(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 700 839**

(51) Int. CI.:

G06F 21/84 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2008 E 08103155 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.09.2018 EP 1975840**

(54) Título: **Procedimiento y dispositivo de visualización segura**

(30) Prioridad:

30.03.2007 FR 0702333

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.02.2019

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

ACHARI, KARIM y
LOHEAC, RONAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y dispositivo de visualización segura

La presente invención concierne a los equipos utilizados para efectuar acciones que implican o que conciernen a objetos de naturaleza confidencial. A título ilustrativo, se pueden citar las acciones de pago que implican un número de cuenta bancaria o que conciernen a una entrada de código confidencial o a un importe que deba cargarse o abonarse. Podrían citarse aún otras acciones tales como por ejemplo acciones de orden médico o civil, que conciernen a datos biológicos o patrimoniales propios de un individuo.

La tendencia actual es confiar preferentemente en equipos particularmente blindados contra las intrusiones o ataques diversos. Esto puede ser realizado a diversos niveles. A nivel de la constitución física del equipo, éste puede estar dentro de una caja inviolable, que resista a la intrusión (tamper resistant en inglés), o que deje traza visible de cualquier tentativa de sabotaje (tamper evident en inglés), o que incluso aporte una respuesta adecuada a una detección de intrusión (tamper responsive en inglés). A nivel de la constitución funcional, los datos sensibles están generalmente encriptados y su tratamiento es sometido a protocolos criptográficos. Se obtiene un grado de seguridad correcto utilizando exclusivamente circuitos electrónicos grabados en la masa. Si se desea mejorar la flexibilidad de utilización del equipo hay que tomar un mínimo de precauciones. Habitualmente se prefiere utilizar componentes de software aptos para ser puestos en práctica por medio de sistemas operativos seguros inaccesibles a terceros.

La flexibilidad de utilización ofrecida por los equipos anteriormente expuestos, continúa siendo limitada. En un modo rico en equipos electrónicos diversos tales como teléfonos móviles, asistentes personales o microrordenadores, se hace sentir una necesidad de flexibilidad comparable para los equipos desinados a ser utilizados para efectuar acciones que implican o que conciernen a objetos de naturaleza confidencial. Se sabe que los sistemas operativos denominados habitualmente abiertos en razón de su amplia difusión, ofrecen una abundancia apreciable de aplicaciones útiles y de fácil manejo que sería interesante poder poner en práctica para satisfacer esta necesidad. Esta apertura a otras aplicaciones de software que las rigurosamente seguras, tiene el inconveniente de poner en peligro la seguridad. Así, una aplicación malintencionada o contaminada por secuencias de ejecución malintencionadas, podría espiar y traicionar procesos seguros del equipo.

Existen soluciones que consisten en autorizar sistemáticamente solo aplicaciones debidamente firmadas, que deban ejecutarse en el equipo. El mecanismo bien conocido de las firmas hace intervenir generalmente certificados controlados por organismos de confianza para garantizar la integridad de la aplicación firmada. Este tipo de soluciones restringe de hecho la calidad de apertura del sistema operativo impidiendo también una ejecución de aplicación no necesariamente malintencionada y de la que habría sido agradable no privarse.

Existen también soluciones que consisten en hacer funcionar el equipo en dos modos diferentes, un modo totalmente abierto y un modo seguro que se reserva a aplicaciones seguras tales como aquéllas para efectuar acciones que implican o que conciernen a objetos de naturaleza confidencial.

La puesta en práctica de un sistema operativo abierto va acompañada generalmente de una pantalla gráfica para visualizar diversas informaciones. Dicha pantalla ofrece una posibilidad de visualización particularmente expresiva del modo seguro o no en el cual está el equipo. Para informar a un usuario del equipo del modo activo, un indicador luminoso tendría el inconveniente de tener que educar al usuario sobre la atención que debe prestarse a este indicador luminoso y sobre la interpretación que hay que darle para distinguir el modo abierto del modo seguro. Se puede igualmente pensar en visualizar un pictograma asociado o no a un texto en el idioma del usuario. Sin embargo, este tipo de visualización plantea un problema de compatibilidad, en términos de seguridad, con una apertura ofrecida a cualquier aplicación. En modo de funcionamiento abierto del terminal, una aplicación malintencionada podría corromper la visualización de modo que equivoque al usuario al visualizar un modo seguro en el cual el terminal no lo estaría. Una ausencia de certidumbre del modo en el cual se encuentra el terminal, presenta un inconveniente considerable.

Se podría pensar en utilizar dos pantallas, una para el modo abierto y una para el modo seguro. Además de los inconvenientes generados en términos de costes y de volumen, esta solución impondría al usuario vigilar dos pantallas diferentes. Esta solución sería también vulnerable a ciertos ataques consistentes en poner un ocultador en la pantalla asignada al modo seguro para equivocar a un usuario no advertido visualizando un falso modo seguro en la pantalla asignada al modo abierto. Los documentos US 2004/226041 y EP 1 677 190 A2 divulgan arquitecturas que permiten visualizar, en zonas diferentes de la pantalla, datos que provienen de varios sistemas, de los que al menos uno es considerado como « seguro ». El objetivo de la presente invención es facilitar un procedimiento de visualización que remedie los inconvenientes antes citados.

De modo más particular, la invención tiene por objeto facilitar un procedimiento de visualización que combine ergonomía y seguridad de la presentación de informaciones.

A tal fin, la presente invención propone un procedimiento de visualización seguro en una pantalla prevista para visualizar un primer conjunto de informaciones editadas por un primer sistema operativo. Este procedimiento comprende una etapa de filtrado en la cual un elemento asigna independientemente del primer sistema operativo, una primera zona de la pantalla al primer conjunto de informaciones y una segunda zona de la pantalla a un segundo

conjunto de informaciones editadas por un segundo sistema operativo. La etapa de filtrado esta combinada con una etapa de visualización real en la cual los dos conjuntos de informaciones son transferidos a la pantalla bajo el control exclusivo del segundo sistema operativo de manera que se produzca una visualización segura del segundo conjunto de informaciones.

Según modos de realización preferidos, la invención comprende una o varias de las características siguientes:

El primer sistema operativo es un sistema operativo abierto y el segundo sistema operativo es un sistema operativo seguro.

En una etapa de visualización virtual, el primer conjunto de informaciones es escrito en una memoria de vídeo virtual bajo el control del primer sistema operativo y cuyo contenido es accesible al segundo sistema operativo.

Según una alternativa, en una etapa de visualización virtual, el primer conjunto de informaciones se escribe en una memoria de vídeo real bajo el control del primer sistema operativo de modo que se puedan combinar primeras señales de vídeo que así resulten con segundas señales de vídeo que resulten del segundo conjunto de informaciones bajo el control del segundo sistema operativo.

El sistema operativo seguro está alojado en un componente de hardware que aísla el sistema operativo abierto en términos de acceso directo a la pantalla.

La segunda zona está situada en la pantalla en una primera posición fácilmente identificable por un usuario.

La primera posición se permuta alternativamente con una segunda posición anteriormente cubierta por la primera zona.

La segunda zona se superpone con o sin transparencia a la primera zona en una o varias posiciones en la pantalla.

Al menos una de las citadas posiciones es móvil sobre la pantalla.

Un dispositivo de visualización seguro en una pantalla prevista para visualizar un primer conjunto de informaciones editadas por un primer sistema operativo, comprende un filtro dispuesto para asignar independientemente del primer sistema operativo, una primera zona de la pantalla al primer conjunto de informaciones y una segunda zona de la pantalla a un segundo conjunto de informaciones editadas por un segundo sistema operativo y para transferir los dos conjuntos de informaciones a la pantalla bajo el control exclusivo del segundo sistema operativo de modo que se produzca una visualización segura del segundo conjunto de informaciones.

