(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 708 086**

(51) Int. CI.:

G06F 21/82 (2013.01)
G06F 21/86 (2013.01)
G06Q 20/20 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.05.2016 PCT/EP2016/060307**

(87) Fecha y número de publicación internacional: **17.11.2016 WO16180767**

(96) Fecha de presentación y número de la solicitud europea: **09.05.2016 E 16725054 (7)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2018 EP 3295364**

(54) Título: **Sistema y método de detección óptica de intrusión, dispositivo electrónico, programa y soporte de grabación correspondientes**

(30) Prioridad:

12.05.2015 FR 1554265

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2019

(73) Titular/es:

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

(72) Inventor/es:

PAVAGEAU, STÉPHANE y
CARABELLI, ANDRÉ

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método de detección óptica de intrusión, dispositivo electrónico, programa y soporte de grabación correspondientes

1. Campo de la Invención

La invención se refiere al campo de la protección de dispositivos electrónicos tales como terminales de pago, por ejemplo, para proteger la introducción de datos sensibles (como los dígitos de un código confidencial introducidos a través de su teclado, o datos de tarjeta leídos por un lector) o incluso teclados independientes, lectores de tarjeta (con chip, con banda, etc.) independientes, etc.

2. Técnica anterior

Uno de los ataques clásicos contra un terminal de pago electrónico consiste en espiar los datos introducidos a través del teclado (integrado en el terminal de pago electrónico o bien independiente y conectado al terminal de pago electrónico), y en particular los dígitos correspondientes, por ejemplo, a un código confidencial introducido por un usuario para proteger una transacción.

Para ello, un posible ataque consiste en insertar, entre las teclas y el circuito impreso, más exactamente entre el accionador y el domo, un elemento "espía" (por ejemplo, un circuito impreso flexible, microinterruptores (en inglés, "microswitches") o incluso detectores por efecto Hall) que recupera la información relacionada con una pulsación de tecla, con el propósito de deducir de la misma los dígitos introducidos por el usuario.

Otro ataque posible consiste en insertar una película y cables sobre el teclado para interceptar las teclas pulsadas por el usuario. Para ello, el defraudador tiene que deteriorar o alterar la superficie de la guía de luz (o reemplazar por completo la guía de luz) implantada en el terminal de pago electrónico, raspándola en algunos lugares, para poder pegar la película espía. Este deterioro no requiere necesariamente quitar la guía de luz del terminal de pago electrónico.

Así pues, se han propuesto algunas soluciones para intentar limitar estos ataques, por ejemplo disminuir extraordinariamente el tamaño del teclado, de forma que se dificulte la inserción de estos elementos de espionaje, o incluso incorporar técnicas de detección del desmontaje del teclado, ya que suele ser necesario tal desmontaje para insertar estos elementos espías.

Otras soluciones consisten en añadir al terminal de pago electrónico, o al teclado independiente, teclas falsas que ejercen una presión permanente y permiten, por lo tanto, detectar la retirada del teclado. Por lo tanto, esta solución requiere la adición de piezas en compresión y genera presiones permanentes en los productos, lo que precisa estructuras mecánicas más rígidas y, por lo tanto, influye en el diseño.

Otras soluciones se basan en añadir un circuito de protección en forma de enrejado.

Sin embargo, estas soluciones requieren consecuentes modificaciones en la arquitectura del teclado, por ejemplo la adición de módulos de detección, y no permiten responder a la magnitud real del fraude, ya que los elementos de espionaje se hacen por su parte cada vez más pequeños y sus técnicas de inserción cada vez más discretas. Además, estas soluciones son muy sensibles a las condiciones climáticas, que provocan, por ejemplo, corrosión de los contactos, migración de los compuestos químicos durante la vida del producto, etc.

Además, también son difíciles de contrarrestar los ataques consistentes en espiar los datos de una tarjeta con chip cuando se inserta esta en un terminal de pago electrónico o en un lector independiente conectado a un terminal de pago electrónico, por ejemplo cuando se efectúan introduciendo una cabeza lectora magnética en la ranura de inserción de tarjeta con chip.

El documento WO 99/40501 A1 propone una técnica de eliminación activa de datos almacenados en un entorno protegido cuando se detecta una intrusión en dicho entorno. Un detector óptico detecta una variación en la intensidad lumínica con respecto a una intensidad lumínica de referencia, lo que permite detectar una intrusión.

El documento US 2008/117046 A1 describe una técnica de detección de intrusión en un equipo electrónico, utilizando secuencias binarias seudoaleatorias, para un sistema que comprende una carcasa que alberga al menos un elemento a proteger, un medio óptico y un generador de bits seudoaleatorios.

Existe, por tanto, la necesidad de una técnica para proteger dispositivos electrónicos utilizados para la introducción o la lectura de datos sensibles, técnica que permita contrarrestar los ataques consistentes en insertar uno o varios elementos espía, y que sea además simple y barata de implementar.

