(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 817**

(51) Int. CI.:

G06F 21/30 (2013.01)
G06F 21/60 (2013.01)
G06F 21/57 (2013.01)
G06F 21/72 (2013.01)
G06F 21/74 (2013.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.02.2013 E 18154262 (2)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 3349134**

(54) Título: **Procedimiento y aparato de protección decontenido digital utilizando autenticación del dispositivo**

(30) Prioridad:

16.02.2012 KR 20120016084

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.04.2020

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu, Suwon-si
Gyeonggi-do 16677, KR

(72) Inventor/es:

CHANG, MOON-SOO;
PARK, SEUL-HAN y
LEE, YANG-SOO

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y aparato de protección decontenido digital utilizando autenticación del dispositivo

Campo técnico

La presente invención se refiere a un aparato de tratamiento de datos. Más particularmente, la presente invención se refiere a un aparato de tratamiento de datos que puede mejorar la seguridad mediante el uso de un sistema operativo seguro separado de un Sistema Operativo (SO) principal y un procedimiento del mismo

Antecedentes de la técnica

Recientemente, puesto que a los aparatos digitales se le solicita procesar un servicio de alta calidad, diversos contenidos digitales se ha proporcionado a los dispositivos de usuario, como televisores, ordenadores y dispositivos portátiles. El contenido digital puede incluir archivos de vídeo, archivos de audio, diversas aplicaciones y similares. Puesto que el contenido digital se proporciona activamente, se han propuesto diversos procedimientos para proteger los derechos de propiedad intelectual de los contenidos digitales.

Un servicio de Gestión De Derechos Digitales (DRM) es un procedimiento para proteger el contenido digital. El servicio DRM gestiona y protege continuamente los derechos de propiedad intelectual del contenido digital utilizando tecnología de cifrado. El servicio DRM es una tecnología para transmitir de forma segura diversos contenidos de un Proveedor De Contenido (CP) a un usuario y proteger el contenido de su distribución ilegítima por parte del usuario que lo ha recibido. La tecnología DRM permite la protección de la información durante los procedimientos de generación, distribución, uso y descarte de contenido digital, y permite que el contenido digital se use de acuerdo con la autorización del usuario, no solo en línea sino también fuera de línea, al tiempo que brinda protección de derechos.

Para usar un contenido al que se aplica la tecnología DRM (contenido de DRM) en un dispositivo de usuario, el dispositivo de usuario debe conectarse primero a un sistema que proporcione un contenido de DRM correspondiente y descargar después el contenido de DRM, metadatos en el contenido de DRM y una licencia. Los metadatos se refieren a datos en los que se almacena información sobre el contenido de DRM, y la licencia se refiere a los datos que indican una clave de cifrado que se utilizará para descifrar un contenido de DRM cifrado y una autorización para acceder al contenido (por ejemplo, la cantidad de veces y el periodo). De acuerdo con los procedimientos, el contenido de DRM y la licencia se almacenan en el dispositivo de usuario, y el contenido de DRM puede consumirse.

Mientras tanto, el dispositivo de usuario emplea una Unidad de Procesamiento Central (CPU) y un Sistema Operativo (SO). El aparato móvil emplea un sistema operativo abierto para realizar una interfaz de programa de aplicación abierta. El sistema operativo abierto juega un papel clave en la mejora de la competitividad en un aparato móvil y un servicio móvil. Además, el sistema operativo de un aparato móvil está estratégicamente abierto por los principales fabricantes y proveedores importantes, por lo que las interfaces de los programas de aplicación, los kits de desarrollo de software y también los archivos de origen están abiertos al público.

El documento US2008256635 desvela un procedimiento y un sistema para detectar malware utilizando un modo de sistema operativo seguro. De acuerdo con una realización particular de la presente divulgación, se recibe un archivo. El archivo se almacena en un directorio seguro. Se evita al menos una operación en el archivo. Se inicia un modo de sistema operativo seguro para detectar si el archivo contiene malware,

El documento WO 2008/116346 se refiere a medios, procedimientos, aparatos y sistemas legibles por máquina para mejorar el marco de gestión de derechos digitales. Una plataforma del servidor puede recibir una solicitud de descarga de contenido e información de primera certificación de una plataforma de cliente. La plataforma del servidor puede examinar si la plataforma del cliente da fe de una característica de la plataforma del cliente que afecta la integridad de la plataforma del cliente mediante el uso de la información de certificación, y cifra y descarga después el contenido a la plataforma del cliente si la plataforma del cliente da fe de la característica de la plataforma del cliente. La plataforma del servidor puede recibir una solicitud de visualización del contenido y la segunda información de certificación de la plataforma del cliente. La plataforma del servidor puede entonces examinar si la plataforma del cliente da fe de su integridad utilizando la segunda información de certificación; y enviar después una clave de contenido a la plataforma del cliente si la plataforma del cliente da fe de su integridad, de modo que la plataforma del cliente pueda descifrar y ver el contenido.

Divulgación de la invención

Problema técnico

Como se ha descrito anteriormente, aunque se utiliza la tecnología DRM, la distribución del contenido digital incluye aún algunas vulnerabilidades de seguridad. Por ejemplo, otro dispositivo de usuario puede interceptar una licencia asignada a un dispositivo de usuario específico o extraer y obtener una licencia o un contenido de DRM descifrado que se almacena en el dispositivo de usuario específico pirateando un sistema operativo del dispositivo de usuario.

Además, el dispositivo de usuario descarga una pluralidad de aplicaciones de Internet, y dichas aplicaciones deben

usarse después de inspeccionar y garantizar la calidad de las aplicaciones por un fabricante de un aparato móvil. En la práctica, sin embargo, no se inspeccionan todas las funciones de las diversas aplicaciones. En consecuencia, los códigos maliciosos dirigidos a los dispositivos móviles están aumentando, y los dispositivos móviles que utilizan un sistema operativo abierto pueden ser atacados por un software que contiene los códigos maliciosos.

Aunque el contenido digital se admite de forma cifrada, si el dispositivo de usuario en sí es vulnerable en seguridad, está limitado para evitar el uso y distribución ilegítimos del contenido digital.

La información anterior se presenta como información de antecedentes solo para ayudar con la comprensión de la presente divulgación. No se ha hecho ninguna determinación, y no se hace ninguna afirmación, en cuanto a si algo de lo anterior podría aplicarse como técnica anterior con respecto a la presente invención.

Solución al problema

Los aspectos de la presente invención tienen por objeto abordar al menos los problemas y/o desventajas anteriormente mencionados y proporcionar al menos las ventajas descritas posteriormente.

Por consiguiente, un aspecto de la presente invención es proporcionar un procedimiento y un aparato para proteger un contenido digital con seguridad reforzada.

Otro aspecto de la presente invención es proporcionar un procedimiento y un aparato para proteger un contenido digital fortaleciendo la función de seguridad de un dispositivo de usuario que consume el contenido digital.

Otro aspecto de la presente invención es proporcionar un procedimiento y un aparato para proteger un contenido digital fortaleciendo el procedimiento de autenticación de la función de seguridad de un dispositivo de usuario.

De acuerdo con un aspecto de la presente invención, un procedimiento para proteger el contenido digital mediante un dispositivo de usuario que incluye un sistema operativo principal y un sistema operativo seguro separado ejecuta contenido digital seguro. El procedimiento incluye solicitar una ejecución del sistema operativo seguro, basándose en que el sistema operativo principal detecta una entrada de la solicitud de ejecución relacionada con el contenido digital seguro; identificar información de pirateo que indica si el sistema operativo principal es pirateado por el sistema operativo seguro; y determinar una operación en el modo seguro basándose en la identificación de la información de pirateo, por el sistema operativo seguro.

De acuerdo con otro aspecto de la presente invención, un procedimiento para proteger el contenido digital mediante un dispositivo de usuario que incluye un sistema operativo principal y un sistema operativo seguro separado ejecuta contenido digital seguro. El procedimiento incluye solicitar una ejecución del sistema operativo seguro basándose en la detección de una entrada de la solicitud de ejecución relacionada con el contenido digital seguro; recopilar información de autenticación del dispositivo que indica un nivel de seguridad del dispositivo, por el sistema operativo seguro; cifrar la información de autenticación del dispositivo y transmitir la información de autenticación del dispositivo cifrado al sistema operativo principal, mediante el sistema operativo seguro; transmitir la información de autenticación del dispositivo a un servidor que proporciona el contenido seguro, por el sistema operativo principal; recibir un resultado de autenticación con respecto al nivel de seguridad del dispositivo determinado en función de la información de autenticación del dispositivo por el servidor, por el sistema operativo principal; y determinar una operación en el modo seguro, basándose en el resultado de autenticación, por el sistema operativo seguro.

La invención se define en las reivindicaciones independientes 1 y 3.

Efectos ventajosos de la invención

La presente invención puede proporcionar un procedimiento y un aparato para proteger el contenido digital fortaleciendo la función de seguridad del dispositivo de un dispositivo de usuario que consume el contenido digital. Además, las realizaciones ejemplares de la presente invención pueden proporcionar un procedimiento y un aparato para proteger un contenido digital con un procedimiento reforzado para autenticar la función de seguridad del dispositivo de usuario.

Breve descripción de los dibujos

la Figura 1 es un diagrama que ilustra una configuración de un sistema de servicios de contenido digital de acuerdo con una realización ejemplar de la presente invención;
la Figura 2 es un diagrama de bloques que ilustra una configuración de un terminal portátil de acuerdo con una realización ejemplar de la presente invención;
la Figura 3 es un diagrama de bloques que ilustra una configuración de un terminal portátil de acuerdo con una realización ejemplar de la presente invención;
la Figura 4 es un diagrama que ilustra un procedimiento de arranque de un dispositivo de usuario de acuerdo con una realización ejemplar de la presente invención;
las Figuras 5 y 6 son diagramas que ilustran procedimientos de autenticación de seguridad de dispositivos de usuario de acuerdo con realizaciones ejemplares de la presente invención; y

la Figura 7 es un diagrama que ilustra un procedimiento de operación de un servidor de servicios de contenido digital de acuerdo con una realización ejemplar de la presente invención.

A lo largo de los dibujos, debe tenerse en cuenta que se usan números de referencia similares para representar elementos, características y estructuras iguales o similares.

Modo para la invención

La siguiente descripción con referencia a los dibujos adjuntos se proporciona para ayudar a una comprensión detallada de diversas realizaciones ejemplares de la invención tal como es definida por las reivindicaciones y sus equivalentes. La misma incluye diversos detalles específicos para ayudar en esa comprensión, pero estos deben considerarse simplemente a modo de ejemplo.

Los expertos en la técnica reconocerán que diversos cambios y modificaciones de las realizaciones descritas en el presente documento pueden realizarse sin apartarse del ámbito de la invención. Además, por razones de claridad y concisión se pueden omitir las descripciones de funciones y construcciones bien conocidas.

Las expresiones y términos usados en la siguiente descripción y reivindicaciones no se limitan a los significados bibliográficos, sino que son usados meramente por el inventor de la presente invención para habilitar una comprensión clara y consistente de la presente invención. Por consiguiente, debería ser evidente para los expertos en la materia que la siguiente descripción de realizaciones ejemplares de la presente invención se proporciona únicamente con fines ilustrativos y no para limitar la invención tal como se define en las reivindicaciones adjuntas y sus equivalentes, y "el/la" incluye referentes plurales a menos que el contexto indique claramente lo contrario. Por lo tanto, por ejemplo, la referencia a "una superficie componente" incluye la referencia a una o más de tales superficies.

Recientemente, los aparatos digitales pueden proporcionar un servicio de alta calidad, por lo que se ha proporcionado diversos contenidos digitales a un dispositivo de usuario, como un televisor, un ordenador y un dispositivo portátil. El contenido digital puede incluir archivos de vídeo, archivos de audio, imágenes, animaciones, texto y varias aplicaciones. A medida que se desarrolla el contenido digital, se han sugerido diversos procedimientos para proteger los derechos sobre las propiedades intelectuales de los contenidos digitales.

Entre ellos, un servicio de Gestión De Derechos Digitales (DRM) es un procedimiento de seguridad en el que el proveedor de contenido proporciona contenido digital cifrado con un dispositivo de usuario y el dispositivo de usuario obtiene una clave de cifrado utilizada para descifrar el contenido digital cifrado y una licencia que indica privilegios (para ejemplo, el número de veces y el período de tiempo) para acceder al contenido de modo que el dispositivo de usuario pueda consumir los contenidos digitales correspondientes. El consumo del contenido digital es realizar una operación sustancial por parte de un dispositivo de usuario utilizando contenido digital, por ejemplo, reproducción de contenido de vídeo, reproducción de contenido de audio y ejecución de aplicaciones específicas.

