(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 386 471**

(51) Int. CI.:

H04N 21/4402 (2011.01)
H04N 21/45 (2011.01)
H04N 21/44 (2011.01)
H04N 21/84 (2011.01)
H04N 21/658 (2011.01)
H04N 21/475 (2011.01)
H04N 21/454 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07723289 .0**
(96) Fecha de presentación: **16.03.2007**
(97) Número de publicación de la solicitud: **2030441**
(97) Fecha de publicación de la solicitud: **04.03.2009**

(54) Título: **Método y aparato para supervisar las actividades de un usuario**

(30) Prioridad:
02.06.2006 US 421892

(45) Fecha de publicación de la mención BOPI:
21.08.2012

(45) Fecha de la publicación del folleto de la patente:
21.08.2012

(73) Titular/es:
ATG Advanced Swiss Technology Group AG
Churerstrasse 47
88088 Pfäffikon, CH

(72) Inventor/es:
HAUKE, Rudolf

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Método y aparato para supervisar las actividades de un usuario

Antecedentes

La invención se refiere a un método y un aparato para supervisar las actividades de un usuario. En principio, dichas aplicaciones son ampliamente conocidas hoy en día para evitar que los niños vean imágenes ofensivas, lean textos ofensivos o escuchen música ofensiva mediante el bloqueo del contenido ofensivo después de detectarlo. El contenido ofensivo se detecta habitualmente usando algoritmos de reconocimiento de contenidos en textos, imágenes o flujos de audio y/o vídeo, y combinaciones de los mismos, y clasificando el contenido reconocido en categorías predefinidas. Esto se puede conseguir mediante comparación del contenido reconocido con ejemplos de violación predefinidos como palabras clave y similares.

En la técnica anterior se usan diferentes niveles de supervisión. La mayoría de las aplicaciones actúan en el nivel de red, por ejemplo, en motores de búsqueda, pasarelas de Internet o servidores intermediarios. Sin embargo, solo el contenido obtenido por medio de una red se puede analizar de esta manera. Aun entonces, los datos encriptados, como los transmitidos por el protocolo HTTPS o en correos electrónicos encriptados, no pueden ser analizados sin la costosa desencriptación del código. Si una entidad de supervisión semejante llegara a ser sorteada con éxito de uno u otro modo, ese mismo contenido ofensivo se podría consumir localmente sin control una y otra vez.

Se conoce una clase diferente de aplicación para supervisar los datos enviados a una impresora, en la que los datos enviados son analizados en el controlador de la impresora en el nivel de sistema operativo. Si se detectan características de billetes de banco dentro de los datos enviados, a la impresora se envía solo una parte de los datos. En lugar de imprimir el resto, se envía una advertencia acerca de falsificación de dinero. Sin embargo, dichas contramedidas requieren privilegios de administrador del sistema para instalar el controlador de impresora apropiado. No es posible instalarlos sin permiso. La supervisión secreta del comportamiento de un usuario no es, así, posible. Además, estas contramedidas se pueden sortear simplemente usando un sistema operativo diferente.

De una forma similar a dicho controlador de impresora, algunos programas de software gráficos deniegan la apertura de archivos que contengan una imagen de un billete bancario. Esta protección se puede sortear simplemente usando un software diferente.

En aplicaciones de supervisión mejoradas, como la descrita en la solicitud de patente PCT WO 2005/109883 A2, los padres son informados automáticamente por medio de un dispositivo portátil de la intrusión ofensiva de un usuario, o del intento de esta intrusión. El dispositivo puede informar también sobre su localización usando un sistema de posicionamiento.

El documento US 2004/0189873 A1 desvela un sistema de sustitución de una señal de televisión que sustituye segmentos de vídeo conocidos como, por ejemplo, publicidad por publicidad de sustitución seleccionada. Los datos de huellas digitales de publicidad conocidos se pueden almacenar en una base de datos de huellas digitales. Cuando se dispone de nuevos datos de huellas digitales, los datos de huellas digitales se pueden transmitir de forma automática o manual a los abonados. Pueden usarse varias técnicas para identificar publicidad basándose en los datos de huellas digitales.

El documento US 2004/0006767 A1 desvela un producto de un sistema, un método y un programa informático para el filtrado selectivo de un contenido censurable a partir de un programa. El filtrado selectivo de contenido censurable a partir de un programa se consigue mediante la aplicación de un proceso de codificación y un proceso de decodificación para la señal de audio y/o vídeo del programa. El proceso de codificación incluye el marcado de material potencialmente censurable en el programa con información de filtrado que identifica el tipo (por ejemplo, audio, contenido violento, contenido sexual, etc.) y el nivel de intensidad (por ejemplo, leve, gráfico, extremo, etc.) del material potencialmente censurable usando códigos de filtro. El proceso de decodificación incluye la comparación, durante la presentación del programa al usuario y antes de emitir el audio o visualizar el vídeo, de la información de filtrado para filtrar criterios, que incluye las configuraciones de filtro suministradas por el usuario, para determinar si se debería realizar el filtrado del contenido potencialmente censurable (es decir, audio y/o vídeo). Si se debe realizar el filtrado, el contenido censurable en el programa se filtra según la información de filtrado que, en la forma de realización preferida, identifica el inicio y la duración del filtrado y, para el filtrado del vídeo del programa, también identifica el área de visualización del vídeo que será bloqueado.

El documento US 2004/0255321 desvela un método para bloquear el contenido que se presentaría a un dispositivo cliente basándose en un perfil de usuario y en etiquetas de contenido. El contenido que tiene etiquetas descriptivas es suministrado a un dispositivo cliente desde un dispositivo servidor. Las etiquetas descriptivas clasifican el contenido. Un perfil de usuario en el dispositivo cliente contiene datos de etiquetas para identificación de categorías de contenido que el usuario no desea que se presenten en el dispositivo cliente. El dispositivo cliente reconoce y evalúa las etiquetas del contenido recibido y bloquea el contenido basándose en el perfil de usuario. El contenido bloqueado no será presentado al usuario. El perfil de usuario puede ser creado de forma automática o manual por el

usuario. El perfil de usuario se crea automáticamente basándose en la historia del uso o información demográfica. El dispositivo cliente tiene un diccionario de etiquetas que puede ser actualizado para establecer una correspondencia con las etiquetas usadas por los sistemas de suministro de contenidos.

El documento US 2003/0227475 desvela un aparato y un método para bloquear anuncios de televisión específicos en el televisor del espectador basándose en las características del anuncio de televisión y sustituyendo el anuncio por un segmento de microprogramación preparado por un proveedor de visualización alternativo. Una unidad lógica y un programa de bloqueo de anuncios en la unidad lógica permiten opciones de visualización alternativas de manera que el usuario puede elegir opciones de microprogramación para sustituir la comunicación no deseada. El programa de bloqueo de anuncios reconoce una identificación digital única de etiqueta que distingue un anuncio en particular de todos los demás anuncios. Alternativamente, el programa de bloqueo de anuncios identifica un anuncio por una "firma de componentes" o una "firma digital global". Al visualizar un anuncio no deseado, el usuario indica que desea bloquear el anuncio a través de uno entre una diversidad de métodos de entrada. El programa de bloqueo de anuncios impide entonces que el anuncio sea visualizado en la televisión del usuario e inicia una programación alternativa que se visualizará en su lugar. El usuario puede configurar la programación alternativa por medio de la lógica de programación alternativa y elegir visualizar segmentos de microprogramación en lugar del anuncio bloqueado. Los segmentos de microprogramación están diseñados para proporcionar un paquete de entretenimiento o intercambio informativo completo en el segmento de tiempo. El proveedor de visualización alternativa puede proporcionar la microprogramación por servicio de suscripción, o por servicio de no suscripción en el que la microprogramación contiene publicidad no intrusiva.

