(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 370 010**

(51) Int. CI.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00110626 .9**
(96) Fecha de presentación: **18.05.2000**
(97) Número de publicación de la solicitud: **1054314**
(97) Fecha de publicación de la solicitud: **22.11.2000**

(54) Título: **APARATO, MÉTODO Y MEDIO QUE ALMACENA UN PROGRAMA DE ORDENADOR PARA EVITAR EL USO NO AUTORIZADO DE UN CONTENIDO.**

(30) Prioridad:
18.05.1999 JP 13669599

(45) Fecha de publicación de la mención BOPI:
12.12.2011

(45) Fecha de la publicación del folleto de la patente:
12.12.2011

(73) Titular/es:
SONY CORPORATION
7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU
TOKYO, JP

(72) Inventor/es:
Hamada, Ichiro y
Fujii, Asako

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Aparato, método y medio que almacena un programa de ordenador para evitar el uso no autorizado de un contenido.

ANTECEDENTES DE LA INVENCION

Campo de la Invención

La presente invención se refiere a un aparato de tratamiento o procesamiento de información, a un método de tratamiento de información y a un medio de proporcionarlos. Más particularmente, la presente invención se refiere un aparato de tratamiento de información, a un método de tratamiento de información y a un medio de proporcionarlos, que son apropiados para aplicaciones en las cuales se debe evitar el uso no autorizado de un contenido.

Descripción de la Técnica Relacionada

Como una técnica convencional para evitar que sea ilegalmente copiado un contenido con un derecho de autor (copyright) protegido, se adoptan un SCMS (Serial Copy Management System: Sistema de gestión de copias en serie) o un CGMS (Copy Generation Management System: Sistema de gestión de generación de copias) en un aparato capaz de grabar un tal contenido. Ejemplos del contenido son datos de audio grabados en un CD (Disco Compacto) y datos de AV grabados en un DVD (Disco Versátil Digital). Dicho contenido puede ser grabado normalmente por una grabadora de MD (Mini Disco), una grabadora de CD-R o en una grabadora de DV (Video Digital). En el SCMS y en el CGMS se añade información predeterminada a un contenido para limitar el número de copias disponibles.

En años recientes, es posible intercambiar un contenido entre un aparato de AV para reproducir o grabar un contenido y un ordenador personal por medio de un bus de IEEE1394. Empleando el ordenador personal una CPU que tenga una potencia de tratamiento incrementada y un disco duro que tenga una capacidad de almacenamiento incrementada, el ordenador personal es capaz de reproducir, grabar y editar un contenido.

De ese modo, si se instala en un ordenador personal un programa de aplicación ilegal para falsificar intencionadamente la información antes mencionada añadida a un contenido, se presentará el problema de una incapacidad de evitar que el contenido sea copiado ilegalmente por el ordenador personal.

El documento EP-A-0 874 300 describe un sistema para proporcionar de manera segura contenido desde una fuente a un sumidero por medio de la interfaz de IEEE 1394 del sumidero.

Además, se conoce por el documento “5C DIGITAL TRANSMISSION CONTENT PROTECTION WHITE PAPER”, DIGITAL TRANSMISSION CONTENT PROTECTION SPECIFICATION, 14 de julio de 1998, páginas I-II, 1, 13, XP002907865, un método de tratamiento de información para proteger contenido de audio/video del copiado ilegal, en el que el contenido es transmitido entre dispositivos que incluyen ordenadores de sobremesa, reproductores de DVD, televisiones digitales y receptores digitales “set-top-box” por medio de interfaces digitales de IEEE 1394 y se realiza la protección de copias usando autenticación e intercambio de claves, encriptación de contenido, información de control de copias.

SUMARIO DE LA INVENCIÓN

Es un objeto de la presente invención proporcionar un aparato de tratamiento de información, un método de tratamiento de información y un medio de proporcionarlos, que son capaces de evitar que sea utilizado ilegalmente un contenido utilizando un programa de aplicación ilegal instalado en un ordenador personal mediante encriptación del contenido antes de suministrar el contenido al programa de aplicación.

Este objeto se consigue por medio de un aparato de tratamiento de información, un método de tratamiento de información y un medio de proporcionarlos de acuerdo con las reivindicaciones independientes. Características ventajosas de la presente invención se definen en las correspondientes reivindicaciones subordinadas.

Con la presente invención, se forma un juicio sobre la validez de un programa de aplicación sobre la base de una clave de autenticación, y una clave de encriptación encriptada mediante el uso de una clave secreta y un contenido encriptado usando la clave de encriptación se suministran al programa de aplicación con dependencia del resultado del juicio. Es así posible evitar que sea ilegalmente utilizado un contenido.

BREVE DESCRIPCION DE LOS DIBUJOS

La figura 1 es un diagrama de bloques que muestra una configuración típica de un ordenador personal al que se aplica la presente invención;

La figura 2 es un diagrama de bloques que muestra una configuración típica de una interfaz de IEEE1394 utilizada en el ordenador personal mostrado en la figura 1;

La figura 3 es un diagrama de bloques que muestra una configuración típica de una unidad de protección de contenido utilizada en la interfaz de IEEE1394 mostrada en la figura 2;

La figura 4 es un diagrama de bloques que muestra una función de una aplicación activada en el ordenador personal;
La figura 5 muestra un diagrama de flujo que representa el tratamiento de entrada de la interfaz de IEEE1394 mostrada en la figura 1; y
La figura 6 muestra un diagrama de flujo que representa el tratamiento de salida de la interfaz de IEEE1394 mostrada en la figura 1.

DESCRIPCION DETALLADA DE LA REALIZACIÓN PREFERIDA

Una configuración típica de un ordenador personal (PC) 1 al que se aplica la presente invención se explica con referencia a la figura 1. Como se muestra en esa figura, el ordenador personal 1 está conectado a aparatos capaces de manipular contenidos mediante un bus 2 de IEEE1394. Ejemplos de tales aparatos son una grabadora de DV (DVR) 3, una “set top box” (STB) 4 y un disco duro (HDD) 5.

Se ha de observar que un contenido comunicado a través del bus 2 de IEEE1394 es encriptado de acuerdo con un método de DTLA con licencia concedida por el DTLA (Digital Transmission Licensing Administrator), una compañía de concesión de licencia, según recomienda un CPTWG (Copy Protection Technical Work Group).

El ordenador personal comprende una interfaz 11 de IEEE1394, una CPU 12, una RAM 13, una ROM 1 y un disco duro 15 que están conectados entre sí por medio de un bus 16. La interfaz 11 de IEEE1394 suministra un contenido recibido de otro aparato, tal como el DVR 3, a través del bus 2 de IEEE1394, a un programa de aplicación activado en el ordenador personal 1. Al programa de aplicación es capaz de realizar el tratamiento, tal como operaciones de reproducción, grabación y edición de un contenido, se le hace referencia en lo que sigue simplemente como una aplicación. Además, la interfaz 11 de IEEE1394 da salida también a un contenido tratado por la aplicación hacia otro aparato a través del bus 2 de IEEE1394.

Se ha de hacer observar que un programa de aplicación es almacenado en el disco duro 15, cargado en la RAM 13 bajo el control de la CPU 12 basándose en un BIOS almacenado en la ROM 14 y activado a continuación. Una persona encargada de un sistema de encriptación tal como el DTLA suministra una clave de autenticación intrínseca Kn al programa de aplicación. Con el fin de obtener esta clave de autenticación, el usuario necesita hacer un contrato o similar con el productor del programa de aplicación. Un tal contrato se hace para evitar que sea usado ilegalmente un contenido con un derecho de autor protegido.