Sin embargo, en el caso de los procedimientos de seguridad, al piratear un sistema operativo del dispositivo de usuario, otro dispositivo de usuario puede interceptar una licencia asignada a un dispositivo de usuario específico, o extraer y obtener una licencia o un contenido digital descifrado almacenado en un dispositivo de usuario específico. Aunque el contenido digital se proporciona de manera cifrada, si el dispositivo de usuario tiene una vulnerabilidad de seguridad, la prevención del contenido digital del uso o distribución no autorizados es limitada.

Por consiguiente, las realizaciones ejemplares de la presente invención proporcionan un procedimiento de protección de contenido reforzado al aumentar el nivel de seguridad del entorno de ejecución en sí mismo dentro del dispositivo de usuario. Para asegurar la estabilidad de un sistema embebido que usa un procesador, las realizaciones ejemplares de la presente invención proporcionan una tecnología de seguridad a nivel de chip sujeta al procesador, dispositivos periféricos y dispositivos de almacenamiento.

Para lograr estos objetos, un dispositivo de usuario de acuerdo con realizaciones ejemplares de la presente invención proporciona dos entornos de ejecución separados que incluyen un entorno de ejecución normal y un entorno de ejecución de seguridad en un procesador. Tal abstracción separa lógicamente el rendimiento de los programas normales y el rendimiento de los programas importantes directamente conectados a la seguridad de un dispositivo estrictamente. El dispositivo de usuario aplica dicha división lógica no solo a un procesador sino también a dispositivos periféricos y a los dispositivos de almacenamiento. La división lógica del entorno de ejecución mediante la abstracción puede desempeñar un papel en la protección del rendimiento de un programa directamente conectado a la seguridad o al recurso del sistema de la amenaza de usuarios o programas maliciosos.

De acuerdo con las realizaciones ejemplares de la presente invención, el dispositivo de usuario incluye un primer Sistema Operativo (SO) (en adelante denominado SO principal) que admite un modo normal y un segundo sistema operativo (en adelante denominado SO seguro) que admite un modo seguro, ejecuta un programa seguro relacionado con la seguridad utilizando un procesador en un área segura administrada por un sistema operativo seguro, y ejecuta un programa normal en un área normal administrada por un sistema operativo principal. Además, el acceso al área segura a través del sistema operativo principal está bloqueado. La división entre el área normal y el área segura no es una división física, sino una división lógica. El área normal indica la operación de las configuraciones de software y hardware administradas en el entorno del sistema operativo principal. El área segura indica la operación de las

configuraciones de software y hardware administradas en el entorno de SO seguro. En consecuencia, algunas de las configuraciones de hardware pueden compartirse entre las áreas normales y seguras.

Por ejemplo, si se solicita el uso de un contenido de vídeo seguro que solicite seguridad, el descifrado, la decodificación y el procesamiento con respecto al archivo de vídeo correspondiente en el área segura en un modo seguro se realiza para su reproducción y salida. Los datos producidos en cada etapa se almacenan en el área segura. Además, no se permite el acceso directo a los datos almacenados en el área segura a través de la aplicación en el modo normal o el sistema operativo principal.

Además, si se solicita el consumo de contenido de vídeo normal que no requiere seguridad, se descifra, decodifica y representa con respecto al archivo de vídeo correspondiente en el área normal en un modo normal para su reproducción y salida. Los datos producidos en cada etapa se almacenan en el área normal.

Cada uno de los contenidos de vídeo normales y el contenido de vídeo seguro se reproducen en diferentes modos de operación y áreas de operación. Sin embargo, el dispositivo de salida que finalmente emite el contenido de vídeo normal y el contenido de vídeo seguro se comparte.

De esta manera, de acuerdo con las realizaciones ejemplares de la presente invención, el dispositivo de usuario puede fortalecer el nivel de protección del contenido digital dividiendo los modos normal y de seguridad y realizando correctamente una operación. Además, para fortalecer aún más el nivel de protección del contenido digital, el dispositivo de usuario puede determinar si el sistema operativo principal está pirateado o no, y bloquear la operación en el modo seguro. De lo contrario, la información de autorización del dispositivo que indica el nivel de seguridad del dispositivo de usuario está autorizada por el servidor del servicio de contenido, y el dispositivo de usuario bloquea la operación en el modo seguro de acuerdo con el resultado.

La Figura 1 es un diagrama que ilustra una configuración de un sistema de servicios de contenido digital de acuerdo con una realización ejemplar de la presente invención.

Con referencia a la Figura 1, el sistema de servicios de contenido digital incluye un dispositivo 100 de usuario y un servidor 10 de servicios de contenido.

El servidor 10 de servicios de contenido es un dispositivo para proporcionar diversos contenidos digitales a dispositivos de usuario inscritos en un servicio de contenido digital y gestionar la información sobre los usuarios inscritos en el servicio y la información de los dispositivos de usuario correspondientes. El servidor 10 de servicios de contenido puede autenticar la información de autenticación del dispositivo recibida desde el dispositivo 100 de usuario, y transmite el resultado al dispositivo 100 de usuario. La información de autenticación del dispositivo incluye la información capaz de evaluar el nivel de seguridad del dispositivo 100 de usuario.

El servidor 10 de servicios de contenido incluye un procesador 11 de control, una unidad 13 de comunicación y una unidad 15 de almacenamiento.

El procesador 11 de control controla las operaciones generales del servidor 10 de servicios de contenido, y controla especialmente la operación del servidor 10 de servicios de contenido en respuesta a la solicitud de autenticación del dispositivo de usuario. La unidad 13 de comunicación realiza la comunicación con el dispositivo de usuario de acuerdo con el control del procesador 11 de control.

La unidad 15 de almacenamiento almacena diversos contenidos digitales proporcionados por un proveedor de contenido, información de usuarios inscritos en un servicio e información sobre los dispositivos de usuario correspondientes. Además, al usar la información de autenticación del dispositivo recibida del dispositivo de usuario, se almacena la información de política que se convierte en un estándar para evaluar la idoneidad del nivel de seguridad del dispositivo de los dispositivos de usuario correspondientes.

El dispositivo 100 de usuario es un dispositivo que consume contenido digital solicitando, recibiendo y reproduciendo los contenidos digitales. Un ejemplo del dispositivo 100 de usuario puede ser un televisor, un terminal móvil, un teléfono inteligente, un teléfono celular, un Reproductor Multimedia Personal (PMP) y un reproductor de archivos de audio.

La Figura 2 es un diagrama que ilustra una configuración de un dispositivo de usuario, en el que el dispositivo de usuario es un aparato móvil tal como un teléfono inteligente de acuerdo con una realización ejemplar de la presente invención.

Con referencia a la Figura 2, el dispositivo 100 de usuario puede estar conectado a un aparato externo (no ilustrado) a través de un módulo 120 de comunicaciones móviles, un módulo 130 de subcomunicación y un conector 165. El "aparato externo" es otro aparato (no ilustrado), como un teléfono celular (un teléfono inteligente, una tableta de Ordenador Personal (PC) o un servidor).

El dispositivo 100 de usuario incluye una pantalla 190 táctil y un controlador 195 de pantalla táctil. Además, el dispositivo 100 de usuario incluye un controlador 110, un módulo 120 de comunicaciones móviles, un módulo 130 de subcomunicación, un módulo 140 multimedia, un módulo 150 de cámara, un módulo 155 del Sistema de

posicionamiento global (GPS), un módulo 160 de entrada/de salida, un módulo 170 de sensor, una unidad 175 de almacenamiento y una unidad 180 de fuente de alimentación. El módulo 130 de subcomunicación incluye al menos uno de un módulo 131 de red de área local (LAN) inalámbrica y un módulo 132 de comunicaciones de corto alcance. El módulo 140 multimedia incluye al menos uno de un módulo 141 de comunicación de radiodifusión, un módulo 142 de reproducción de audio y un módulo 143 de reproducción de vídeo. El módulo 150 de cámara incluye al menos una de una primera cámara 151 y una segunda cámara 152. El módulo 160 de entrada/salida incluye un botón 161, un micrófono 162, un altavoz 163, un motor 164 de vibración, el conector 165 y un teclado 166 opcional.

El controlador 110 incluye una memoria 112 de solo lectura (ROM) que almacena un programa de control para controlar una unidad 111 central de procesamiento (CPU) y el dispositivo 100 de usuario, una memoria 113 de acceso aleatorio (RAM) que almacena una señal o entrada de datos desde el exterior del dispositivo 100 de usuario o que se utiliza como área de almacenamiento para una operación realizada en el dispositivo 100 de usuario, y un cargador 114 de arranque que realiza el arranque cuando el dispositivo 100 de usuario está encendido. La CPU 111 puede incluir un procesador de un solo núcleo, un procesador de doble núcleo, un procesador de triple núcleo, un procesador de cuatro núcleos o similares. La CPU 111, la ROM 112 y la RAM 113 pueden conectarse entre sí a través de buses internos.

El controlador 110 puede controlar el módulo 120 de comunicaciones móviles, el módulo 130 de subcomunicación, el módulo 140 multimedia, el módulo 150 de cámara, el módulo 155 de GPS, el módulo 160 de entrada/salida, el módulo 170 de sensor, la unidad 175 de almacenamiento, la unidad 180 de fuente de alimentación, una primera pantalla 190a táctil, una segunda pantalla 190b táctil y el controlador 195 de pantalla táctil.

El controlador 110 usa una CPU 111 para mantener entornos de múltiples sistemas operativos correspondientes a cada uno de los principales sistemas operativos y al sistema operativo seguro, y realiza una operación en dos modos separados del modo normal y el modo seguro respectivamente correspondientes al sistema operativo principal y al sistema operativo seguro, si necesario. El modo seguro indica un modo que realiza una ejecución de seguridad que solicita seguridad en un área segura, y el modo normal indica un modo que realiza una ejecución sin seguridad que no solicita seguridad en un área normal. De acuerdo con las realizaciones ejemplares de la presente invención, el controlador 110 incluye una unidad 200 principal que realiza la ejecución sin seguridad (ejecución normal) en el entorno del sistema operativo principal y una unidad 300 de seguridad que realiza la ejecución de seguridad en el entorno del sistema operativo seguro. El controlador 110 realiza una operación por la unidad 200 principal y la unidad 300 de seguridad separando el modo normal y el modo seguro. El sistema operativo principal se ejecuta en la unidad 200 principal, y el sistema operativo seguro se ejecuta de manera separada en la unidad 300 de seguridad. Además, el acceso del sistema operativo principal al área de memoria utilizada por el sistema operativo seguro está bloqueado. En consecuencia, incluso cuando el SO principal es un SO abierto, es posible que el código malicioso no acceda al SO seguro ni al área de memoria utilizada por el SO seguro.

En consecuencia, la unidad 200 principal y la unidad 300 de seguridad incluyen una pluralidad de módulos de funciones que se solicitan para realizar la ejecución normal y la ejecución de seguridad, respectivamente. Ejemplos de las configuraciones de la unidad 200 principal y la unidad 300 de seguridad se ilustran en la Figura 3.

El controlador 110 ejecuta un programa normal, una aplicación normal o contenido digital que no solicita seguridad en un modo normal, y ejecuta un programa que solicita seguridad, una aplicación que solicita seguridad o contenido seguro que solicita seguridad en un modo seguro. De acuerdo con una realización ejemplar de la presente invención, el contenido digital que solicita seguridad (es decir, el contenido seguro) puede ser contenido protegido por un sistema de protección de contenido, como DRM. Además, todo el contenido que solicita seguridad puede dividirse en contenido que solicita alta seguridad y contenido que solicita seguridad relativamente baja. El contenido que solicita alta seguridad es procesado por la unidad 300 de seguridad, y el contenido que solicita una seguridad relativamente baja se procesa en la unidad 200 principal. Por ejemplo, el controlador 110 puede descifrar, decodificar y reproducir secuencias de audio y/o vídeo correspondientes a contenidos seguros en el modo seguro.