Particularmente, el primer sistema operativo del dispositivo es abierto y el segundo sistema operativo del dispositivo es seguro.

El filtro comprende en entrada una memoria de vídeo virtual dispuesta para recibir el primer conjunto de informaciones bajo el control del primer sistema operativo abierto y en salida una memoria de vídeo real para combinar los dos conjuntos de informaciones.

El filtro está dispuesto para recibir primeros datos de vídeo generados por un procesador estándar y segundo datos de vídeo generados por un procesador seguro, y para transferir a una memoria de vídeo una combinación de los primeros y de los segundos datos de vídeo.

El filtro está dispuesto para recibir primeras señales de vídeo que provienen de un primer controlador de vídeo y segundas señales de vídeo que provienen de un segundo controlador de vídeo, y para transferir a la pantalla una combinación de las primeras y de las segundas señales de vídeo.

El filtro está dispuesto para colocar la segunda zona en la pantalla en una primera posición fácilmente identificable por un usuario.

El filtro está dispuesto para permutar la citada primera posición alternativamente con una segunda posición anteriormente cubierta por la primera zona.

El filtro está dispuesto para superponer con o sin transparencia la segunda zona a la primera zona en una o varias posiciones en la pantalla.

El filtro está dispuesto para hacer mover al menos una de las citadas posiciones en la pantalla.

Otras características y ventajas de la invención se pondrán de manifiesto en la lectura de la descripción que sigue de un modo de realización preferido de la invención, dada a modo de ejemplo y refiriéndose a los dibujos anejos.

La figura 1 representa esquemáticamente un ejemplo de terminal en el cual es inútil poner en práctica la invención;

La figura 2 representa etapas de procedimiento de acuerdo con la invención;

La figura 3 representa un primer esquema de dispositivo de acuerdo con la invención;

La figura 4 representa un segundo esquema de dispositivo de acuerdo con la invención:

La figura 5 representa un tercer esquema del dispositivo de acuerdo con la invención.

Se describe ahora un ejemplo de puesta en práctica de dispositivo de visualización seguro en una pantalla prevista para visualizar un primer conjunto de informaciones editadas por un primer sistema operativo. Se observará en el dispositivo, un filtro dispuesto para asignar independientemente del primer sistema operativo, una primera zona de la pantalla al primer conjunto de informaciones y una segunda zona de la pantalla a un segundo conjunto de informaciones editadas por un segundo sistema operativo y para transferir los dos conjuntos de informaciones a la pantalla bajo el control exclusivo del segundo sistema operativo de modo que se produzca una visualización segura del segundo conjunto de informaciones.

Refiriéndose a la figura 1, un terminal 1 de pago comprende un teclado 2, una pantalla 3, un acoplador de comunicación 4 y un lector 5 de tarjeta inteligente, de tarjeta magnética o de tarjeta sin contacto. Un terminal de pago comprende también otros elementos no representados aquí tales como por ejemplo una impresora. La pantalla 3 esta ventajosamente equipada con un panel táctil que permite realizar funciones de teclas numéricas similares las de un teclado por presión sobre un lugar de la pantalla señalado por una imagen particular.

Por ejemplo, un usuario introduce su tarjeta inteligente en el lector 5 a través de una ranura, mira un importe de transacción visualizado en la pantalla 3 y si está de acuerdo en pagar esta cantidad, introduce su código PIN tecleando los números en las teclas del teclado y validando este código por medio de una tecla prevista a tal efecto. El terminal verifica entonces la validez del código dialogando con el chip y carga la cuenta del usuario dialogando además con un servidor distante, no representado, por medio de un acoplador de comunicación 4. El acoplador de comunicación 4 es de naturaleza alámbrica tal como se encuentran a veces en las cajas de grandes almacenes o de naturaleza inalámbrica por medio por ejemplo de ondas electromagnéticas.

En el caso de un teléfono móvil, con un chip residente en el teléfono y un acoplador de comunicación 4 constituido por su antena habitual, la invención es interesante para prevenirse por ejemplo contra aplicaciones malintencionadas que enviaran un código confidencial del usuario por ejemplo por mensaje de texto (SMS).

Es interesante equipar el terminal 1 con un sistema operativo abierto. El calificativo « abierto » debe tomarse en su sentido más amplio adoptado habitualmente en el mundo usuario. En otras palabras, el calificativo designa naturalmente los sistemas operativos realmente abiertos tales como son los sistemas UNIX y LINUX de origen. Aquí, el calificativo « abierto » designa también los sistemas de amplia difusión comercial tales como son por ejemplo diferentes versiones de Microsoft Windows™. Aunque los programas fuente del núcleo y numerosos primitivos de tales sistemas operativos siguen estando bajo el control de su propietario, el sentido común les atribuye el calificativo « abierto » por estar ampliamente difundidos suficientes accesos al sistema operativo. Esta amplia difusión permite desarrollar numerosas aplicaciones y numerosas plataformas de hardware que enriquecen de modo apreciable la oferta de productos y que de algún modo establecen un amplio colectivo de usuarios y de desarrolladores que comparten entornos comunes. Actualmente tales sistemas operativos se han acostumbrado a desarrollar interfaces gráficas tomadas por su fácil manejo y su flexibilidad. Se puede entonces integrar accesos a aplicaciones denominadas del comercio tales como está representado en la figura 1, una hoja de cálculo, un calculador, una aplicación de telecomunicación o diversas aplicaciones multimedia. Sin embargo, la apertura de tales sistemas operativos a numerosas aplicaciones tiene la contrapartida de ofrecer también un acceso a aplicaciones malintencionadas tales como softwares espías y otros virus desagradables.

Con el fin de permitir adquirir, tatar y comunicar por vía de visualización o de transmisión datos sensibles sin temor a intromisiones por una aplicación malintencionada, el equipo pasa a un modo seguro que éste muestra en un rótulo o un pictograma. El rótulo o el pictograma tienen la función de indicar el modo seguro o no seguro en el cual está el terminal. En este caso el rótulo es mostrado por ejemplo en la parte inferior de la pantalla 3 que constituye una posición fácilmente identificable por el usuario. Hay otras posiciones fácilmente identificables por ejemplo en la parte superior, en la derecha, en la izquierda o moviéndose de arriba abajo de la pantalla 3. Como tipos de datos sensibles en el caso de un terminal de pago, se piensa naturalmente en los datos de cuenta y en el código de tarjeta bancaria. Se puede pensar también en otros tipos de datos tales como de modo no limitativo datos médicos, datos biométricos o sociales.

Hay muchas ventajas en visualizar una tira, un rótulo o cualquier otro grafismo en la pantalla en lugar de encender o apagar un indicador luminoso opcionalmente de diferentes colores. El indicador luminoso correría el riesgo de ser fácilmente enmascarado. Por otra parte, el indicador luminoso necesitaría que el usuario conociese los significados sin ambigüedad mientras que en una tira, basta inscribir un texto claro « modo seguro » o « modo no seguro » acompañado opcionalmente con signos conocidos tales como candado abierto o cerrado. Una visualización en pantalla no es fija, se puede adaptar el idioma o el tamaño de las fuentes en función de los usuarios. Por otra parte, los usuarios, habituados a dirigir su mirada a la pantalla, encuentran un entorno cómodo que les evita distraer su mirada hacia otros lugares del equipo. Gracias a la protección ofrecida por la invención, la modularidad que acaba de ser expuesta puede ser puesta en práctica con un grado de seguridad altamente apreciable.