3. Compendio de la invención

La invención propone una nueva solución que no presenta el conjunto de dichos inconvenientes de la técnica anterior, en forma de un sistema para detectar una intrusión en un dispositivo electrónico.

Según la invención, el sistema comprende al menos un sensor óptico conectado a al menos un módulo de seguridad del dispositivo electrónico, estando configurado el sensor óptico y el módulo de seguridad para detectar una variación de la intensidad lumínica medida por el sensor óptico con respecto a una intensidad lumínica de referencia asociada con al menos una fuente luminosa predeterminada dentro del dispositivo electrónico, siendo la variación de la intensidad lumínica representativa de un riesgo de intrusión en el dispositivo electrónico.

Además, el dispositivo electrónico comprende medios para transmitir hacia la fuente luminosa al menos una señal aleatoria de encendido/apagado o una señal aleatoria de variación, y la detección óptica implementada por el sensor óptico y el módulo de seguridad tiene en cuenta la señal aleatoria transmitida.

Así, la invención propone una solución nueva e inventiva para detectar mediante detección óptica una tentativa de intrusión (por ejemplo, a través de la inserción de un elemento espía o la alteración una pieza tal como la guía de luz del teclado) en un dispositivo electrónico tal como, por ejemplo, un terminal de pago electrónico, un teclado protegido independiente (que puede estar conectado a un terminal de pago electrónico o a cualquier otro dispositivo electrónico tal como, por ejemplo, una aplicación de televisión de pago), un lector de tarjetas (con chip o con banda) protegido independiente (que puede estar conectado a un terminal de pago electrónico o a cualquier otro dispositivo electrónico).

Para ello, la invención, según sus diferentes modos de realización, implementa uno o varios sensores ópticos que permiten medir variaciones de la intensidad lumínica, en el dispositivo electrónico protegido, con respecto a una intensidad lumínica de referencia asociada con al menos una fuente luminosa predeterminada.

Por lo tanto, la adición de este o estos sensores ópticos en lugares estratégicos dentro del dispositivo electrónico, asociados con una o varias fuentes luminosas dentro del dispositivo electrónico, permite detectar múltiples tipos de intrusión que provocan la alteración de la intensidad lumínica (y más particularmente la luminancia medida por este o estos sensores) en el dispositivo electrónico, por ejemplo, por desplazamiento, adición o deterioro de componentes del dispositivo electrónico.

Por ejemplo, de esta forma se puede detectar, dependiendo de la colocación del o los sensores ópticos, una intrusión que consista en modificar la superficie de la guía de luz de un teclado o en desplazar la guía de luz, así como una intrusión que consista en añadir una cabeza lectora en la ranura de inserción de tarjeta con memoria.

Para ello, se añaden uno o varios sensores:

- ya sea en asociación con una o varias fuentes luminosas existentes de antemano en el dispositivo electrónico, tales como los diodos utilizados para la retroiluminación de un teclado, a través de una guía de luz, o la retroiluminación de la ranura de inserción de tarjeta con memoria,
- o en asociación con una o varias fuentes luminosas que no están presentes en el dispositivo electrónico, sino que se añaden específicamente para la implementación de la invención.

Este o estos sensores que están conectados al módulo de seguridad del dispositivo electrónico pueden transmitir a dicho módulo de seguridad sus mediciones de intensidad lumínica en el dispositivo electrónico, por ejemplo sus mediciones de luminancia, y permitir así la detección de variaciones inesperadas o no conformes de esta intensidad lumínica medida.

Por lo tanto, según los distintos modos de realización de la invención, su implementación consiste únicamente en añadir sensores ópticos, o incluso fuentes luminosas asociadas en caso de que no estén presentes de antemano en el dispositivo electrónico, y programar el módulo de seguridad para que procese las señales recibidas por los sensores y pueda detectar un riesgo de intrusión en el dispositivo electrónico.

La invención se aplica, por consiguiente, a la protección de cualquier dispositivo electrónico que comprenda un módulo de seguridad, tal como un terminal de pago electrónico, un teclado o un lector de tarjetas independiente, etc.

Por ejemplo, el sensor pertenece al grupo que comprende al menos:

- una fotorresistencia;
- un fotodiodo;
- un sensor tipo DTC.

Según una característica particular, la fuente luminosa predeterminada corresponde a un diodo electroluminiscente.

Así pues, según este modo de realización, la invención emplea al menos un sensor óptico capaz de detectar variaciones en la intensidad lumínica asociada con al menos una fuente luminosa de tipo diodo electroluminiscente.

En efecto, esta realización permite, en particular, utilizar para otra función las fuentes luminosas de este tipo ya

instaladas en el dispositivo electrónico a proteger para, por ejemplo, proporcionar retroiluminación al teclado a través de una guía de luz. En consecuencia, los sensores ópticos colocados estratégicamente en el dispositivo electrónico permiten detectar en particular intrusiones destinadas a mover, reemplazar o deteriorar/alterar la guía de luz para insertar uno o varios elementos espía sobre las teclas del teclado, con el propósito de espiar los dígitos de un código confidencial introducidos por un usuario.

