(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 306 868**

(51) Int. Cl.:
H04N 7/167 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03725268 .1**
(86) Fecha de presentación : **05.03.2003**
(87) Número de publicación de la solicitud: **1488642**
(87) Fecha de publicación de la solicitud: **22.12.2004**

(54) Título: **Protocolo de control de acceso, por intervalos de duraciones específicas, a informaciones cifradas.**

(30) Prioridad: **06.03.2002 FR 02 02857**

(45) Fecha de publicación de la mención BOPI:
16.11.2008

(45) Fecha de la publicación del folleto de la patente:
16.11.2008

(73) Titular/es: **Viaccess**
Les Collines de l'Arche, Tour Opera C
92057 Paris La Defense, FR

(72) Inventor/es: **Becker, Claudia;**
Codet, André;
Fevrier, Pierre y
Guionnet, Chantal

(74) Agente: **Ponti Sales, Adelaida**

DESCRIPCIÓN

Protocolo de control de acceso, por intervalos de duraciones específicas, a informaciones cifradas.

La invención concierne un protocolo o un método de control de acceso, por intervalos de duraciones específicas, a informaciones cifradas.

En este texto los términos "protocolo" y "método" se utilizan como sinónimos.

Actualmente, la transmisión de informaciones cifradas conoce un auge sin precedentes, debido a la explosión manifiesta de las prestaciones de servicios realizadas a partir de la transmisión de datos soporte de informaciones, de tipos muy diferentes.

De manera general, los procesos de control de acceso a datos cifrados, cuando estos datos se transmiten en modo punto-multipunto por ejemplo, se llevan a cabo comparando los criterios de acceso proporcionados en mensajes de control de acceso, mensajes ECM, con respecto a propiedades o derechos de acceso, que posee cada abonado, estando inscritos estos derechos de acceso en el descodificador que se pone a disposición de cada abonado, o mejor, en el módulo de control de acceso, realizado con la forma de una tarjeta de microprocesador por ejemplo y atribuida a cada abonado.

De una manera más específica, se recuerda que las informaciones se codifican a nivel de un centro de emisión, por medio de una llave de servicio. La llave de servicio está contenida en una palabra de control. La palabra de control se cifra por medio de una llave de explotación y el criptograma de la palabra de control se transmite, hacia al menos un terminal de descodificación asociado a un módulo de control de acceso provisto de un procesador de seguridad.

Las informaciones cifradas y los mensajes de control de acceso periódico, mensajes ECM, comprenden el criptograma de la palabra de control y criterios de acceso, cambiándose periódicamente la palabra de control y el criptograma de la palabra de control. El acceso a las informaciones cifradas a nivel de cada terminal de descodificación está condicionado a la verificación del valor verdadero de los criterios de acceso con respecto a al menos un derecho de acceso inscrito en el módulo de control de acceso, a continuación al descifrado del criptograma de la palabra de control por medio de la llave de explotación, con el fin de restituir la palabra de control y efectuar la descodificación de las informaciones cifradas por medio de esta última.

Para una descripción más detallada de estos procesos de control de acceso, se podrá útilmente reportarse a las disposiciones de la norma UTE C90-007 enero 1994.

Actualmente, en referencia a los textos y disposiciones de la susodicha norma, en ausencia de disposiciones que regulen las modalidades de tratamiento, las emisiones sucesivas de un programa televisado, la visualización de un programa cifrado grabado o el acceso a un programa, en el caso de una nueva emisión, son equivalentes a una nueva emisión, desde el punto de vista del control de acceso propiamente dicho.

En particular, no es posible, actualmente, controlar específicamente, por intervalos temporales, el número de visualizaciones, ni la vuelta atrás, en el caso de una grabación.

Como consecuencia, cuando los sistemas de control de acceso están provistos además de un sistema de gestión de portafichas electrónico, que permite gestionar totalmente el control de acceso en términos de gestión contable por ejemplo, cualquier nueva visualización o cualquier vuelta atrás, en el caso de una grabación, se traducen o bien por un débito sistemático del portafichas electrónico del abonado en el modo de acceso llamado de compra impulsiva de tiempo, o bien por un acceso ilimitado, en el caso en el que se autorice el acceso en todos los demás modos de acceso comercializados.

US 2001/0012366 A1 describe un sistema de control de acceso a programas emitidos en los cuales se utiliza un número de orden asignado a escenas sucesivas.

WO 01/20836 A trata de la diseminación de llaves de cifrado/descifrado, llaves secretas y/o llaves públicas-privadas, y la utilización de llaves efímeras en las transmisiones punto a punto.

EP-A-0 884 906 describe un sistema de control de acceso que utiliza descriptores de modo de acceso (DMA).

La presente invención tiene por objeto poner remedio a los inconvenientes y limitaciones de los procesos de control de acceso de la técnica anterior.

En particular, de manera más específica, la presente invención tiene por objeto un protocolo de control de acceso a informaciones cifradas, por periodos de duraciones específicas, con un valor de duración determinado ajustable.

Otro objeto de la presente invención es la realización de un protocolo de control de acceso a informaciones cifradas por intervalos de duraciones específicas, pudiendo definirse el origen de cualquier intervalo de duración específica en referencia a una acción específica de cada abonado.

Otro objeto de la presente invención, debido al carácter ajustable de la duración del intervalo de acceso y/o del origen del susodicho intervalo de acceso en referencia a una acción específica de cada abonado, es la realización de una pluralidad de nuevos servicios, relacionados con la emisión de programas televisados, servicios como el servicio de previsualización de un programa televisado durante una duración determinada, servicio de acceso de control de vuelta atrás, después de una grabación de un programa televisado, servicio de conteo del número de visualizaciones en el caso de la emisión en bucle de programas televisados.

Otro objeto de la presente invención es la realización de un protocolo de control de acceso, que permite, gracias a la identificación de todo o parte de un programa ya visualizado por un abonado, y pues al que ya se ha acordado el acceso, de discriminar cualquier periodo ya visualizado por ese abonado, y autorizar de ese modo una gestión optimizada de las visualizaciones, con el criterio de un número determinado de una misma visualización respectivamente de una nueva visualización.

Otro objeto de la presente invención es, en el caso de la grabación de programas televisados, la realización de un protocolo de control de acceso que permite limitar el número de lecturas, así como la amplitud de vuelta atrás autorizada.

El protocolo de control de acceso a informaciones cifradas, objeto de la invención, se realiza a nivel de un centro de emisión. El cifrado se efectúa por medio de una llave de servicio contenida en una palabra de control. La palabra de control se cifra por medio de una llave de explotación y el protocolo de control de acceso consiste al menos en transmitir, hacia al menos un terminal de descodificación asociado a un módulo de control de acceso provisto de un procesador de seguridad, las informaciones cifradas y mensajes de control de acceso periódicos, mensajes ECM, que comprenden criterios de acceso y el criptograma de la palabra de control. La palabra de control y el criptograma de la palabra de control se cambian periódicamente. El acceso a las informaciones cifradas a nivel de cada terminal de descodificación está condicionado al valor verdadero de los criterios de acceso con respecto a al menos un derecho de acceso inscrito en el módulo de control de acceso, después al descifrado del criptograma de la palabra de control por medio de la llave de explotación, con el propósito de restituir la palabra de control y efectuar la descodificación de las informaciones cifradas.