Refiriéndose a la figura 2, se explican ahora etapas preferidas para poner en práctica un procedimiento de visualización seguro en una pantalla prevista para visualizar un primer conjunto de informaciones editadas por un primer sistema operativo. Se observará una etapa de filtrado en la cual un elemento asigna independientemente del primer sistema operativo, una primera zona de la pantalla al primer conjunto de informaciones y una segunda zona de la pantalla a un segundo conjunto de informaciones editadas por un segundo sistema operativo. La etapa de filtrado está combinada con una etapa de visualización real en la cual los dos conjuntos de informaciones son transferidos a la pantalla bajo control exclusivo del segundo sistema operativo de modo que se produzca una visualización segura del segundo conjunto de informaciones.

De este modo, el segundo sistema operativo puede ser un obstáculo para una corrupción de la visualización del segundo conjunto de informaciones por una aplicación ejecutada en el entorno del primer sistema operativo.

Para poner en práctica el procedimiento, se utiliza una pantalla tal como la pantalla 3 habitualmente prevista para visualizar un conjunto de informaciones editadas por un sistema operativo abierto. Estas informaciones resultan de aplicaciones que están instaladas para utilizar los recursos del sistema operativo cuyo calificativo « abierto », como se ha visto anteriormente, se basa esencialmente en el hecho de que se difunden suficientes componentes para permitir desarrollar un amplio abanico de aplicaciones que, generalmente en ausencia de evaluación desde el punto de vista de la seguridad, no ofrecen ninguna garantía en cuanto a la utilización que las mismas hacen de los recursos del sistema. Una ventaja sin embargo es que la visualización de las informaciones se beneficia de un grafismo familiar al usuario y permite numerosas intervenciones del usuario por medio de un teclado 2 o de características táctiles de la propia pantalla.

En una etapa 10 habitual, el sistema operativo abierto (SEO) está a la escucha permanente de diferentes interrupciones o interacciones de origen software o hardware. Las interacciones de origen hardware son las que conciernen a periféricos, en el sentido amplio, listados por un programa habitualmente activado durante el lanzamiento del sistema operativo y denominado BIOS, acrónimo de la expresión inglesa « Basic Input Output System » para expresar « Sistema de Base de Entradas Salidas ».

Una transición 11 validada en cada interacción de una aplicación para visualizar informaciones, activa una etapa 12. La etapa 12 es ejecutada generalmente por un controlador de pantalla (driver en inglés) instalado con el SEO. Habitualmente, el controlador de pantalla transcribe las informaciones recibidas en una memoria de vídeo periódicamente explorada por un circuito de mando de la pantalla. Con el fin de preparar las etapas siguientes del procedimiento, el controlador de pantalla del SEO está configurado para transcribir las informaciones recibidas en una memoria de vídeo virtual. La memoria de vídeo virtual es por ejemplo simplemente una zona reservada de la memoria controlada por el SEO hacia la cual el controlador de pantalla del SEO configurado a tal efecto, encamina los datos que haya que visualizar. Con el fin de poder ejecutar la etapa de filtrado, el contenido de la memoria de vídeo virtual es hecho accesible al menos en lectura al sistema operativo seguro. En la etapa 12, la visualización controlada del SEO, es entonces de naturaleza virtual. Por oposición a una visualización real en la que la imagen reproducida en la pantalla es la efectivamente generada bajo control del SEO, en el caso de una visualización virtual no se reproduce una imagen en la pantalla tal como es generada. Otra manera de preparar las etapas siguientes del procedimiento es configurar el controlador de pantalla para transcribir las informaciones recibidas en una memoria de vídeo real conectada a un controlador de vídeo. Contrariamente al hábito en que el controlador de vídeo está conectado a la pantalla, el controlador de vídeo está conectado a un componente de tratamiento de la información de modo que en la etapa 12, la visualización bajo control del SEO, es aquí todavía de naturaleza virtual.

En la etapa 20 independiente del SEO, un sistema operativo seguro (SES), está en escucha permanente de diferentes interrupciones o interacciones de origen software o hardware. El SES se distingue del SEO en que su microprograma (firmware en inglés), es de difusión restringida y controlada. Se puede obtener un sistema seguro utilizando un sistema propietario o un sistema de base abierto pero montado sobre una capa de software que aísla el sistema de acceso a aplicaciones. Se apreciará el grado de seguridad ofrecido por el SES porque un desarrollo de aplicaciones adaptadas al SES, necesita pertenecer a un círculo limitado de personas autorizadas y utilizar herramientas de desarrollo específicas y adecuadas.

En una etapa de filtrado, el sistema operativo seguro asigna independientemente del sistema operativo abierto, en una subcapa 22 una primera zona de la pantalla al primer conjunto de informaciones y en una subetapa 24 una segunda zona de la pantalla a un segundo conjunto de informaciones editadas por el sistema operativo seguro.

La subetapa 22 es activada por una transición 21 validada por la recepción de datos de visualización que provienen del SEO y la subcapa 24 es activada por una transición 23 validada por la recepción de los datos de visualización que provienen del SES.

Si por ejemplo la pantalla 3 tiene una superficie de visualización de 640 pixeles por 480 pixeles, una superficie reducida de visualización de 640 pixeles por 455 pixeles es asignada a la zona 3a y este valor reducido de superficie es comunicado al SEO como la superficie total de visualización disponible. La superficie restante de visualización de 640 pixeles por 25 pixeles es asignada entonces a la zona 3b sin que el SEO lo conozca. Naturalmente los valores dados anteriormente son solo a modo de ilustración y se comprenderá que el realizador de la invención sigue siendo libre de

elegir cualesquiera otros valores. Como se verá en lo que sigue, es también posible asignar la totalidad de la superficie de la pantalla a la zona 3a y asignar partes de pantalla no necesariamente conexas a la zona 3b.

Una etapa 26 de visualización real es activada por una transición 25 validada bajo control exclusivo del sistema operativo seguro. En la etapa 26 los dos conjuntos de informaciones son transferidos a la pantalla de modo que el segundo conjunto de informaciones es visualizado de modo seguro.

Con el fin de mejorar la seguridad del procedimiento, el sistema operativo seguro está ventajosamente alojado en un componente de hardware que aísla el sistema operativo abierto en términos de acceso directo a la pantalla.

La situación de cada una de las zonas en la pantalla resulta de un direccionamiento en memoria de vídeo real efectuado en etapa 26. Tomando el ejemplo numérico anteriormente enunciado simplemente para ilustrar el propósito, el segundo conjunto de información es por ejemplo dirigido a las primeras líneas de la memoria de vídeo real que corresponden a los 640 pixeles por 25 pixeles de la parte inferior de la pantalla y el primer conjunto de información es dirigido entonces a las líneas siguientes de la memoria de vídeo real que corresponden a los 640 pixeles por 455 pixeles de la parte superior de la pantalla. Así, la situación de la segunda zona en esta primera posición en la parte inferior de la pantalla es fácilmente identificable por un usuario.

En el caso en que la virtualidad de la visualización se obtenga no por encaminamiento de las informaciones de imagen a la entrada de la memoria de vídeo sino por encaminamiento a la salida del controlador de vídeo, se interviene no sobre las direcciones sino sobre las señales que son utilizadas para la actualización de la pantalla, típicamente las señales de reloj, las señales de control y/o las señales de datos.

Ninguna aplicación malintencionada que utilice los recursos ofrecidos por un primer sistema operativo, en este caso el sistema operativo abierto, puede acceder a la segunda zona que está reservada a un segundo sistema operativo, en este caso el sistema operativo seguro. Resultan buenas cualidades de credibilidad sobre el contenido visualizado en la segunda zona.