El término técnico “sistema” utilizado en esta memoria implica un aparato total completo que incluye una pluralidad de aparatos y medios.

La clave de autenticación Kn incluye un par de valores, a saber, una ID y una firma. Un resultado obtenido de la aplicación de una fórmula de tratamiento predeterminada a uno de los dos valores es el otro valor. Aplicando la fórmula de tratamiento predeterminada tanto a la ID como a la firma, es posible verificar si son un par correcto o no. El único componente que muestra esta fórmula de tratamiento predeterminada, es decir, el único componente capaz de formar un juicio de validez de la clave de autenticación Kn, es una unidad 31 de gestión de clave. Además, puesto que es extremadamente difícil encontrar inversamente la fórmula de tratamiento predeterminada a partir de la ID y de la firma, la clave de autenticación no puede ser falsificada en la práctica.

La figura 2 es un diagrama de bloques que muestra detalles de una configuración típica de una interfaz 11 de IEEE1394. Una unidad de control 21 controla los componentes empleados en la interfaz 11 de IEEE1394. Una unidad 22 de entrada/salida recibe un contenido encriptado de acuerdo con el método de DTLA del bus 2 de IEEE1394, que hace pasar el contenido a una unidad de detección 23 de CCI (Copy Control Information). La unidad de detección 23 de CCI hace seguir el contenido recibido de la unidad 22 de entrada/salida a una unidad 24 de encriptación/desencriptación de DTLA. La unidad 23 de detección de CCI detecta una CCI de 2 bits grabada en la cabecera del contenido, que suministra la CCI a una unidad de control 21, a la unidad 24 de encriptación/desencriptación y a una unidad 25 de protección de contenido.

Se ha de hacer observar que la CCI es información sobre el control de operaciones permitidas para copiar un contenido al que se añade la CCI. La CCI puede tener uno de 4 valores, a saber, 00, 10, 01 y 11. Un valor de CCI de 00 representa control de “Libre Copia”, lo que significa que se permiten un número ilimitado de operaciones para copiar un contenido. Un valor de CCI de 10 representa control de “Posible Generador de una Copia”, lo que indica que el contenido puede ser copiado sólo una vez. Un valor de CCI de 01 representa control de “No más Copias”, lo que indica una segunda generación de un contenido. Una segunda generación es un resultado de copiar un contenido con un valor de CCI de 10. Una operación para copiar una segunda generación no está permitida. Un valor de CCI de 11 representa control de “Nunca Copiar”, que indica que no está permitida una operación para copiar un contenido.

La unidad 24 de encriptación/desencriptación de DTLA desencripta un contenido, el cual fue encriptado de acuerdo con el método de DTLA y es recibido de la unidad 23 de detección de CCI, y suministra el resultado de la desencriptación a la unidad 25 de protección de contenido. Además, la unidad 24 de encriptación/desencriptación de DTLA encripta un contenido recibido de la unidad 25 de protección de contenido adoptando el método de DTLA y

suministra el resultado de la encriptación a la unidad 22 de entrada/salida. Se ha de hacer observar que la encriptación y la desencriptación en la unidad 24 de encriptación/desencriptación de DTLA se realizan después de haber sido completado el trabajo de autenticación mutua definido por el método de DTLA entre la unidad 24 de encriptación/desencriptación de DTLA y la DVR 3 que sirve como un aparato que genera un contenido.

La unidad 25 de protección de contenido encripta un contenido recibido de la unidad 24 de encriptación/desencriptación de DTLA y suministra el contenido encriptado a la aplicación. Además, la unidad 25 de protección de contenido desencripta un contenido encriptado recibido de la aplicación y suministra el contenido desencriptado a la unidad 24 de encriptación/desencriptación de DTLA. Se usa una unidad 26 de almacenamiento de clave para almacenar una pluralidad de claves de fuente Ks para todos los valores de CCI. Las claves de fuente Ks se usan en el tratamiento de encriptación realizado por la unidad 25 de protección de contenido.

La figura 3 es un diagrama de bloques que muestra detalles de una configuración típica de la unidad 25 de protección de contenido. La unidad 31 de gestión de clave forma un juicio en cuanto a si es válida o no una clave de autenticación Kn recibida de una unidad 41 de gestión de clave de una aplicación mostrada en la figura 4. Si se encuentra que es válida la clave de autenticación Kn, los componentes empleados en la unidad 25 de protección de contenido son controlados para que intercambien contenidos con la aplicación.

Para exponerlo con detalle, la unidad 31 de gestión de clave aplica una fórmula de tratamiento predeterminada a una ID incluida en la clave de autenticación Kn recibida de la aplicación. A continuación, la unidad 31 de gestión de clave forma un juicio en cuanto a si el resultado de aplicar la fórmula predeterminada a la ID es igual o no a una firma incluida en la misma clave de autenticación Kn. Si el resultado de aplicar la fórmula predeterminada a la ID se encuentra que es igual a la firma incluida en la misma clave de autenticación, es decir, si se encuentra que la clave de autenticación es válida, la unidad 31 de gestión de clave forma adicionalmente un juicio en cuanto a si la ID y la firma forman o no una clave válida aplicando una fórmula de tratamiento predeterminada a la ID y a la firma. Si la clave Kn que comprende la ID y la firma se encuentra válida, la unidad 31 de gestión de clave obtiene por lectura una clave de fuente Ks que corresponde a un valor de CCI suministrado por la unidad 23 de detección de CCI desde la unidad 26 de almacenamiento de clave. La unidad 31 de gestión de clave genera entones una clave de encriptación Kc utilizando la clave de fuente Ks y un número aleatorio, suministrando la clave de encriptación Kc a la unidad 32 de encriptación/desencriptación . Se ha de observar que la clave de encriptación Kc es actualizada a intervalos normalmente en el margen de 30 a 120 segundos. La unidad 31 de gestión de clave da salida a un valor de CCI hacia una unidad 33 de adición de información encriptada cada vez que se actualiza la clave de encriptación Kc. Además, la unidad 31 de gestión de clave genera una clave secreta Ka basándose en información para calcular una clave secreta Ka tal como una clave de autenticación y encripta la clave de encriptación Kc utilizando la clave secreta Ka. La clave secreta Ka encriptada es enviada como salida a la unidad 41 de gestión de clave de la aplicación. Se ha de observar que la información para calcular la clave secreta Ka es recibida de la unidad 41 de gestión de clave.

La unidad 32 de encriptación/desencriptación encripta un contenido desencriptado recibido de la unidad 24 de encriptación/desencriptación de DTLA utilizando la clave de encriptación Kc recibida de la unidad 31 de gestión de clave y da salida al contenido encriptado hacia la unidad 33 de adición de información encriptada. La unidad 32 de encriptación/desencriptación desencripta un contenido encriptado recibido de la unidad 33 de adición de información encriptada y da salida al contenido desencriptado hacia la unidad 24 de encriptación/desencriptación.