El documento WO 03/017640 A2 desvela un sistema ITV que supervisa y almacena datos relacionados con difusiones de vídeo digital. Dichos datos pueden incluir archivos de sonido digital, archivos de imágenes, datos de suscripción, programas de software, información de programas de televisión, contenido de publicidad ITV y similares. El sistema de supervisión almacena información sobre un conjunto de datos predeterminado que está siendo supervisado en un flujo de vídeo digital, en uno o más archivos de registro. Los archivos de registro se pueden usar a continuación para generar una pluralidad de informes definidos por el usuario. Los informes pueden ser usados por organismos de radiodifusión, operadores de cable y proveedores de contenidos, y similares para establecer servicios generales de auditoría y facturación.

El documento WO 02/37853 A1 desvela un proceso de filtrado basado en el lado de salida de un decodificador multimedia. Un navegador (310a) supervisa la posición de reproducción actual del contenido multimedia y compara esa posición con objetos de navegación (316a). Cada objeto de navegación (316a) define una posición de arranque, una posición de parada y una acción de filtrado para realizar en la parte del contenido multimedia que comienza en la posición de arranque y termina en la posición de parada. Cuando la posición de reproducción actual se encuentra dentro de la parte de contenido multimedia definida por un objeto de navegación en particular, el navegador (310a) activa la acción de filtrado que se asignó al objeto de navegación (316a). Entre las acciones de filtrado se incluyen salto, reproducción muda, reencuadre, etc., de la parte de contenido multimedia definida por un objeto de navegación. Se pueden usar una diversidad de sistemas para implementar la presente invención, por ejemplo sistemas de ordenador (consumidor y servidor), sistemas de televisión y sistemas de audio.

El documento WO 2005/109883 desvela un sistema de supervisión y control de uso de un dispositivo para realizar supervisión parental y control de dispositivos conectados a una red doméstica que incluye un módulo de permisos que recibe y almacena órdenes de control de un progenitor que define los permisos con respecto a uno o más hijos. Los permisos especifican niveles de acceso a dispositivos conectados a una red doméstica y/o clasificaciones de contenidos de medios consumibles por medio de los dispositivos. Un módulo de control concede a un niño acceso a los dispositivos y/o contenidos de medios por medio de los dispositivos basándose en los niveles de acceso. Un módulo de supervisión supervisa el uso por parte del niño de los dispositivos y/o el consumo por parte del niño de los contenidos de medios mediante los dispositivos, almacena una historia de uso relacionada y comunica la historia de uso al progenitor.

El documento US 2003/0012399 A1 desvela un sistema de filtrado y un método de filtrado para una película pornográfica usado para filtrar el flujo de datos de imágenes pornográficas transmitido, en el que el flujo de datos de imagen incluye imágenes pornográficas. El sistema de filtrado para una película pornográfica incluye un dispositivo de recogida de imágenes y un motor de distinción de imágenes pornográficas. El dispositivo de recogida de imágenes recibe una entrada del flujo de datos de imagen y controla la salida del flujo de datos de imagen a un dispositivo de reproducción. El dispositivo de recogida de imágenes incluye además una unidad de recogida, una unidad de duplicación y una unidad de interceptación. La unidad de recogida se usa para recoger los datos de imagen del flujo de datos de imagen. La unidad de duplicado se usa para copiar los datos de imagen recogidos como datos de imagen duplicados, y exportar los datos de imagen duplicados al motor de distinción de imágenes pornográficas para realizar el proceso de distinción. Cuando los datos de imagen duplicados se identifican mediante el motor de distinción de imágenes pornográficas e indica que se incluye una imagen pornográfica, el motor de distinción de imágenes pornográficas transmite una señal de control a la unidad de interceptación. La unidad de interceptación intercepta de inmediato la parte restante de los datos de imagen en el flujo de datos de imagen.

Sumario de la invención

Un objeto de la invención es especificar un método y un aparato para supervisar las actividades de un usuario mediante el cual se pueda analizar cualquier contenido, en el que no sea posible sortear el análisis.

Según la presente invención, este problema se resuelve mediante la supervisión de la salida cuando es accesible digitalmente en una forma en la que sea enviada finalmente en una interfaz (analógica) al usuario, es decir, antes de que se visualice en un dispositivo apto para la lectura humana, en una memoria intermedia de tramas del dispositivo gráfico. Así, se puede esperar que el contenido de cualquier fuente, incluso si se encripta durante la transmisión, sea reproducido en una forma visualmente perceptible, en particular sin encriptación. Así sucederá cada vez que sea consumido el contenido. Además, la supervisión del contenido de la memoria intermedia de tramas actúa de forma completamente independiente de la fuente del contenido, es decir, del medio del que ha sido cargado. El dispositivo gráfico puede ser, en particular, un adaptador gráfico, un controlador gráfico integrado para un dispositivo portátil o una unidad de tratamiento gráfico para una impresora.

El contenido debe estar disponible digitalmente en la memoria intermedia de tramas cuando no pueda ser visualizado de otro modo. Así, si el usuario quiere ver o imprimir cierto contenido, el contenido será reproducido en la memoria intermedia de tramas en la forma de una imagen digital. A partir de la memoria intermedia de tramas, puede ser recuperado y analizado fácilmente según la presente invención. Dicha memoria intermedia de tramas puede estar situada no solo en una memoria gráfica dedicada, sino también en la memoria principal de un ordenador, en particular como un almacenamiento temporal del sistema operativo, a partir de la cual se copia a una memoria gráfica real, o como un área de memoria gráfica compartida.

El método según la presente invención comprende etapas de recuperación de datos de imagen a partir de la memoria intermedia de tramas de un dispositivo gráfico, examen de dichos datos de imagen, identificación de un atributo ofensivo dentro de dichos datos de imagen y reacción a dicho atributo de una forma predefinida. La recuperación de los datos de imagen desde la memoria intermedia de tramas es ventajosa con respecto a la recogida de los datos en un controlador gráfico (antes de que se escriban en la memoria intermedia de tramas), dado que incluso se pueden examinar dichos datos que se escriben directamente en la memoria intermedia de tramas, sorteando al controlador gráfico. Dicho acceso directo a la memoria intermedia de tramas se usa para conseguir un mejor rendimiento y es proporcionado por casi todos los sistemas operativos populares.

La invención se realiza en hardware, por ejemplo, en un procesador gráfico para adaptadores gráficos, dispositivos móviles o impresoras, que naturalmente tienen acceso directo a la memoria intermedia de tramas.

Preferentemente, dicha etapa de reacción comprende el rechazo de la salida de al menos una parte de dichos datos de imagen. Así, se puede evitar que un niño tenga perjuicios psicológicos con un esfuerzo pequeño.

En una forma de realización diferente, dicha, etapa de reacción comprende la sustitución de al menos una parte de dichos datos de imagen por un sustituto predefinido. De este modo, se evitan perjuicios psicológicos en un niño y se puede informar o advertir del atributo ofensivo.

Preferentemente, dicha etapa de reacción comprende el registro de dicha identificación en una memoria. La información sobre dicha identificación se puede así conservar para un uso posterior, en particular para comunicarla a una entidad de vigilancia.