Según el mismo principio, este modo de realización permite asimismo utilizar las fuentes luminosas de este tipo ya instaladas en el dispositivo electrónico para proporcionar retroiluminación a la ranura de inserción de tarjeta con memoria, con el fin de detectar en particular intrusiones destinadas a añadir aquí una cabeza lectora para explorar la banda magnética de la tarjeta una vez insertada, y extraer de ella datos sensibles.

Por último, si el dispositivo electrónico a proteger no posee medios de retroiluminación, la adición de una o varias fuentes luminosas de tipo diodo electroluminiscente tiene la ventaja de ser barata y requerir poco espacio para implementar de manera óptima la invención.

Este modo de realización se aplica no solo a cualquier terminal de pago electrónico, sino también a cualquier dispositivo electrónico que se pueda conectar a un terminal de pago electrónico, tal como un teclado o un lector de tarjetas, independiente y protegido, por ejemplo, así como a cualquier dispositivo electrónico que se pueda conectar a otro dispositivo electrónico (un teclado conectado a un televisor o un terminal interactivo, etc.) y que requiera la protección de los datos tratados.

Según un aspecto particular de la invención, el sensor óptico está soldado a un circuito impreso de dicho dispositivo electrónico, y conectado a dicho módulo de seguridad a través de un convertidor analógico-digital, que puede formar parte físicamente del módulo de seguridad de dicho dispositivo electrónico. El convertidor analógico-digital se utiliza, por ejemplo, para sensores de tipo fotorresistencia, que no emiten señal digital.

Así pues, según este modo de realización de la invención, el o los sensores ópticos están soldados al circuito impreso del dispositivo electrónico, entre los demás componentes, y conectados al módulo de seguridad del dispositivo electrónico a través de un convertidor analógico-digital que permite el procesamiento de las señales recibidas por el o los sensores ópticos.

Según una característica particular de la invención, el sensor óptico está implantado en el dispositivo electrónico en una ubicación elegida en función de al menos un criterio perteneciente al grupo que comprende:

- una contribución de al menos una fuente luminosa predeterminada dentro del dispositivo electrónico;
- un gradiente de luminancia alrededor de la ubicación;
- una contribución de una fuente luminosa externa al dispositivo electrónico.

Así pues, según este modo de realización de la invención, la ubicación del o los sensores ópticos responde a una estrategia particular de detección, lo que permite lograr un compromiso entre una detección óptima de las intrusiones y una minimización de falsas alertas de detección.

Por ejemplo, en caso de que las fuentes luminosas asociadas con los sensores ópticos correspondan a los ledes utilizados para la retroiluminación del teclado a través de una guía de luz, una estrategia de elección de la ubicación de los sensores consistirá en tener en cuenta la contribución de cada led.

En efecto, una ubicación juiciosa de un sensor corresponde, por ejemplo, a un lugar donde esté "sometido" solamente a la contribución principal de un único led, de manera que una variación en la intensidad lumínica medida por este sensor se pueda analizar fácilmente como un cambio de contexto para el led en cuestión (por ejemplo, la alteración o desplazamiento de la guía de luz situada sobre este led). Si tal ubicación no es posible, entonces conviene colocar un sensor, por ejemplo, en un lugar donde esté sometido a una contribución "equilibrada" de varios ledes (el 50% de la intensidad lumínica es debida a cada uno de los dos ledes próximos al sensor). Otra estrategia puede consistir asimismo en utilizar varios sensores en distintos emplazamientos para “equilibrar” las contribuciones de varios ledes y así poder analizar las variaciones de intensidad lumínica propias de cada led.

Según otro ejemplo, es posible realizar una simulación óptica de la luminancia, analizando la luminancia medida sobre toda su superficie por un sensor óptico plano situado en el centro de la guía de luz, con el fin de obtener una simulación del gradiente de luminancia en cada punto de la guía de luz. La elección de la ubicación del o los sensores depende entonces de este gradiente de luminancia, sabiendo que cuanto mayor sea el gradiente de luminancia en una ubicación dada, más sensible será el sensor óptico ubicado en este punto a las variaciones de luminancia y a los movimientos de la guía de luz, por ejemplo. Por lo tanto, se deben evitar estas ubicaciones con fuerte gradiente de luminancia.

Por último, es importante tener en cuenta, en la medida de lo posible, la influencia de la luz externa sobre el dispositivo electrónico a proteger, que puede variar sin que exista relación alguna con una intrusión en el dispositivo.

Según un aspecto particular de la invención, el sistema de detección comprende asimismo un filtro infrarrojo o ultravioleta aplicado sobre al menos una parte de la superficie a proteger del dispositivo electrónico.