Específicamente, cuando se recibe una solicitud para ejecutar un contenido digital específico de acuerdo con la solicitud del usuario, el controlador 110 confirma si el contenido digital específico es un contenido seguro o un contenido normal. Si el contenido digital específico es un contenido seguro, el controlador 110 cambia a un modo seguro y procesa un contenido específico en el área segura. Por ejemplo, si el contenido digital específico es un contenido de vídeo al que se aplica DRM, el controlador 110 descifra, decodifica, representa el flujo de audio y/o vídeo del contenido de vídeo en el modo seguro, y almacena el resultado del procedimiento en el área de almacenamiento segura a la que se limita el acceso. Además, el controlador 110 controla de modo que los datos de audio y/o vídeo almacenados en el área de almacenamiento segura en el modo seguro se envían a través del módulo 140 multimedia. De esta manera, el controlador 110 controla para que el contenido seguro se procese utilizando un área 179 de almacenamiento segura a la que el acceso está limitado en el modo seguro, por lo que es difícil piratear el contenido seguro.

En el controlador 110, la unidad 200 principal y la unidad 300 de seguridad están incluidas en la CPU 111. La configuración de la CPU 111 se ilustra en la Figura 3.

La Figura 3 es un diagrama de bloques que ilustra una configuración de un terminal portátil de acuerdo con una

realización ejemplar de la presente invención.

Con referencia a la Figura 3, la CPU 111 incluye la unidad 200 principal que realiza la ejecución normal, la unidad 300 de seguridad que realiza la ejecución de seguridad y una unidad 270 de comunicación de seguridad que realiza una comunicación entre la unidad 200 principal y la unidad 300 de seguridad. La unidad 200 principal utiliza un sistema operativo principal y realiza, en un modo normal, la ejecución de un programa normal, una aplicación normal o un contenido normal que no requiere seguridad. Si se necesita la ejecución de un programa seguro, una aplicación segura o un contenido seguro que solicite seguridad, la ejecución se instruye o solicita a la unidad 300 de seguridad a través de la unidad 270 de comunicación de seguridad.

Un sistema 210 operativo principal se ejecuta en la unidad 200 principal, y un sistema 310 operativo seguro se ejecuta de manera separada en la unidad 300 de seguridad. Además, el sistema 210 operativo principal puede no acceder directamente a la unidad 300 de seguridad, y puede indicar o solicitar la ejecución de una función, un hilo y un procedimiento específicos a través de la unidad 270 de comunicación de seguridad. La unidad 270 de comunicación de seguridad permite que un aparato de tratamiento de datos o un aparato móvil realice la conmutación entre un modo seguro y un modo no seguro. La unidad 270 de comunicación de seguridad puede dividir un área de memoria a la que puede acceder la unidad 200 principal y un área de memoria a la que puede acceder la unidad 300 de seguridad, en un hardware que utiliza un bit predeterminado. En consecuencia, el acceso de la unidad 200 principal al área de memoria utilizada por la unidad 300 de seguridad está bloqueado. En consecuencia, si el sistema 210 operativo principal de la unidad 200 principal es un sistema operativo abierto, es posible que el código malicioso no acceda al sistema 310 operativo seguro y al área de memoria utilizada por el sistema 310 operativo seguro. A continuación se describe un procedimiento para procesar un contenido que solicita seguridad en la unidad 300 de seguridad.

La unidad 300 de seguridad ejecuta un programa seguro, una aplicación segura o un contenido seguro que solicita seguridad en un modo seguro de acuerdo con una solicitud de la unidad 200 principal.

La unidad 200 principal incluye un sistema 210 operativo principal, una unidad 220 de descifrado, una unidad 230 de decodificación, una unidad 240 de representación y una unidad 250 de aplicación. La unidad 300 de seguridad incluye un sistema 310 operativo seguro, una unidad 340 de servicios de seguridad, una unidad 320 de servicios de suministro y un Sistema 330 de Archivo Seguro (SFS).

El sistema 210 operativo principal es un sistema operativo principal del dispositivo 100 de usuario. El sistema 210 operativo principal realiza una operación general del dispositivo 100 de usuario en el modo normal, y realiza especialmente una ejecución de un programa normal, una aplicación normal o un contenido normal que no requiere seguridad, en un modo normal. Cuando se necesita la ejecución de un programa seguro, una aplicación segura y un contenido seguro que solicite seguridad, el sistema 210 operativo principal instruye o solicita la ejecución correspondiente a la unidad 300 de seguridad a través de la unidad 270 de comunicación de seguridad.

Cuando se solicita la ejecución de contenido, la unidad 220 de descifrado lee un flujo de audio y/o vídeo correspondiente al contenido solicitado de ejecución desde un área 177 de almacenamiento normal, y determina si el flujo de audio y/o vídeo es un flujo de audio y/o vídeo que requiere seguridad. La unidad 220 de descifrado puede confirmar si un sistema de protección de contenido tal como DRM se aplica a la transmisión de audio y/o vídeo, y puede determinar si la transmisión de audio y/o vídeo requiere seguridad. Además, cuando se incluye un identificador que permite la transmisión de audio y/o vídeo en el modo seguro se incluye en la transmisión de audio y/o vídeo, la unidad 220 de descifrado puede determinar si la transmisión de audio y/o vídeo requiere seguridad.

Si el contenido que se solicita que se ejecute es una transmisión de audio y/o vídeo que no requiere seguridad, la unidad 220 de descifrado almacena las transmisiones de audio y/o vídeo que no solicitan seguridad en el área 177 de almacenamiento normal en una forma de dividirse en una unidad de carga útil, y solicita decodificación. Si la ejecución de las secuencias de audio y/o vídeo solicitadas son secuencias de audio y/o vídeo que requieren seguridad, la unidad 220 de descifrado divide las secuencias de audio y/o vídeo solicitadas de seguridad en una unidad de carga útil, y solicita al sistema 210 operativo principal que realice el descifrado de seguridad con respecto a la transmisión de audio y/o vídeo de seguridad solicitada en una unidad de carga útil. Además, si la información que indica que se ha completado el descifrado de seguridad se recibe del OS 210 principal, la unidad 220 de descifrado solicita a la unidad 230 de decodificación que realice la decodificación.

La unidad 230 de decodificación incluye un módulo 232 de decodificación de vídeo y un módulo 234 de decodificación de audio. Si se solicita decodificar transmisiones de audio y/o vídeo normales que no requieren seguridad, la unidad 230 de decodificación decodifica transmisiones de audio y/o vídeo en una unidad de carga útil almacenada en el área 177 de almacenamiento normal en datos de audio y/o vídeo en un unidad de cuadro que usa el códec de audio y/o vídeo a través del módulo 232 de decodificación de vídeo y/o el módulo 234 de decodificación de audio en el modo normal. La unidad 230 de decodificación almacena los datos de audio y/o vídeo decodificados en el área 177 de almacenamiento normal, y solicita a la unidad 240 de representación que realice la representación. Cuando se solicita decodificar una secuencia de vídeo que solicita seguridad, la unidad 230 de decodificación solicita al sistema 210 operativo principal que realice la decodificación de seguridad en un modo seguro. Además, si la información que indica que se ha completado la decodificación de seguridad se recibe del OS 210 principal, la unidad 230 de decodificación solicita a la unidad 240 de representación que realice la representación.

La unidad 240 de representación incluye un módulo 242 de representación de vídeo y un módulo 244 de representación de audio. Si se le solicita que procese datos de audio y/o vídeo normales que no requieren seguridad, la unidad 240 de representación realiza la representación de vídeo mediante el módulo 242 de representación de vídeo y/o el módulo 244 de representación de audio en un modo normal, de modo que los datos de vídeo decodificados almacenado en el área 177 de almacenamiento normal se genera en señales de vídeo bidimensionales y tridimensionales que pueden visualizarse en una pantalla, y genera las señales de vídeo generadas. La unidad 240 de representación representa los datos de audio decodificados en una señal de audio analógica.

Mientras tanto, cuando se le solicita que muestre datos de vídeo que requieren seguridad, la unidad 240 de representación solicita al sistema 210 operativo principal que realice la representación de seguridad en un modo seguro. Además, cuando la información que indica que la representación de seguridad se completa desde el sistema 210 operativo principal, la unidad 240 de representación solicita la salida de la señal de vídeo y audio representada. La señal de vídeo representada y la señal de audio se emiten a través de un dispositivo de visualización y un altavoz, respectivamente.

La unidad 250 de aplicación incluye una aplicación de descarga de contenido, una aplicación de reproducción de contenido o similar, y realiza una función correspondiente cuando la aplicación se ejecuta de acuerdo con una solicitud del usuario.

El sistema 310 operativo seguro es un sistema operativo seguro del dispositivo 100 de usuario. El sistema 310 operativo seguro ejecuta contenido seguro que solicita seguridad en el modo seguro. Si al menos una de una solicitud de descifrado, una solicitud de decodificación y una solicitud de representación con respecto a una secuencia de vídeo que solicita seguridad o una solicitud de descifrado con respecto a una secuencia de audio que solicita seguridad se recibe del OS 210 principal a través de la unidad 270 de comunicación de seguridad, el OS seguro 310 transmite la solicitud recibida a la unidad 340 de servicios de seguridad.

La unidad 320 de servicios de suministro recibe una clave de seguridad e información de autenticación de proveedores de servicios de protección de contenido externo (tales como proveedores de servicios DRM) y almacena la clave de seguridad y la información de autenticación en el SFS 330. Además, la clave de seguridad y la información de autenticación pueden ser almacenadas en el SFS 330 por adelantado por un fabricante del aparato.

El SFS 330 es un área de almacenamiento accesible en modo seguro e incluye diversos programas e información para ejecutar un contenido seguro que requiere seguridad, como una ejecución de descifrado, una ejecución de decodificación y una ejecución de representación con respecto a una señal de audio y/o vídeo que solicita seguridad. Además, el SFS 330 almacena una clave de seguridad e información de autenticación almacenada por la unidad 320 de servicios de suministro.

La unidad 340 de servicios de seguridad incluye un servicio 342 de descifrado de seguridad que realiza un descifrado de seguridad, un servicio 344 de decodificación de seguridad que realiza una decodificación de seguridad y un servicio 346 de representación de seguridad que realiza una representación de seguridad. La unidad 340 de servicios de seguridad realiza el descifrado de seguridad a través del servicio 342 de descifrado de seguridad. La unidad 340 de servicios de seguridad realiza la decodificación de seguridad a través del servicio 344 de decodificación de seguridad. La unidad 340 de servicios de seguridad realiza la prestación de seguridad a través del servicio 346 de representación de seguridad.

Si una solicitud de descifrado con respecto a un flujo de vídeo que solicita seguridad se transmite desde el OS 310 seguro, la unidad 340 de servicios de seguridad realiza el descifrado de seguridad con respecto a un flujo de vídeo que solicita seguridad utilizando una clave de seguridad e información de autenticación almacenada en el SFS 330 y almacena, en el área 179 de almacenamiento segura, la secuencia de vídeo en la que se realiza el descifrado de seguridad. Además, si una solicitud de decodificación con respecto a una secuencia de vídeo que solicita seguridad se transmite desde el OS 310 seguro, la unidad 340 de servicios de seguridad realiza una decodificación de seguridad con respecto a una secuencia de vídeo que solicita seguridad utilizando un códec de vídeo correspondiente, y almacena un transmisión de vídeo decodificada de seguridad en el área 179 de almacenamiento segura. Además, si una solicitud de representación con respecto a los datos de vídeo que solicita seguridad se transmite desde el OS 310 seguro, la unidad 340 de servicios de seguridad realiza la representación de seguridad para que los datos de vídeo decodificados se generen en una señal de vídeo que se mostrará en una pantalla bidimensional o tridimensional, y emite la señal de vídeo a la unidad 200 principal.

En respuesta a una solicitud de descifrado con respecto a un flujo de vídeo que solicita seguridad del sistema 310 operativo seguro, la unidad 340 de servicios de seguridad realiza el descifrado de seguridad con respecto a un flujo de audio que solicita seguridad utilizando una clave de seguridad e información de autenticación almacenada en el SFS 330, y la unidad 340 de servicios de seguridad almacena el flujo de audio descifrado de seguridad en el área 179 de almacenamiento segura.

Con referencia de nuevo a la Figura 2, cuando el dispositivo 100 de usuario está encendido, el cargador 114 de arranque inicia el dispositivo 100 de usuario. Cuando se inicia el arranque, el cargador 114 de arranque carga primero el SO seguro y carga el SO principal cuando el SO seguro está completamente cargado.