En una forma de realización preferida, dicha etapa de reacción comprende la comunicación de un mensaje a una entidad de vigilancia, comprendiendo dicho mensaje un indicador para dicha identificación y/o indicadores para las identificaciones registradas anteriormente. Así se hace posible que la entidad de vigilancia reaccione ante la identificación del atributo. Esta forma de realización es de particular interés si el atributo se asigna a actividades delictivas o terroristas.

Ventajosamente, dicha etapa de reacción comprende la espera al establecimiento de una conexión a Internet antes de comunicar dicho mensaje. Así, la información sobre la identificación no se pierde.

Una forma de realización avanzada comprende una etapa de determinación de una localización de dicho dispositivo por medio de un sistema de posicionamiento, en el que dicho mensaje comprende dicha localización. Con ello, la entidad de vigilancia es informada sobre dónde encontrar al usuario. Esto resulta de particular interés en caso de actividades delictivas o terroristas.

En una forma de realización especial, se detecta un teléfono móvil cercano y se determina dicha localización usando dicho teléfono móvil cercano. Los teléfonos móviles están muy extendidos. Por ello, existe una alta probabilidad de que haya alguno en cobertura. Proporcionan un modo sencillo de determinar la localización del usuario.

En otra forma de realización preferida, se detecta un teléfono móvil cercano y dicho mensaje es comunicado por medio de dicho teléfono móvil cercano. De esta forma, se puede comunicar un mensaje de respuesta incluso sin una

conexión a Internet. Sin embargo, el mensaje también puede ser comunicado por una conexión a Internet por medio de un teléfono móvil. Según se describe anteriormente, existe una alta probabilidad de que exista un teléfono móvil en cobertura.

Según la invención, dicho examen de etapa comprende una clasificación basada en contenidos de dichos datos de imagen. Ello permite un examen e identificación de alta calidad de atributos ofensivos.

Una posibilidad para dicha clasificación basada en contenidos comprende un reconocimiento óptico de caracteres. De esta forma, se puede usar un texto en pantalla para el examen.

Preferentemente, dicho dispositivo gráfico es un adaptador gráfico o una unidad de tratamiento gráfico de una impresora.

Dicha memoria intermedia de tramas puede estar integrada en dicho dispositivo gráfico o puede ser un área de memoria compartida en una memoria principal.

En formas de realización preferidas, dicho atributo ofensivo se hace corresponder con categorías predefinidas para determinar dicha etapa de reacción. Ello permite proporcionar diferentes reacciones para diferentes escenarios. Por ejemplo, el contenido sexualmente explícito ligero podría solo ser bloqueado, mientras que el contenido sexualmente explícito intenso podría ser bloqueado y comunicado a los padres como entidad de vigilancia, mientras que el contenido delictivo o terrorista solo se comunicaría a la autoridad gubernamental sin ningún bloqueo.

En una implementación mejorada, dicho atributo ofensivo es una variación en dichos datos de imagen, predefinida de manera que sea reconocible por el método. De esta forma, se pueden rastrear los documentos que contengan dicha variación.

La invención se puede usar ventajosamente en un aparato en la forma de un controlador gráfico para un adaptador gráfico para un ordenador, o un teléfono móvil o un ordenador de bolsillo o un equipo de televisión digital, o una unidad de tratamiento gráfico para una impresora.

Breve descripción de las diversas vistas de los dibujos

La figura 1 muestra un sistema informático que pone en práctica la invención.

La figura 2 muestra un organigrama del método según la presente invención

La figura 3 muestra la implementación de un sistema informático que usa una unidad de supervisión de software, no según la invención,

La figura 4 muestra una forma de realización de un sistema informático que usa una combinación de unidad de supervisión de hardware y software, no según la invención,

La figura 5 muestra una forma de realización solo de bloqueo, no según la invención, sin acceso a Internet.

Descripción detallada de la invención

La figura 1 muestra un sistema informático 1 de ejemplo que pone en práctica la invención. Se conecta un monitor al mismo como un dispositivo apto para la lectura humana 2. El sistema informático 1 se conecta a Internet 3. El sistema informático 1 se puede dividir esquemáticamente en un nivel de hardware 4, un nivel de sistema operativo 5 y un nivel de aplicación 6.

El nivel de hardware 4 comprende un adaptador de red 7, un adaptador gráfico como un dispositivo gráfico 8 y un sistema de posicionamiento 9, una CPU (no mostrada) y una memoria principal (no mostrada). El dispositivo gráfico 8 comprende una memoria gráfica como memoria intermedia de tramas 10, un controlador gráfico (no mostrado) y una unidad de supervisión 11. El dispositivo apto para la lectura humana 2 está conectado a un puerto analógico del adaptador gráfico. En una forma de realización alternativa (no mostrada) el dispositivo apto para la lectura humana 2 puede ser una pantalla plana conectada a un puerto digital del adaptador gráfico.

El nivel de sistema operativo 5 comprende un controlador gráfico 12 que está encapsulado por el sistema operativo con el fin de proporcionar una interfaz de programación de aplicaciones a aplicaciones que se ejecutan en el nivel de aplicación 6 para una interfaz gráfica de usuario estándar.

El nivel de aplicación 6 comprende una aplicación de navegador de ejemplo 13. En este caso, un usuario puede decidir qué páginas web de Internet descargar y visualizar tecleando en un teclado (no mostrado) y con clics de ratón (no mostrado). También puede abrir archivos ya guardados localmente en el sistema informático 1 en lugar de descargarlos de Internet 3. Dichos archivos pueden ser páginas web completas, imágenes o textos aislados o

archivos de audio y/o vídeo únicos. Dichos archivos se pueden abrir localmente desde un disco duro, un disco flexible, un disco compacto, un lápiz de memoria o cualquier otro medio de almacenamiento o dispositivo periférico. La supervisión actúa independientemente del medio de fuente.

Por ejemplo, si el usuario decide cargar y visualizar una cierta página web de Internet 3, se envía una solicitud HTTP o HTTPS al servidor de Internet apropiado por medio del adaptador de red 7. A continuación se recibe una respuesta respectiva por parte de la aplicación de navegador 13 por medio del adaptador de red 7, que contiene los textos y las imágenes de la página web solicitada. La aplicación de navegador 12 reconstruye la estructura de la página web cargada y envía el contenido, es decir, textos e imágenes, al controlador gráfico encapsulado 12. El controlador gráfico 12 reproduce los textos e imágenes y escribe el contenido de la página web en la memoria intermedia de tramas 10 del dispositivo gráfico 8 en la forma de datos de imágenes digitales. La imagen digital en la memoria intermedia de tramas 10 es leída periódicamente por el controlador gráfico. Sus píxeles son convertidos en intensidades de color analógicas y se envían al dispositivo apto para la lectura humana 2 en el que se hacen visibles, reproduciendo ópticamente la página web cargada.

La memoria intermedia de tramas 10 es el último lugar en el que el contenido que será enviado está disponible digitalmente dentro del sistema informático 1. Además, en la memoria intermedia de tramas 10 cualquier contenido que será enviado es finalmente desencriptado. Así, según la presente invención, la unidad de supervisión 11 en el dispositivo gráfico 8 recupera al menos una parte de los datos de imagen de la memoria intermedia de tramas 10. Preferentemente, recupera todos los datos de imagen de la memoria intermedia de tramas 10, es decir, la imagen digital completa que será enviada. Esto último se asemeja a tomar una captura de pantalla, pero en el nivel de hardware 4. Preferentemente, antes de la recuperación de los datos de imagen, la unidad de supervisión 11 espera hasta que se ha escrito completamente una trama respectiva en la memoria intermedia de tramas 10. De esta forma, no se omiten datos de imagen.