En un primer modo de realización preferido, el procedimiento de visualización es mejorado para luchar contra un ataque que consistiera en cubrir la parte inferior de la pantalla con una cinta adhesiva o por cualquier otro medio y en lanzar después una aplicación malintencionada que visualizara una falsa tira en la parte inferior de la primera zona de modo que equivoque al usuario. La mejora consiste en permutar alternativamente la primera posición con una segunda posición anteriormente cubierta por la primera zona. Esto es realizable por ejemplo invirtiendo el orden de direccionamiento en la memoria de vídeo real. Esto es apropiado para desanimar a los defraudadores porque ocultar ahora la parte superior y la parte inferior de la pantalla conduciría a una superficie útil de visualización considerablemente reducida. Además, el desplazamiento de la primera zona que resulta de la permutación tendría por efecto enmascarar alternativamente una parte de esta zona. Para evitar fatigar inútilmente al usuario con el movimiento de la tira de seguridad, se puede prever una frecuencia de alternancia bastante baja que vaya del minuto a la semana pero de modo preferente, aleatoria o seudoaleatoria y por consiguiente imprevisible para un defraudador. Asimismo, la alternancia de las posiciones en la pantalla no está limitada a la parte superior y a la parte inferior sino que también puede seguir de modo aleatorio o circular un lado cualquiera en la periferia de la pantalla tanto en la izquierda o la derecha como en la parte superior o en la parte inferior.

En un segundo modo de realización preferido, la mejora consiste en no restringir el tamaño de la primera zona en comparación con el de la pantalla. La segunda zona es entonces visualizada de modo transparente en sobreimpresión de uno o varios lugares de la primera zona. Esto permite disponer de la extensión más amplia para visualizar la imagen generada bajo control del SEO. Esto ofrece también más posibilidades para visualizar la imagen generada bajo control del SES. Se puede por ejemplo hacer que se mueva un rótulo de arriba abajo de la pantalla para indicar el modo seguro en el cual se encuentra o hacer que se muevan uno o varios pictogramas en diferentes lugares de la pantalla. Un grado de transparencia puede ser modulado por medio de coeficientes cuya configuración va del brillo, a la ocultación total (ausencia de transparencia). Las zonas (3a) y (3b) pueden así tener una intersección no nula y de valor cualquiera.

Refiriéndose a la figura 3, un equipo electrónico tal como el terminal 1 de la figura 1, comprende una memoria 7 en todo o en parte de tipo memoria viva y un procesador estándar 6, es decir un procesador disponible en el comercio. La disponibilidad en el comercio de la documentación que acompaña generalmente al procesador permite sin embargo estudiar sus vulnerabilidades en perjuicio de la seguridad. El procesador 6 está conectado con la memoria 7 de modo que puede tratar los datos que están almacenados en la misma. El término « dato » debe ser tomado en su más amplia acepción y puede designar tanto una dirección, un registro de control o una instrucción como un valor de variable.

Un circuito específico 33, por ejemplo de tipo circuito integrado para aplicación específica (ASIC acrónimo inglés de Application Specific Integrated Circuit) o combinación de circuitos integrados específicos y/o estándares, pone en práctica un sistema operativo seguro. Mecanismos no descritos aquí pueden permitir detectar modificaciones de hardware o de software del SEO o asegurarse de un funcionamiento conforme a lo que se espera del SES. A modo de ejemplo, el sistema operativo seguro (SES) está por ejemplo microprogramado en el propio circuito específico 33 o en una memoria grabada reinscriptible (no representada) unida físicamente al circuito específico 33. El SES controla la señal de reinicialización del procesador 6 de modo que se bloquee en caso de detección de un ataque. El circuito

específico 33 accede por otra parte a un bus 37 de puertos de acceso de pruebas, por ejemplo de tipo JTAG (acrónimo inglés de Joint Test Action Group) conectado al procesador 6. El acceso del circuito 33 al bus 37 permite al SES instalar y lanzar un núcleo de sistema operativo abierto (SEO) 10 en memoria 7 para ser ejecutado por el procesador 6. El bus 37 es utilizado también por el SES para autenticar el núcleo de SEO en el lanzamiento (boot en inglés). El SEO está configurado a su vez para validar si es necesario firmas de aplicaciones cargadas en memoria 7. En caso de detección de un ataque del SEO, es posible por ejemplo dejar que el SES deje de compartir con el SEO de modo que tome un control completo de la visualización, o neutralizar el SEO o recargar una versión de SEO por defecto. Esto aumenta todavía la seguridad de utilización.

La memoria 7 contiene también controladores de periféricos para permitir al SEO controlar periféricos de menor sensibilidad tales como la gestión de potencia, propiedades audio o una unión serie compartiendo opcionalmente algunos con el SES si es necesario, por ejemplo conexiones inalámbricas 4, un acoplador Ethernet o la visualización en la pantalla 3 a propósito de la cual se darán precisiones suplementarias en lo que sigue de la descripción.

Los periféricos más sensibles tales como por ejemplo el lector de tarjeta 5, un detector biométrico, si existe, teclas numéricas del teclado 2 o de la pantalla táctil 3, están bajo el control exclusivo del SES. El SES controla también otros periféricos compartiéndoles con el SEO, estos son por ejemplo una impresora, teclas funcionales del teclado 2, un módem o la batería de reserva.

El circuito específico 33 dispone de un mando 35 para conmutar por medio de un conmutador 27, los datos intercambiados con un panel táctil combinado con la pantalla u opcionalmente ciertas teclas del teclado 2 o hacia una conexión 8 con destino al SEO, o hacia una unión 9 con destino al SES. En la figura 3, la conexión 9 está empalmada al circuito específico 33 para el caso en que éste aloje el SES.

Una alternativa posible a la arquitectura de hardware descrita refiriéndose a la figura 3 es realizable funcionalmente alojando el SES en memoria 7. Es entonces preferible en este caso dar al SES un control altamente seguro de la memoria 7, por ejemplo por medio de una estructura de protección en anillos en un modelo similar al enseñado por la patente EP0208192B1 o por medio de una unidad de gestión de memoria (MMU, de Memory Management Unit en inglés). Según esta alternativa, el conmutador 27 es realizable en forma de software en una capa segura del SES.

El control del panel táctil es requisado por el SES para detección de un evento que puede dar lugar a un basculamiento a modo seguro como por ejemplo una introducción de tarjeta inteligente en el lector 5 o un paso de tarjeta de pista magnética. Se observará que no es necesario introducir la tarjeta en una ranura como por ejemplo en el caso de una tarjeta sin contacto. Según la tecnología empleada, son posibles diferentes variantes para permitir al SES requisar el panel táctil. Se puede citar un control permanente del panel táctil por el SES, incluso en modo no seguro en el transcurso del cual el SES retransmite entonces pura y simplemente las señales que provienen del panel táctil al SEO. Este control permanente permite entonces al SES no retransmitir las señales al SEO en modo seguro. Se puede citar todavía una conmutación del panel táctil hacia el SEO en modo no seguro y hacia el SES en modo seguro.

Estando prevista la pantalla 3 para visualizar un conjunto de informaciones editadas por el sistema operativo 10, el SEO dispone de un controlador de pantalla 13 que reside en memoria 7. Habitualmente, dicho controlador de pantalla está configurado para ordenar las informaciones en una memoria de vídeo de visualización 34 cuya exploración periódica lleva las informaciones en la pantalla 3 a imagen de un espejo.