Es remarcable por el hecho de que consiste en atribuir, a cada mensaje de control de acceso, mensaje ECM, un número que verifica una función monótona no decreciente, representando los mensajes ECM_j, consecutivos, de número T_j sucesivo, una base de tiempos formada por una pluralidad de intervalos de tiempo elementales de transmisión de quanta sucesivos elementales de información cifrada. Consiste a continuación en detectar, a nivel de cada terminal de descodificación, el número de cada mensaje de control de acceso, mensaje ECM_j, después a petición del usuario de ese terminal de descodificación de un acceso condicional a al menos una parte de las informaciones cifradas, en seleccionar el número de un mensaje de control de acceso, que corresponde al instante de emisión de esa petición, y en constituir un origen de tiempo de esa base de tiempos.

Se permite el acceso por parte del usuario a las informaciones cifradas en función de un criterio de acceso específico a partir de ese origen de la base de tiempos, a lo largo de un intervalo temporal que corresponde a una pluralidad de intervalos de tiempo elementales que definen una pluralidad de quanta sucesivos elementales de informaciones cifradas.

El protocolo de control de acceso objeto de la presente invención se adapta particularmente a la transmisión punto-multipunto de informaciones cifradas, en particular de programas de televisión, y a la gestión de los servicios de televisión por peaje, en general.

Se comprenderá mejor con la lectura de la descripción y con la observación de las figuras que vienen a continuación en las cuales:

- la figura 1a representa, a título puramente ilustrativo, un organigrama general de realización del protocolo objeto de la presente invención;

- la figura 1b representa diferentes diagramas temporales ilustrativos de un intervalo temporal que constituye un intervalo hacia atrás, un intervalo hacia delante y un intervalo adelante-atrás respectivamente;

- la figura 1c representa, a título ilustrativo, diferentes ejemplos de realización de función monótona no decreciente;

- la figura 2 representa, a título puramente ilustrativo, un organigrama específico de realización del protocolo objeto de la presente invención, más particularmente adaptado a la gestión de servicios de las características de un servicio de previsualización de un programa TV televisado cifrado, un servicio de vuelta atrás, un servicio de gestión del número de visualizaciones, en el caso de una emisión en bucle.

Se dará ahora una descripción más detallada del protocolo de control de acceso a informaciones cifradas según el objeto de la presente invención en referencia a la figura 1a y las figuras siguientes.

De una manera general, se recuerda que el protocolo objeto de la presente invención se realiza a nivel de un centro de emisión CE, por una parte, y a nivel de una pluralidad de terminales de descodificación D_k, por otra parte, estando

asociado a cada terminal de descodificación un módulo de control de acceso constituido, por ejemplo, por una tarjeta de microprocesador dedicada provista de un procesador de seguridad.

Las informaciones I se cifran a nivel del centro de emisión CE por medio de una llave de servicio contenida en una palabra de control CW, cifrándose esa palabra de control por medio de una llave de explotación de manera conocida en sí misma.

Se emiten las informaciones cifradas I* y los mensajes de control de acceso periódicos, mensajes llamados ECM. Los mensajes citados anteriormente comprenden criterios de acceso. El criptograma de la palabra de control CW, la palabra de control en particular, se cambian periódicamente. El acceso a las informaciones cifradas a nivel de cada terminal de descodificación D_k está condicionado a la verificación del valor verdadero de los criterios de acceso vehiculados por los mensajes de control de acceso ECM con respecto a al menos un derecho de acceso inscrito en el módulo de control de acceso asociado a cada terminal de descodificación D_k.

El descifrado del criptograma de la palabra de control se efectúa a nivel de cada terminal de descodificación y en particular del módulo de control de acceso por medio de la llave de explotación, con el fin de restituir la palabra de control CW y efectuar la descodificación de las informaciones cifradas I*.

Según un aspecto remarcable del protocolo de control de acceso de control de acceso a informaciones cifradas de la presente invención, éste consiste además en particular en el centro de emisión CE, en atribuir a cada mensaje de control de acceso, mensajes ECM, un número T_j que verifica una función monótona no decreciente, designándose, por esta razón, los mensajes de control de acceso, ECM_j donde j designa la posición del susodicho número.

Según un aspecto particularmente remarcable del protocolo objeto de la presente invención, los mensajes de control ECM_j consecutivos de número sucesivo T_j representan una base de tiempos formada por una pluralidad de intervalos de tiempo elementales de transmisión de quanta sucesivos elementales de informaciones cifradas. Se comprende de ese modo que entre dos números sucesivos T_{j-1}, T_j por ejemplo y que corresponden a al menos un intervalo de tiempo δ representativo de la periodicidad de emisión de los mensajes de control ECM_j se transmite de ese modo un quantum elemental de informaciones cifradas designado $\delta I^*_{(j-1)}$ hacia cada terminal de descodificación D_k.

A nivel de cada susodicho terminal de descodificación D_k el protocolo objeto de la presente invención consiste entonces, en una etapa B, en detectar a nivel de cada uno de los terminales de descodificación citados anteriormente el número T_j de cada mensaje de control de acceso ECM_j. La operación de detección del número de cada mensaje de control de acceso se ve acompañada por una memorización de ese número instantáneo.

Según otro aspecto particularmente remarcable del protocolo objeto de la presente invención, éste consiste, a petición del usuario del terminal de descodificación D_k considerado en un acceso condicional a al menos una parte de las informaciones cifradas, en seleccionar en una etapa C el número de un mensaje de control de acceso ECM_j que corresponde al instante de emisión de la petición UR.

Se concibe en particular que al emitir el usuario una petición UR en el terminal de descodificación, pudiendo emitirse esa petición a partir de un selector de programas como un mando a distancia por ejemplo o por medio de cualquier otro medio, se localiza el instante de emisión de la petición con respecto al número instantáneo T_j detectado en la etapa B precedente, y en particular con respecto a un acontecimiento anterior, como un acceso previo, así como se describirá más adelante en la descripción. Ese acontecimiento anterior puede corresponder a un acceso previo que define el origen de la base de tiempos de número T_{jo}.

En particular, el número T_{jo} que constituye el origen de tiempos de la base de tiempos puede ventajosamente corresponder al número del mensaje ECM_{jo} del último acceso controlado, no gratuito, precedente, memorizado en el módulo de control de acceso, o la tarjeta, atribuida al usuario, así como se describirá más adelante en la descripción, número T_{jo}, el cual se dispone en la etapa A.