La unidad 33 de adición de información encriptada añade un valor de CCI de 2 bits e información de encriptación de 1 bit a un contenido encriptado recibido de la unidad 32 de encriptación/desencriptación. La información de encriptación de 1 bit es conmutada desde “par” a “impar” cada vez que se actualiza la clave de encriptación Kc. El contenido encriptado con el valor de CCI de 2 bits y la información de encriptación de 1 bit añadida al mismo es suministrado a una unidad 42 de análisis de contenido encriptado de la aplicación mostrada en la figura 4. Además, la unidad 33 de adición de información encriptada da salida también a un contenido encriptado recibido de la unidad 42 de análisis de contenido encriptado hacia la unidad 32 de encriptación/desencriptación.

La figura 4 es un diagrama de bloques funcional que muestra una aplicación capaz de reproducir, grabar y editar un contenido. La unidad 41 de gestión de clave se utiliza para almacenar una clave de autenticación Kn asignada a un programa de aplicación. La unidad 41 de gestión de clave da salida también a la clave de autenticación Kn, junto con información para calcular la clave secreta Ka, hacia la unidad 31 de gestión de clave empleada en la unidad 25 de protección de contenido antes de que se inicie un intercambio de contenido con la aplicación. Además, la unidad 41 de gestión de clave desencripta la clave Kc encriptada utilizando la clave sereta Ka y recibida de la unidad 31 de gestión de clave de acuerdo con información que muestra si ha sido o no conmutada la información de “impar” o “par”, dando salida a la clave Kc de encriptación desencriptada hacia una unidad 43 de encriptación/desencriptación. La información de “impar” o “par” que es recibida de la unidad 42 de análisis de información encriptada muestra el estado de actualización de la clave de encriptación Kc incluida en la información de encriptación.

La unidad 42 de análisis de contenido encriptado da salida a un contenido encriptado usando la clave de encriptación Kc y recibido de la unidad 33 de adición de información encriptada, hacia la unidad 43 de encriptación/desencriptación y la información de encriptación añadida al mismo hacia la unidad 41 de gestión de

clave. Además, la unidad 42 de análisis de contenido encriptado da salida también a un contenido encriptado recibido de la unidad 43 de encriptación/desencriptación hacia la unidad 33 de adición de información encriptada.

La unidad 43 de encriptación/desencriptación desencripta un contenido encriptado utilizando la clave de encriptación Kc y recibido desde la unidad 42 de análisis de contenido encriptado utilizando la clave de encriptación Kc recibida de la unidad 41 de gestión de clave, dando salida al contenido desencriptado hacia una unidad 44 de tratamiento de contenido. Además, la unidad 43 de encriptación/desencriptación encripta un contenido recibido desde la unidad 44 de tratamiento de contenido y da salida al contenido encriptado hacia la unidad 42 de análisis de contenido encriptado.

La unidad 44 de tratamiento del contenido realiza el tratamiento, tal como una operación de reproducción, grabación o edición sobre un contenido suministrado a la misma de acuerdo con una operación realizada por el usuario. Se ha de observar que, puesto que la unidad 44 de tratamiento de contenido recibe un valor de CCI incluido en la información de encriptación analizada por la unidad 42 de análisis de contenido encriptado, la unidad 44 de tratamiento de contenido no realiza tratamiento que viole el valor de CCI, tal como una operación de copiado que excediera un número máximo de operaciones de copia permitidas.
Se ha de observar que, implementando la interfaz 11 de IEEE1394 en un único LSI (Large Scale Integrated Circuit), es posible evitar una operación ilegal, tal como una operación para leer un contenido desencriptado desde una posición en un circuito.

A continuación se explica el tratamiento o procesamiento de entrada para suministrar un contenido a una aplicación con referencia a un diagrama de flujo mostrado en la figura 5. Antes de que se realice este tratamiento de entrada, el contenido encriptado de acuerdo con el método de DTLA es suministrado a la interfaz 11 de IEEE1394 y la CCI de la misma es detectada por la unidad 23 de detección de CCI y suministrada a la unidad 31 de gestión de clave empleada en la unidad 25 de protección de contenido. El contenido encriptado de acuerdo con el método de DTLA es desencriptado por la unidad 24 de encriptación/desencriptación de DTLA y suministrado a la unidad 32 de encriptación/desencriptación empleada en la unidad 25 de protección de contenido.

Como se muestra en la figura 5, el diagrama de flujo comienza con un paso S1 en el que la unidad 41 de gestión de clave de la aplicación efectúa una petición para una entrada de contenido, y da salida a una clave de autenticación Kn e información para calcular una clave secreta Ka almacenada en ella hacia la unidad 31 de gestión de clave empleada en la unidad 25 de protección de contenido.

En el siguiente paso S2, la unidad 31 de gestión de clave forma un juicio en cuanto a si es válida o no la clave de autenticación Kn recibida de la unidad 41 de gestión de clave. Si el resultado del juicio indica que es válida la clave de autenticación Kn, el flujo del proceso continúa hacia el paso S3.

En el paso S3, la unidad 31 de gestión de clave obtiene por lectura una clave de fuente Ks correspondiente al valor de la CCI procedente de la unidad 26 de almacenamiento de clave y después genera una clave de encriptación Kc desde la fuente Ks y un número aleatorio, dando salida a la clave de encriptación Kc hacia la unidad 32 de encriptación/desencriptación. Además, la unidad 31 de gestión de clave repone a 0 un temporizador. El temporizador es utilizado para medir un tiempo para actualizar la clave de encriptación Kc.

En el siguiente paso S4, la unidad 31 de gestión de clave genera una clave secreta Ka utilizando la información para calcular la clave secreta Ka. A continuación, la unidad 31 de gestión de clave encripta la clave de encriptación Kc utilizando la clave secreta Ka y da salida a la clave de encriptación Kc encriptada hacia la unidad 41 de gestión de clave de la aplicación. La unidad 41 de gestión de clave desencripta la clave de encriptación Kc encriptada.

En el siguiente paso S5, la unidad 32 de encriptación/desencriptación encripta un contenido desencriptado recibido de la unidad 24 de encriptación/desencriptación de DTLA utilizando la clave de encriptación Kc recibida de la unidad 32 de gestión de clave y da salida al contenido encriptado hacia la unidad 33 de adición de información encriptada.

En el siguiente paso S6, la unidad 33 de adición de información encriptada genera información de encriptación que comprende un valor de CCI e información que muestra el estado de actualización de la clave de encriptación Kc, añadiendo la información de encriptación generada a un contenido encriptado recibido de la unidad 32 de encriptación/desencriptación. Puesto que la clave de encriptación Kc no ha sido actualizada en este caso, la información de estado es par. La unidad 33 de adición de información encriptada da salida a continuación al contenido encriptado, con la información de encriptación añadida al mismo, hacia la unidad 42 de análisis de contenido encriptado de la aplicación. La unidad 42 de análisis de contenido encriptado forma un juicio en cuanto a si la información que muestra el estado de actualización de la clave de encriptación Kc ha sido conmutada o no y da salida al resultado del juicio hacia la unidad 41 de gestión de clave. Sobre la base del resultado del juicio, la unidad 41 de gestión de clave suministra la clave de encriptación Kc actual a la unidad 43 de encriptación/desencriptación. La unidad 43 de encriptación/desencriptación desencripta el contenido utilizando la clave de encriptación Kc y da salida al contenido desencriptado hacia la unidad 44 de tratamiento de contenido.