Así, dicho filtro infrarrojo o ultravioleta, aplicado por ejemplo sobre la totalidad o parte del teclado de un terminal de pago electrónico, permite limitar o incluso eliminar por completo la influencia de la luz externa sobre el terminal, sin reducir las prestaciones de la retroiluminación del teclado ofrecidas al usuario del terminal. Para ello, este filtro está asociado únicamente, por ejemplo, a las fuentes y el detector de luz infrarroja, con independencia de la retroiluminación.

La invención se refiere asimismo a un método para detectar una intrusión en un dispositivo electrónico que emplea un sistema de detección tal como el descrito más arriba. Según la invención, dicho método de detección comprende un paso de detección óptica de una intrusión cuando al menos un valor absoluto de una diferencia entre:

- una intensidad lumínica medida por al menos un sensor óptico y
- una intensidad lumínica de referencia

supera un umbral predeterminado.

Por lo tanto, según este modo de realización se detecta una intrusión en el dispositivo electrónico así protegido cuando una variación de la intensidad lumínica medida por al menos un sensor óptico supera un umbral predeterminado, lo que puede depender, por ejemplo:

- del sensor óptico en cuestión;
- del intervalo entre dos mediciones (de hecho, una variación rápida de la luminancia hace que sea muy probable una intrusión o un intento de intrusión);
- de una tolerancia que tenga en cuenta criterios tales como el envejecimiento del led asociado con el sensor, la acumulación de polvo en el dispositivo electrónico, etc.

En particular, el paso de detección óptica también tiene en cuenta también un resultado de medida adicional de la temperatura y/o de la intensidad lumínica obtenido por otro sensor.

Por lo tanto, cuando se lleva a cabo adicionalmente, por ejemplo, un control de la temperatura en otro lugar dentro del dispositivo electrónico, también por razones de seguridad, se pueden correlacionar estas variaciones de la temperatura medida con las variaciones en la intensidad medidas según los distintos modos de realización de la invención.

Según una característica particular de la invención, el método comprende un paso de transmitir hacia al menos una de las fuentes luminosas internas del dispositivo electrónico al menos una señal aleatoria de encendido/apagado o una señal aleatoria de variación, y el paso de detección óptica tiene en cuenta la señal aleatoria transmitida.

Así, según una primera variante de realización, se pueden enviar a los ledes señales aleatorias (alternancias de encendidos y apagados largos y cortos, por ejemplo, o en lugar de un valor 0 o 1 de iluminación, el uso de valores intermedios) conocidos únicamente por el procesador del módulo de seguridad del dispositivo electrónico y, de este modo, se puede verificar la correspondencia con las señales recibidas por el sensor. Esto permite, en particular, evitar que un pirata deslumbre gradualmente el sensor y luego "puentee" el sensor con una resistencia equivalente, o incluso espíe la señal de la fotorresistencia, para reemplazarla por una señal equivalente.

Según otra variante, se prevé encender los ledes alternativamente, lo que conduce no solo a alternancias de encendido/apagado, sino también a distintos niveles de intensidad lumínica para cada sensor, cuando depende en particular de la contribución de varios ledes.

Según un aspecto particular de la invención, el método de detección comprende un paso de generar una alarma cuando se detecta una intrusión durante el paso de detección óptica, siendo la alarma de un tipo perteneciente al grupo que comprende al menos:

- el paso del dispositivo electrónico al modo "robo";
- la visualización de un mensaje de alarma en el dispositivo electrónico;
- una combinación de los tipos de alarma arriba indicados.

Por tanto, cuando se detecta una posible intrusión, la alarma generada puede consistir en un mensaje en el dispositivo electrónico así protegido, que ya no puede funcionar "normalmente" (por ejemplo, si se trata de un terminal de pago electrónico o de un accesorio conectado a un terminal de pago electrónico, ya no se puede realizar ninguna transacción). A continuación, se debe devolver obligatoriamente a fábrica dicho dispositivo electrónico, como establecen las técnicas actuales conocidas para proteger terminales de pago electrónico y como ocurre, por ejemplo, en otras técnicas de detección de apertura y de fraude.

Por ejemplo, el método comprende un paso de almacenar al menos un valor de intensidad lumínica medido por al menos un sensor óptico.

En particular, el método de detección comprende un paso de comparar al menos un valor de intensidad lumínica medido por al menos un sensor con al menos un valor de intensidad lumínica previamente almacenado.

Por lo tanto, este modo de realización prevé que se registren las últimas medidas de intensidad de los sensores ópticos antes del apagado del terminal de pago electrónico, para poder compararlas con las primeras mediciones de los sensores ópticos que se realicen cuando se reinicie el dispositivo electrónico.