En la figura 1a en la etapa C se ha representado simbólicamente la serie de los números sucesivos T_{j-1}, T_j, T_{j+1} y el acontecimiento de una petición del usuario UR, considerándose el origen de la base de tiempos T_{jo} inferior a la secuencia de los números sucesivos T_{j-1}, T_j, T_{j+1}. En cualquier caso, se comprenderá que el valor T_{jo} de un acceso precedente puede sin embargo ser superior al valor instantáneo T_j que localiza la emisión de la petición UR por el usuario.

Es el caso, por ejemplo, en el caso del acceso a programas emitidos en bucle con los mismos parámetros de control de acceso ECM_j o en el caso del acceso a programas grabados.

La etapa C de selección del número del mensaje de control de acceso puede entonces venir seguida de una etapa D que consiste en autorizar el acceso por el usuario a las informaciones cifradas en función de un criterio de acceso específico a partir del origen T_{jo} de la base de tiempos a lo largo de un intervalo temporal que corresponde a una pluralidad de intervalos de tiempo elementales que definen una pluralidad de quanta sucesivos elementales de informaciones cifradas.

En la figura 1a y por esa razón se ha representado por

$$\Delta(T_{jo}, td, tf)$$

el intervalo temporal de acceso concedido al usuario, intervalo temporal en el cual:

- jo representa la posición del número T_{jo} que define el origen de la base de tiempos;

- td representa un desfase de números en la base de tiempos con respecto al origen T_{jo} citado anteriormente;

- tf representa otro desfase de números con respecto al origen T_{jo} citado anteriormente.

A título de ejemplo no limitativo se indica que los desfases citados anteriormente corresponden a al menos un intervalo de tiempo elemental δ tomado igual al periodo de emisión de los mensajes de control de acceso ECM_j.

En esas condiciones, cada intervalo de tiempo elemental sucesivo en el instante j de recepción del mensaje ECM_j se designa: $\delta(j)$ y el quantum de información elemental correspondiente:

$$\delta\, I^*_{(j)} = \delta_{(j)}(I^*)$$

Se comprende de ese modo que el usuario, gracias a la petición UR formulada, se ve autorizado a un acceso a la información $\Delta I^* = \Delta(T_{jo}, td, tf)(I^*)$ a lo largo de una pluralidad de intervalos de tiempo elementales $\delta_{(j)}$ en la etapa E final en la figura 1, para quanta de información sucesivos $\delta I^*_{(j)}$ a lo largo del intervalo temporal $\Delta(T_{jo}, td, tf)$.

La figura 1b tiene como propósito ilustrar los parámetros de definición de números de acceso instantáneos que corresponden a la petición del usuario, de accesos precedentes del usuario memorizados en la tarjeta para constituir el origen T_{jo} de la base de tiempos correspondiente y el desfase temporal de inicio td respectivamente de fin tf con respecto al origen de la base temporal T_{jo}, permitiendo de ese modo los parámetros T_{jo}, td y tf definir el intervalo temporal correspondiente al acceso autorizado según el criterio de acceso específico, así como se menciona anteriormente en la descripción.

En la figura 1b, en el punto 1), se ha representado la sucesión de los números de recepción de los mensajes ECM_j, que se considera que designa la posición del número instantáneo del mensaje ECM_j correspondiente.

En referencia a los puntos 2), 3) y 4) de la figura 1b, se indica que:

- T_{jo} origen de la base temporal es el último acceso precedente memorizado en la tarjeta del usuario, acceso no gratuito por ejemplo, para el programa de informaciones cifradas I* considerado;

- td es el desfase con respecto al origen T_{jo} que corresponde al inicio de la zona temporal, o intervalo temporal, cuyo acceso se autoriza según un criterio de acceso específico;

- tf es el desfase con respecto al origen T_{jo} que corresponde al fin de la zona temporal, o intervalo temporal, cuyo acceso se autoriza según el criterio de acceso específico.

En referencia a los puntos 2), 3) y 4) de la figura 1b, se indica que:

- la zona temporal, o intervalo, es hacia atrás para td < = 0 y tf > = 0;

- el intervalo, o zona temporal, es hacia delante para td > = 0 y tf > = 0;

- la zona temporal, o intervalo, queda a caballo, es decir hacia delante y hacia detrás para td < = 0 y tf > = 0.

De una manera específica no limitativa, se recuerda que el número instantáneo de un mensaje ECM_j es siempre no decreciente cuando se emite un programa transmitido. Por el contrario, cuando ese programa se emite en bucle, o cuando corresponde a un programa grabado en un vídeo y reproducido, el valor T_{jo} memorizado en la tarjeta atribuida al abonado puede corresponder a un acceso precedente y situarse relativamente en el intervalo, o zona temporal, definido por T_{jo}, td y tf, así como se representa en los puntos 2), 3) y 4) de la figura 1b. Esas tres situaciones son las situaciones de interés para la realización del protocolo objeto de la presente invención.

Ahora se describirán diferentes modos de realización de un número T_j que verifica una función monótona no decreciente en relación a la figura 1c.

En el punto 1 de la figura 1c, se ha representado una función monótona no decreciente formada por una función continuamente creciente del periodo de emisión de los mensajes de control ECM_j. A título de ejemplo, cada número T_j es creciente a lo largo de la duración del tiempo elemental $\delta_{(I)}$ y verifica la relación:

$$T_{j-1} \leq T_j \leq T_{j+1}.$$

En el punto 2 de la figura 1c, se ha representado una función monótona no decreciente formada por una función creciente por escalones del instante de emisión de los mensajes de control ECM_j.

En particular, en referencia al punto 2 de la susodicha figura, se comprende que cada mensaje de control ECM_j puede ser repetido a lo largo de uno o varios intervalos de tiempo elementales, entre los números sucesivos T_{j-1}, T_j y siguientes. Un modo operatorio como ese permite definir una base de tiempos de resolución diferente al periodo de emisión de los mensajes de control ECM_j.

Así como se ha representado además en el mismo punto 2, cada número T_j puede estar definido por una fecha. En el ejemplo dado en la figura 2, la fecha es un valor temporal, expresado en segundos. Cada escalón T_{j-1}, T_j y siguientes, por ejemplo, queda entonces definido por el intervalo temporal representado por las dos fechas distintas.

El protocolo objeto de la presente invención tiene por objeto permitir la gestión del número de visualizaciones NV realizadas de un mismo programa emitido y/o grabado por un usuario, pudiendo comprender cada visualización uno o varios accesos a ese mismo programa, dos o varios accesos diferentes que pueden pertenecer a la misma visualización y el número de visualizaciones, en esta situación, al no sufrir cambios, no se imputa ninguna facturación suplementaria, en una situación como esa, al usuario.