La unidad de supervisión 11 examina los datos de imagen recuperados para uno o varios atributos ofensivos. La imagen digital se puede clasificar en una de entre varias categorías. Por ejemplo, si se detecta al menos una silueta de una persona en una actitud arbitraria, y una fracción grande de colores de piel, la imagen digital recuperada se clasifica al menos como "reveladora", cuando no "sexualmente explícita", dependiendo de una configuración de selectividad predefinida. La unidad de supervisión 11 puede usar también reconocimiento óptico de caracteres para la búsqueda, recuperación y análisis de texto a partir de la imagen digital en cuanto a atributos ofensivos. Para el examen de los datos de imagen y la identificación de atributos de imagen ofensivos se puede usar el espectro completo de reconocimiento de imagen. Por ejemplo, se puede usar un algoritmo de "Búsqueda de Imágenes según su apariencia". Detecta características invariantes, es decir, características que no varían si la imagen es transformada por algún grupo de transformación que usa histogramas de características. Sin embargo, la invención en sí es independiente de los algoritmos de reconocimiento de imágenes existentes. Con ello, la invención puede usar también métodos futuros de reconocimiento de imagen.

Si se identifica dicho atributo ofensivo o combinación de atributos ofensivos en la imagen digital, la unidad de supervisión 11 puede reaccionar de dos formas diferentes. Por una parte puede denegar, es decir, bloquear la salida de la imagen digital al dispositivo apto para la lectura humana 2 en partes o en su totalidad mediante la modificación de partes o de la totalidad de la memoria intermedia de tramas 10, o mediante la desconexión de las señales eléctricas de salida al dispositivo apto para la lectura humana 2. La modificación de la memoria intermedia de tramas 10 puede comprender fundido en negro, fundido en blanco u otra mutilación, o sustitución por una alternativa, por ejemplo, una advertencia. Dicha advertencia puede ser la imagen de un padre que regaña u otra imagen llamativa. En particular, la salida del área de dicho atributo ofensivo se puede denegar de esta forma. Por otra parte, la unidad de supervisión 11 puede comunicar un mensaje acerca de la identificación del atributo ofensivo a una entidad de vigilancia. El mensaje puede comprender simplemente un indicador para la identificación o puede comprender también la categoría del atributo identificado. El mensaje puede comprender adicionalmente información de localización. Para este fin, la localización del sistema informático 1 se adquiere usando el sistema de posicionamiento 9. A continuación, la localización se incluye en el mensaje. La entidad de vigilancia será así informada sobre la localización del usuario.

Las dos posibilidades, bloqueo e información sobre la identificación del atributo ofensivo, se pueden combinar. Así, si un niño ve imágenes ofensivas en Internet 3 en el dispositivo apto para la lectura humana 2, es posible a la vez bloquear el contenido ofensivo e informar a los padres por medio de un mensaje.

La forma de realización de la figura 1 muestra otra posibilidad para determinar la localización, para identificar el usuario y/o para comunicar un mensaje a una entidad de vigilancia. Para este fin, el sistema de supervisión 11 detecta cualquier teléfono móvil 14 dentro de la cobertura del sistema informático 1 mediante una interfaz inalámbrica 15. La interfaz inalámbrica 15 puede ser una interfaz radioeléctrica como, por ejemplo, el estándar Bluetooth. Alternativamente, puede ser un puerto de infrarrojos. Si se detecta un teléfono móvil 14, la localización del sistema informático 1 puede ser detectada aproximadamente mediante la consulta de la información de celda actual del teléfono móvil 14. La identidad del usuario se puede identificar mediante la consulta del número de teléfono del teléfono móvil 14. Además, el mensaje a la entidad de vigilancia se puede enviar por medio del teléfono móvil 14 como un mensaje corto o como una llamada, en particular una llamada de datos que usa HCSD, GPRS, UMTS o

cualquier otro protocolo. También es posible simplemente indicar la identificación de un atributo ofensivo mediante una señal radioeléctrica única especial enviada por medio del teléfono móvil 14. La localización del usuario puede ser determinada por la entidad de vigilancia usando los datos proporcionados por el operador de red celular. Preferentemente, la transmisión por medio del teléfono móvil se lleva a cabo de forma secreta, de manera que el usuario no es informado de ello.

Si el sistema informático 1 tiene una conexión permanente a Internet 3, se puede enviar un mensaje acerca de la identificación del atributo ofensivo inmediatamente después de la identificación del atributo ofensivo. El mensaje se puede enviar por medio del adaptador de red 7 a un servidor remoto predefinido en Internet 3 como una entidad de vigilancia. La cantidad de datos que se enviarán se puede mantener baja para una huella digital baja. El servidor remoto puede remitir el mensaje a un progenitor o a otra autoridad.

Si no se dispone de una conexión permanente a Internet 3, se puede registrar la identificación de un atributo ofensivo en una memoria. Es posible almacenar varias identificaciones en ella hasta que se establezca una conexión a Internet en un momento dado. La información almacenada puede comprender el tipo del atributo ofensivo o puede comprender simplemente un indicador para la identificación en sí. Adicionalmente, puede comprender la localización del sistema informático 1 en el momento de la identificación del atributo ofensivo. Alternativamente, la localización se podría determinar en el momento de la comunicación del mensaje. Por ejemplo, en un ordenador portátil que tiene un adaptador de red inalámbrico 7, las posibles identificaciones se registran y almacenan hasta que en un momento dado estén bajo la cobertura de una red inalámbrica. Se puede usar cualquier conexión a Internet 3, por ejemplo por medio de un módem, una LAN, un módem por cable, un teléfono móvil, un enlace ascendente de satélite, una línea eléctrica o RDSI.

En lugar de comunicar el mensaje por medio de Internet 3, se puede comunicar directamente por medio de un teléfono móvil 14 en la cobertura del sistema informático 1 según se describe anteriormente. Las identificaciones de atributos ofensivos se pueden registrar en una memoria y comunicar a la entidad de vigilancia en el momento en que esté accesible un teléfono móvil 14. Por ejemplo, la unidad de supervisión 11 puede esperar hasta que se realice un intercambio entre un teléfono móvil 14 y el sistema informático 1 por parte del usuario. Entonces, una transmisión adicional no llamaría la atención.

Además, la unidad de supervisión 11 en sí puede estar equipada con una antena para comunicación celular, como el sistema GSM. Así, puede funcionar en sí misma como un dispositivo de transmisión si está bajo la cobertura de una red celular. Alternativamente, puede recibir y desencriptar comunicación de otro teléfono móvil 14 que esté en cobertura. Los datos de identidad obtenidos de esta forma pueden ser enviados a continuación a la entidad de vigilancia.

La unidad de supervisión 11 representada en la figura 1 se puede implementar completamente en hardware, en particular si está diseñada solo para el bloqueo. Si, adicional o alternativamente, está diseñada para comunicar un mensaje acerca de la identificación, puede comprender incluso su propio emisor y su propia antena. En el último caso, se puede usar como antena la caja metálica de un ordenador. Alternativamente, la comunicación se puede realizar mediante un hardware de acceso directo al adaptador de red 7 o por medio de un controlador gráfico que se ejecuta en la capa del sistema operativo 5, que tiene acceso a conexiones de alto nivel.

La invención se puede integrar en un adaptador gráfico según se describe anteriormente. Sin embargo, el dispositivo gráfico 8 puede ser también una unidad de tratamiento gráfico de una impresora.