Además, de acuerdo con una realización ejemplar de la presente invención, el cargador 114 de arranque confirma si el sistema operativo principal está pirateado en un procedimiento de arranque. Por ejemplo, la piratería del sistema operativo principal puede ser un enraizamiento del sistema operativo principal (por ejemplo, el enraizamiento del sistema operativo Android). El enraizamiento de Android es el procedimiento que permite a los usuarios de teléfonos inteligentes, tabletas y otros dispositivos que ejecutan el sistema operativo móvil Android obtener un control privilegiado (conocido como "acceso raíz") dentro del subsistema de Android. El enraizamiento a menudo se realiza con el objetivo de superar las limitaciones que los operadores y los fabricantes de hardware ponen en algunos dispositivos, lo que resulta en la capacidad de alterar o reemplazar las aplicaciones y configuraciones del sistema, ejecutar aplicaciones especializadas que requieren permisos de nivel de administrador o realizar otras operaciones que de otro modo inaccesible para un usuario normal de Android. En Android, el enraizamiento puede facilitar también la eliminación completa y el reemplazo del sistema operativo del dispositivo, generalmente con una versión más reciente de su sistema operativo actual.

Por ejemplo, el cargador 114 de arranque se refiere a una imagen binaria ROM del sistema operativo principal legítimamente equipado en el dispositivo 100 de usuario para confirmar si la imagen binaria ROM es similar al sistema operativo principal del dispositivo 100 de usuario o no. Si se determina que la imagen binaria ROM no es similar, se decide que un usuario ha cambiado el sistema operativo principal. De lo contrario, si se confirma la firma de un distribuidor que distribuye el sistema operativo principal o similar, y no hay una firma adecuada en la imagen binaria de la ROM con respecto al sistema operativo principal del dispositivo 100 de usuario en el punto de arranque, se decide que el usuario ha cambiado el sistema operativo principal. La imagen binaria ROM del SO principal legítimamente equipado se almacena en el área 177 de almacenamiento normal.

Si se determina que el SO principal está pirateado, el cargador 114 de arranque almacena la información de pirateo del SO principal en el área 179 de almacenamiento segura. El cargador 114 de arranque puede almacenar información de pirateo del sistema operativo principal en el área 179 de almacenamiento segura en el modo seguro a través de la unidad 300 de seguridad.

Cuando se solicita la ejecución de un contenido seguro o luego se solicita la ejecución de seguridad, la información de pirateo del sistema operativo principal puede usarse como un estándar para decidir si el controlador 110 se opera o no en un modo seguro.

El cargador 114 de arranque confirma la integridad de cada uno de los módulos de función de la unidad 300 de seguridad en un procedimiento de arranque. El cargador 114 de arranque carga el sistema operativo seguro y confirma una imagen binaria de cada uno de los módulos de función de la unidad 300 de seguridad en el momento del arranque, y confirma la firma de un distribuidor de cada uno de los módulos de función. Si no existe una firma adecuada de un distribuidor en una imagen binaria de cada uno de los módulos de funciones en el momento del arranque, se decide que la integridad de cada uno de los módulos de funciones está dañada. Cada uno de los módulos de función de la unidad 300 de seguridad puede ser, por ejemplo, la unidad de servicios de provisión 320, la unidad 340 de servicios de seguridad y el SFS 330. La imagen binaria normal de cada uno de los módulos de función de la unidad 300 de seguridad se almacena en el área 177 de almacenamiento normal, y la imagen binaria normal de cada uno de los módulos de función de la unidad 300 de seguridad en el momento del arranque puede proporcionarse desde el unidad 300 de seguridad de acuerdo con una solicitud del cargador 114 de arranque.

El cargador 114 de arranque almacena el resultado obtenido al confirmar la integridad de cada uno de los módulos de función de la unidad 300 de seguridad en el área 179 de almacenamiento segura bajo el modo seguro a través de la unidad 300 de seguridad. El resultado obtenido al confirmar la integridad de cada uno de los módulos de función de la unidad 300 de seguridad puede usarse también como un estándar para decidir si el controlador 110 se opera o no en un modo seguro, cuando se solicita la ejecución de un contenido seguro o se solicita la ejecución de seguridad.

La unidad 175 de almacenamiento puede almacenar una señal o datos que son de entrada/salida correspondientes a una operación del módulo 120 de comunicaciones móviles, el módulo 130 de subcomunicación, el módulo 140 multimedia, el módulo 150 de cámara, el módulo 155 de GPS, módulo 160 de entrada/de salida, el módulo 170 de sensor o la pantalla 190 táctil, de acuerdo con el control del controlador 110. La unidad 175 de almacenamiento puede almacenar programas de control y aplicaciones para controlar el dispositivo 100 de usuario o el controlador 110.

La expresión "unidad de almacenamiento" incluye la unidad 175 de almacenamiento, la ROM 112 en el controlador 110, la RAM 113 o una tarjeta de memoria (no ilustrada) montada en el dispositivo 100 de usuario (por ejemplo, una tarjeta SD y una tarjeta de memoria). La unidad de almacenamiento puede incluir una memoria no volátil, una memoria volátil, una unidad de disco duro (HDD) o una unidad de estado sólido (SSD).

La unidad 175 de almacenamiento puede incluir el área 177 de almacenamiento normal y el área 179 de almacenamiento segura. El área 177 de almacenamiento normal puede almacenar datos y programas normales, y el área 179 de almacenamiento segura puede almacenar datos y programas a los que solo los componentes a los que se les permiten acceder pueden acceder en el modo seguro. De acuerdo con una realización ejemplar de la presente invención, el área 177 de almacenamiento normal puede almacenar un flujo de audio y/o vídeo correspondiente al contenido descargado usando al menos uno del módulo 120 de comunicaciones móviles, el módulo 131 de LAN inalámbrica y el módulo 132 de comunicaciones de corto alcance. Además, el área 177 de almacenamiento normal

puede almacenar datos de audio y/o vídeo descifrados, datos de audio decodificados y/o datos de vídeo, y similares que se generan al momento de realizar el descifrado y la decodificación con respecto al contenido normal en el modo normal. El área 179 de almacenamiento segura puede almacenar los datos descifrados de audio y/o vídeo, datos decodificados de audio y/o vídeo, y similares que se generan en el momento del descifrado o decodificación con respecto a un contenido seguro en un modo seguro. La expresión "unidad de almacenamiento" puede incluir la unidad 175 de almacenamiento, la ROM 112 en el controlador 110, la RAM 113 y una tarjeta de memoria (no ilustrada) montada en el dispositivo 100 de usuario (por ejemplo, una tarjeta SD y una tarjeta de memoria). La unidad de almacenamiento puede incluir una memoria no volátil, una memoria volátil, una unidad de disco duro (HDD) o una unidad de estado sólido (SSD).

El módulo 120 de comunicaciones móviles permite que el dispositivo 100 de usuario se conecte a un dispositivo externo mediante una comunicación móvil utilizando al menos una (una o más) antenas (no ilustradas) de acuerdo con el control del controlador 110. El módulo 120 de comunicaciones móviles transmite/recibe señales inalámbricas para una comunicación de voz, una comunicación de vídeo, un servicio de mensajes cortos (SMS) y un servicio de mensajería multimedia (MMS) con un teléfono celular (no ilustrado), un teléfono inteligente (no ilustrado), una tableta u otros dispositivos (no ilustrados) que tienen números de teléfono ingresados al dispositivo 100 de usuario.

El módulo 130 de subcomunicación puede incluir al menos uno del módulo 131 de LAN inalámbrica y el módulo 132 de comunicaciones de corto alcance. Por ejemplo, el módulo 130 de subcomunicación puede incluir solo el módulo 131 de LAN inalámbrica, el módulo 132 de comunicaciones de corto alcance solamente, o tanto el módulo 131 de LAN inalámbrica como el módulo 132 de comunicaciones de corto alcance.

El módulo 131 de LAN inalámbrica puede conectarse a Internet de acuerdo con el control del controlador 110 en un lugar donde está instalado un punto de acceso inalámbrico (AP) (no ilustrado). El módulo 131 de LAN inalámbrica es compatible con un estándar de LAN inalámbrica del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) (IEEE 802.11x). El módulo 132 de comunicaciones de corto alcance puede realizar de forma inalámbrica una comunicación de corto alcance entre el dispositivo 100 de usuario y un aparato de formación de imágenes (no ilustrado) de acuerdo con el control del controlador 110. La comunicación de corto alcance puede incluir Bluetooth, Asociación de datos infrarrojos (IrDA) y similares.

El dispositivo 100 de usuario puede incluir al menos uno del módulo 120 de comunicaciones móviles, el módulo 131 de LAN inalámbrica y el módulo 132 de comunicaciones de corto alcance. Por ejemplo, el dispositivo 100 de usuario puede incluir una combinación del módulo 120 de comunicaciones móviles, el módulo 131 de LAN inalámbrica y el módulo 132 de comunicaciones de corto alcance.

Al menos uno del módulo 120 de comunicaciones móviles, el módulo 131 de LAN inalámbrica y el módulo 132 de comunicaciones de corto alcance transmiten una señal de solicitud para solicitar contenido seguro de un proveedor de contenido externo bajo el control del controlador 110, o pueden recibir contenido seguro en respuesta a una solicitud de contenido seguro. Además, al menos uno del módulo 120 de comunicaciones móviles, el módulo 131 de LAN inalámbrica y el módulo 132 de comunicaciones de corto alcance pueden solicitar o recibir datos clave e información de autenticación para descifrar o autenticar un contenido protegido como DRM bajo el control del controlador 110.

El módulo 140 multimedia puede incluir el módulo de comunicación de radiodifusión 141, el módulo 142 de reproducción de audio o el módulo 143 de reproducción de vídeo. El módulo 141 de comunicación de radiodifusión puede recibir una señal de transmisión (por ejemplo, una señal de transmisión de TeleVision (TV), una señal de radiodifusión o una señal de difusión de datos) y una información adicional de difusión (por ejemplo, Guía de programas eléctricos (EPS) o Eléctrico Guía de servicio (ESG)) transmitida desde una estación de difusión a través de la antena de difusión (no ilustrada) de acuerdo con el control del controlador 110. El módulo 142 de reproducción de audio puede reproducir un archivo de audio digital (por ejemplo, un archivo que tiene una extensión de nombre de archivo de mp3, wma, ogg o wav) almacenado o recibido de acuerdo con el control del controlador 110. El módulo 143 de reproducción de vídeo puede reproducir un archivo de vídeo digital (por ejemplo, un archivo que tiene una extensión de nombre de archivo de mpeg, mpg, mp4, avi, mov o mkv) almacenado o recibido de acuerdo con el control del controlador 110. El módulo 143 de reproducción de vídeo puede reproducir un archivo de audio digital.

El módulo 140 multimedia puede incluir el módulo 142 de reproducción de audio y el módulo 143 de reproducción de vídeo excluyendo el módulo de comunicación de radiodifusión 141. El módulo 142 de reproducción de audio o el módulo 143 de reproducción de vídeo de la unidad 140 multimedia pueden incluirse en el controlador 110. El módulo 140 multimedia procesa y emite datos de audio y/o vídeo almacenados en el área 177 de almacenamiento normal en el modo normal bajo el control del controlador 110, y procesa y emite datos de audio y/o vídeo almacenados en el área 179 de almacenamiento segura en el modo seguro.

El módulo 150 de cámara puede incluir al menos una de la primera cámara 151 y la segunda cámara 152 que captura una imagen fija o una imagen en movimiento de acuerdo con el control del controlador 110. Además, la primera cámara 151 o la segunda cámara 152 pueden incluir una fuente de luz auxiliar (por ejemplo, un flash (no ilustrado)) que proporciona una cantidad de luz requerida para capturar una imagen. La primera cámara 151 está montada en la superficie frontal del dispositivo 100 de usuario, y la segunda cámara 152 está montada en la superficie trasera del dispositivo 100 de usuario. De acuerdo con otro procedimiento, la primera cámara 151 y la segunda cámara 152 están

dispuestas adyacentes (por ejemplo, el espacio entre la primera cámara 151 y la segunda cámara 152 es mayor que 1 cm y menor que 8 cm) y puede capturar una imagen fija tridimensional y una imagen en movimiento tridimensional.

El módulo 155 de GPS puede recibir una señal de radio de una pluralidad de satélites GPS (no ilustrados) en la órbita de la tierra, y puede calcular una ubicación del dispositivo 100 de usuario usando el tiempo de llegada del satélite GPS (no ilustrado) al dispositivo 100 de usuario.

El módulo 160 de entrada/salida puede incluir al menos uno de la pluralidad de botones 161, el micrófono 162, el altavoz 163, el motor 164 de vibración, el conector 165 y el teclado 166 opcional.

El botón 161 puede formarse en la superficie frontal, la superficie lateral o la superficie posterior de la carcasa del dispositivo 100 de usuario, e incluir al menos uno de un botón de encendido/bloqueo (no ilustrado), un botón de volumen (no ilustrado), un botón de menú, un botón de inicio, un botón de retroceso y un botón de búsqueda.