Por el contrario, el paso de un acceso a otro acceso, del usuario en un mismo programa en condiciones diferentes al criterio de acceso específico mencionado anteriormente en la descripción, es objeto de la contabilización de dos visualizaciones distintas, una visualización y otra visualización, siendo objeto la otra visualización de un incremento del número de visualizaciones y de una facturación suplementaria imputada al usuario, así como se describirá posteriormente en la descripción.

En referencia a la figura 2, se indica que, para garantizar la gestión del número de visualizaciones NV de programas, a petición del usuario, según el criterio de acceso específico en el intervalo temporal definido precedentemente en la descripción y fuera de ese intervalo temporal, pudiendo consistir éste, así como se ha representado en la susodicha figura 2, en una etapa E_0, en definir un número máximo autorizado de visualizaciones para el programa cifrado emitido que contiene las informaciones cifradas I*, designándose por NVM el número máximo autorizado de visualizaciones. El protocolo objeto de la invención puede consistir, además, en definir una primera variable booleana AV cuyo valor verdadero es representativo de la autorización del acceso hacia delante a las informaciones cifradas I* más allá del origen y fuera del intervalo temporal definido precedentemente en la descripción, autorizándose el acceso a las informaciones más allá del origen y fuera del intervalo temporal, con un criterio de acceso distinto del criterio de acceso específico que define el acceso al intervalo temporal citado anteriormente, sin incremento del número de visualizaciones.

Puede consistir igualmente en definir una segunda variable booleana AR cuyo valor verdadero es representativo de la autorización del acceso hacia atrás a las informaciones cifradas más allá del origen y fuera del intervalo temporal, con un criterio de acceso distinto del criterio de acceso específico mencionado precedentemente, sin incremento del número de visualizaciones.

De una manera general, se recuerda que, en un modo de realización preferencial del protocolo objeto de la presente invención, el criterio de acceso específico a la zona o intervalo de acceso temporal definido precedentemente en la descripción, en particular por los parámetros td y tf de desfase con respecto al origen de la base de tiempos T_{jo}, puede ventajosamente consistir en dar un acceso libre en ese intervalo al usuario, es decir un acceso sin facturación.

Además, se indica, a título de ejemplo puramente ilustrativo, que las variables booleanas AV y AR se designan de modo que presentan el valor 1 para el valor verdadero de éstas y el valor cero para el valor complementario del valor verdadero o valor falso de estas últimas.

En la etapa E_0 de la figura 2, se dispone, durante la emisión de la petición UR del usuario, definidos por la posición j del número T_j del mensaje de control de acceso ECM_j correspondiente:

- variables NV, T_{jo} cuando se ha efectuado un acceso precedente a ese mismo programa de datos cifrados, representando T_{jo} el valor memorizado que sirve de origen para el siguiente acceso a partir de la petición UR, y designando NV el número de visualizaciones ya realizadas;

- NVM número máximo autorizado de visualizaciones;

- variables booleanas AV y AR;

- intervalo temporal $\Delta(T_{jo}, td, tf)$.

Finalmente, se indica que, para la realización del protocolo objeto de la presente invención, puede ser ventajoso, cuando el usuario no ha realizado ningún acceso y pues ninguna visualización del programa de datos cifrados correspondiente, inicializar el número de visualizaciones NV con el valor cero.

En estas condiciones, así como se ha representado en la figura 2, el protocolo objeto de la invención puede consistir en someter la variable NV, a una prueba de verificación de existencia. Esa prueba se designa, la etapa E_1:

$$\exists(NV)?$$

En caso de respuesta negativa a la prueba E_1, es decir si existe una variable NV igual a cero para las informaciones cifradas I* consideradas, entonces se llama a una etapa E_2, la cual consiste en comparar el valor del número de visualizaciones NV por comparación de inferioridad estricta con el valor del número máximo de visualizaciones NVM.

Se comprende, por supuesto, que, en esta situación de partida, la respuesta a la prueba E_2 es, en general, siempre positiva, ya que el número de visualizaciones NV es igual a cero en esa situación.

En caso de respuesta positiva a la prueba E_2, se llama a una etapa E_4, la cual consiste en incrementar con una unidad el valor del número de visualizaciones según la relación:

$$NV = NV + 1.$$

Se comprende, en esas condiciones, que el acceso al programa de informaciones cifradas I* es el primer acceso.

En esas condiciones, la etapa E_4 puede entonces ir seguida de una etapa E_5 que consiste, para la primera visualización, en actualizar el origen de la base de tiempos, es decir el valor T_{jo}, con el valor T_j que no es otro que el número de recepción de la petición UR, es decir el número de recepción del mensaje ECM_j correspondiente.

La etapa E_5 de actualización del origen de la base de tiempos puede entonces ir seguida de un acceso al quantum de información elemental, en la etapa E_6, designándose ese quantum de información elemental $\delta I^*_{(j)}$. Se comprende, en esas condiciones, que el primer acceso corresponde a una primera visualización y que, en esas condiciones, el criterio de acceso aplicado es un criterio de acceso distinto del criterio de acceso específico correspondiente a un acceso libre.

Por el contrario, en caso de respuesta positiva a la susodicha prueba E_1, existe al menos un acceso anterior debido a la existencia del valor NV, el cual es diferente de cero.

En esas condiciones, la etapa E_1 va seguida de una etapa E_7, la cual consiste en comparar y en someter el número de visualizaciones NV a una prueba de comparación de inferioridad o igualdad con el número máximo autorizado de visualizaciones NVM.

En caso de respuesta negativa a la susodicha prueba E_7, se rechaza el acceso a las informaciones cifradas, en la etapa E_3, ya que el usuario ha sobrepasado manifiestamente su cuota de visualizaciones NVM.

Por el contrario, en caso de respuesta positiva a la prueba de comparación de inferioridad o igualdad de la etapa E_7, el protocolo objeto de la invención consiste en someter el número instantáneo T_j a una prueba de pertenencia al intervalo temporal en la etapa E_8.

La prueba de la etapa E_8 de pertenencia al intervalo temporal del número instantáneo T_j verifica la relación:

$$(T_{jo} + td) <= T_j <= (T_{jo} + tf).$$

En caso de respuesta positiva a la prueba E_8, se autoriza el acceso al quantum de información cifrada $\delta I^*_{(j)}$ en función del criterio de acceso específico durante el intervalo temporal a las informaciones cifradas en la etapa E_6 descrita precedentemente en la descripción.

Se comprende, en particular, que el acceso durante el intervalo temporal consiste, por supuesto, en autorizar el acceso sucesivo a cada quantum de información que recubre el intervalo temporal, así como se ha mencionado anteriormente en la descripción.

Se comprende igualmente que, cuando el criterio de acceso específico corresponde a un criterio de acceso libre, es decir, en ausencia de facturación imputada al usuario, entonces se realiza directamente el acceso, en la etapa E_6, en ausencia de cualquier incremento del número de visualizaciones NV.