Así, una diferencia considerable entre las medidas de intensidad tomadas antes del apagado y después del reinicio es motivo de alerta, ya que entonces resulta muy probable que el dispositivo electrónico haya sufrido un intento de ataque y que, por ejemplo, se haya dañado la guía de luz. En efecto, el ataque a los elementos de seguridad (en inglés, “pucks") (teclas falsas, pasadores de seguridad, detectores) requiere alterar la guía de luz, y el hecho de instalar un elemento espía en el espacio de la guía de luz requiere la alteración o la eliminación de la guía de luz.

Además, este almacenamiento de los valores de intensidad lumínica medidos con anterioridad hace posible garantizar una alta fiabilidad de detección, ya que permite tener en cuenta los criterios de desgaste de los componentes del dispositivo electrónico, por ejemplo, para no detectar intrusiones en caso de variaciones pequeñas y/o lentas en la intensidad lumínica medida.

Por ejemplo, el método de detección lo desencadena un suceso perteneciente al grupo que comprende al menos:

- la activación de las medidas de seguridad del dispositivo electrónico;
- cualquier apagado del dispositivo electrónico;
- cualquier reinicio del dispositivo electrónico;
- periódicamente;
- antes de una transacción protegida;
- una combinación de al menos dos sucesos de los arriba indicados.

La invención también se refiere a un dispositivo electrónico que comprende al menos un sistema de detección de una intrusión como el descrito en lo que antecede, para ejecutar el método de detección de intrusión que se ha descrito en lo que antecede. Dicho dispositivo electrónico es, por ejemplo, un terminal de pago electrónico, un teclado independiente, un lector de tarjetas independiente o cualquier otro dispositivo electrónico que esté expuesto al mismo problema de seguridad.

La invención se refiere asimismo a un programa informático descargable desde una red de comunicaciones y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, que comprende instrucciones de código de programa para ejecutar un método de detección como el descrito en lo que antecede, cuando este programa es ejecutado por un procesador.

Por último, la invención se refiere a un soporte de grabación legible por ordenador en el cual se ha grabado un programa informático que comprende instrucciones para ejecutar los pasos del método de detección que se ha descrito en lo que antecede.

4. Figuras

Se apreciarán más claramente otras características y ventajas de la invención al leer la descripción que sigue de un modo de realización preferido, ofrecido como simple ejemplo ilustrativo y no limitante, y los dibujos adjuntos, en los cuales:

- la Figura 1 muestra un ejemplo de diagrama de un sistema de detección de intrusión según un modo de realización particular de la invención;
- la Figura 2 muestra un ejemplo de guía de luz implementada en un terminal de pago electrónico que comprende un sistema como el ilustrado en la Figura 1, según un modo de realización particular de la invención;
- la Figura 3 muestra un ejemplo de simulación óptica de la luminancia medida por un sensor óptico plano para una guía de luz como la ilustrada en la Figura 2, según un modo de realización particular de la invención;
- la Figura 4 ilustra los pasos principales del método de detección de intrusión, según un modo de realización de la invención;
- las Figuras 5 y 6 ilustran dos ejemplos de arquitectura simplificada de un sistema o módulo de detección de intrusión, según un modo de realización particular de la invención.

5. Exposición

5.1. Principio general

El principio general de la invención consiste en utilizar sensores ópticos para detectar una posible intrusión en un dispositivo electrónico gracias a la detección de variaciones inadecuadas de la intensidad lumínica en el dispositivo electrónico en cuestión.

Para ello, la invención emplea, según estos distintos modos de realización, al menos un sensor óptico conectado al módulo de seguridad del dispositivo electrónico, configurado para detectar variaciones inadecuadas de intensidad lumínica con respecto a una intensidad lumínica asociada con al menos una fuente luminosa dentro del dispositivo electrónico.

Un dispositivo electrónico de este tipo corresponde, por ejemplo, a un terminal de pago electrónico o un accesorio de pago (teclado independiente o lector de tarjetas independiente conectados a un terminal de pago electrónico), o un teclado protegido independiente que puede estar conectado a otro dispositivo, por ejemplo, como parte de una aplicación de televisión de pago, etc.

La descripción que sigue intenta describir la invención para un terminal de pago electrónico, pero se entiende que la invención no está limitada a un dispositivo de este tipo y puede aplicarse en particular a cualquier dispositivo electrónico que se enfrente a los mismos problemas de seguridad y, por lo tanto, deba estar sujeto a medidas de seguridad especiales relacionadas, en particular, con la naturaleza sensible de los datos procesados por dicho dispositivo electrónico, tales como, por ejemplo, los datos introducidos en un teclado (código confidencial para una transacción financiera electrónica o para una conexión protegida o un acceso protegido a un edificio o servicio) o datos leídos de una tarjeta (con chip, con banda, etc.) a través de un lector de tarjetas.