El micrófono 162 genera una señal eléctrica al recibir una entrada de una voz o un sonido de acuerdo con el control del controlador 110.

El altavoz 163 puede emitir, al exterior del dispositivo 100 de usuario, un sonido correspondiente a varias señales (por ejemplo, una señal inalámbrica, una señal de transmisión, un archivo de audio digital, un archivo de vídeo digital, una fotografía de imagen o similar) del módulo 120 de comunicaciones móviles, el módulo 130 de subcomunicación, el módulo 140 multimedia o el módulo 150 de cámara de acuerdo con el control del controlador 110. El altavoz 163 puede emitir un sonido (por ejemplo, un sonido de operación de botón o un sonido de conexión de comunicación correspondiente a una comunicación telefónica) correspondiente a una función realizada por el dispositivo 100 de usuario. Se pueden formar uno o más altavoces 163 en una posición o posiciones apropiadas del alojamiento del dispositivo 100 de usuario.

El motor 164 de vibración puede convertir una señal eléctrica en una vibración mecánica de acuerdo con el control del controlador 110. Por ejemplo, cuando se recibe una comunicación de voz desde otro aparato (no ilustrado), el dispositivo 100 de usuario en un modo de vibración opera el motor 164 de vibración. Se pueden formar uno o más motores 164 de vibración en la carcasa del dispositivo 100 de usuario. El motor 164 de vibración puede realizar una operación en respuesta a una operación táctil de un usuario que toca la pantalla 190 táctil y un movimiento continuo de un toque en la pantalla 190 táctil.

El conector 165 puede usarse como una interfaz para conectar el dispositivo 100 de usuario con un aparato externo (no ilustrado) o una fuente de alimentación (no ilustrada). De acuerdo con el control del controlador 110, los datos almacenados en la unidad 175 de almacenamiento del dispositivo 100 de usuario a través de un cable de alambre conectado al conector 165 pueden transmitirse a un aparato externo (no ilustrado) o los datos pueden recibirse de un aparato externo (no ilustrado). Se introduce una energía eléctrica o se carga una batería (no ilustrada) desde una fuente de alimentación (no ilustrada) a través de un cable de alambre conectado al conector 165.

El teclado 166 puede recibir una entrada clave de un usuario para controlar el dispositivo 100 de usuario. El teclado 166 incluye un teclado físico (no ilustrado) formado en el dispositivo 100 de usuario o un teclado virtual (no ilustrado) visualizado en la pantalla 190 táctil. El teclado físico (no ilustrado) formado en el dispositivo 100 de usuario puede excluirse de acuerdo con el diseño o la estructura del dispositivo 100 de usuario.

El módulo 170 de sensor puede incluir al menos un sensor que detecta un estado del dispositivo 100 de usuario. Por ejemplo, el módulo 170 de sensor puede incluir un sensor de proximidad que detecta si un usuario se acerca al dispositivo 100 de usuario, un sensor de iluminancia (no ilustrado) que detecta la cantidad de luz cerca del dispositivo 100 de usuario y un sensor de movimiento (no ilustrado) que detecta una operación (por ejemplo, un giro del dispositivo 100 de usuario, aceleración o vibración aplicada al dispositivo 100 de usuario) del dispositivo 100 de usuario. Al menos un sensor detecta un estado, genera una señal correspondiente a la detección y transmite la señal generada al controlador 110. Los sensores del módulo 170 de sensor pueden agregarse o eliminarse de acuerdo con el rendimiento del dispositivo 100 de usuario.

La unidad 175 de almacenamiento puede almacenar una señal o datos que se introducen/salen en correspondencia con la operación del módulo 120 de comunicaciones móviles, el módulo 130 de subcomunicación, el módulo 140 multimedia, el módulo 150 de cámara, el módulo 155 de GPS, el módulo 160 de entrada/salida, el módulo 170 de sensor y la pantalla 190 táctil de acuerdo con el control del controlador 110. La unidad 175 de almacenamiento puede almacenar programas de control y aplicaciones para controlar el dispositivo 100 de usuario o el controlador 110.

La unidad de suministro de energía 180 puede suministrar energía a una o más baterías (no ilustradas) dispuestas en la carcasa del dispositivo 100 de usuario de acuerdo con el control del controlador 110. Una o más baterías (no ilustradas) suministran energía al dispositivo 100 de usuario. Además, la unidad 180 de fuente de alimentación puede suministrar entrada de energía desde una fuente de alimentación externa (no ilustrada) al dispositivo 100 de usuario a través de un cable de alambre conectado al conector 165.

La pantalla 190 táctil puede proporcionar interfaces de usuario (por ejemplo, una comunicación, transmisión de datos, difusión y fotografía) correspondientes a diversos servicios con un usuario. De acuerdo con una realización ejemplar

de la presente invención, se puede proporcionar una interfaz de usuario para realizar aplicaciones tales como una aplicación de descarga de contenido o una aplicación de reproducción de contenido.

La pantalla 190 táctil puede transmitir, al controlador 195 de pantalla táctil, y una señal analógica correspondiente a al menos un toque recibido como entrada a la interfaz de usuario. La pantalla 190 táctil puede recibir una entrada de al menos un toque a través del cuerpo del usuario (por ejemplo, un dedo que incluye un pulgar) o un medio de entrada táctil (por ejemplo, un lápiz óptico). Además, la pantalla 190 táctil puede introducir un movimiento continuo de un toque entre al menos un toque. La pantalla 190 táctil puede transmitir una señal analógica correspondiente a un movimiento continuo de una entrada táctil al controlador 195 de pantalla táctil. Por ejemplo, una solicitud para ejecutar una aplicación de descarga de contenido por parte de un usuario, o una señal analógica correspondiente a varias selecciones de usuario generadas durante la ejecución de la aplicación de descarga de contenido, puede transmitirse al controlador 195 de pantalla táctil.

Un toque de acuerdo con realizaciones ejemplares de la presente invención no se limita a un contacto de la pantalla 190 táctil con el cuerpo del usuario o los medios de entrada táctiles, y el toque puede incluir no contacto (por ejemplo, una distancia entre el toque pantalla 190 y el cuerpo del usuario o el medio de entrada táctil es de 1 mm o menos). La distancia detectable por la pantalla 190 táctil puede cambiarse de acuerdo con el rendimiento o la estructura del dispositivo 100 de usuario.

La pantalla 190 táctil puede implementarse mediante un tipo resistivo, un tipo capacitivo, un tipo infrarrojo y un tipo de onda acústica.

El controlador 195 de pantalla táctil convierte una señal analógica recibida desde la pantalla 190 táctil en una señal digital (por ejemplo, coordenadas X e Y) y transmite la señal digital al controlador 110. El controlador 110 puede controlar la pantalla 190 táctil usando la señal digital recibida desde el controlador 195 de pantalla táctil. Por ejemplo, el controlador 110 puede permitir que se seleccione un icono de acceso directo (no ilustrado) visualizado en la pantalla 190 táctil en respuesta al toque o puede ejecutar un icono de acceso directo (no ilustrado). Además, el controlador 195 de pantalla táctil puede incluirse en el controlador 110.

A continuación se describe un procedimiento en el dispositivo 100 de usuario configurado como se describe anteriormente para confirmar un nivel de seguridad del dispositivo 100 de usuario, bloquear la operación del modo seguro en sí mismo de acuerdo con el resultado y fortalecer el nivel de protección con respecto al contenido digital. con referencia a las Figuras 4 a 7. Las Figuras 4 y 5 son diagramas que ilustran ejemplos de acuerdo con la presente invención en los que el dispositivo 100 de usuario determina si el SO principal está pirateado o no y bloquea la realización de una operación del dispositivo de usuario en un modo seguro. Las Figuras 6 y 7 son diagramas que ilustran un ejemplo de acuerdo con la presente invención en el que el servidor 10 de servicios de contenido autentica la información de autenticación del dispositivo que indica el nivel de seguridad del dispositivo del dispositivo 100 de usuario, y el dispositivo 100 de usuario bloquea la realización de una operación del dispositivo 100 de usuario en el modo seguro.

La Figura 4 es un diagrama que ilustra un procedimiento de arranque de un dispositivo de usuario de acuerdo con una realización ejemplar de la presente invención.

Con referencia a la Figura 4, cuando el dispositivo 100 de usuario está encendido, el cargador 114 de arranque comienza a iniciarse en la etapa 301. El cargador 114 de arranque carga un sistema operativo seguro en la etapa 303, y confirma la integridad con respecto a cada uno de los módulos de función de la unidad 300 de seguridad en la etapa 304. El cargador 114 de arranque solicita a la unidad 300 de seguridad que almacene el resultado de confirmación de integridad de cada uno de los módulos de función. La unidad 300 de seguridad almacena el resultado de confirmación de integridad en el área 179 de almacenamiento segura en el modo seguro de acuerdo con la solicitud.

El cargador 114 de arranque confirma si el sistema operativo principal está pirateado en la etapa 305. De acuerdo con el resultado de la confirmación, si se confirma que el SO principal está pirateado, el cargador 114 de arranque solicita a la unidad 300 de seguridad que almacene la información de pirateo del SO principal en la etapa 307. La unidad 300 de seguridad almacena la información de pirateo del sistema operativo principal en el área 179 de almacenamiento segura en el modo seguro de acuerdo con la solicitud.

El cargador 114 de arranque carga el sistema operativo principal en la etapa 309 y finaliza el arranque.

Las Figuras 5 y 6 son diagramas que ilustran procedimientos de autenticación de seguridad de dispositivos de usuario de acuerdo con realizaciones ejemplares de la presente invención.

Con referencia a la Figura 5, la unidad 200 principal recibe una entrada de una solicitud de ejecución de un servicio de seguridad en la etapa 401. La solicitud de ejecución del servicio de seguridad es una solicitud con respecto a diversos servicios que solicitan seguridad, por ejemplo, una solicitud para obtener contenidos seguros desde el exterior y una solicitud de ejecución con respecto a los contenidos seguros. En el que la unidad 200 principal incluye el sistema operativo principal y la unidad 300 de seguridad incluye el sistema operativo seguro.

Cuando se ingresa una solicitud de servicios de seguridad, la unidad 200 principal informa a la unidad 300 de seguridad

que la solicitud de servicios de seguridad se ingresa en la etapa 405. En consecuencia, la unidad 300 de seguridad confirma si la información de pirateo del sistema operativo principal existe en el área 179 de almacenamiento segura en la etapa 407. Si la información de pirateo del sistema operativo principal no existe, la unidad 300 de seguridad ejecuta el servicio de seguridad solicitado en un modo seguro. Sin embargo, si existe la información de pirateo del sistema operativo principal, la unidad 300 de seguridad continúa con la etapa 409 y bloquea el modo seguro. Además, la unidad 300 de seguridad informa a la unidad 200 principal que el modo seguro está bloqueado en la etapa 411.

En consecuencia, la unidad 200 principal proporciona al usuario un mensaje de información que informa que el modo seguro está bloqueado y que la solicitud del servicio de seguridad no puede realizarse en la etapa 413.

En otras palabras, el sistema operativo principal confirma si el sistema operativo principal está pirateado, y si se confirma que el sistema operativo principal está pirateado, el sistema operativo seguro bloquea el modo seguro.

En consecuencia, el dispositivo 100 de usuario confirma si el sistema operativo principal está pirateado, y si se confirma que el sistema operativo principal está pirateado, el dispositivo 100 de usuario determina que el nivel de seguridad del dispositivo 100 de usuario no satisface el valor estándar y bloquea el operación del modo seguro para que se pueda fortalecer el nivel de seguridad con respecto al contenido seguro.

De acuerdo con otra realización ejemplar de la presente invención, el nivel de seguridad del dispositivo 100 de usuario se autentica desde el servidor 10 de servicios de contenido digital y la operación en el modo seguro puede bloquearse de acuerdo con el resultado. Tal procedimiento se ilustra en la Figura 6.

Con referencia a la Figura 6, si se solicita acceso al servidor de servicios de contenido digital 10 en la etapa 501, la unidad 200 principal, es decir, el SO principal, solicita información de autenticación del dispositivo desde la unidad 300 de seguridad, es decir, el SO seguro, en la etapa 503. La conexión al servidor 10 de servicios de contenido digital se puede generar al momento de solicitar la descarga con respecto al contenido digital. La información de autenticación del dispositivo es información sobre diversas causas que pueden determinar el nivel de seguridad del dispositivo 100 de usuario, por ejemplo, la información de pirateo del sistema operativo principal, y/o información sobre los resultados de confirmación de integridad en cada uno de los módulos de función de la unidad 300 de seguridad.