Un mecanismo interesante para poner en práctica el dispositivo de visualización seguro según la invención, consiste en impedir al SEO un acceso directo a la memoria de vídeo 34 real. El controlador de pantalla 13 está configurado entonces de modo que las informaciones editadas por el SEO sean enviadas a una memoria de vídeo virtual (MVV) 28.

La memoria de vídeo virtual 28 es utilizada entonces a la entrada de un filtro dispuesto para asignar independientemente del sistema operativo abierto, una primera zona 3a de la pantalla al primer conjunto de informaciones editadas por el sistema operativo abierto. El filtro permite asignar una segunda zona 3b de la pantalla a un segundo conjunto de informaciones editadas por el sistema operativo seguro.

El filtro puede ser realizado de diferentes maneras. A modo ilustrativo, la utilización de un mecanismo de acceso directo a memoria 30 (DMA de Direct Memory Access en inglés) permite acelerar la transferencia desde la memoria de vídeo virtual 28 hasta la pantalla pasando por la memoria de vídeo real 34. Otras maneras de realizar el filtro serán expuestas más adelante en la descripción.

Un mando 36 del DMA bajo control del SES permite disponer la memoria de vídeo real 34 para transferir los dos conjuntos de informaciones a la pantalla bajo control exclusivo del sistema operativo seguro. De este modo, se produce una visualización segura del segundo conjunto de informaciones porque siendo la segunda zona 3b inaccesible al SEO, ninguna aplicación ejecutable por medio del SEO puede introducir informaciones falsas en la misma.

Refiriéndose a la figura 3, el aseguramiento del dispositivo de visualización resulta de la combinación de la memoria de vídeo virtual 28, del filtro que asocia el circuito especifico 33 a un acceso de memoria directo a la memoria 28 y de la memoria virtual real 34 que constituyen cada uno un componente de hardware dispuesto para aislar el sistema operativo abierto en términos de acceso directo a la pantalla 3 por medio del sistema operativo seguro. Este modo de

realización ofrece un mejor grado de confianza que el otorgado naturalmente a un modo de realización de software porque ningún fallo, ninguna intrusión de software puede permitir que una aplicación malintencionada del mundo abierto acceda a la zona protegida de la pantalla.

En el caso de la alternativa anteriormente expuesta en la que interviene un mecanismo de tipo protección en anillos o por MMU, se puede concebir una realización del filtro en forma de software en una capa de alto grado de protección de la estructura en anillos o de control MMU. Asociado o no a la gestión del teclado, el SES asigna por ejemplo las diferentes zonas por traslación de direcciones.

En la figura 1 se observa que la segunda zona está materializada por una tira situada en la parte inferior de la pantalla 3 que constituye una primera posición fácilmente identificable por un usuario. Si la pantalla es una reproducción línea a línea de la memoria 34, el SES controla el DMA de modo que recopia las informaciones extraídas de la memoria 25 en direcciones en cabeza de memoria 34 y las informaciones que señalan el modo seguro o no seguro en direcciones en cola de memoria 34. Gracias al dispositivo expuesto anteriormente, se comprenderá que el SES puede requerir otras zonas en el interior de la normalmente asignada al SEO, por ejemplo para incrustar una ventana de entrada de código secreto, naturalmente cuando el SES manda visualizar el modo seguro de modo que levante cualquier ambigüedad sobre la confianza que haya que otorgar a la ventana de entrada.

Para permutar alternativamente la primera posición con una segunda posición anteriormente cubierta por la primera zona, basta que el SES modifique simplemente las direcciones de la memoria 34 a las cuales transferir las informaciones editadas por el SEO y las editadas por el SES. Cuando la zona 3b pasa de la parte inferior de la pantalla a la parte superior de la pantalla, la zona 3a es desplazada hacia abajo y recíprocamente. La frecuencia de permutación es suficientemente baja para no perturbar al usuario. Ventajosamente, la frecuencia de permutación es configurable con posibilidad de ser complementada con una composición aleatoria o seudoaleatoria y/o una detección de actividad del usuario de modo que se fije un posicionamiento en curso de interacción del usuario con una cualquiera de las zonas de la pantalla. El panel táctil es muestreado en forma de mediciones por el sistema operativo, que establece una correspondencia con una región presionada o tocada de la pantalla. Esto permite por ejemplo asociar un mando a una imagen o reconocer una firma manuscrita trazada por el usuario en la pantalla. Este lugar es identificado por una parte por las coordenadas de la presión detectada sobre la pantalla, es decir sobre el panel táctil y por otra las coordenadas de la imagen en la pantalla, es decir de modo más exacto en la primera zona asignada al SEO. Un desplazamiento de la primera zona sobre la pantalla provoca una traslación de las coordenadas reales de la imagen. Para poner en concordancia las coordenadas de la imagen con las del punto de presión, el dispositivo está dispuesto para trasladar las coordenadas del punto de presión en función de la posición de la primera zona de modo que se restituya la concordancia del punto de presión con la imagen que conviene.

El mecanismo que acaba de describirse muestra una ventaja suplementaria de una visualización de la segunda zona por superposición a la primera zona. Siendo las coordenadas virtuales, es decir las coordenadas tales como son vistas por el sistema operativo, gracias a la visualización por superposición, las mismas que las coordenadas reales de visualización en la pantalla, no es necesario poner en práctica un mecanismo complicado para restituir la concordancia del punto de presión en un panel táctil con la imagen que conviene.

Refiriéndose a la figura 4, el dispositivo comprende un primer componente estándar en el cual el procesador estándar 6 está conectado a la memoria 7 por un bus de sistema 19. Un elemento DMA 16 conectado al bus 19 permite hacer transferencias de la memoria 7 hacia una memoria de vídeo 14 conectada a su vez al bus 19. Por otra parte, la memoria de vídeo 14 está conectada a un controlador de vídeo 15 previsto habitualmente para ser conectado a una pantalla. El procesador estándar 6 está previsto para ejecutar un sistema operativo abierto.

El dispositivo comprende también un segundo componente similar al precedente y en el cual un bus 29 une una memoria viva 32 a una memoria de vídeo 34 que está conectada a un controlador de vídeo 38. A diferencia del primer componente, un procesador seguro 31 es el que está conectado al bus 29. Es posible elegir entre varios medios para asegurar un procesador o combinar todos o parte de estos diversos medios. Un primer medio consiste en concebir el propio procesador con una arquitectura de tipo propietario. Un segundo medio consiste en proteger el conjunto del segundo componente en una caja físicamente resistente a las intrusiones o capaz de detectarlas y de aportar opcionalmente una respuesta adecuada. Un tercer medio consiste en dotar al procesador de un sistema operativo seguro tal como el definido anteriormente.

En la puesta en práctica explicada refiriéndose a la figura 4, el controlador de vídeo 38 controla la totalidad de la pantalla 3 transmitiéndole de manera conocida una señal de reloj para la sincronización, una señal de trama y una señal de pixel en una trama que codifica componentes de luz y/o de color. Un filtro 17 está conectado por una parte al bus 19 y por otra al bus 29. El elemento DMA 16 está configurado de modo que transfiera los datos de vídeo hacia el filtro 17 en lugar de transferirles hacia la memoria de vídeo 14. El filtro 17 es controlado por el procesador 31 (control simbolizado por la flecha de sentido único que va del bus 29 hacia el filtro 17) de modo que combina los datos de vídeo generados bajo control del sistema operativo abierto con los datos de vídeo generados bajo control del sistema operativo seguro. Los datos de vídeo generados bajo control del sistema operativo abierto son los que provienen del bus 19 y los datos de vídeo generados bajo control del sistema operativo seguro son los que provienen del bus 29. Según la variante retenida entre las anteriormente expuestas, la combinación puede consistir en:

- asignar coordenadas de visualización X, Y distintas a los dos tipos de datos de vídeo (provenientes del bus 19 y provenientes del bus 29), de modo fijo o móvil;

- compartir ciertas coordenadas de visualización X, Y para al menos una parte de los dos tipos de datos de vídeo al mezclar las señales, por ejemplo añadiéndolas de modo que se cree un efecto de sobreimpresión transparente, en este caso también de modo fijo o móvil.