Por el contrario, en caso de respuesta negativa a la prueba de la etapa E_8, se autoriza el acceso a las informaciones cifradas, según un criterio de acceso distinto del criterio de acceso específico, condicionado al valor verdadero de las variables booleanas mencionadas precedentemente en la descripción.

Se comprende en efecto que, teniendo en cuenta el valor de las variables booleanas citado anteriormente, es posible discriminar la contribución de cualquier nuevo acceso, aguas arriba o aguas abajo del origen citado anteriormente, a una nueva visualización o, al contrario, la ausencia de contribución a una nueva visualización.

De ese modo, en ausencia de pertenencia del número T_j instantáneo al intervalo temporal citado anteriormente, es decir en caso de respuesta negativa a la prueba E_8, la autorización de acceso según el criterio de acceso distinto del criterio de acceso específico condicionado al valor verdadero de las variable booleanas, puede consistir, así como se ha representado en la figura 2, en someter, en una etapa E_9, al número T_j instantáneo representativo del instante de emisión de la petición UR y a la primera variable booleana AV a una primera prueba lógica que comprende la verificación de la igualdad o de la superioridad del número T_j instantáneo con respecto al origen T_{jo}, así como la verificación del valor verdadero de la primera variable booleana AV para autorizar el acceso hacia delante a las informaciones cifradas.

La prueba E_9 consiste igualmente en someter al número T_j instantáneo y a la segunda variable booleana AR a una segunda prueba lógica que comprende la verificación de la igualdad o de la inferioridad del susodicho número T_j con respecto al origen T_{jo}, así como la verificación del valor verdadero de la segunda variable booleana AR para autorizar el acceso hacia atrás a las informaciones cifradas.

En la figura 2, en la prueba E_9, la primera y la segunda pruebas lógicas verifican la relación:

$$(T_j >= T_{jo} Y\ AV = 1)$$

O

$$(T_j <= T_{jo} Y\ AR = 1)$$

En caso de respuesta positiva a la prueba E_9, es decir en caso de respuesta positiva a una u otra de las primera respectivamente segunda pruebas lógicas mencionadas anteriormente, se autoriza el acceso hacia delante respectivamente hacia atrás en ausencia de incremento del número de visualizaciones a las informaciones cifradas.

Se comprende en efecto que, para cualquier petición UR correspondiente a un número de recepción T_j fuera del intervalo temporal definido en la etapa E_8 y superior al origen T_{jo}, el valor verdadero de la variable booleana AV, que indica una petición de avance es decir de continuar la visualización, indica que el usuario desea proceder a proseguir la visualización anterior para continuar esta última, Esto puede ser realizado por el usuario en detrimento de la no visualización del conjunto de los quanta de informaciones cifradas comprendidas entre T_{jo} y T_j.

Lo mismo ocurre para la segunda prueba lógica, mientras que sin embargo, el número instantáneo T_j es, esta vez, inferior al valor T_{jo} de origen. Este puede ser el caso, por ejemplo, o bien cuando se retoma un programa emitido en bucle o, en el caso correspondiente, cuando se realiza una vuelta atrás en una grabación de un vídeo. De la misma forma, en una situación como esa, el usuario desea proceder a la visualización de un episodio anterior al cual ha tenido acceso o no precedentemente.

Para garantizar la autorización del acceso hacia delante respectivamente hacia atrás, en ausencia de incremento del número de visualizaciones, esta visualización queda garantizada, después de la respuesta positiva a la prueba E_9, por la llamada a la etapa de actualización del valor de origen T_{jo}, el cual se actualiza con el valor T_j, en la etapa E_5. La etapa E_5 va seguida entonces por la llamada a la etapa E_6 de acceso al quantum de información elemental cifrada $\delta I^*_{(j)}$.

Por el contrario, en caso de respuesta negativa en la etapa E_9, al no ser verificadas ninguna de las primera y segunda pruebas lógicas, en esas condiciones, el protocolo objeto de la invención consiste en someter el número de visualizaciones NV a una prueba de comparación de inferioridad estricta con el número máximo autorizado de visualizaciones NVM en la etapa E_2.

En caso de respuesta negativa a la susodicha prueba E_2, se rechaza el acceso al quantum de información elemental cifrada $\delta I^*_{(j)}$, E_3, habiendo agotado el usuario su cuota de visualizaciones para el programa considerado. Por el contrario, en caso de respuesta positiva a la prueba E_2, el número de visualizaciones NV se ve sometido a un incremento de una unidad, en la etapa E_4 mencionada precedentemente en la descripción, viniendo seguida esta etapa E_4 de una autorización de acceso hacia delante respectivamente hacia detrás a las informaciones cifradas por medio de la etapa de actualización E_5 mencionada precedentemente en la descripción.

Se comprende de ese modo que, por el efecto del incremento en la etapa E_4, habiendo escogido el usuario un acceso constitutivo de una nueva visualización, ésta le será imputada como tal, al ser el nuevo acceso constitutivo de una nueva visualización.

Un ejemplo de realización del protocolo objeto de la presente invención, para un servicio correspondiente a una vuelta atrás simple en una grabación, a partir de un aparato como un vídeo, se describirá a continuación en relación a la figura 2.

A título de ejemplo no limitativo, en esa situación, el número máximo de visualizaciones NVM puede, por ejemplo, ser tomado igual a 1 y el intervalo o la zona temporal, para el cual se autoriza el acceso según el criterio de acceso específico y, en particular, según un acceso libre, queda definido por los parámetros que vienen a continuación:

- $td < 0$

- $tf = 0$.

En una aplicación como esa al susodicho servicio, las variables booleanas se fuerzan respectivamente:

- AV = 1

- AR = 0.

Se comprende que, en esas condiciones, se le atribuye al usuario un intervalo máximo de visualización por vuelta atrás, tal como se ha definido precedentemente. Fuera de ese intervalo, sólo se autoriza la visualización por acceso hacia delante a partir de la posición T_{jo} debido al valor verdadero respectivamente falso de las susodichas variables booleanas.

Un segundo ejemplo de realización del protocolo objeto de la presente invención, en una aplicación a un servicio de previsualización, también designado “Preview” en lengua anglosajona, se describirá en relación a la misma figura 2.

El susodicho servicio de previsualización corresponde, de hecho a una autorización gratuita de acceso hacia delante con respecto al origen de la base de tiempos.

En una situación como esa, a título de ejemplo no limitativo, el número máximo de visualizaciones puede, por ejemplo, tomarse como igual a uno; NVM = 1.