La unidad 300 de seguridad procede a la etapa 505 de acuerdo con la solicitud en la etapa 503, y recopila información de autenticación del dispositivo en el modo seguro. Por ejemplo, la unidad 300 de seguridad recopila la información de seguridad que indica si el modo seguro es compatible, la información de pirateo del SO principal que indica si el SO principal está pirateado y la información de integridad que indica los resultados de confirmación de integridad de cada una de los módulos de función de la unidad 300 de seguridad. Además, la información del tiempo de recopilación que indica el momento en que se recopila la información de autenticación del dispositivo se incluye en la información de autenticación del dispositivo.

La unidad 300 de seguridad cifra la información de autenticación del dispositivo en la etapa 507, y transmite la información de autenticación del dispositivo cifrado a la unidad 200 principal en la etapa 509.

Cuando se transmite la información de autenticación del dispositivo, la unidad 200 principal transmite la información de autenticación del dispositivo junto con una solicitud de autenticación del dispositivo al servidor 10 de servicios de contenido digital en la etapa 511.

Si el servidor 10 de servicios de contenido digital recibe la solicitud de autenticación del dispositivo y la información de autenticación del dispositivo, el servidor 10 de servicios de contenido digital realiza una operación como se ilustra en la Figura 7.

La Figura 7 es un diagrama que ilustra un procedimiento de operación de un servidor de servicios de contenido digital de acuerdo con una realización ejemplar de la presente invención.

Con referencia a la Figura 7, si el servidor de servicios de contenido digital 10 en la etapa 601 recibe una solicitud de autenticación del dispositivo e información de autenticación del dispositivo, la información de autenticación del dispositivo recibida se descifra y la información de autenticación del dispositivo se confirma a través de las etapas 603 a 609. El servidor de servicios de contenido digital 10 en la etapa 603 confirma la información de seguridad para confirmar si el dispositivo 100 de usuario admite el modo seguro. Si se determina que el dispositivo 100 de usuario no admite el modo seguro, el servidor del servicio de contenido digital 10 continúa con la etapa 613, informa al dispositivo 100 de usuario que la autenticación ha fallado y finaliza el procedimiento de autenticación.

Si el dispositivo 100 de usuario admite el modo seguro, el servidor 10 de servicios de contenido continúa con la etapa 605, confirma la información de pirateo del sistema operativo principal y confirma si el sistema operativo principal del dispositivo 100 de usuario está pirateado. De acuerdo con el resultado de la confirmación, si se determina que el sistema operativo principal está pirateado, el servidor 10 de servicios de contenido continúa con la etapa 613, informa al dispositivo 100 de usuario que la autenticación ha fallado y finaliza el procedimiento de autenticación.

Si se confirma que el sistema operativo principal del dispositivo 100 de usuario no está pirateado, el servidor 10 de servicios de contenido continúa con la etapa 607, y confirma la información de integridad, y confirma si la integridad

de cada uno de los módulos de función incluidos en el dispositivo 100 de usuario para soportar el modo seguro está dañado. De acuerdo con el resultado de la confirmación, si se determina que existe integridad dañada, el servidor 10 de servicios de contenido continúa con la etapa 613, informa al dispositivo 100 de usuario que la autenticación ha fallado y finaliza el procedimiento de autenticación.

Si se confirma que la integridad del dispositivo 100 de usuario es completamente normal, el servidor 10 de servicios de contenido continúa con la etapa 609 y confirma el tiempo para recopilar información de autenticación del dispositivo. El tiempo para recibir información de autenticación del dispositivo y el tiempo de recopilación incluido en la información de autenticación del dispositivo se comparan entre sí. Si la diferencia es mayor que un valor estándar establecido, se determina que la información de autenticación del dispositivo no está disponible. El servidor 10 de servicios de contenido continúa con la etapa 613, informa al dispositivo 100 de usuario que la autenticación ha fallado y finaliza el procedimiento de autenticación.

Si la diferencia es menor que un valor estándar establecido, se determina que la información de autenticación del dispositivo está disponible. El servidor 10 de servicios de contenido continúa con la etapa 611, informa al dispositivo 100 de usuario que la autenticación ha tenido éxito y finaliza el procedimiento de autenticación.

De acuerdo con la operación del servidor 10 de servicios de contenido como se describió anteriormente, el dispositivo 100 de usuario en la etapa 513 de la Figura 6 pueden recibir el resultado de autenticación. Cuando se recibe la autenticación, la unidad 200 principal transmite el resultado de la autenticación a la unidad 300 de seguridad en la etapa 515. Además, la unidad 200 principal continúa con la etapa 517, y la unidad 200 principal puede proporcionar al usuario el resultado de la autenticación.

La unidad 300 de seguridad que recibe el resultado de autenticación confirma el resultado de autenticación en la etapa 519. De acuerdo con el resultado de la confirmación, si falla la autenticación, la unidad 300 de seguridad continúa con la etapa 521 y bloquea el modo seguro. Además, en la etapa 523, la unidad 300 de seguridad informa a la unidad 200 principal que el modo seguro está bloqueado. En consecuencia, en la etapa 525, la unidad 200 principal proporciona al usuario un mensaje de información que indica que el modo seguro está bloqueado y, en consecuencia, la solicitud de servicios de seguridad no puede realizarse. De acuerdo con el bloqueo del modo seguro, el dispositivo 100 de usuario normalmente puede realizar la operación de descargar o ejecutar un contenido normal, pero no puede realizar la operación de descargar o ejecutar un contenido seguro.

Si el resultado de la autenticación indica que la autenticación fue exitosa, la unidad 300 de seguridad continúa con la etapa 527 y normalmente ejecuta el modo seguro del dispositivo y, en consecuencia, accede al servidor 10 de servicios de contenido para que se realice la solicitud del usuario.

De esta manera, el nivel de seguridad con respecto al contenido seguro puede fortalecerse confirmando la autenticación sobre si el nivel de seguridad del dispositivo 100 de usuario es apropiado para el valor estándar en asociación con el servidor 10 de servicios de contenido digital, y bloqueando el operación del modo seguro si se determina que el nivel de seguridad del dispositivo 100 de usuario no es apropiado para el valor estándar.

De acuerdo con las realizaciones ejemplares de la presente invención descritas anteriormente, se supone que cuando está presente una solicitud de acceso al servidor 10 de servicios de contenido digital, la información de autenticación del dispositivo se recopila y se transmite al servidor 10 de servicios de contenido digital para que se realice un procedimiento de autenticación. Sin embargo, de acuerdo con otra realización ejemplar, la información de autenticación del dispositivo se recopila periódicamente y se transmite al servidor 10 de servicios de contenido digital para que se realice un procedimiento de autenticación. De lo contrario, cada vez que se produce la entrada de solicitud de servicios de seguridad, la información de autenticación del dispositivo se recopila y transmite al servidor 10 de servicios de contenido digital para que se realice un procedimiento de autenticación.

De acuerdo con una realización ejemplar de la presente invención, se realiza una descripción del aparato de tratamiento de datos de seguridad de acuerdo con la presente invención con un ejemplo de un aparato móvil, pero los expertos en la materia a los que pertenece la presente invención lo entienden fácilmente que la presente invención se puede aplicar a aparatos que usan un sistema operativo tal como un televisor digital, un decodificador, una ordenador personal y una ordenador portátil.

Además, los procedimientos de acuerdo con la realización ejemplar de la presente invención pueden realizarse mediante una forma de instrucción de programa que puede realizarse por diversos medios informáticos y puede almacenarse en un medio legible por ordenador no transitorio. El medio legible por ordenador no transitorio puede incluir instrucciones de programa, archivos de datos, estructuras de datos o similares por separado o en combinación. Las instrucciones del programa almacenadas en el medio pueden diseñarse y configurarse especialmente para la presente invención o pueden ser conocidas y estar disponibles para los expertos en el campo del software informático.

Las realizaciones ejemplares de la presente invención pueden proporcionar un procedimiento y un aparato para proteger el contenido digital reforzando la función de seguridad del dispositivo de un dispositivo de usuario que consume el contenido digital. Además, las realizaciones ejemplares de la presente invención pueden proporcionar un procedimiento y un aparato para proteger un contenido digital con un procedimiento reforzado para autenticar la función de seguridad del dispositivo de usuario.

Aunque se ha mostrado y descrito la invención con referencia a ciertas realizaciones ejemplares de la misma, se entenderá por los expertos en la materia que pueden realizarse diversos cambios en forma y detalles en la misma sin alejarse del alcance de la invención como se define por las reivindicaciones adjuntas y sus equivalentes.

REIVINDICACIONES

1. Un procedimiento de protección del contenido digital en un dispositivo de usuario que incluye un sistema operativo principal y un sistema operativo seguro, comprendiendo el procedimiento:

solicitar (405), por un sistema operativo principal, un sistema operativo seguro para identificar información de pirateo que indique si el sistema operativo principal es pirateado en respuesta a la recepción de una solicitud de ejecución de la aplicación;
identificar (407), mediante el sistema operativo seguro, la información de pirateo; y
determinar, mediante el sistema operativo seguro, si ejecutar la aplicación en el sistema operativo seguro en función de la información de pirateo;
en el que la aplicación no puede ejecutarse cuando la información de pirateo indica que el sistema operativo principal está pirateado (409); en el que el sistema operativo seguro solo es operado por un área segura de un procesador principal del dispositivo de usuario.

2. El procedimiento de la reivindicación 1, en el que la información de pirateo se obtiene en un procedimiento de arranque del dispositivo de usuario y se almacena en un área de almacenamiento segura a la que se bloquea el acceso por el sistema operativo principal.

3. Aparato para proteger el contenido digital de un dispositivo de usuario, comprendiendo el aparato:

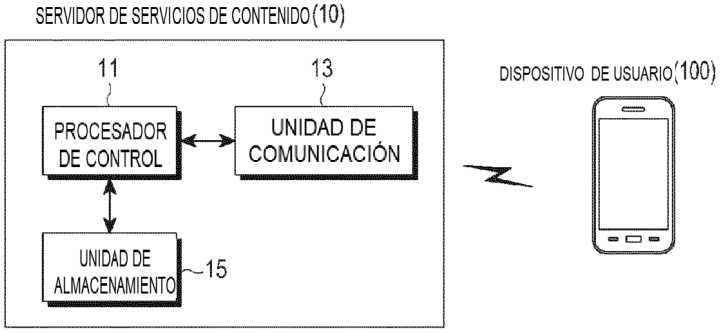
un controlador (110) configurado para:

solicitar, por un sistema operativo principal, un sistema operativo seguro para identificar información de pirateo que indique si el sistema operativo principal es pirateado en respuesta a la recepción de una solicitud de ejecución de la aplicación,
identificar la información de pirateo utilizando el sistema operativo seguro, y
determinar si se debe ejecutar la aplicación en el sistema operativo seguro en función de la información de pirateo utilizando el sistema operativo seguro;