Naturalmente, la invención no se limita a la supervisión de la salida de una aplicación de navegador de Internet 13. Cualquier aplicación que produzca una salida visible en el dispositivo apto para lectura humana 2 será supervisada automáticamente y, así, se examinará cuando todas las salidas estén accesibles desde la memoria intermedia de tramas 10. Así, incluso las aplicaciones futuras estarán sometidas a supervisión.

Por ejemplo, usando reconocimiento óptico de caracteres, se pueden supervisar las actividades en chat en busca de palabras sexualmente ofensivas o de palabras que indiquen un encuentro entre el usuario y otra persona. Si dichas palabras son identificadas y comunicadas a los padres del usuario, estos pueden tomar medidas contra la amenaza de pedófilos. Por otra parte, es posible llevar el seguimiento de un pedófilo para organizar un encuentro en un chat. En este caso, se puede informar al organismo gubernamental pertinente, en particular en conjunción con los datos de identidad o la información celular obtenidos de un teléfono móvil cercano 14. Se pueden usar también otros teléfonos inalámbricos para este fin, por ejemplo, mediante la recuperación del número de teléfono del usuario o al menos de un vecino en una estación de base en cobertura. En caso de actividades de chat, se puede suponer que se establecerá una conexión a Internet, con lo que se puede enviar un mensaje de advertencia a corto plazo a la entidad de vigilancia respectiva.

En la figura 2 se representa el flujo del método según la presente invención. Las posibles reacciones son el bloqueo del atributo ofensivo o la comunicación de un mensaje de respuesta a la entidad de vigilancia, o ambos.

En la figura 3 se muestra otra implementación que no es según la invención. Funciona de modo similar al de la figura

1. Sin embargo, la unidad de supervisión 11 se implementa puramente en software y se ejecuta en el nivel de aplicación 6. La unidad de supervisión 11 es un simple proceso de aplicación ejecutable que se ejecuta en segundo plano. Recupera datos de imagen de la memoria intermedia de tramas 10 en el adaptador gráfico tomando capturas de pantalla en intervalos regulares. El examen de los datos de imagen y la identificación de atributos ofensivos se llevan a cabo según se describe anteriormente, pero dentro del proceso de aplicación. Esta implementación no requiere privilegios de administrador del sistema para su instalación ni un hardware especial. Es incluso más sencillo realizar comunicación a Internet 3 ya que se dispone funciones de conexiones de alto nivel. La desventaja de esta implementación puede ser que tal vez no se permita a la unidad de supervisión 11 escribir en la memoria intermedia de tramas 10. Así, el bloqueo se hace más difícil. Se puede conseguir determinando la aplicación responsable para un atributo identificado y forzando el cierre de esta aplicación o cubriendo el área de atributos, o toda la pantalla, con una ventana de nivel superior. Dicha ventana de nivel superior puede incluso tener una forma irregular. Sin embargo, es posible la comunicación de un mensaje de respuesta acerca de la identificación.

En cualquier caso, puede ser deseable implementar solo la respuesta, pero no el bloqueo, ya que en el caso de que se bloqueara apreciablemente algún contenido el usuario podría detectarlo. Si lo detecta, tal vez no prosiga con las actividades ofensivas, con lo cual se complica el seguimiento. Esto resulta válido para cualquier forma de realización, con independencia de la clase de implementación.

Como en la implementación de hardware puro de la figura 1, la implementación de software puro de la figura 2 puede usar también un teléfono móvil cercano 14 u otro teléfono inalámbrico según se describe anteriormente para la identificación del usuario, la determinación de la localización del sistema informático 1 y/o la comunicación de un mensaje de respuesta a una entidad de vigilancia.

En la figura 4 se muestra otra forma de realización no según la invención. En este caso, la unidad de supervisión 11 es una combinación de una unidad de hardware 11b y una unidad de software 11a. La recuperación de los datos de imagen se realiza dentro del nivel de hardware 4. A continuación se transfiere al nivel de sistema operativo 5 en el que tiene lugar el examen y, potencialmente, la identificación.

La figura 5 muestra una forma de realización no según la invención sin ninguna conexión a Internet 3. Está diseñada solo para bloquear atributos ofensivos. Para este fin, se proporciona un controlador gráfico que comprende la unidad de supervisión 11 en software. Por ejemplo, un reproductor multimedia 16 reproduce un flujo combinado de audio/vídeo de un archivo localizado en un disco duro 17. Cualquier información que se reproduzca en la memoria intermedia de tramas 10 es examinada en busca de atributos ofensivos, por ejemplo, una gran fracción de piel desnuda. Si se identifican los atributos ofensivos, es posible cubrirlos, o la pantalla completa, con fundido en negro u otra forma de mutilación.

La invención no se limita a actividades de supervisión de niños. También es útil para supervisar actividades delictivas o terroristas. Simplemente se tienen que adaptar los criterios para la identificación y la clasificación. Por ejemplo, el reconocimiento de imagen se podría preparar para armas, ciertas fórmulas químicas, bombas, diagramas de plantas nucleares o símbolos predefinidos. El reconocimiento óptico de caracteres se puede preparar para palabras clave apropiadas que describan fanatismo religioso, nombres de personas extremistas u organizaciones como "Osama bin Laden" y "al Qaeda", convocatorias de ataques o instrucciones para construir trampas o bombas, por ejemplo. Es posible incluso integrar una variación especial en los datos de documentos digitales que sean secretos o que se distribuyan intencionadamente. La variación de datos está predefinida como un "atributo ofensivo" y así se reconocerá. Así, los documentos que contienen la variación se pueden rastrear por todo el mundo. Si dicho documento se visualiza o se imprime en algún lugar, la supervisión según la presente invención señalará el suceso a una autoridad predefinida. Así, será posible localizar y detener al usuario respectivo o someterlo a mayor observación.

Para este fin se prefiere la versión de software, según se describe anteriormente. Como no se requiere ningún privilegio de administrador del sistema para la instalación, el software apropiado se puede distribuir sin el conocimiento del público. Por ejemplo, se puede empaquetar o integrar en un software libre popular como lectores de documentos. Muchas personas usan esta clase de software. Como con frecuencia se proponen nuevas versiones, es posible también distribuir actualizaciones del software de vigilancia empaquetado/integrado.

Es posible incluso preparar sitios web populares de tal manera que el software de supervisión se inyecte en los ordenadores que consultan estos sitios web, usando brechas de seguridad disponibles comúnmente en navegadores y sistemas operativos. Por ejemplo, se puede implementar una rutina de descarga dentro de una imagen para producir un desbordamiento de pila dentro del navegador. Si se visualiza el sito web, que muestra la imagen preparada, el sistema informático 1 usado para la visualización descargará e instalará el software de supervisión. Este procedimiento se puede usar especialmente para imágenes que son de interés para una cierta audiencia, por ejemplo, imágenes o mapas de un objetivo de ataque potencial como, por ejemplo, edificios públicos o militares, en particular si dichas intenciones han sido comunicadas por el servicio de inteligencia. Además, se puede preparar de forma apropiada un fichero de delincuentes en línea. Si un delincuente o un terrorista consulta el fichero para ver lo que se sabe de él, puede rastreársele usando la invención.

La invención no se limita a sistemas de ordenador 1. También se puede aplicar a teléfonos móviles, asistentes digitales personales, decodificadores, equipos de televisión y cualquier otro dispositivo electrónico. La memoria intermedia de tramas puede estar en una memoria gráfica dedicada o en un área de memoria compartida en la memoria principal.