La zona temporal de acceso según el criterio de acceso específico, como el criterio de acceso libre mencionado precedentemente en la descripción, queda entonces definida por:

td = 0

tf > 0

En esas condiciones, para el servicio de previsualización, las variables booleanas de mando de marcha hacia delante respectivamente hacia atrás del vídeo pueden tomarse como iguales a AV = 0 y AR = 0. En esas condiciones, en el marco del susodicho servicio de previsualización, se habilita pues al usuario únicamente a visualizar el susodicho intervalo o zona temporal a lo largo de un número de quanta sucesivos de informaciones cifradas determinado por la amplitud |tf – td| determinada de manera específica. Se recuerda que la amplitud de la susodicha zona temporal puede corresponder, por ejemplo, a tres minutos de visualización.

Un tercer modo de realización del protocolo objeto de la presente invención, en una aplicación o control del número de visualizaciones durante la emisión de un programa en bucle por ejemplo, se describirá a continuación en relación a la misma figura 2.

En esta aplicación, se puede definir el número máximo de visualizaciones NVM de manera arbitraria para el programa de informaciones cifradas considerado.

A título de ejemplo no limitativo, la amplitud de la zona temporal, para la cual se autoriza el acceso según el criterio de acceso específico, es decir el acceso libre, puede fijarse, arbitrariamente, al valor nulo, es decir td = 0 Y tf = 0.

En esas condiciones, se comprende que el usuario se ve autorizado a consultar cualquier programa de informaciones cifradas emitido en bucle según un criterio de acceso diferente del criterio de acceso específico, correspondiendo ese criterio de acceso a la verificación de al menos un derecho de acceso inscrito en la tarjeta asignada a ese usuario.

En esta situación, sólo se autoriza la marcha hacia delante simple, es decir el acceso a los quanta sucesivos de informaciones cifradas, tomando las variables booleanas los valores:

- AV = 1

- AR = 0.

Referencias citadas en la descripción

Esta lista de referencias citadas por el solicitante es solamente para conveniencia del lector. Aunque se ha tomado el máximo cuidado en la recopilación de las referencias, no se pueden excluir errores u omisiones y la OEP se descarga de cualquier responsabilidad en este aspecto.

Documentos de patente citados en la descripción

- US 20010012366 A1 [0011]
- WO 0120836 A [0012]
- EP 0884906 A [0013].

REIVINDICACIONES

1. Método de control de acceso a informaciones cifradas a nivel de un centro de emisión por medio de una llave de servicio contenida en una palabra de control, estando cifrada esa palabra de control por medio de una llave de explotación, consistiendo al menos ese protocolo de control de acceso en transmitir, hacia al menos un terminal de descodificación asociado a un módulo de control de acceso provisto de un procesador de seguridad, las susodichas informaciones cifradas y mensajes de control de acceso periódicos, mensajes ECM, que comprenden criterios de acceso y el criptograma de la palabra de control, cambiándose periódicamente la palabra de control y el criptograma de la palabra de control, estando condicionado el acceso a las susodichas informaciones cifradas a nivel de cada terminal de descodificación a la verificación del valor verdadero de los susodichos criterios de acceso con respecto a al menos un derecho de acceso inscrito en el módulo de control de acceso, después al descifrado del susodicho criptograma de la palabra de control por medio de la llave de explotación, con el propósito de restituir la susodicha palabra de control y efectuar la descodificación de las susodichas informaciones cifradas,

Caracterizado por el hecho de que el susodicho método consiste:

- en atribuir, a cada mensaje de control de acceso, mensaje ECM, un número (T_j) que verifica una función monótona no decreciente, representando los mensajes ECM_j consecutivos de número sucesivo una base de tiempos formada por una pluralidad de intervalos de tiempo elementales de transmisión de quanta sucesivos elementales de información cifrada,

- en detectar, a nivel de cada terminal de descodificación, el número (T_j) de cada mensaje de control de acceso, mensaje ECM_j, después a petición (UR) del usuario de ese terminal de descodificación en un acceso condicional controlado a al menos una parte de las susodichas informaciones cifradas,

- en seleccionar el número de un mensaje de control de acceso, mensaje ECM_j, que corresponde al instante de emisión de la susodicha petición, y en constituir un origen de tiempo (T_{jo}) de la susodicha base de tiempos; y

- en permitir el acceso a las susodichas informaciones cifradas por el susodicho usuario en función de un criterio de acceso específico a partir del susodicho origen (T_{jo}) de la susodicha base de tiempos, a lo largo de un intervalo temporal que corresponde a una pluralidad de intervalos de tiempo elementales que definen una pluralidad de quanta sucesivos elementales de informaciones cifradas, estando definido el susodicho intervalo temporal a partir del susodicho origen (T_{jo}) por un primer desfase (td) con respecto al susodicho origen que corresponde al inicio del acceso en función del susodicho criterio de acceso específico y por un segundo desfase (tf) que corresponde al final del acceso en función del susodicho criterio de acceso específico.

2. Método según la reivindicación 1, **caracterizado** por el hecho de que la susodicha función monótona no decreciente es una función continuamente creciente del periodo de emisión de los mensajes de control ECM_j.

3. Método según la reivindicación 1, **caracterizado** por el hecho de que la susodicha función monótona no decreciente es una función creciente en escalones del instante de emisión de los mensajes de control ECM_j.

4. Método según la reivindicación 3, **caracterizado** por el hecho de que cada escalón está definido por un número constante a lo largo de varios periodos de emisión de los mensajes de control ECM_j, lo que permite definir una base de tiempos de resolución distinta del periodo de emisión de los mensajes de control ECM_j.

5. Método según la reivindicación 4, **caracterizado** por el hecho de que cada número está definido por una fecha, quedando definido cada escalón por el intervalo temporal representado por dos fechas distintas.

6. Método según la reivindicación 1, **caracterizado** por el hecho de que el susodicho criterio de acceso específico corresponde a un acceso libre.

7. Método según una de las reivindicaciones 2 a 6, **caracterizado** por el hecho de que el susodicho intervalo temporal es o bien un intervalo hacia atrás del susodicho origen, td < = 0 Y tf < = 0, o bien un intervalo hacia delante del susodicho origen, td > = 0 Y tf > = 0, o también un intervalo hacia delante y hacia atrás, td < = 0 Y tf > = 0.

8. Método según una de las reivindicaciones 1 a 7, **caracterizado** por el hecho de que, para garantizar una gestión del número de visualizaciones (NV) a petición del usuario según el susodicho criterio de acceso específico en el susodicho intervalo temporal y fuera del susodicho intervalo temporal, éste consiste al menos:

- en definir un número máximo autorizado de visualizaciones (NVM);

- en someter el número de visualizaciones (NV) a una prueba de comparación de inferioridad o de igualdad con el susodicho número máximo de visualizaciones autorizadas (NVM); y en caso de respuesta negativa a la susodicha prueba de comparación de inferioridad o de igualdad,

- en rechazar el acceso a las informaciones cifradas y en someter el susodicho número (T_j) actual a una prueba de pertenencia al susodicho intervalo temporal en caso contrario; y según un criterio de pertenencia del susodicho número (T_j) instantáneo al susodicho intervalo temporal,

- en autorizar el acceso según el criterio de acceso específico durante el susodicho intervalo temporal a las susodichas informaciones cifradas y en autorizar el acceso según un criterio de acceso distinto del susodicho criterio de acceso específico condicionado al valor verdadero de variables booleanas representativas de la autorización de acceso hacia delante respectivamente acceso hacia detrás, en caso contrario.