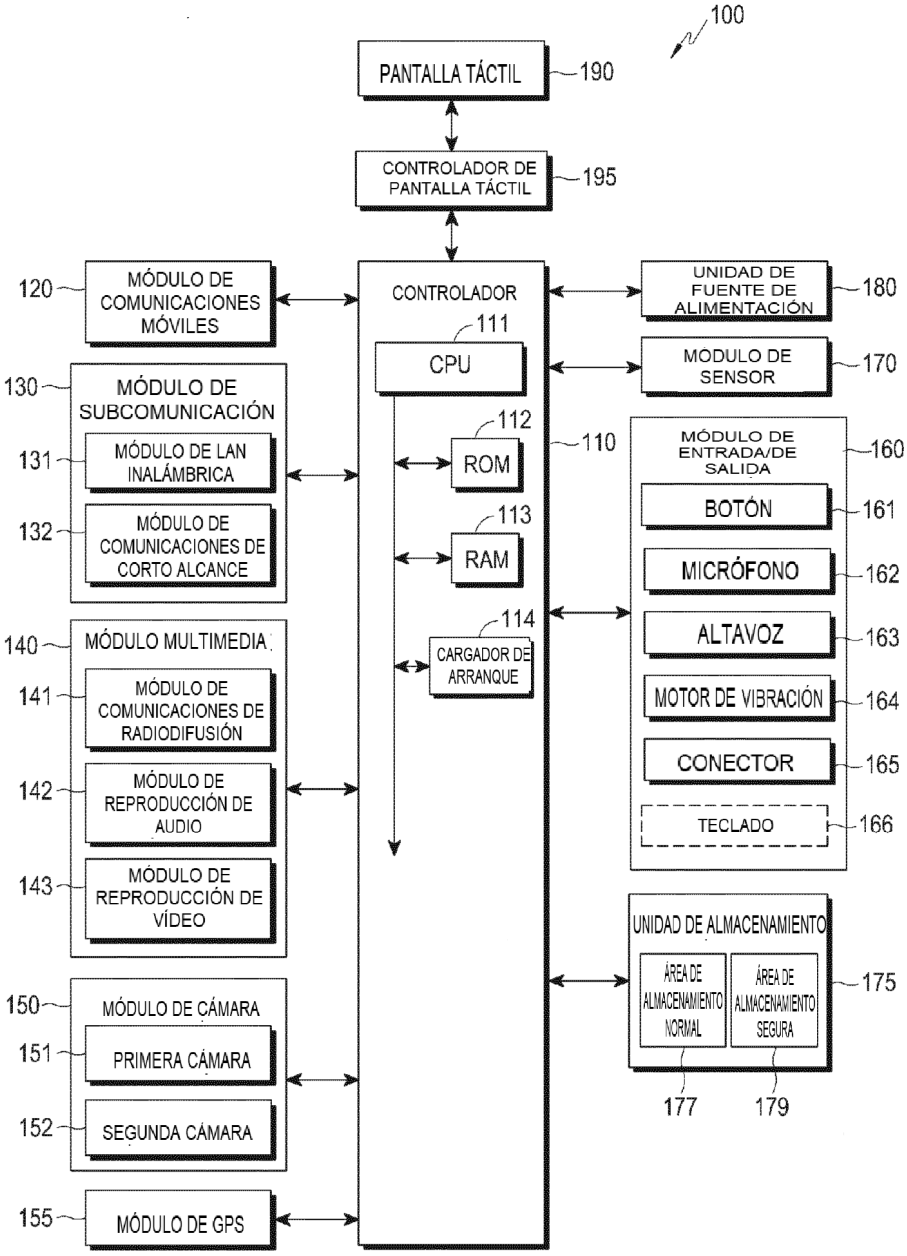
en el que el contenido digital seguro no puede ejecutarse cuando la información de pirateo indica que el sistema operativo principal está pirateado,
en el que el sistema operativo seguro solo es operado por un área segura del controlador.

4. El aparato de la reivindicación 4, en el que la información de pirateo se obtiene cuando el dispositivo de usuario se arranca y se almacena en un área de almacenamiento segura a la que se bloquea el acceso por el sistema operativo principal.

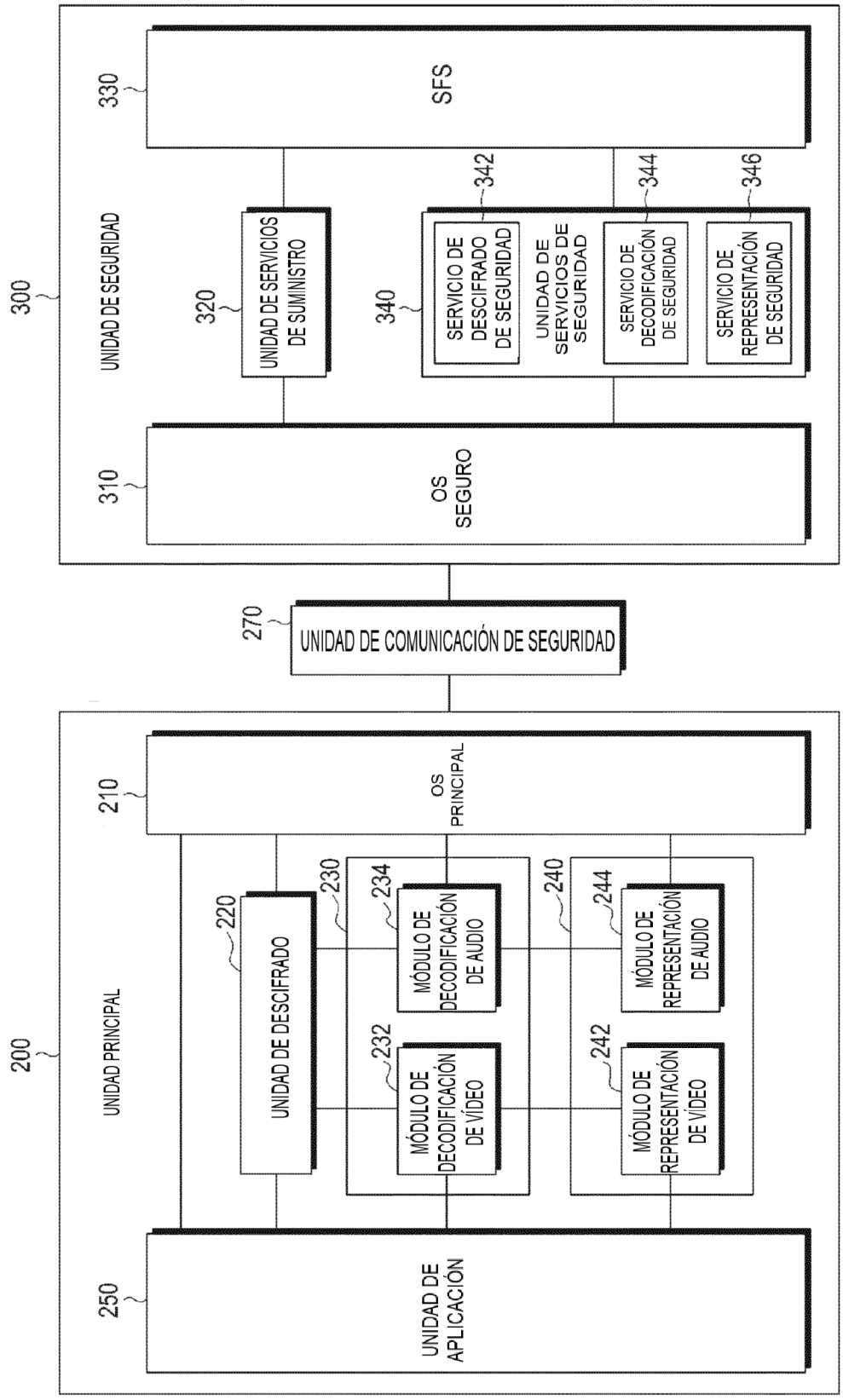
[Fig. 1]


SERVIDOR DE SERVICIOS DE CONTENIDO (10)
11
13
PROCESADOR DE CONTROL
UNIDAD DE COMUNICACIÓN
UNIDAD DE ALMACENAMIENTO
15
DISPOSITIVO DE USUARIO (100)

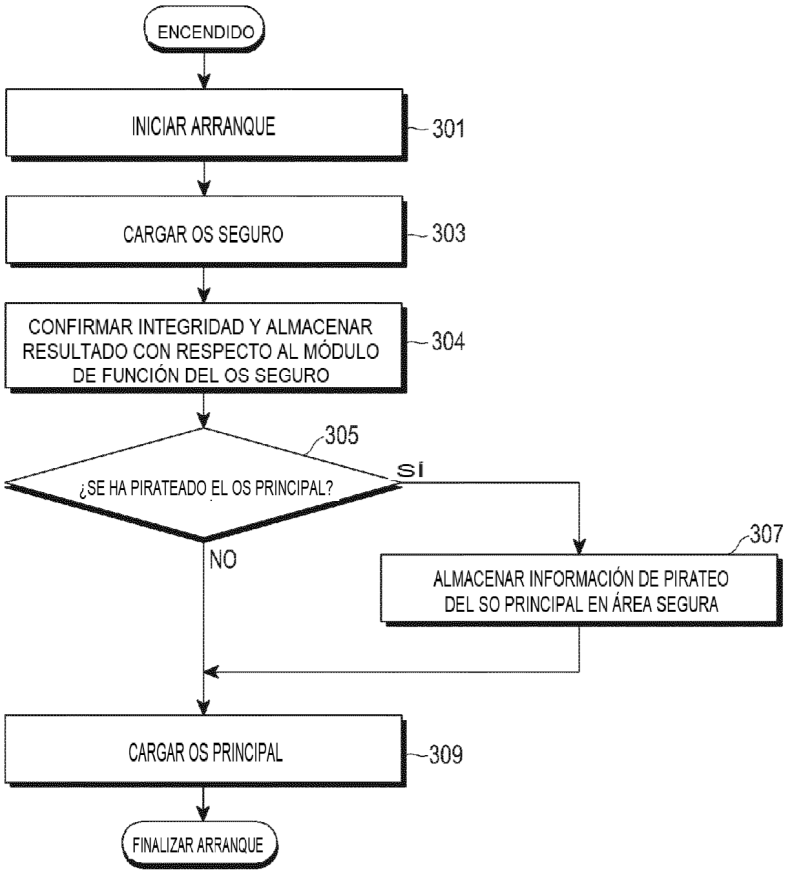
[Fig. 2]


100
PANTALLA TÁCTIL
190
CONTROLADOR DE PANTALLA TÁCTIL
195
CONTROLADOR
111
CPU
112
ROM
113
RAM
114
CARGADOR DE ARRANQUE
110
120
MÓDULO DE COMUNICACIONES MÓVILES
130
MÓDULO DE SUBCOMUNICACIÓN
131
MÓDULO DE LAN INALÁMBRICA
132
MÓDULO DE COMUNICACIONES DE CORTO ALCANCE
140
MÓDULO MULTIMEDIA
141
MÓDULO DE COMUNICACIONES DE RADIODIFUSIÓN
142
MÓDULO DE REPRODUCCIÓN DE AUDIO
143
MÓDULO DE REPRODUCCIÓN DE VÍDEO
150
MÓDULO DE CÁMARA
151
PRIMERA CÁMARA
152
SEGUNDA CÁMARA
155
MÓDULO DE GPS
UNIDAD DE FUENTE DE ALIMENTACIÓN
180
MODULO DE SENSOR
170
MÓDULO DE ENTRADA/DE SALIDA
160
BOTÓN
161
MICRÓFONO
162
ALTAVOZ
163
MOTOR DE VIBRACIÓN
164
CONECTOR
165
TECLADO
166
UNIDAD DE ALMACENAMIENTO
ÁREA DE ALMACENAMIENTO NORMAL
ÁREA DE ALMACENAMIENTO SEGURA
175
177
179

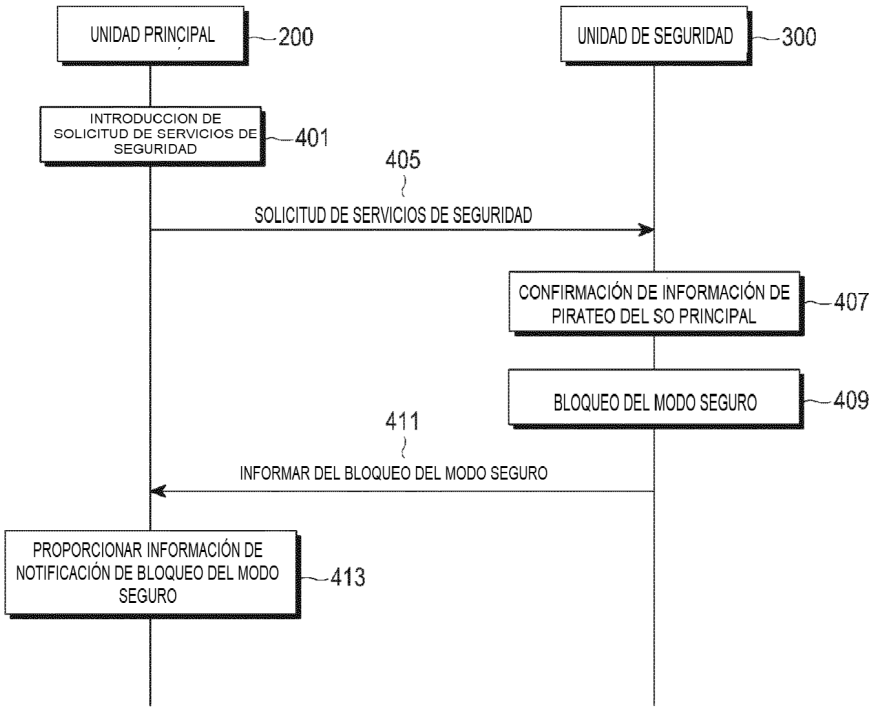
[Fig. 3]