A medida que se produce la combinación de los datos de vídeo, el filtro 17 les transmite a la memoria de vídeo 34 por el bus 29. Con el fin de mejorar la fluidez de la imagen y aligerar el procesador 31, un elemento DMA 18 está configurado para transferir hacia el filtro 17 datos de vídeo que provienen de la memoria 32 o directamente del procesador 31 y para transferir hacia la memoria 34 los datos de vídeo combinados por el filtro 17.

En la puesta en práctica explicada refiriéndose a la figura 5, las señales generadas por el controlador de vídeo 38 son encaminadas hacia un filtro 39. Asimismo, las señales generadas por el controlador de vídeo 15 son encaminadas hacia el filtro 39. El elemento DMA 16 está configurado de modo estándar para transferir los datos de vídeo hacia la memoria de vídeo 14. El filtro 39 es controlado por el procesador 31 (control simbolizado por la flecha en sentido único que va del bus 29 hacia el filtro 39) de modo que se combinen señales de vídeo generadas bajo control del sistema operativo abierto con señales de vídeo generadas bajo control del sistema operativo seguro. Las señales de vídeo generadas bajo control del sistema operativo abierto son las que provienen de controlador de vídeo 15 y las señales de vídeo generadas bajo control del sistema operativo seguro son las que provienen del controlador de vídeo 38. Según la variante retenida entre las anteriormente expuestas, la combinación puede consistir en:

- actuar de manera constante o variable sobre la señal de reloj de modo que se conmuten las dos señales de vídeo (provenientes del controlador 15 y provenientes del controlador 38), en partes distintas de la pantalla 3;

- para cada uno o todos los pixeles de la pantalla 3, mezclar las señales, por ejemplo añadiéndolas de modo que se cree un efecto de sobreimpresión transparente. La movilidad del pictograma o de la tira de seguridad igual que el posicionamiento de una ventana de entrada segura puede entonces ser gestionada completamente por una aplicación bajo control del SES visualizando su imagen sobre fondo neutro, disponiendo los dos sistemas operativos de la totalidad de la superficie de visualización.

A medida que se produce la combinación de las señales de vídeo, el filtro 39 las transmite a la pantalla 3 igual que lo hubiera hecho un controlador de vídeo. Esta puesta en práctica permite explotar la totalidad de las funcionalidades de visualización del primer componente tales como por ejemplo funcionalidades de aceleración gráfica o de visualización 3D previstas de base en tándem con el controlador de vídeo 15 en numerosos componentes del comercio.

En términos de industrialización, se apreciará la posibilidad ofrecida por la invención de conciliar la facilidad de manejo de numerosos equipos de tratamiento de la información producidos a gran escala con la robustez requerida para tratamientos seguros de informaciones sensibles.

Naturalmente, la presente invención no está limitada a los ejemplos y al modo de realización, descritos y representados, sino que la misma es susceptible de numerosas variantes accesibles al experto en la técnica.

REIVINDICACIONES

1. Procedimiento de visualización seguro en una pantalla prevista para visualizar un primer conjunto de informaciones editadas por un primer sistema operativo no seguro, que comprende:

- una etapa (22, 23) de filtrado en la cual un elemento asigna independientemente del primer sistema operativo, una primera zona de la pantalla al primer conjunto de informaciones y una segunda zona de la pantalla a un segundo conjunto de informaciones editadas por un segundo sistema operativo seguro, estando el citado sistema operativo alojado en un componente de hardware que aísla el sistema operativo no seguro de un acceso directo a la pantalla;

- una etapa (26) de visualización real en la cual los dos conjuntos de informaciones son transferidos a la pantalla bajo control exclusivo del segundo sistema operativo seguro de modo que se produzca una visualización segura del segundo conjunto de informaciones.

2. Procedimiento de visualización según la reivindicación 1, caracterizado por que comprende una etapa (12) de visualización virtual en la cual el primer conjunto de informaciones es escrito en una memoria de vídeo virtual bajo el control del primer sistema operativo y cuyo contenido es accesible al segundo sistema operativo.

3. Procedimiento de visualización según la reivindicación 1, caracterizado por que comprende una etapa (12) de visualización virtual en la cual el primer conjunto de informaciones es escrito en una memoria de vídeo real bajo control del primer sistema operativo de modo que puedan combinar primeras señales de vídeo que así resultan con segundas de vídeo que resultan del segundo conjunto de informaciones bajo control del segundo sistema operativo.

4. Procedimiento de visualización según una de las reivindicaciones precedentes, caracterizado por que la segunda zona está situada en la pantalla en una primera posición fácilmente identificable por un usuario.

5. Procedimiento de visualización según la reivindicación 4, caracterizado por que la citada primera posición es alternativamente permutada con una segunda posición cubierta anteriormente por la primera zona.

6. Procedimiento de visualización según una de las reivindicaciones precedentes, caracterizado por que la segunda zona está superpuesta con o sin transparencia a la primera zona en una o varias posiciones de la pantalla.

7. Procedimiento de visualización según la reivindicación 6, caracterizado por que al menos una de las citadas posiciones es móvil sobre la pantalla.

8. Dispositivo de visualización segura en una pantalla (3) prevista para visualizar un primer conjunto de informaciones editadas por un primer sistema operativo no seguro, caracterizado por que comprende:

- un filtro (17, 30, 39) dispuesto para asignar independientemente del primer sistema operativo, una primera zona (3a) de la pantalla al primer conjunto de informaciones y una segunda zona (3b) de la pantalla a un segundo conjunto de informaciones editadas por un segundo sistema operativo seguro, estando el citado sistema operativo seguro alojado en un componente hardware que aísla el sistema operativo no seguro de un acceso directo a la pantalla;

- medios de transferencia de los dos conjuntos de informaciones a la pantalla bajo control exclusivo del segundo sistema operativo seguro de modo que se produzca una visualización segura del segundo conjunto de informaciones

9. Dispositivo de visualización segura según la reivindicación 8, caracterizado por que el filtro comprende en entrada una memoria de vídeo virtual (26) dispuesta para recibir el primer conjunto de informaciones bajo control del primer sistema operativo no seguro y en salida una memoria de vídeo real (34) para combinar los dos conjuntos de informaciones.

10. Dispositivo de visualización según la reivindicación 8, caracterizado por que el filtro (17) está dispuesto para recibir primeros datos de vídeo generados por un procesador estándar (6), en el cual se ejecuta el primer sistema operativo y segundos datos de vídeo generados por un procesador seguro (31) en el cual se ejecuta el segundo sistema operativo, y para transferir a una memoria de vídeo (34) una combinación de los primeros y segundos datos de vídeo.

11. Dispositivo de visualización según la reivindicación 8, caracterizado por que el filtro (39) está dispuesto para recibir primeras señales de vídeo que provienen de un primer controlador de vídeo (15) y segundas señales de vídeo que provienen de un segundo controlador de vídeo (38), y para transferir a la pantalla (3) una combinación de las primeras y de las segundas señales de vídeo.

12. Dispositivo de visualización según las reivindicaciones 8 a 11, caracterizado por que el filtro (17, 30, 39) está dispuesto para colocar la segunda zona en la pantalla (3) en una primera posición fácilmente identificable por un usuario.