9. Método según la reivindicación 8, **caracterizado** por el hecho de que éste consiste además:

- en definir una primera variable booleana (AV) cuyo valor verdadero es representativo de la autorización del acceso hacia delante a las susodichas informaciones cifradas más allá del susodicho intervalo temporal, según un criterio de acceso distinto del susodicho criterio de acceso específico;

- en definir una segunda variable booleana (AR) cuyo valor verdadero es representativo de la autorización del acceso hacia detrás a las susodichas informaciones cifradas más allá del susodicho intervalo temporal según un criterio de acceso distinto del susodicho criterio de acceso específico.

10. Método según la reivindicación 8 ó 9, **caracterizado** por el hecho de que, en ausencia de pertenencia del susodicho número (T_j) instantáneo al susodicho intervalo temporal, la susodicha autorización de acceso según un criterio de acceso distinto del susodicho criterio de acceso específico condicionada al valor verdadero de las susodichas variable booleanas consiste:

- en someter al susodicho número (T_j) instantáneo y a la susodicha primera variable booleana (AV) a una primera prueba lógica que comprende la verificación de la igualdad o de la superioridad del susodicho número (T_j) instantáneo con respecto al susodicho origen (T_{jo}) y la verificación del valor verdadero de la susodicha primera variable booleana, para autorizar el acceso hacia delante a las susodichas informaciones cifradas, o a una segunda prueba lógica que comprende la verificación de la igualdad o de la inferioridad del susodicho número (T_j) instantáneo con respecto al susodicho origen (T_{jo}) y la verificación del valor verdadero de la susodicha segunda variable booleana, para autorizar el acceso hacia atrás a las susodichas informaciones cifradas, y, en caso de respuesta positiva a una u otra de las primera respectivamente segunda pruebas lógicas,

- en autorizar el acceso hacia delante respectivamente hacia atrás en ausencia de incremento del número de visualizaciones a las susodichas informaciones cifradas; y, en caso de respuesta negativa a una y a otra de las primera respectivamente segunda pruebas lógicas,

- en someter el susodicho número de visualizaciones (NV) a una prueba de comparación de inferioridad con el número máximo de visualizaciones autorizadas (NVM); y, en caso de respuesta negativa a la susodicha prueba de comparación de inferioridad,

- en rechazar el acceso a las informaciones cifradas y en someter al susodicho número de visualizaciones (NV) a un incremento de una unidad después a autorizar el acceso hacia delante respectivamente hacia atrás a las susodichas informaciones cifradas, en caso contrario.

11. Método según la reivindicación 10, **caracterizado** por el hecho de que, para un control de acceso específico correspondiente a un servicio de vuelta atrás simple en una grabación y un número máximo de visualizaciones autorizadas NVM = 1, el susodicho intervalo temporal es un intervalo hacia atrás definido por td < 0 Y tf = 0, la primera variable booleana toma el valor verdadero, siendo autorizada la marcha hacia delante, y la segunda variable booleana trasera toma el valor complementario al valor verdadero, no siendo autorizada la marcha atrás.

12. Método según la reivindicación 10, **caracterizado** por el hecho de que, para un control de acceso específico correspondiente a un acceso de previsualización de acceso libre, el susodicho intervalo temporal es un intervalo hacia delante definido por td = 0 Y tf > 0, el número máximo de visualizaciones autorizadas es NVM = 1, tomando la primera y la segunda variables booleanas el valor complementario al valor verdadero, no siendo autorizadas la grabación y/o la vuelta atrás.

13. Método según la reivindicación 10, **caracterizado** por el hecho de que, para una emisión de informaciones cifradas en bucle, el susodicho número máximo de visualizaciones autorizadas se fija en un valor determinado, el susodicho intervalo temporal de acceso a las informaciones cifradas presenta un valor específico, la primera variable booleana toma el valor verdadero y la segunda variable booleana toma el valor complementario al valor verdadero.

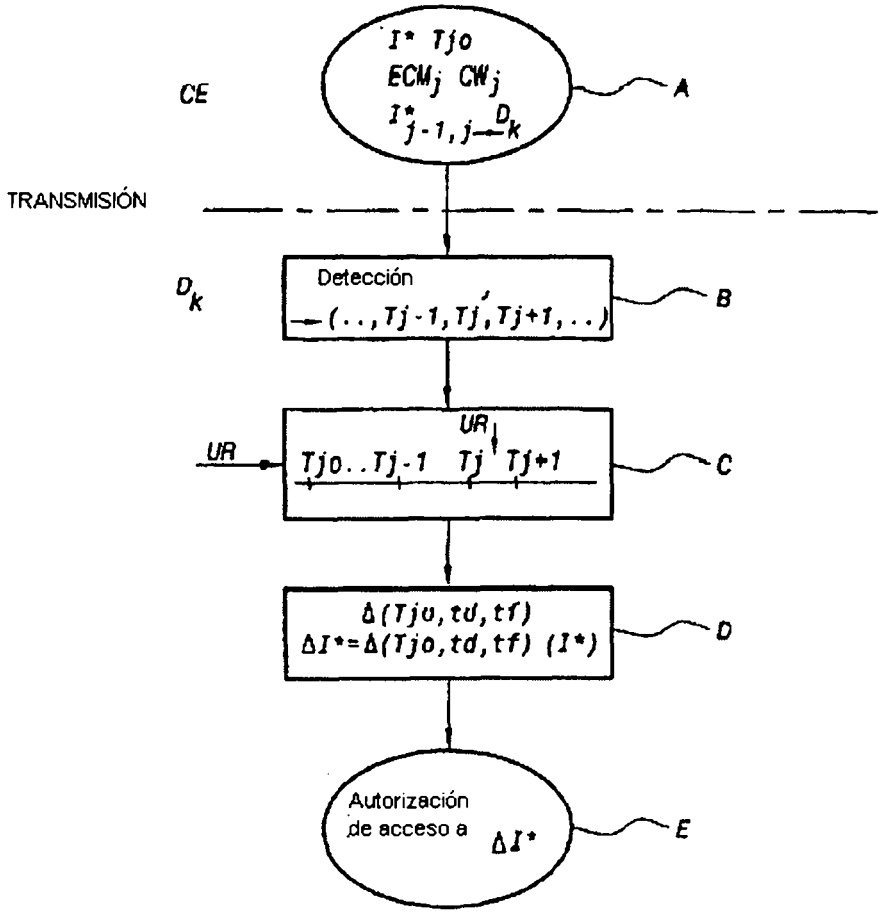
CE
I* Tjo
ECMj CWj
I*j-1,j—Dk
A
TRANSMISIÓN
Dk
Detección
—(..,Tj-1,Tj',Tj+1,..)
B
UR
UR
Tjo..Tj-1 Tj Tj+1
C
Δ(Tjo,td,tf)
ΔI*=Δ(Tjo,td,tf) (I*)
D
Autorización
de acceso a
ΔI*
E