300
UNIDAD DE SEGURIDAD
330
SFS
320
UNIDAD DE SERVICIOS DE SUMINISTRO
340
342
SERVICIO DE DESCIFRADO DE SEGURIDAD
UNIDAD DE SERVICIOS DE SEGURIDAD
344
SERVICIO DE DECODIFICACIÓN DE SEGURIDAD
346
SERVICIO DE REPRESENTACIÓN DE SEGURIDAD
310
OS SEGURO
270
UNIDAD DE COMUNICACIÓN DE SEGURIDAD
200
UNIDAD PRINCIPAL
210
OS PRINCIPAL
220
UNIDAD DE DESCIFRADO
230
234
MÓDULO DE DECODIFICACIÓN DE AUDIO
232
MÓDULO DE DECODIFICACIÓN DE VÍDEO
240
244
MÓDULO DE REPRESENTACIÓN DE AUDIO
242
MÓDULO DE REPRESENTACIÓN DE VÍDEO
250
UNIDAD DE APLICACIÓN

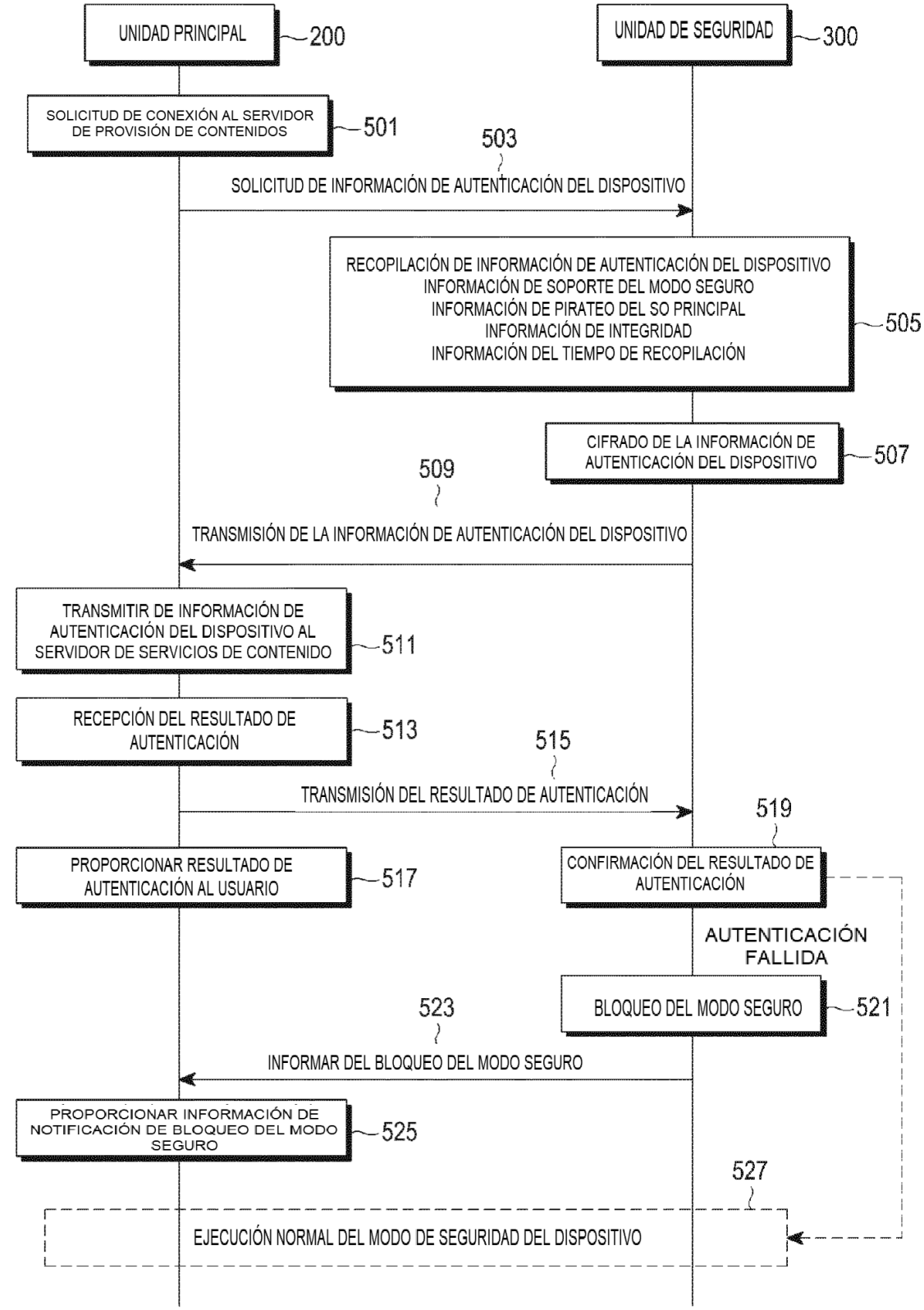
[Fig. 4]


ENCENDIDO
INICIAR ARRANQUE
301
CARGAR OS SEGURO
303
CONFIRMAR INTEGRIDAD Y ALMACENAR RESULTADO CON RESPECTO AL MÓDULO DE FUNCIÓN DEL OS SEGURO
304
305
¿SE HA PIRATEADO EL OS PRINCIPAL?
SÍ
NO
307
ALMACENAR INFORMACIÓN DE PIRATEO DEL SO PRINCIPAL EN ÁREA SEGURA
CARGAR OS PRINCIPAL
309
FINALIZAR ARRANQUE

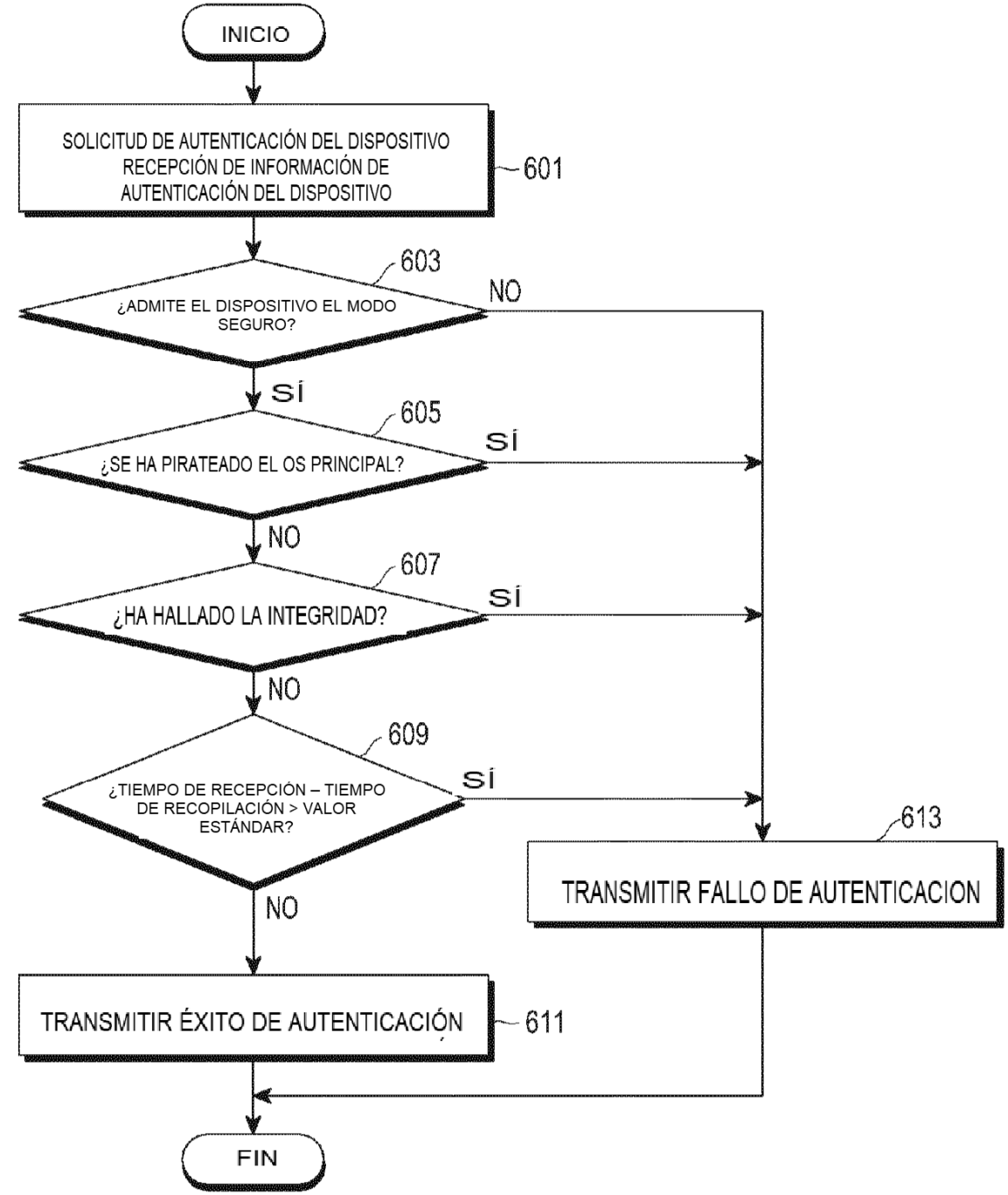
[Fig. 5]


UNIDAD PRINCIPAL
200
UNIDAD DE SEGURIDAD
300
INTRODUCCION DE SOLICITUD DE SERVICIOS DE SEGURIDAD
401
405
SOLICITUD DE SERVICIOS DE SEGURIDAD
CONFIRMACIÓN DE INFORMACIÓN DE PIRATEO DEL SO PRINCIPAL
407
BLOQUEO DEL MODO SEGURO
409
411
INFORMAR DEL BLOQUEO DEL MODO SEGURO
PROPORCIONAR INFORMACIÓN DE NOTIFICACIÓN DE BLOQUEO DEL MODO SEGURO
413

[Fig. 6]


UNIDAD PRINCIPAL
200
UNIDAD DE SEGURIDAD
300
SOLICITUD DE CONEXIÓN AL SERVIDOR DE PROVISIÓN DE CONTENIDOS
501
503
SOLICITUD DE INFORMACIÓN DE AUTENTICACIÓN DEL DISPOSITIVO
RECOPILACIÓN DE INFORMACIÓN DE AUTENTICACIÓN DEL DISPOSITIVO
INFORMACIÓN DE SOPORTE DEL MODO SEGURO
INFORMACIÓN DE PIRATEO DEL SO PRINCIPAL
INFORMACIÓN DE INTEGRIDAD
INFORMACIÓN DEL TIEMPO DE RECOPILACIÓN
505
CIFRADO DE LA INFORMACIÓN DE AUTENTICACIÓN DEL DISPOSITIVO
507
509
TRANSMISIÓN DE LA INFORMACIÓN DE AUTENTICACIÓN DEL DISPOSITIVO
TRANSMITIR DE INFORMACIÓN DE AUTENTICACIÓN DEL DISPOSITIVO AL SERVIDOR DE SERVICIOS DE CONTENIDO
511
RECEPCIÓN DEL RESULTADO DE AUTENTICACIÓN
513
515
TRANSMISIÓN DEL RESULTADO DE AUTENTICACIÓN
519
PROPORCIONAR RESULTADO DE AUTENTICACIÓN AL USUARIO
517
CONFIRMACIÓN DEL RESULTADO DE AUTENTICACIÓN
AUTENTICACIÓN FALLIDA
BLOQUEO DEL MODO SEGURO
521
523
INFORMAR DEL BLOQUEO DEL MODO SEGURO
PROPORCIONAR INFORMACIÓN DE NOTIFICACIÓN DE BLOQUEO DEL MODO SEGURO
525
527
EJECUCIÓN NORMAL DEL MODO DE SEGURIDAD DEL DISPOSITIVO

[Fig. 7]


INICIO
SOLICITUD DE AUTENTICACIÓN DEL DISPOSITIVO
RECEPCIÓN DE INFORMACIÓN DE AUTENTICACIÓN DEL DISPOSITIVO
601
603
¿ADMITE EL DISPOSITIVO EL MODO SEGURO?
NO
SÍ
605
¿SE HA PIRATEADO EL OS PRINCIPAL?
SÍ
NO
607
¿HA HALLADO LA INTEGRIDAD?
SÍ
NO
609
¿TIEMPO DE RECEPCIÓN – TIEMPO DE RECOPILACIÓN > VALOR ESTÁNDAR?
SÍ
NO
613
TRANSMITIR FALLO DE AUTENTICACION
TRANSMITIR ÉXITO DE AUTENTICACIÓN
611
FIN