REIVINDICACIONES

1. Un método para supervisar las actividades de un usuario en un dispositivo electrónico que comprende un nivel de hardware (4), un nivel de sistema operativo (5) y un nivel de aplicación (6), comprendiendo las actividades una salida de contenido cargado desde una fuente de contenidos, es decir, el medio desde el que se ha cargado el contenido mediante una aplicación en el nivel de aplicación (6), que finalmente envía el contenido a un dispositivo apto para la lectura humana por medio de un dispositivo gráfico (8) que tiene una memoria intermedia de tramas (10) y un procesador gráfico dispuesto en el interior del nivel de hardware (4), en el que la memoria intermedia de tramas (10) es el último lugar en el que está disponible digitalmente el contenido que será enviado, en el que la imagen digital en la memoria intermedia de tramas (10) es leída periódicamente por el procesador gráfico y enviada al dispositivo apto para la lectura humana (2), comprendiendo el método las etapas de:

- recuperación de datos de imagen de la memoria intermedia de tramas (10);

- examen de los datos de imagen mediante la realización de una clasificación de los datos de imagen basada en los contenidos;

- identificación de un atributo ofensivo dentro de los datos de imagen, realizándose la identificación a partir del examen de los datos de imagen e independientemente de la fuente de contenidos de los datos de imagen; y

- reacción al atributo de una forma predefinida por modificación de partes o de la totalidad de la memoria intermedia de tramas (10),

en el que las etapas son realizadas por una unidad de supervisión (11) comprendida en el dispositivo gráfico (8).

2. El método según la reivindicación 1, en el que la etapa de reacción comprende la denegación de la salida de al menos una parte de los datos de imagen.

3. El método según cualquiera de las reivindicaciones 1 o 2, en el que la etapa de reacción comprende la sustitución de al menos una parte de los datos de imagen por un sustituto predefinido.

4. El método según cualquiera de las reivindicaciones 1 a 3, en el que la etapa de reacción comprende el registro de una identificación del atributo ofensivo en una memoria.

5. El método según cualquiera de las reivindicaciones 1 a 4, en el que la etapa de reacción comprende la comunicación de un mensaje a una entidad de vigilancia, comprendiendo el mensaje al menos uno de entre un indicador para una identificación del atributo ofensivo y una pluralidad de indicadores para identificaciones registradas anteriormente.

6. El método según la reivindicación 5, en el que la etapa de reacción comprende la espera para el establecimiento de una conexión a Internet antes de la comunicación del mensaje.

7. El método según cualquiera de las reivindicaciones 5 o 6, que comprende además la etapa de determinación de la localización del dispositivo por medio de un sistema de posicionamiento y en el que el mensaje comprende la localización.

8. El método según cualquiera de las reivindicaciones 1 a 7, en el que la clasificación basada en contenidos comprende un reconocimiento óptico de caracteres.

9. El método según cualquiera de las reivindicaciones 1 a 8, que comprende además la atribución del atributo ofensivo a categorías predefinidas para determinar la manera predefinida.

10. El método según cualquiera de las reivindicaciones 1 a 9, en el que el atributo ofensivo es una variación en los datos de imagen, predefinida para ser reconocible por el método.

11. El método según la reivindicación 10, que comprende además la búsqueda de un documento que contiene la variación.

12. Un aparato para supervisar las actividades de un usuario en un dispositivo electrónico que comprende un nivel de hardware (4), un nivel de sistema operativo (5) y un nivel de aplicación (6), comprendiendo las actividades una salida de contenido cargado desde una fuente de contenidos, es decir, el medio desde el que se ha cargado el contenido mediante una aplicación en el nivel de aplicación (6), que finalmente envía el contenido a un dispositivo apto para la lectura humana (2) por medio de un dispositivo gráfico (8) que tiene una memoria intermedia de tramas (10) y un procesador gráfico dispuesto en el interior del nivel de hardware (4), en el que la memoria intermedia de tramas es el último lugar en el que está disponible digitalmente el contenido que será enviado, en el que la imagen digital en la memoria intermedia de tramas (10) es leída periódicamente por el procesador gráfico y enviada al

dispositivo apto para la lectura humana (2), siendo el aparato una unidad de supervisión (11) comprendida en el dispositivo gráfico (8) y que comprende:

- una unidad de recuperación configurada para recuperar datos de imagen de la memoria intermedia de tramas;

- una unidad de examen e identificación configurada para examinar los datos de imagen mediante la realización de una clasificación basada en contenidos de los datos de imagen de manera que se identifique un atributo ofensivo dentro de los datos de imagen, en el que la identificación se basa en el examen de los datos de imagen e independientemente de la fuente de contenidos de los datos de imagen; y

- una unidad de reacción configurada para reaccionar con el atributo de una forma predefinida por modificación de parte o la totalidad de la memoria intermedia de tramas (10).

13. El aparato según la reivindicación 12, en el que el aparato incluye al menos uno entre un controlador gráfico para un adaptador gráfico para un ordenador, un teléfono móvil, un ordenador de bolsillo, un equipo de televisión digital y una unidad de tratamiento gráfico para una impresora.

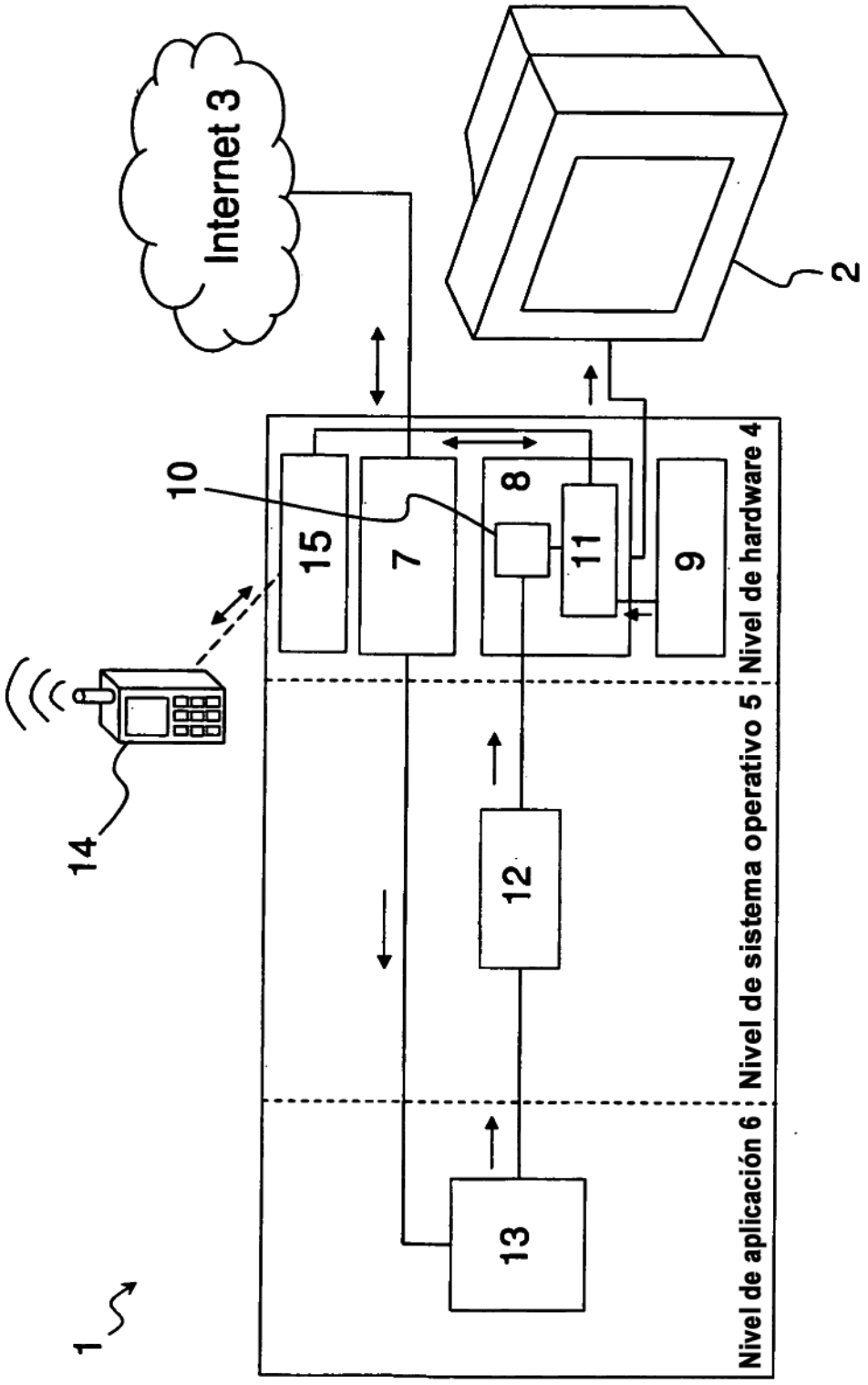
Internet 3
2
10
15
7
8
11
9
14
12
13
1
Nivel de hardware 4
Nivel de sistema operativo 5
Nivel de aplicación 6