Por lo tanto, la invención, según sus diversos modos de realización, hace uso de la siguiente observación: las intrusiones actualmente más frecuentes en los terminales de pago electrónico, a través de su teclado o de un teclado conectado al mismo, tienen el efecto de cambiar el trayecto de los rayos luminosos dentro del terminal (o más particularmente el teclado), debido a la degradación, desplazamiento, eliminación o incluso adición de componentes en el terminal (por ejemplo, la presencia de pegamento sobre una superficie óptica altera considerablemente el comportamiento de los rayos luminosos). Por lo tanto, se puede implementar una detección óptica de una intrusión de manera simple y poco costosa mediante la adición de sensores ópticos.

Además, la mayoría de los terminales de pago actuales disponen de una función que consiste en mejorar la ergonomía del teclado a través de una retroiluminación, proporcionada a su vez por una pluralidad de fuentes luminosas situadas en el circuito impreso del terminal y una guía de luz integrada en el teclado del terminal. Algunos terminales de pago actuales disponen asimismo de una función equivalente que consiste en mejorar la ergonomía del lector de tarjetas con chip a través de una retroiluminación de la ranura de inserción de tarjeta con chip, proporcionada por al menos una fuente luminosa ubicada en el circuito impreso del terminal cerca de esta ranura. Así, muy frecuentemente están presentes de antemano fuentes luminosas internas para proporcionar estas funciones de retroiluminación, y se las puede asociar a los captores ópticos de la invención con el objetivo de detectar intrusiones a través de la detección de variaciones inadecuadas de la intensidad lumínica con respecto a una intensidad lumínica de referencia relacionada con al menos una fuente luminosa dentro del terminal.

Por último, se describirá más particularmente un modo de realización basado en la detección de la variación de medidas de luminancia realizadas por uno o varios sensores ópticos, aunque la expresión "intensidad lumínica" sea la más frecuentemente utilizada. Por lo tanto, la magnitud física medida por el o los sensores, según los distintos modos de realización de la invención, puede corresponder a una luminancia o a cualquier otra magnitud que permita obtener los mismos resultados de detección óptica.

Así pues, la invención, según sus distintos modos de realización, permite superar inconvenientes tales como el envejecimiento, ya que los contactos, sensores y fuentes luminosas utilizadas no requieren contacto (aparte de los contactos en la placa de circuito impreso del terminal de pago electrónico) para implementar la detección óptica.

La invención también permite, según sus diversos modos de realización, complementar o incluso prescindir del serigrafiado del "FPC" (del inglés "Flexible Printed Circuit", o circuito impreso flexible) o bien de tener piezas en compresión, como sucede en algunas metodologías de la técnica anterior.

Además, la invención, según sus diversos modos de realización, también permite reducir el número de falsas teclas de seguridad a implantar y, por lo tanto, reducir las presiones continuas sobre el producto, por lo que la detección óptica refuerza notablemente el nivel de seguridad.

5.2. Descripción de un modo de realización

5.2.1 Ejemplo de sistema de detección de intrusión

Se describirá ahora, en relación con la Figura 1, un primer modo de realización de la invención, en forma de un sistema de detección de intrusión que comprende, por ejemplo, dos sensores ópticos C1 y C2, asociados a tres

fuentes luminosas SL1, SL2 y SL3. Este sistema de detección de intrusión está implementado, por ejemplo, en el circuito impreso de un terminal de pago electrónico, un teclado protegido independiente, un lector de tarjetas (con chip o con banda) protegido independiente, etc.

Los dos sensores ópticos están conectados al módulo de seguridad MS, de manera que el módulo de seguridad MS puede procesar y analizar las señales que estos reciben, a fin de detectar posibles intrusiones en el terminal de pago electrónico, y asimismo ajustar los valores en función de los acontecimientos (envejecimiento de los ledes, acumulación de polvo, etc.).

Por ejemplo, los dos sensores ópticos son fotorresistencias, que generan una resistencia proporcional a la señal recibida. Este valor analógico se transmite después al microprocesador del módulo de seguridad, por ejemplo, a través de un convertidor analógico-digital.

También es posible utilizar sensores de tipo fotodiodo.

Un tercer tipo de sensor es un sensor de tipo cámara o CCD (del inglés "Charge-Coupled Device", o dispositivo de carga acoplada) que, además de la información de "intensidad", puede complementarla con información de tipo "longitud de onda", lo que le puede hacer menos sensible a la luz externa. Este sensor también tiene la ventaja de poder emitir una señal digital, lo que permite prescindir de la adición de un convertidor analógico-digital.

Por último, se puede utilizar cualquier otro sensor de luz que permita obtener una información de intensidad lumínica.

Por su parte, las tres fuentes luminosas SL1 a SL3 corresponden, por ejemplo, a diodos electroluminiscentes implantados en el circuito impreso del terminal de pago electrónico para proporcionar retroiluminación al teclado, mediante el uso conjunto de una guía de luz.