En el siguiente paso S7, la unidad 31 de gestión de clave forma un juicio en cuanto a si se ha dado salida o no a todos los contenidos procedentes de la unidad 25 de protección de contenido hacia la aplicación. Si el resultado del juicio indica que no se ha dado salida a todos los contenidos procedentes de la unidad 25 de protección de contenido hacia la aplicación, el flujo del proceso continúa al paso S8. En el paso S8, la unidad 31 de gestión de clave se refiere a su propio temporizador para detectar un tiempo en el que se utilizó la presente clave de encriptación Kc. La unidad 31 de gestión de clave forma entonces un juicio en cuanto a si el tiempo detectado ha excedido o no un periodo predeterminado de normalmente 30 segundos a 120 segundos. Si el resultado del juicio indica que el intervalo entre el tiempo detectado y el tiempo más reciente para actualizar la clave de encriptación Kc no ha excedido el periodo predeterminado, el flujo del proceso vuelve al paso S5 par repetir el procesamiento del mismo y las subsiguientes partes del tratamiento.

Por el contrario, si el resultado del juicio formado en el paso S8 indica que el tiempo detectado ha excedido al periodo predeterminado, el flujo del proceso prosigue al paso S9. En el paso S9, la unidad 31 de gestión de clave genera o actualiza la clave de encriptación Kc utilizando la clave de fuente Ks y un número aleatorio regenerado, dando salida a la nueva clave de encriptación Kc hacia la unidad 32 de encriptación/desencriptación. Además, la unidad 31 de gestión de clave repone a 0 su propio temporizador.

A continuación, el flujo del proceso vuelve al paso S4. Las subsiguientes partes del proceso son repetidas hasta que el resultado del juicio formado en el paso S7 indica que se ha dado salida a todos los contenidos desde la unidad 25 de protección de contenido hacia la aplicación. Sin embargo, se ha de observar que la información que indica el estado de actualización de la clave de encriptación Kc está conmutado de “par” a “impar”, ya que la clave de encriptación Kc es actualizada en el paso S9. Como se ha descrito anteriormente, la información que indica el estado de actualización de la clave de encriptación Kc está incluida en la información de encriptación añadida en el paso S6. La clave de encriptación Kc suministrada desde la unidad 41 de gestión de clave hacia la unidad 32 de encriptación/desencriptación es también actualizada de acuerdo con la información que indica el estado de actualización de la clave de encriptación Kc.

Por el contrario, si el resultado del juicio formado en el paso S2 indica que no es válida la clave de autenticación Kn, el flujo del proceso continúa al paso S10. En el paso S10, la unidad 31 de gestión de clave informa a la unidad 41 de gestión de clave del hecho de que la autenticación termina con el estado de no-funciona.

La siguiente descripción explica el tratamiento para dar salida a un contenido tratado por una aplicación hacia el bus 2 de IEEE1394 haciendo referencia a un diagrama de flujo mostrado en la figura 6. Este tratamiento de salida es realizado después de que el contenido editado por la unidad 44 de tratamiento de contenido de la aplicación es suministrado a la unidad 43 de encriptación/desencriptación.

Como se muestra en la figura, el diagrama de flujo comienza con un paso S21 en el que la unidad 41 de gestión de clave efectúa una petición de una operación para dar salida a un contenido hacia el bus 2 de IEEE1394. La unidad 41 de gestión de clave da también salida a una clave de autenticación Kn almacenada, a información para calcular la clave secreta Ka y al valor de CCI fijado para el contenido de salida, hacia la unidad 31 de gestión de clave empleada en la unidad 25 de protección de contenido.

En el siguiente paso S22, la unidad 31 de gestión de clave forma un juicio en cuanto a si la clave de autenticación Kn recibida desde la unidad 41 de gestión de clave es válida o no válida. Si el resultado del juicio indica que la clave de autenticación Kn es válida, el flujo del proceso continúa hacia el paso S23.

En el paso S23, la unidad 31 de gestión de clave obtiene por lectura una clave de fuente Ks correspondiente al valor de CCI suministrado por la unidad 41 de gestión de clave desde la unidad 26 de almacenamiento de clave y a continuación genera una clave de encriptación Kc a partir de la clave de fuente Ks y un número al azar, dando salida a la clave de encriptación Kc hacia la unidad 32 de encriptación/desencriptación. En el paso S24 siguiente, la unidad 31 de gestión de clave genera una clave secreta Ka utilizando la información para calcular la clave secreta Ka procedente de la unidad 41 de gestión de clave. A continuación, la unidad 31 de gestión de clave encripta la clave de encriptación Kc generada en el paso S22 usando la clave secreta Ka y da salida a la clave de encriptación Kc encriptada hacia la unidad 41 de gestión de clave de la aplicación. La unidad 41 de gestión de clave desencripta clave de encriptación Kc encriptada y da salida a la clave de encriptación Kc desencriptada hacia la unidad 43 de encriptación/desencriptación.

En el paso siguiente S25, la unidad 43 de encriptación/desencriptación de la aplicación encripta un contenido desencriptado recibido de la unidad 44 de tratamiento de contenido utilizando la clave de encriptación Kc recibida de la unidad 41 de gestión de clave y da salida al contenido encriptado hacia la unidad 32 de encriptación/desencriptación por medio de la unidad 33 de adición de información encriptada.
En el siguiente paso S26, la unidad 32 de encriptación/desencriptación desencripta el contenido encriptado recibido de la unidad 43 de encriptación/desencriptación de la aplicación usando la clave de encriptación Kc recibida desde la unidad 31 de gestión de clave en el paso S23 y da salida al contenido desencriptado hacia la unidad 24 de encriptación/desencriptación de DTLA.

En el siguiente paso S27, la unidad 24 de encriptación/desencriptación de DTLA encripta el contenido desencriptado recibido de la unidad 32 de encriptación/desencriptación empleada en la unidad 25 de protección de contenido de acuerdo con el método de DTLA y da salida al contenido encriptado hacia la unidad 22 de entrada/salida.

En el siguiente paso S28, la unidad 22 de entrada/salida da salida al contenido que ha sido encriptado de acuerdo con el método de DTLA, y es recibido de la unidad 24 de encriptación/desencriptación de DTLA, hacia el bus 2 de IEEE1394.

Se ha de hacer observar que, si el resultado del juicio formado en el paso S22 indica que es válida la clave de autenticación Kn, el flujo del proceso sigue hacia el paso S29. En el paso S29, la unidad 31 de gestión de clave notifica a la unidad 41 de gestión de clave de la aplicación que la autenticación de la clave de autenticación Kn termina en el estado de no-funciona.

Además, en el tratamiento de salida, la clave de encriptación Kc puede ser también cambiada periódicamente como sucede con el tratamiento de entrada descrito anteriormente.

Como se ha descrito anteriormente, de acuerdo con la realización, la unidad 25 de protección de contenido de la interfaz 11 de IEEE1394 intercambia contenidos sólo con una aplicación que tiene una clave de autenticación Kn válida. Sin embargo, una aplicación capaz de copiar ilegalmente un contenido es concebiblemente capaz de adquirir una clave de autenticación Kn válida mediante la utilización de alguna técnica y, por tanto, utilizando ilegalmente un contenido. Con el fin de resolver este problema, en esta presente invención, la unidad 31 de gestión de clave de la unidad 25 de protección de contenido para formar un juicio sobre la validez de una clave de autenticación Kn almacena una lista de revocación de claves de autenticación Kn utilizadas ilegalmente. En el procesamiento para la autenticación de una clave de autenticación Kn, la unidad 31 de gestión de clave compara también la clave de autenticación con las puestas en la lista de revocación además de un juicio sobre la adaptación mutua de una ID y una firma que están incluidas en la clave de autenticación Kn. Una clave de autenticación Kn que concuerda con una de la lista de revocación no se determina que sea una clave válida incluso si la ID y la firma incluidas en la clave de autenticación Kn concuerdan entre sí.