Fig. 1

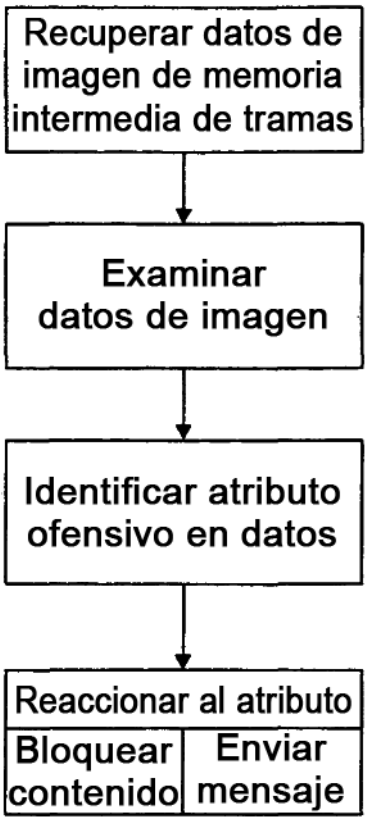
Recuperar datos de imagen de memoria intermedia de tramas
Examinar datos de imagen
Identificar atributo ofensivo en datos
Reaccionar al atributo
Bloquear contenido
Enviar mensaje

Fig. 2

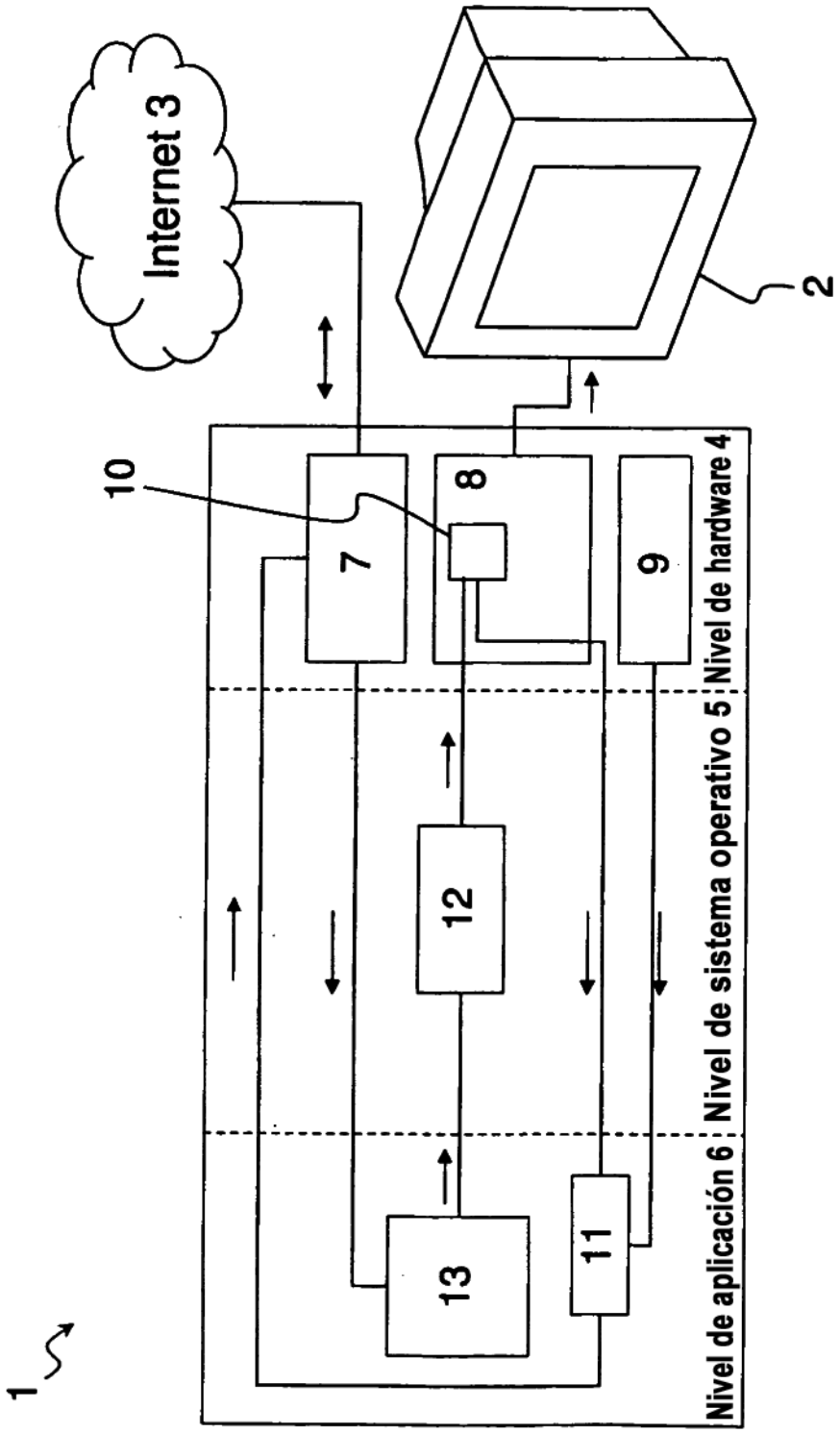
Internet 3
2
10
7
8
9
12
13
11
Nivel de aplicación 6
Nivel de sistema operativo 5
Nivel de hardware 4
1

