador programado para:

- recibir mensajes ECM (Entitlement Control Message) que contienen al menos un criptograma CW* de una palabra de control CW que permite descifrar un contenido multimedia,

- descifrar este criptograma CW*, y

- transmitir la palabra de control descifrada a un descodificador para descodificar el contenido multimedia codificado a partir de esta palabra de control CW descifrada,

caracterizado por que

- cada procesador comprende una memoria (78) que contiene una base (79) de datos que comprende:
  . captchas (Completely Automated Public Turing test to tell Computers and Humans Apart) pre-registrados específicos al procesador de seguridad, y
  . las respuestas correctas pre-registradas a los captcha, estando cada respuesta correcta asociada con el captcha correspondiente, estando cada captcha específico asociado por mediación de una

relación predefinida con un identificador de este procesador de seguridad que contiene la respuesta correcta a este captcha con el fin de permitir la identificación de este procesador de seguridad a partir de este captcha entre el indicado conjunto de varios procesadores de seguridad, y

- cada procesador está igualmente programado para:
  . transmitir uno de los captcha pre-registrados a un terminal de recepción con el fin de iniciar su visualizado en una pantalla,
  . en respuesta a la utilización de este captcha (Completely Automated Public Turing test to tell Computers and Human Apart), desde este terminal de recepción,:
    - obtener al menos una respuesta a este captcha y comparar esta respuesta con la respuesta correcta pre-registrada contenida en la base de datos, y
    - limitar (122) el descifrado de los criptogramas CW* si ninguna respuesta a este captcha corresponde a la respuesta correcta pre-registrada contenida en la base de datos.

13. Procesador electrónico (76) de seguridad para la puesta en práctica de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8, estando este procesador programado para:

- recibir mensajes ECM (Entitlement Control Message) que contienen al menos un criptograma CW* de una palabra de control CW que permite descodificar un contenido multimedia,

- descifrar este criptograma CW*, y

- transmitir la palabra de control descifrada a un descodificador para descodificar el contenido multimedia codificado a partir de esta palabra de control CW descifrada,

caracterizado por que

-el procesador comprende una memoria (78) que contiene al menos una respuesta correcta a un captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) específica al procesador de seguridad,

estando el captcha específico asociado por mediación de una relación predefinida con un identificador de este procesador de seguridad que contiene la respuesta correcta a este captcha con el fin de permitir la identificación de este procesador de seguridad a partir de este captcha entre un conjunto de procesadores de seguridad, y

-este procesador está igualmente programado para, en respuesta a al menos una utilización de este captcha (Completely Automated Public Turing test to tell Computers and Humans Apart), desde un terminal de recepción,:

. obtener al menos una respuesta a este captcha y comparar este respuesta con la respuesta correcta contenida en su memoria, y

. limitar (122) el descifrado de los criptogramas CW* si ninguna respuesta a este captcha corresponde a la respuesta correcta contenida en la memoria,

en el cual el procesador está igualmente programado para construir este captcha específico a partir de su identificador y luego transmitirlo al terminal de recepción con el fin de iniciar su visualizado en una pantalla.

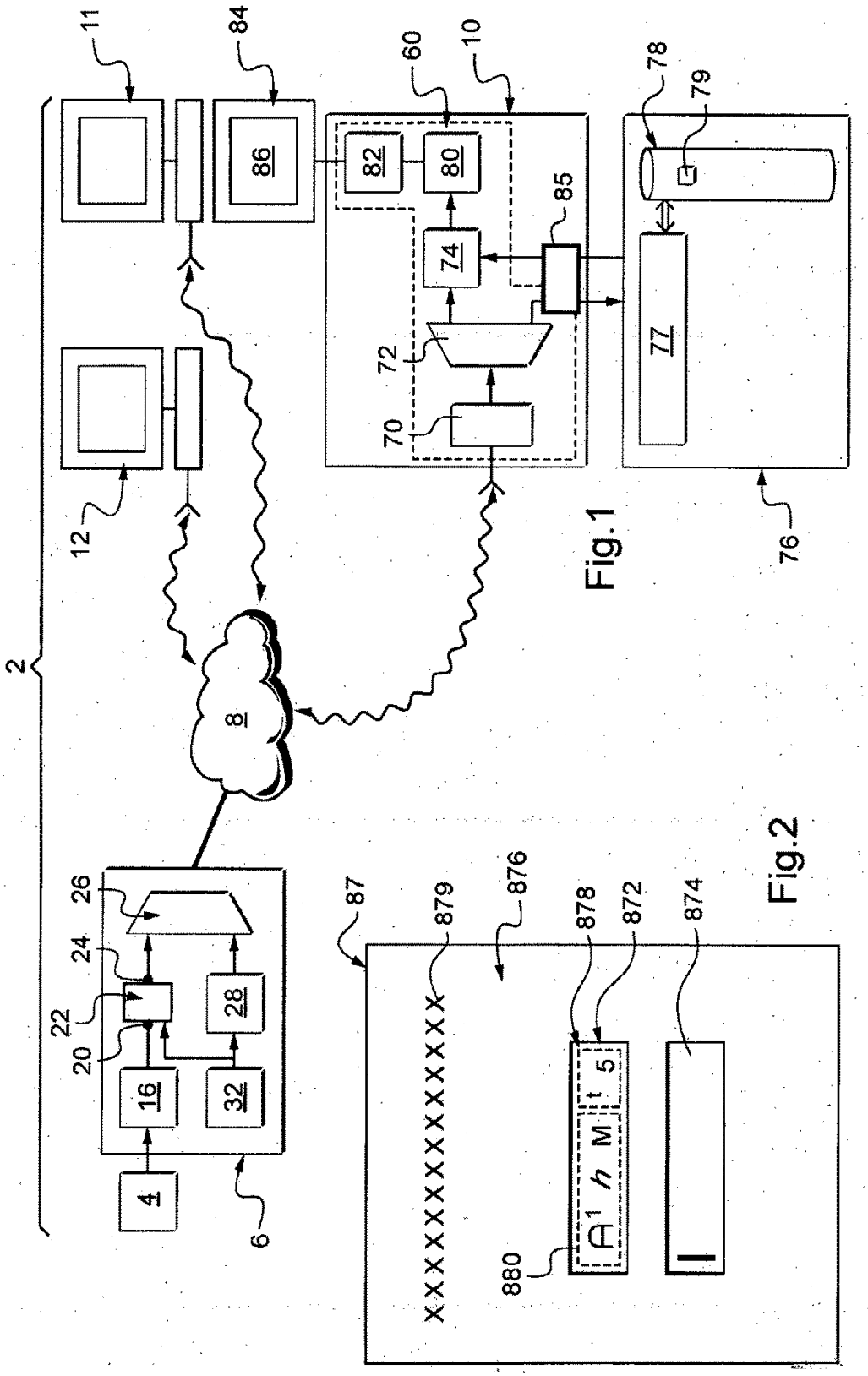
11
84
60
10
78
79
86
82
80
85
74
72
70
77
12
76
2
8
26
24
22
20
28
16
32
4
6
87
879
876
878
872
874
880
XXXXXXXXXXXXXXX
A1 h M t 5