Se ha de hacer observar que se concibe una técnica mediante la cual una clave de autenticación Kn recién añadida a la lista de revocación es recibida por la unidad 31 de gestión de clave a través de una red tal como la Internet o el bus 2 de IEEE1394. De acuerdo con una técnica concebible de utilización de la lista de revocación, se catalogan claves de autenticación individualmente en la lista. Se concibe también una técnica de utilizar la lista de revocación mediante la cual se catalogan una pluralidad de claves de autenticación Kn simultáneamente en la lista en una operación de tandas. En este caso, cada una de las claves de autenticación Kn tiene un valor predeterminado en el lado de MSB (Most Significant Bit: Bit más significativo) de la ID de la clave Kn. Catalogando una pluralidad de claves de autenticación Kn de este modo, es posible determinar que son válidas todas las aplicaciones hechas por un fabricante concreto de software. Un ejemplo de un tal fabricante de software es un productor de software que se ha visto que viola un contrato que esté hecho cuando se suministra una clave de autenticación Kn.

Además, la unidad 25 de protección de contenido es también capaz de detectar un acontecimiento de dar salida a un contenido hacia una aplicación y, si el número de tales acontecimientos es comunicado al propietario del copyright de contenido o al administrador del sistema a través de unos medios tales como la Internet, se puede exigir que el usuario pague una tasa por usar el contenido o el sistema de encriptación y puede ser reconocido el estado de utilización del sistema de encriptación.

Se ha de hacer observar que la presente invención puede ser también aplicada para paquetes isócronos y asíncronos de un contenido transmitido a través de un bus de IEEE139, así como paquetes de un contenido transmitido a través de otro medio.

El programa de ordenador ejecutado para realizar las partes de tratamiento descrito anteriormente puede ser presentado al usuario por medio de un medio de proporcionarlo, tal como un medio de grabación de información como un CD-ROM o a través de un medio de proporcionarlo en la forma de una red tal como la Internet o un satélite digital.

REIVINDICACIONES

1. Un aparato de tratamiento de información que comprende:

unos medios de recepción (31) para recibir una clave de autenticación Kn;
unos medios de generación (31) de clave de encriptación para generar una clave de encriptación Kc;
unos medios de encriptación (32) para encriptar un contenido utilizando dicha clave de encriptación Kc:
unos medios de generación (31) de cave secreta Ka para generar una clave secreta Ka;
unos medios de suministro (33) para suministrar dicha clave de encriptación Kc encriptada utilizando la citada clave secreta Ka generada por dichos medios de generación (31) de clave secreta y el citado contenido encriptado por dichos medios de encriptación (32), y unos medios (31) de formación de juicio,
en el que
dicho aparato (1) de tratamiento de información está adaptado para ejecutar un programa de aplicación capaz de editar el contenido con una información de derecho de autor de 2 bits añadida al mismo; y
dichos medios de recepción (31), dichos medios (31) de generación de clave de encriptación, dichos medios de encriptación (32), dichos medios (31) de generación de clave secreta, dichos medios de suministro (33) y dichos medios (31) de formación de juicio son parte de una interfaz (11) de IEEE1394 a la cual es suministrado el citado contenido con la información de derechos de autor de 2 bits añadida al mismo y desde la cual se hace pasar el contenido al citado programa de aplicación que tiene una clave de autenticación Kn y una clave secreta Ka; en el que
dichos medios (31) de generación de clave de encriptación están adaptados para generar la citada clave de encriptación Kc utilizando una clave de fuente Ks correspondiente a dicha información de derecho de autor de 2 bits añadida a un contenido de entrada y un número aleatorio, en el que por cada uno de los cuatro diferentes patrones de bits que pueden ser expresados por medio de la citada información de derechos de autor de 2 bits existe una clave de fuente (Ks);
los citados medios de formación de juicio (31) están adaptados para realizar un juicio sobre la validez del citado programa de aplicación usando ID y firma incluidas en la citada clave de autenticación Kn recibida desde dicho programa de aplicación por los citados medios de recepción (31);
dichos medios (31) de generación de clave secreta están adaptados para generar dicha clave secreta Ka usando la citada clave de autenticación Kn recibida de dicho programa de aplicación; y
dichos medios de suministro (33) están adaptados para suministrar la citada clave de encriptación Kc encriptada y dicho contenido encriptado al citado programa de aplicación con dependencia de un resultado de dicho juicio formado por los ciados medios (31) de formación de juicio.

2. Un aparato de tratamiento de información de acuerdo con la reivindicación 1, en el que
dichos medios de formación de juicio (31) están adaptados para realizar un juicio sobre la validez de la citada clave de autenticación Kn por referencia a una lista de revocación.

3. Un aparato de tratamiento de información de acuerdo con la reivindicación 1 o la 2, en el que
la citada información de derechos de autor incluye Información de Control de Copia de 2 bits que indica “Libre Copia”, “Posible Generador de Una Copia”, “No Más Copia” o “Nunca Copiar”.

4. Un aparato de tratamiento de información de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que
la citada clave de encriptación es actualizada a intervalos predeterminados.

5. Un método de tratamiento de información realizado en un aparto (1) de tratamiento de información, comprendiendo el citado método de tratamiento de información:

un paso de recepción para la recepción de una clave de autenticación Kn;
un paso (S3) de generación de cave de encriptación para generar una clave de encriptación Kc;
un paso (S4) de encriptación para encriptar el contenido usando dicha clave de encriptación Kc;
un paso (S24) de generación de clave secreta para generar una clave secreta (Ka); y
un paso de suministro (S28) para suministrar la citada clave de encriptación Kc encriptada usando la citada clave secreta Ka generada en el citado paso (S24) de generación de clave secreta y dicho contenido encriptado en el citado paso (S4) de medios de encriptación, y
un paso de formación de juicio,
en el que
dicho aparato (1) de tratamiento de información está adaptado para ejecutar un programa de aplicación capaz de editar el contenido con una información de derechos de autor de 2 bits añadida al mismo; y
dicho paso de recepción, dicho paso (S3) de generación de clave de encriptación, dicho paso (S4) de encriptación, dicho paso (S24) de generación de clave secreta , dicho paso (S28) de su ministro y dicho paso de formación de juicio son ejecutados en una interfaz (11) de IEEE1394 a la que es suministrado dicho contenido con la información de derechos de autor añadida al mismo y desde la cual el contenido es hecho pasar al citado programa de aplicación que tiene una clave de autenticación Kn y una clave secreta Ka; en el que

en el citado paso (S3) de generación de clave de encriptación, la citada clave de encriptación Kc es generada usando una clave de fuente Ks correspondiente a la citada información de derechos de autor de 2 bits añadida a un contenido de entrada y un número aleatorio, en el que para cada uno de los cuatro patrones de bits diferentes que pueden ser expresados por medio de la citada información de derechos de autor de 2 bits existe una clave de fuente Ks;

en dicho paso de formación de juicio se realiza un juicio sobre la validez del citado programa de aplicación utilizando ID y firma incluidas en la citada clave de autenticación Kn recibida de dicho programa de aplicación en el citado paso de recepción;

en dicho paso (S24) de generación de clave secreta Ka es generada la citada clave secreta utilizando dicha clave de autenticación Kn recibida del citado programa de aplicación; y

en dicho paso de suministro, la citada clave de encriptación Kc encriptada y dicho contenido encriptado son suministrados a dicho programa de aplicación con dependencia del resultado de dicho juicio formado en el citado paso de formación de juicio.