13. Dispositivo de visualización según la reivindicación 12, caracterizado por que el filtro (17, 30, 39) está dispuesto para permutar la citada primera posición alternativamente con una segunda posición cubierta anteriormente por la primera zona.

14. Dispositivo de visualización según una de las reivindicaciones 8 a 11, caracterizado por que el filtro (17, 30, 39) está dispuesto para superponer con o sin transparencia la segunda zona a la primera zona en una o varias posiciones en la pantalla.

15. Dispositivo de visualización según la reivindicación 14, caracterizado por que el filtro (17, 30, 39) está dispuesto para hacer que se mueva al menos una de las citadas posiciones en la pantalla.

Fig.1

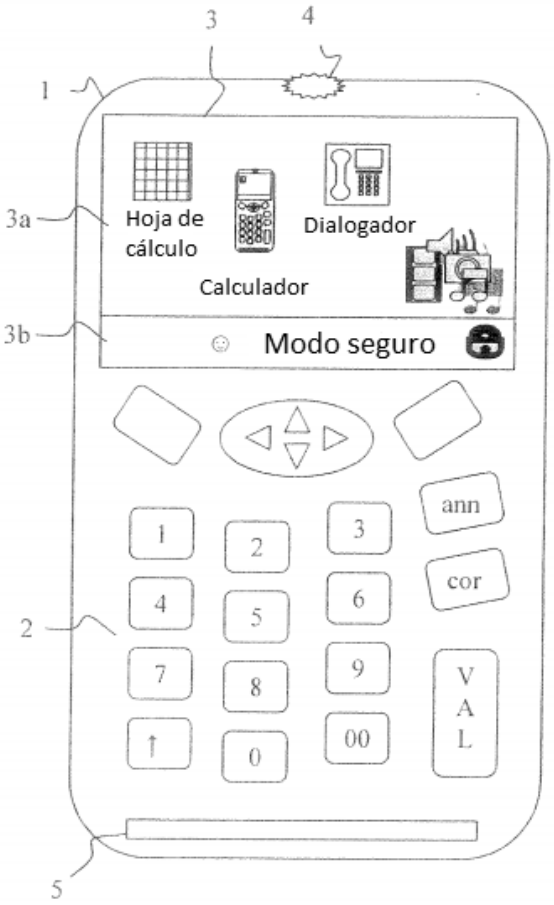

3
4
1
3a
Hoja de cálculo
Calculador
Dialogador
3b
Modo seguro
ann
cor
2
1
2
3
4
5
6
7
8
9
0
00
V
A
L
5

Fig. 2

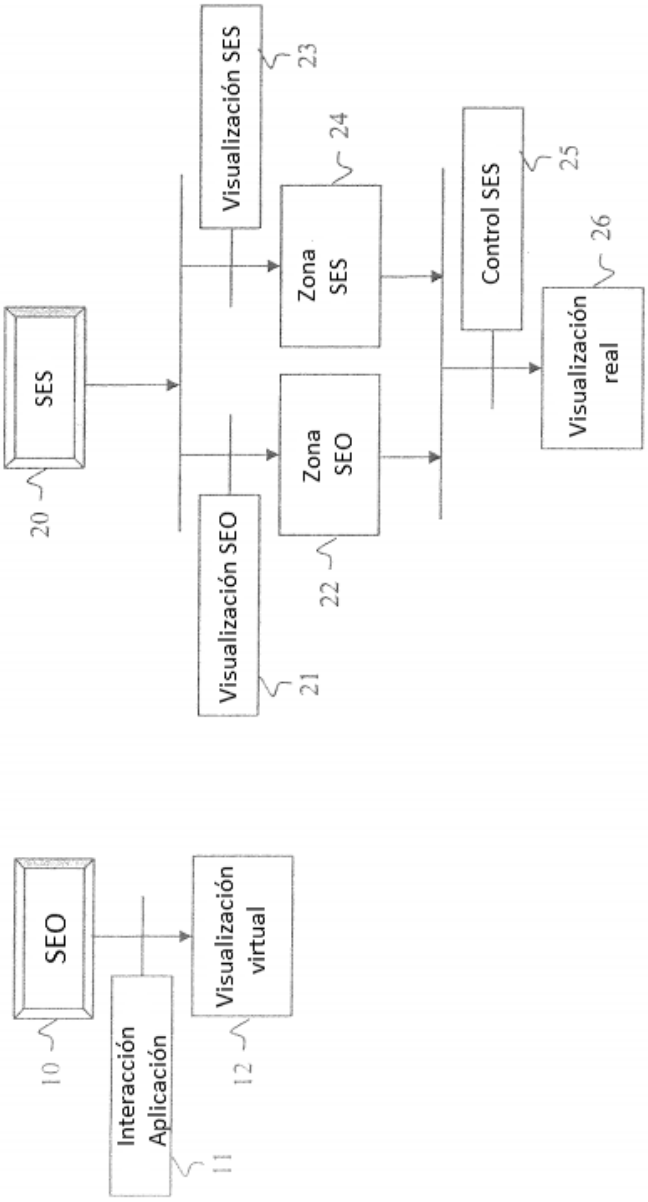

SES
20
Visualización SES
23
Visualización SEO
21
Zona SES
24
Zona SEO
22
Control SES
25
Visualización real
26
SEO
10
Interacción Aplicación
11
Visualización virtual
12

Fig.3

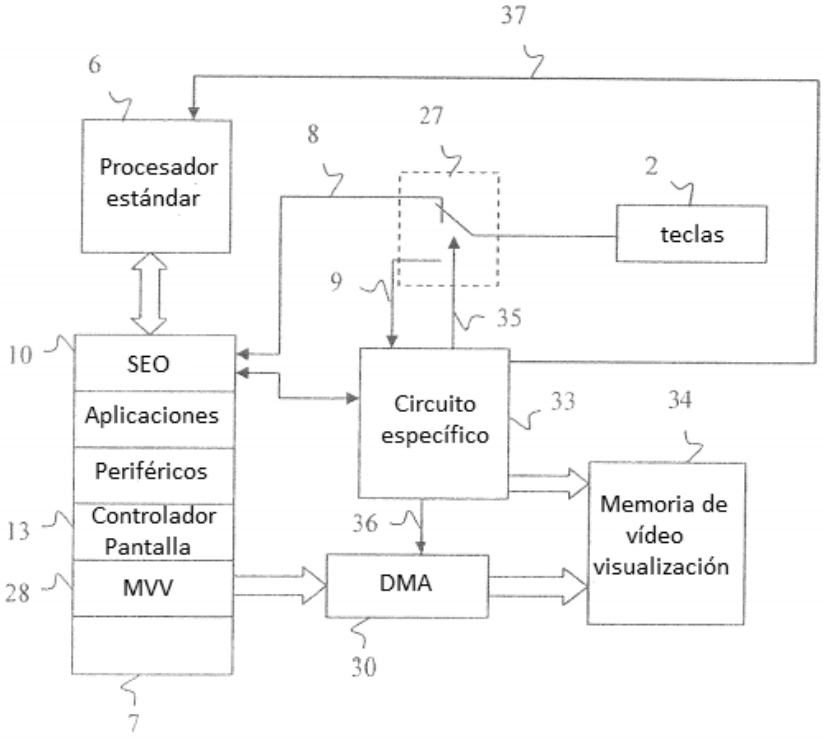

37
6
Procesador estándar
8
27
2
teclas
9
35
10
SEO
Aplicaciones
Periféricos
Controlador Pantalla
13
28
MVV
Circuito específico
33
34
Memoria de vídeo visualización
36
DMA
30
7