Por ejemplo, en la Figura 2 se ilustra una guía de luz de este tipo, debajo de una carcasa de un terminal de pago electrónico. Dicha guía de luz está destinada a propagar de manera óptima a todas las teclas del teclado la luz emitida por los diodos, con el fin de retroiluminar ergonómicamente y de manera uniforme el teclado que se presenta al usuario.

La Figura 3 ilustra (en escala de grises) una simulación óptica que muestra la densidad de rayos luminosos en una guía de luz (es decir, la magnitud óptica luminancia). Para obtener tal simulación, se ha situado un "sensor virtual" óptico plano debajo de la guía de luz, por completo o en parte, y mide los rayos luminosos que la atraviesan, en ambos sentidos (desde el interior del terminal de pago electrónico hacia fuera y viceversa).

Tal simulación permite, en su uso tradicional, simular la iluminación de las teclas para configurar las formas de la guía de luz y optimizar la homogeneidad de la iluminación que se presenta al usuario.

En este caso de uso, la simulación permitirá asimismo elegir juiciosamente o de manera estratégica las ubicaciones de los sensores ópticos, a fin de que la detección óptica de una intrusión sea óptima (con un compromiso entre una tasa elevada de detección de intrusiones reales y una baja tasa de falsa detección).

Por tanto, el sensor o sensores se colocan:

- de manera que los desplazamientos relativos de la guía de luz y del sensor (por ejemplo, en el momento del montaje del terminal de pago electrónico, o si el terminal de pago electrónico se cae) sean poco sensibles. Para ello es necesario elegir, por ejemplo, una ubicación donde el gradiente de luminancia (en la simulación) no sea demasiado elevado en un margen de algunos milímetros. Por ejemplo, en la Figura 3 se identifican estas ubicaciones preferidas;
- de manera que, siempre que sea posible, cada led contribuya a la iluminación de cada sensor. Por ejemplo, en la Figura 1 se puede suponer que el sensor óptico C1 es principalmente sensible a la intensidad lumínica emitida únicamente por la fuente luminosa SL1;
- de manera que, cuando no es posible que cada led contribuya a la iluminación de cada sensor con poca influencia de la luz externa, un sensor sea sensible a una contribución equilibrada de varias fuentes luminosas. Por ejemplo, en la Figura 1 se puede suponer que el sensor óptico C2 es sensible, a partes iguales, a la intensidad lumínica emitida por las dos fuentes luminosas SL2 y SL3;
- minimizando la influencia de la luz externa, que puede variar sin que ello sea sinónimo de intrusión en el terminal de pago electrónico. Para ello, es posible aplicar, en la totalidad o en parte del teclado del terminal, un filtro infrarrojo que permita limitar o incluso eliminar por completo la influencia de la luz externa al terminal, al tiempo que no se menoscaban las prestaciones de la retroiluminación del teclado a ojos del usuario del terminal. En este caso, también es posible agregar, bajo el filtro infrarrojo, una fuente infrarroja específica, y uno o varios detectores de infrarrojo, para estar totalmente aislados del exterior. La medición se podría hacer apagando las fuentes luminosas de iluminación del teclado. Para limitar la influencia de la luz externa, un sensor podría medir la luz externa, y tomar en cuenta esta medida en los

cálculos de comparación.

Por supuesto, se pueden considerar otros elementos a la hora de colocar los sensores ópticos, con el objetivo de que las mediciones de luminancia permitan de manera óptima detectar una intrusión en el terminal de pago electrónico.

El hecho de disponer de varios sensores también puede permitir asegurar la verificación: si un valor, proporcionado por un sensor, cae significativamente, mientras que otro sensor, que se supone que mide la misma fuente luminosa, no ha bajado, esto presagia un intento de fraude.

Análogamente, si el terminal de pago electrónico a proteger no posee fuentes luminosas internas (por ejemplo, por que no ofrece la función de retroiluminación del teclado o de la ranura de inserción de tarjeta con chip), se añaden fuentes luminosas específicas de la invención, asociadas con los sensores ópticos utilizados.

Por último, la elección de la ubicación del o los sensores ópticos permite parametrizar el método de detección óptica para tener en cuenta el contexto específico de la implementación del sistema de detección óptica. Por lo tanto, ahora se describirá con más detalle la implementación del método de detección óptica según este modo de realización de la invención.

Según otras variantes, una fuente luminosa puede corresponder a una fuente incandescente, un neón, etc.

5.2.2 Ejemplo de método de detección de intrusión

La Figura 4 ilustra los pasos principales para un sensor óptico dado, sabiendo que este método de detección óptica se puede implementar con independencia del número de sensores ópticos utilizados y que puede correlacionar los resultados obtenidos para cada sensor óptico con el fin de optimizar la detección de intrusión. Estos pasos principales son ejecutados, por ejemplo, por el módulo de seguridad del terminal de pago electrónico, o un módulo asociado, a partir de las señales recibidas y transmitidas por el o los sensores ópticos.