6. Un método de tratamiento de información de acuerdo con la reivindicación 5, en el que la citada clave de encriptación Kc es actualizada a intervalos predeterminados.

7. Un medio de proporcionar que tiene gravado en el mismo un programa para ser leído por un ordenador para activar un aparato (1) de tratamiento de información para realizar el método de tratamiento de información de acuerdo con las reivindicaciones 5 ó 6.

FIG.1

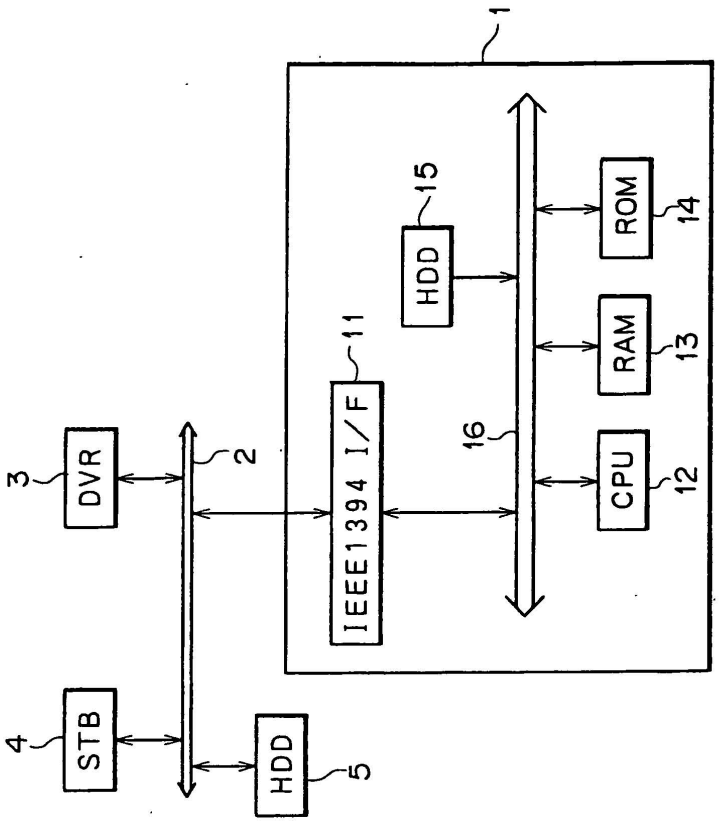


FIG.2

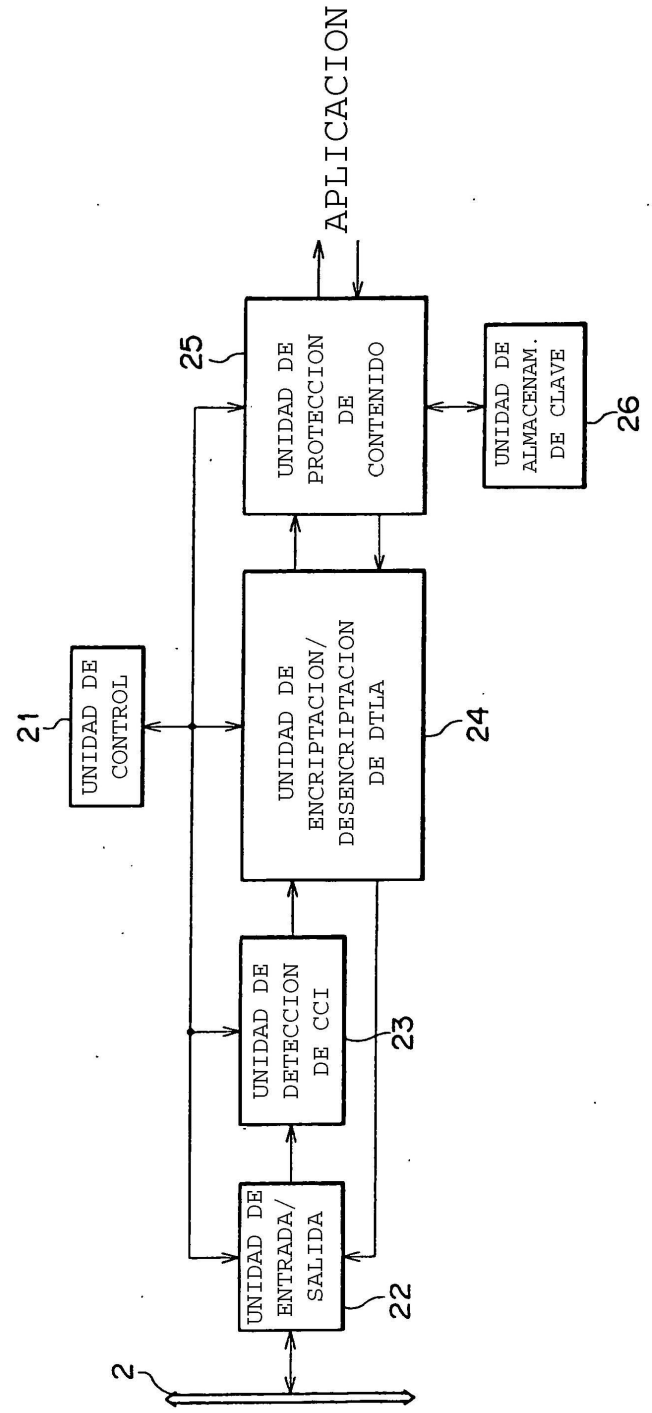

APLICACION
25
UNIDAD DE PROTECCION DE CONTENIDO
UNIDAD DE ALMACENAM. DE CLAVE
26
UNIDAD DE ENCRIPTACION/ DESENCRIPTACION DE DTLA
24
21
UNIDAD DE CONTROL
UNIDAD DE DETECCION DE CCI
23
UNIDAD DE ENTRADA/ SALIDA
22
2
11