Fig. 4

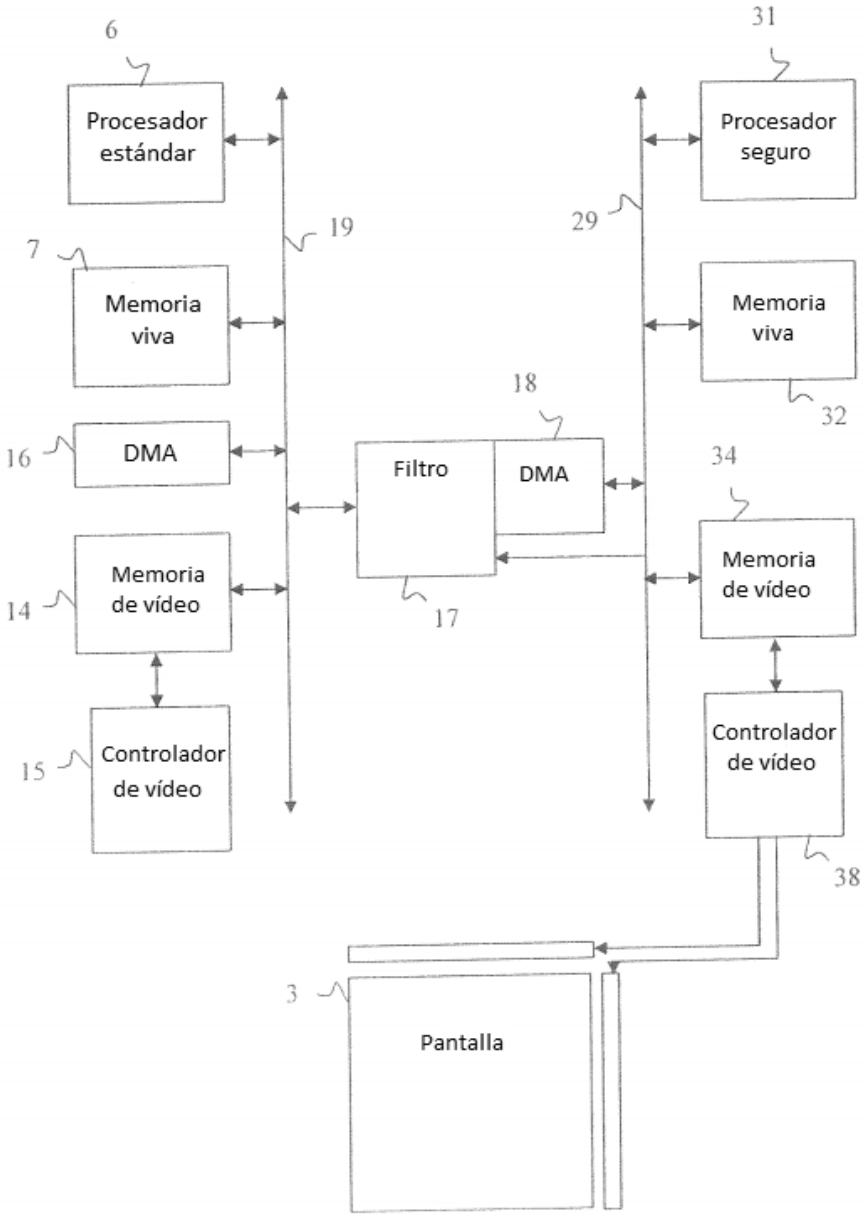
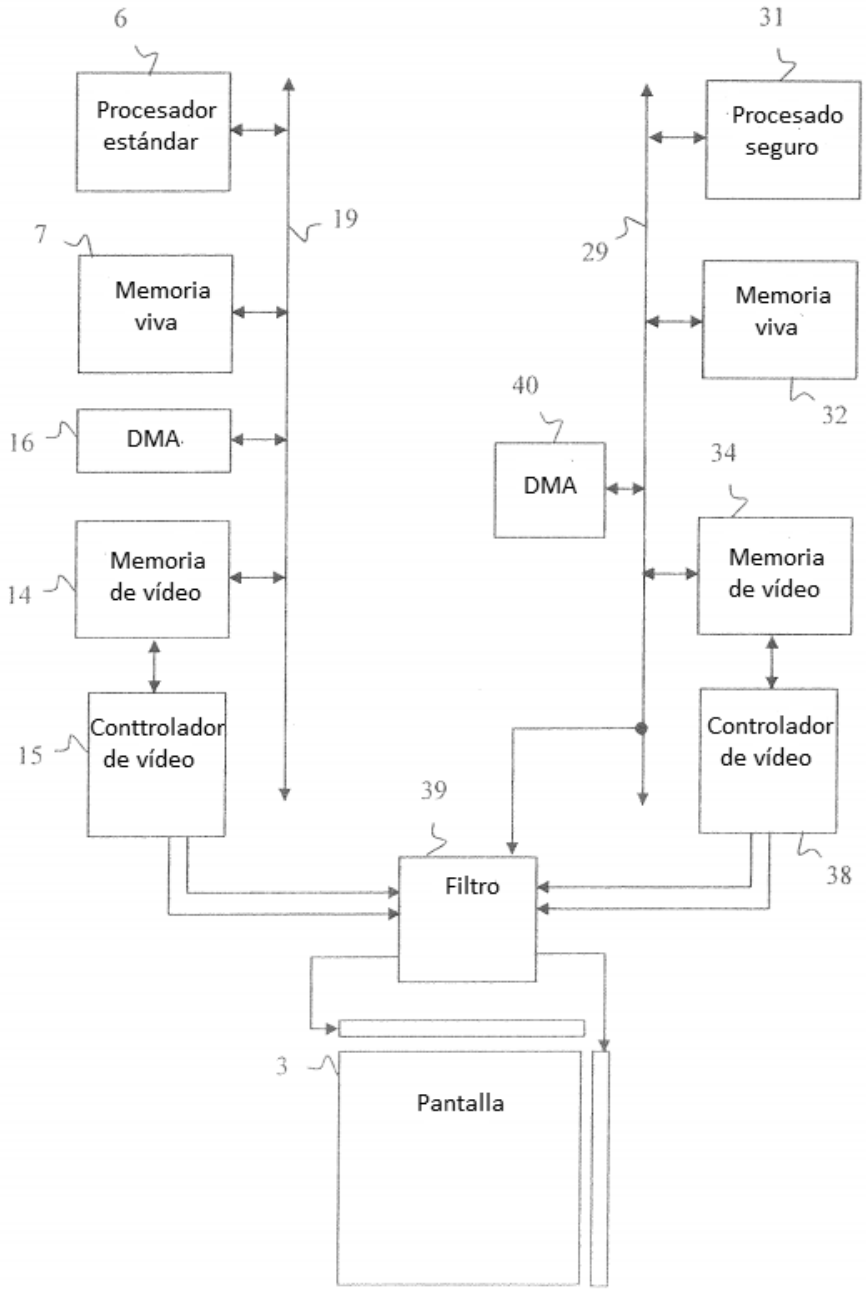

6
Procesador estándar
7
Memoria viva
16
DMA
14
Memoria de vídeo
15
Controlador de vídeo
19
18
Filtro
DMA
17
31
Procesador seguro
29
Memoria viva
32
34
Memoria de vídeo
Controlador de vídeo
38
3
Pantalla

Fig.5


6
Procesador estándar
19
7
Memoria viva
16
DMA
14
Memoria de vídeo
15
Conttrolador de vídeo
31
Procesado seguro
29
Memoria viva
32
40
DMA
34
Memoria de vídeo
Controlador de vídeo
38
39
Filtro
3
Pantalla