Fig. 3

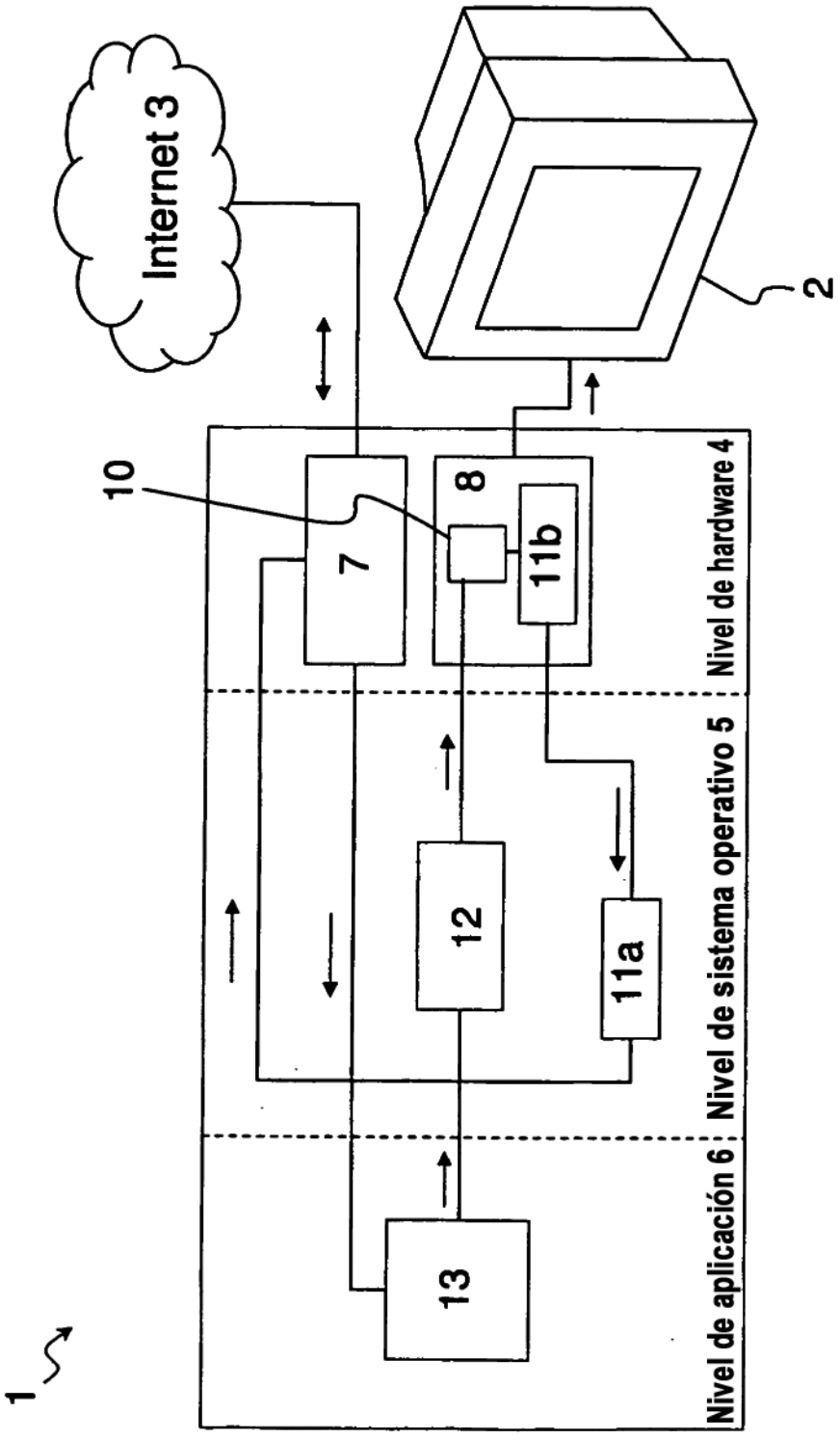
Internet 3
2
10
7
8
11b
Nivel de hardware 4
Nivel de sistema operativo 5
12
11a
Nivel de aplicación 6
13
1

Fig. 4

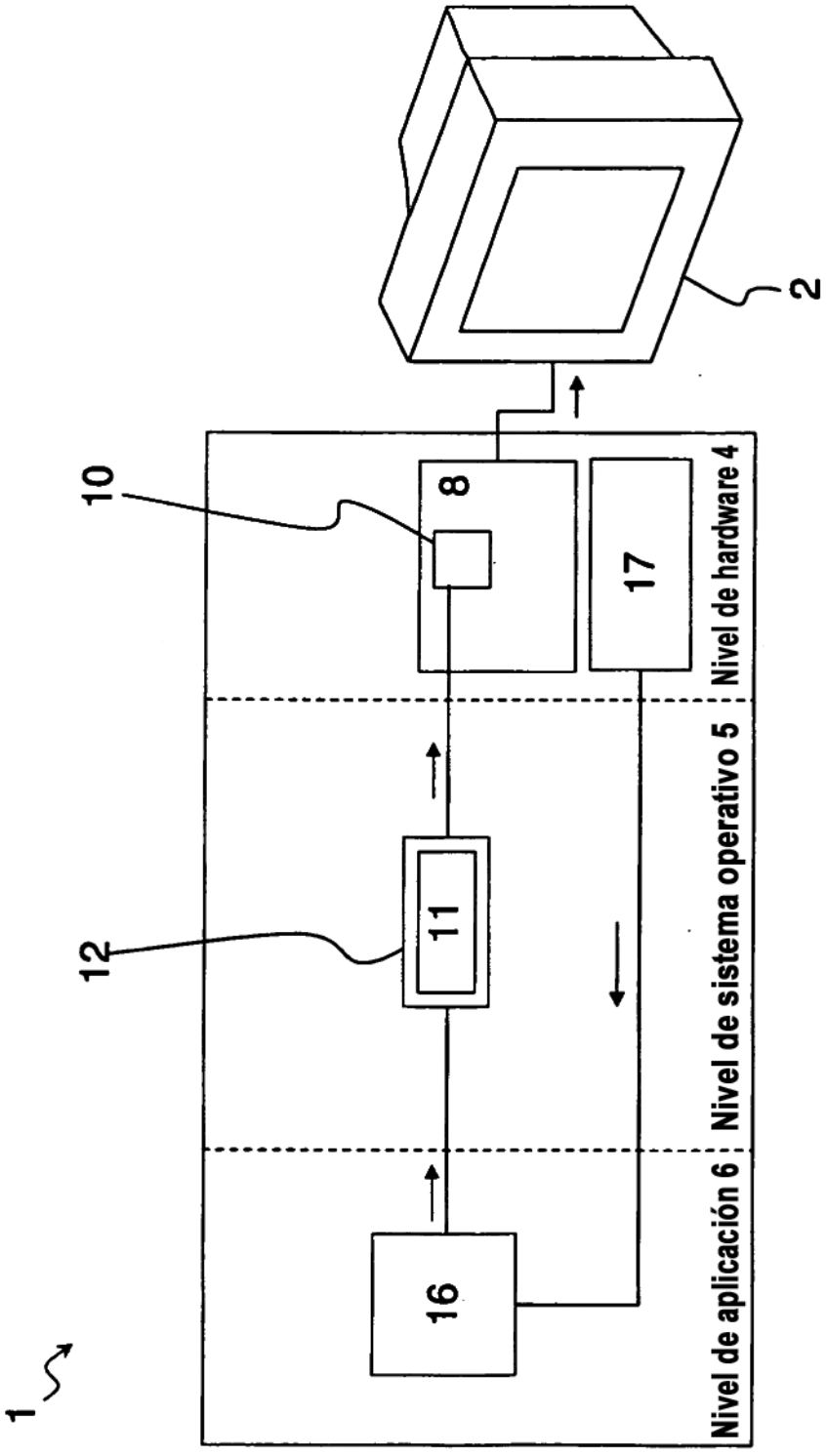
2
10
8
17
Nivel de hardware 4
Nivel de sistema operativo 5
12
11
Nivel de aplicación 6
16
1

Fig. 5