FIG.3

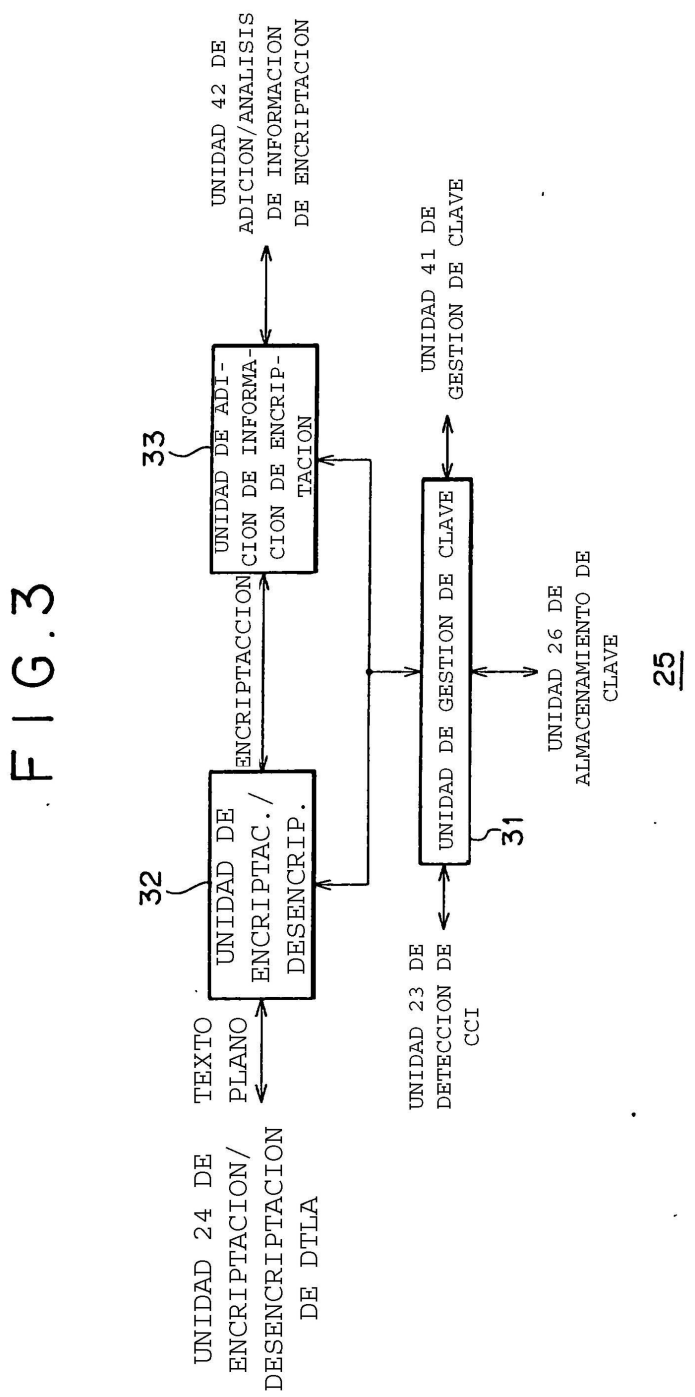

UNIDAD 24 DE ENCRIPTACION/ DESENCRIPTACION DE DTLA
TEXTO PLANO
32
UNIDAD DE ENCRIPTAC./ DESENCRIP.
ENCRIPTACCION
33
UNIDAD DE ADICION DE INFORMACION DE ENCRIPTACION
UNIDAD 42 DE ADICION/ANALISIS DE INFORMACION DE ENCRIPTACION
UNIDAD 23 DE DETECCION DE CCI
UNIDAD DE GESTION DE CLAVE
31
UNIDAD 41 DE GESTION DE CLAVE
UNIDAD 26 DE ALMACENAMIENTO DE CLAVE
25

FIG.4

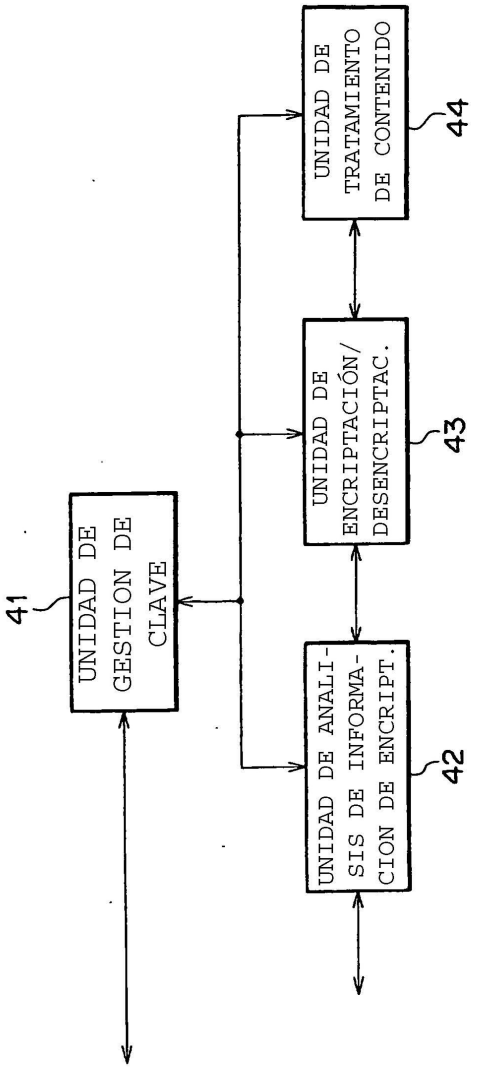

UNIDAD DE GESTION DE CLAVE
41
UNIDAD DE ANALI-SIS DE INFORMA-CION DE ENCRIPT.
42
UNIDAD DE ENCRIPTACIÓN/ DESENCRIPTAC.
43
UNIDAD DE TRATAMIENTO DE CONTENIDO
44