Fig.1

Fig.2

Fig.4

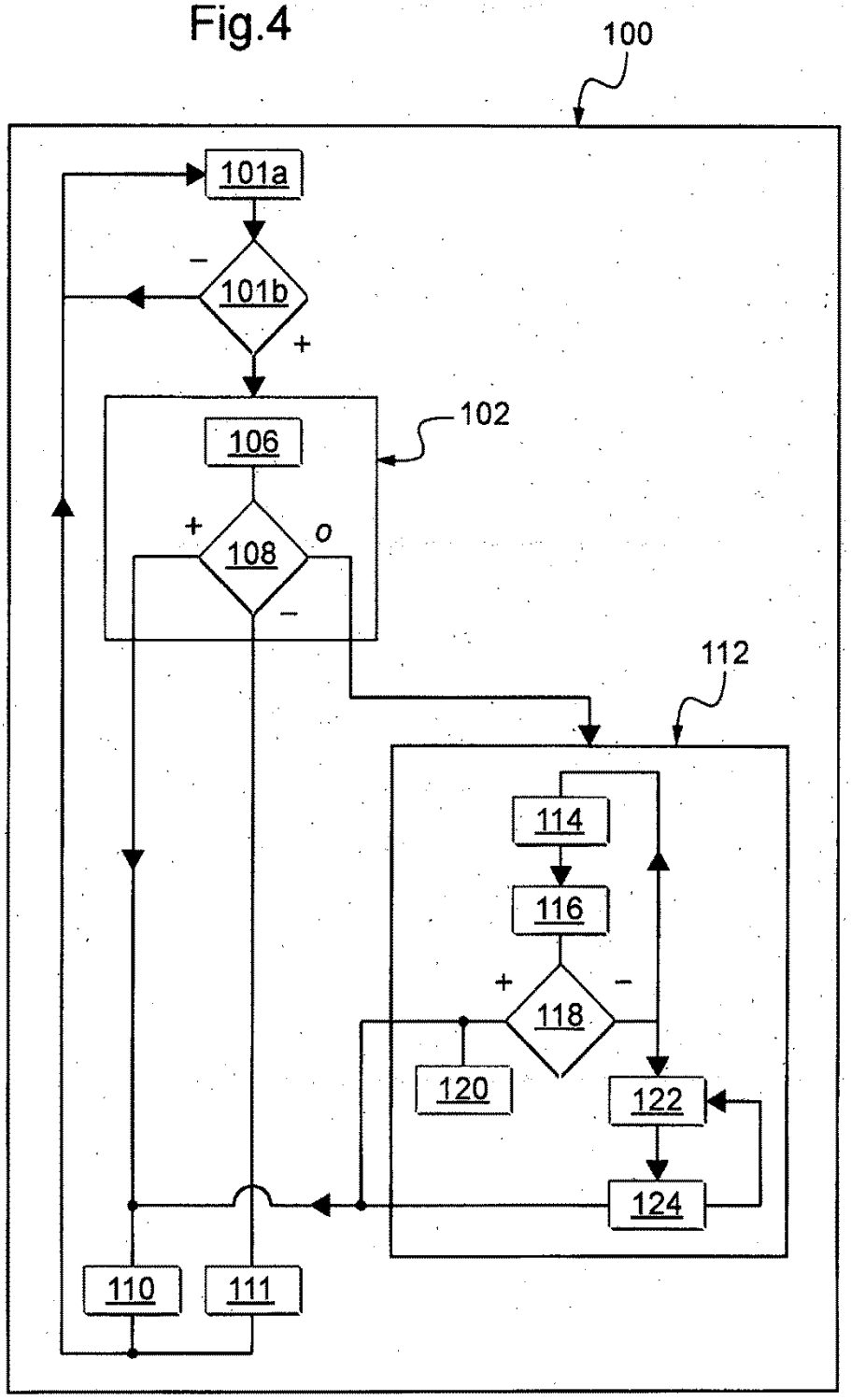

Fig.3

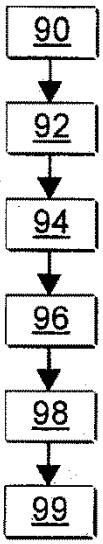

Fig.5