FIG.1a

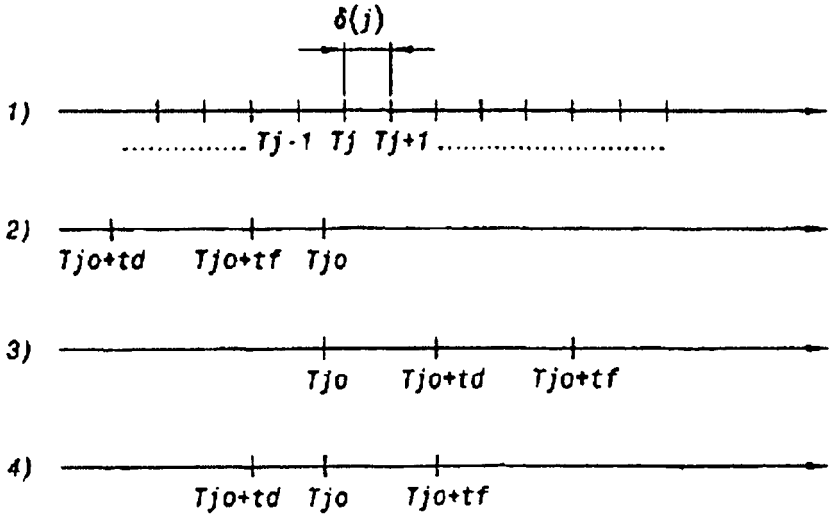
δ(j)
1)
..... Tj-1 Tj Tj+1 .....
2)
Tjo+td Tjo+tf Tjo
3)
Tjo Tjo+td Tjo+tf
4)
Tjo+td Tjo Tjo+tf

FIG.1b

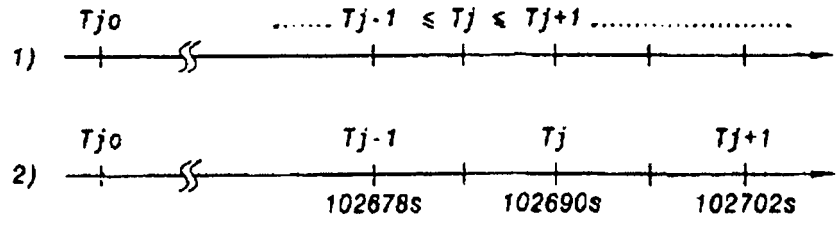
Tjo
..... Tj-1 ≤ Tj ≤ Tj+1 .....
1)
Tjo
Tj-1
Tj
Tj+1
2)
102678s
102690s
102702s

FIG.1c

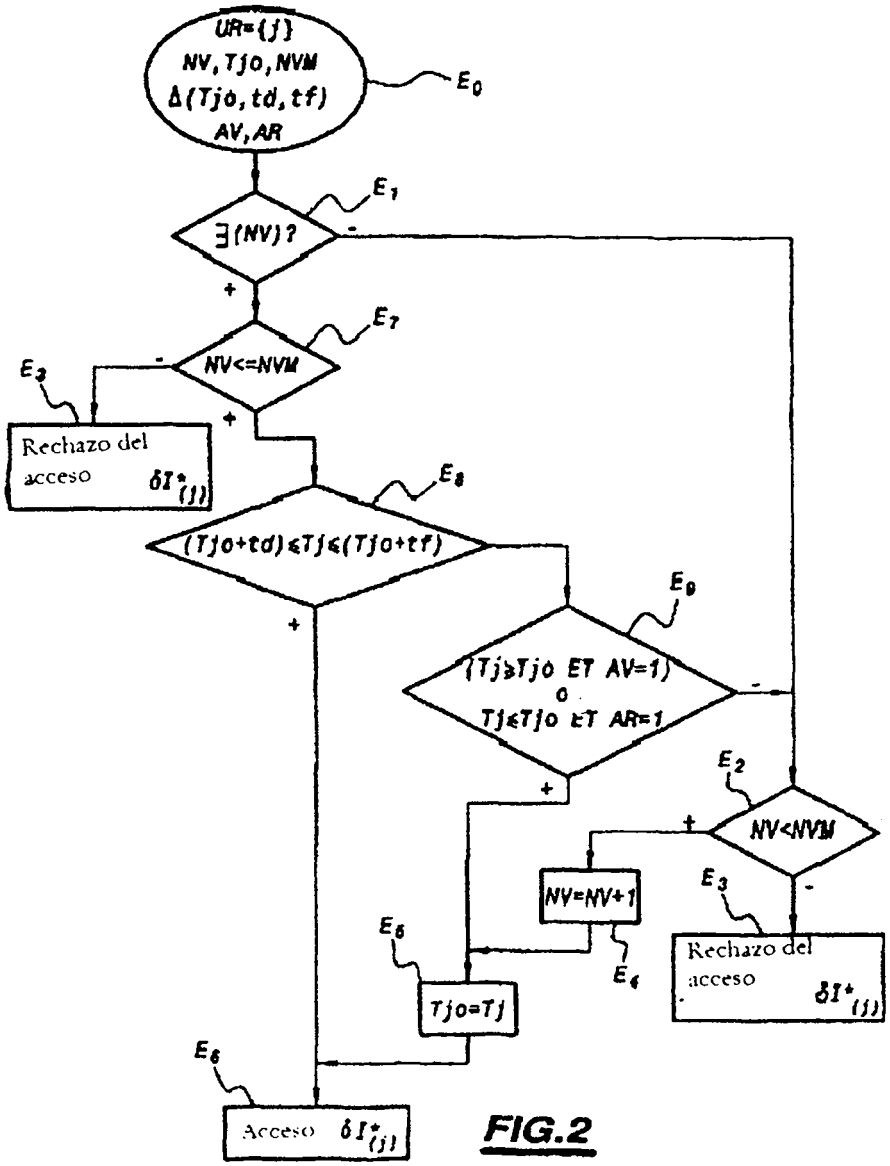
UR={j}
NV, Tjo, NVM
Δ(Tjo, td, tf)
AV, AR
E0
E1
∃(NV)?
E7
NV<=NVM
E3
Rechazo del acceso δI*(j)
E8
(Tjo+td)≤Tj≤(Tjo+tf)
E9
(Tj≥Tjo ET AV=1)
o
Tj≤Tjo ET AR=1
E2
NV<NVM
NV=NV+1
E4
E5
Tjo=Tj
E6
Acceso δI*(j)

FIG.2