FIG.5

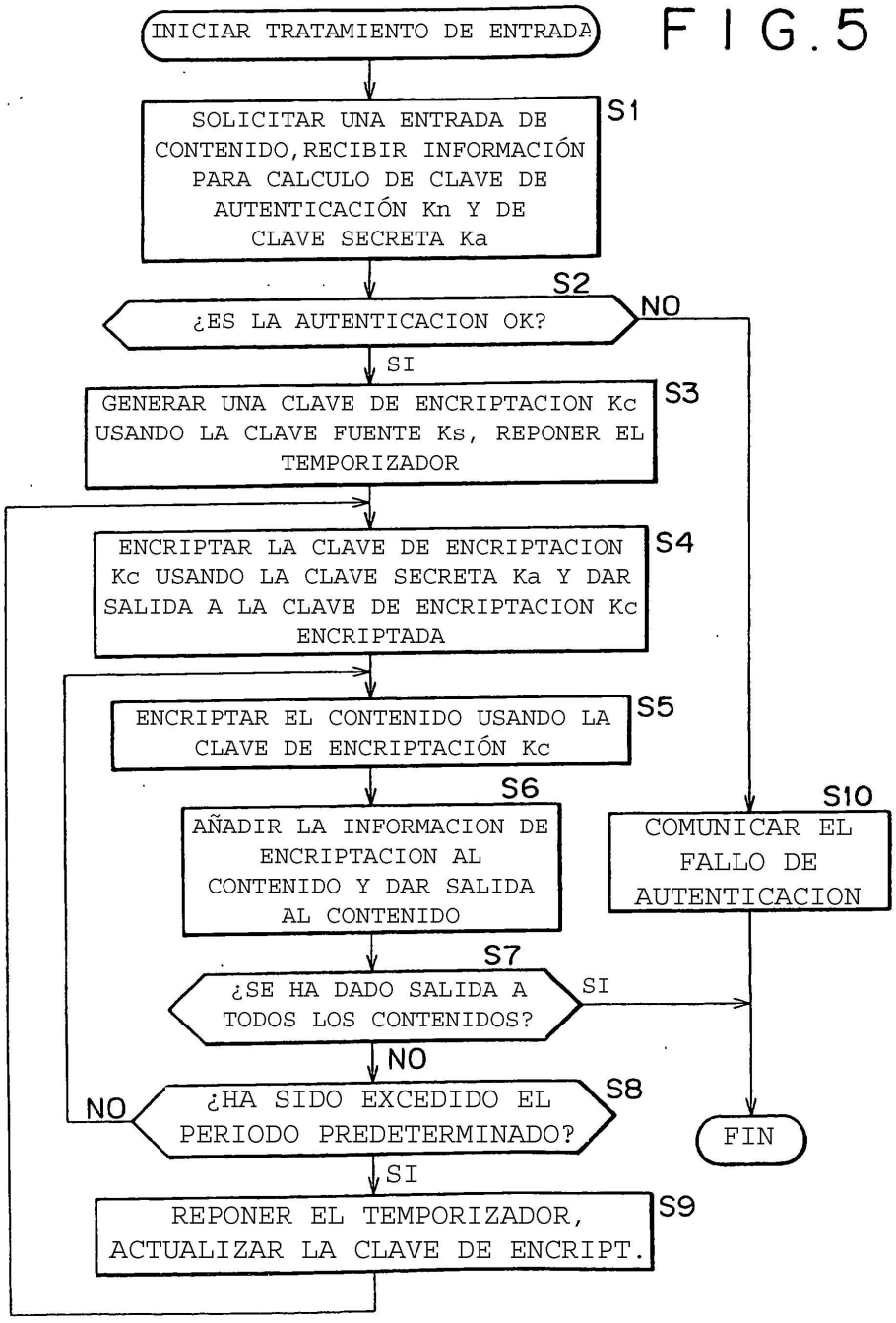
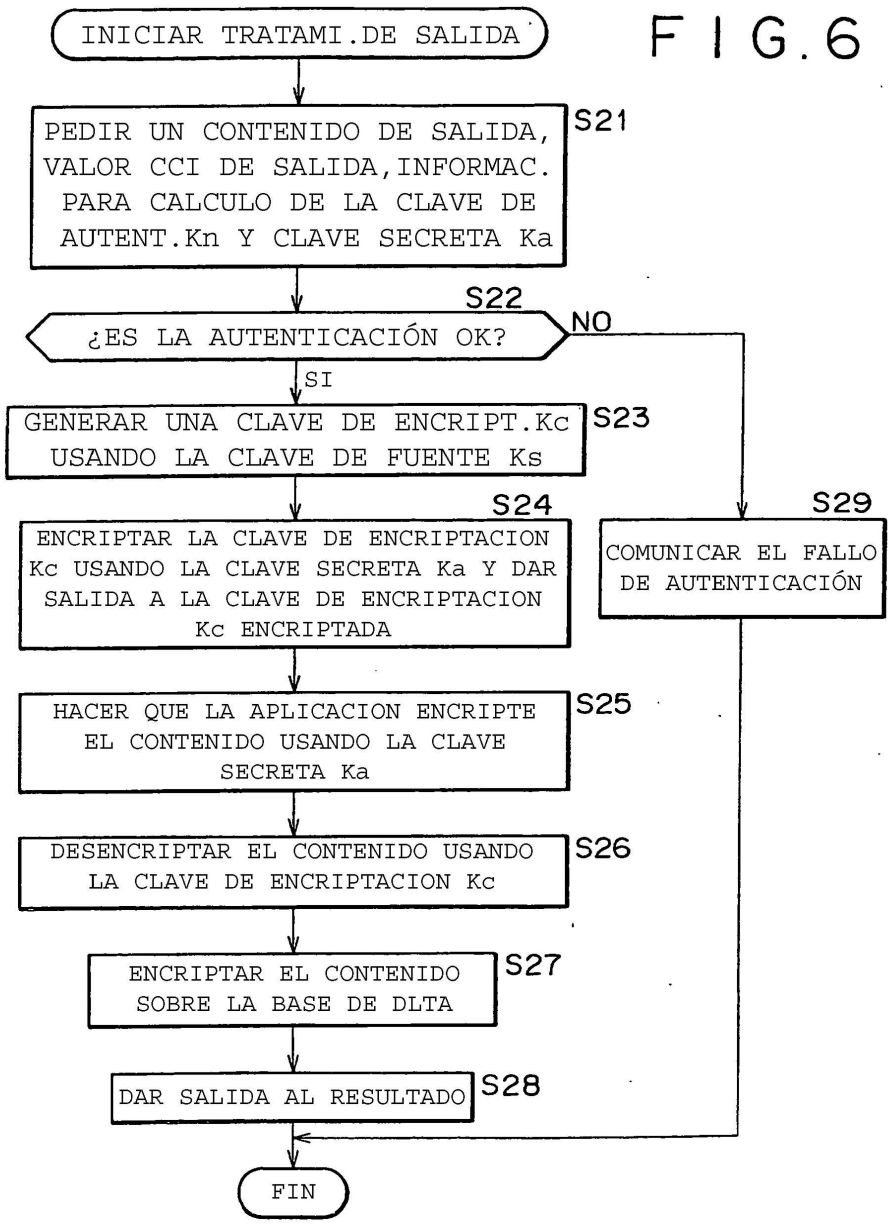

INICIAR TRATAMIENTO DE ENTRADA
SOLICITAR UNA ENTRADA DE CONTENIDO, RECIBIR INFORMACIÓN PARA CALCULO DE CLAVE DE AUTENTICACIÓN Kn Y DE CLAVE SECRETA Ka
S1
¿ES LA AUTENTICACION OK?
S2
NO
SI
GENERAR UNA CLAVE DE ENCRIPTACION Kc USANDO LA CLAVE FUENTE Ks, REPONER EL TEMPORIZADOR
S3
ENCRIPTAR LA CLAVE DE ENCRIPTACION Kc USANDO LA CLAVE SECRETA Ka Y DAR SALIDA A LA CLAVE DE ENCRIPTACION Kc ENCRIPTADA
S4
ENCRIPTAR EL CONTENIDO USANDO LA CLAVE DE ENCRIPTACIÓN Kc
S5
AÑADIR LA INFORMACION DE ENCRIPTACION AL CONTENIDO Y DAR SALIDA AL CONTENIDO
S6
COMUNICAR EL FALLO DE AUTENTICACION
S10
¿SE HA DADO SALIDA A TODOS LOS CONTENIDOS?
S7
SI
NO
¿HA SIDO EXCEDIDO EL PERIODO PREDETERMINADO?
S8
NO
SI
REPONER EL TEMPORIZADOR, ACTUALIZAR LA CLAVE DE ENCRIPT.
S9
FIN

FIG.6


INICIAR TRATAMI.DE SALIDA
PEDIR UN CONTENIDO DE SALIDA, VALOR CCI DE SALIDA, INFORMAC. PARA CALCULO DE LA CLAVE DE AUTENT.Kn Y CLAVE SECRETA Ka
S21
S22
¿ES LA AUTENTICACIÓN OK?
NO
SI
GENERAR UNA CLAVE DE ENCRIPT.Kc USANDO LA CLAVE DE FUENTE Ks
S23
S24
ENCRIPTAR LA CLAVE DE ENCRIPTACION Kc USANDO LA CLAVE SECRETA Ka Y DAR SALIDA A LA CLAVE DE ENCRIPTACION Kc ENCRIPTADA
S29
COMUNICAR EL FALLO DE AUTENTICACIÓN
HACER QUE LA APLICACION ENCRIPTE EL CONTENIDO USANDO LA CLAVE SECRETA Ka
S25
DESENCRIPTAR EL CONTENIDO USANDO LA CLAVE DE ENCRIPTACION Kc
S26
ENCRIPTAR EL CONTENIDO SOBRE LA BASE DE DLTA
S27
DAR SALIDA AL RESULTADO
S28
FIN