Así pues, el método de detección comprende un primer paso 41 de cálculo de un valor absoluto de una diferencia entre una intensidad lumínica, o luminancia, medida por un sensor óptico y una intensidad lumínica, o luminancia, de referencia. Esta luminancia de referencia puede estar asociada a una o varias fuentes luminosas, puede tener en cuenta la influencia de la luz externa (por ejemplo, mediante el uso de un sensor adicional que mida la luz externa) u otros criterios.

Además, se puede recalcular en cada medición la intensidad de referencia, ya sea tomando directamente el último valor medido o empleando los n últimos valores medidos con su marca de tiempo, y suavizándolos luego con una media móvil o "deslizante", para poder tener en cuenta, por ejemplo, criterios tales como el envejecimiento de la guía de luz o de los ledes, o la acumulación de polvo en los mismos, etc. Por lo tanto, se implementan algoritmos de comparación, teniendo en cuenta las mediciones de intensidad ya realizadas, con el fin de asegurar la fiabilidad de la detección de intrusión.

A continuación se efectúa una comparación con un umbral predeterminado, para determinar si la variación de luminancia calculada supera o no este umbral.

Si es así, entonces se detecta una intrusión durante un paso 42 de detección de intrusión, seguido de un paso 43 de generación de alarma.

Según variantes de realización, el resultado de la comparación se interpreta de distintas maneras, por ejemplo, cuando hay que correlacionarlo con otros parámetros, tales como el resultado de un control de temperatura implementado por separado, el resultado del método de detección relativo a uno u otros varios sensores, un parámetro temporal que permita detectar solamente variaciones rápidas en la luminancia y descartar variaciones lentas atribuibles más bien al funcionamiento normal de un terminal de pago electrónico (envejecimiento de la guía de luz o de los ledes o acumulación de polvo en los mismos, etc.), etc.

Análogamente, el umbral de comparación que permite detectar o no una posible intrusión en el terminal de pago electrónico depende de una pluralidad de parámetros, tales como la ubicación del sensor o el porcentaje de contribución de las fuentes luminosas asociadas.

Además, según este modo de realización de la invención el método de detección se puede ejecutar, por ejemplo, en el momento de activar las medidas de seguridad del terminal de pago electrónico, con el fin de optimizar la seguridad del terminal de pago electrónico cuando se utilice.

También se puede ejecutar el procedimiento en cada apagado del terminal y en cada reinicio del terminal, a fin de detectar principalmente las intrusiones que se produzcan fuera de los períodos de uso del terminal de pago electrónico. De hecho, las intrusiones que requieren el desmontaje de un terminal de pago electrónico rara vez son posibles durante su uso, y con frecuencia ocurren después de un robo de este terminal de pago electrónico y una

nueva puesta en servicio una vez que se ha realizado la intrusión. Por lo tanto, el método de detección según este modo de realización prevé almacenar, en cada apagado del terminal de pago electrónico, las mediciones de luminancia realizadas por el o los sensores, con el fin de compararlas con las primeras mediciones realizadas cuando se reinicia el terminal de pago electrónico.

Por último, se puede ejecutar periódicamente el procedimiento de detección durante el uso del terminal de pago electrónico, a fin de detectar intrusiones incluso cuando el terminal de pago electrónico está encendido. Una vez detectada una intrusión, según el modo de realización descrito en lo que antecede, se genera una alarma con el fin de pasar el terminal al modo "robo". Por ejemplo, la alarma generada puede consistir en un mensaje en el terminal, en el cual ya no se puede realizar ninguna transacción. A continuación, se debe devolver obligatoriamente a fábrica dicho terminal, como establecen las técnicas actuales conocidas de protección de terminales de pago electrónico y como ocurre, por ejemplo, en otras técnicas de detección de apertura y fraude.

5.3. Variantes de realización

Según algunas variantes de realización, las mediciones de luminancia realizadas por los sensores ópticos son sometidas a variaciones voluntarias de la iluminación de las fuentes luminosas asociadas, con el propósito de asegurar la detección óptica de acuerdo con la invención.

Por ejemplo, según una primera variante de realización, se pueden enviar a los ledes señales aleatorias (por ejemplo, alternancias de encendidos y apagados "largos y cortos") conocidas únicamente por el procesador del módulo de seguridad del terminal de pago electrónico, y así se puede verificar la correspondencia con las señales recibidas por el sensor. Esto permite, en particular, evitar que un atacante deslumbre gradualmente el sensor, utilizando una fuente luminosa adicional, y después "puentee" el sensor con una resistencia equivalente, o incluso espíe la señal emitida por la fotorresistencia, para reemplazarla por una señal equivalente. En efecto, si esta señal emitida varía dependiendo de las señales aleatorias no predecibles emitidas por los ledes, no es posible "simularla".

Según otra variante, se prevé encender los ledes alternativamente, lo que conduce no solo a alternancias de encendidos y apagados, sino también a diferentes niveles de intensidad lumínica para cada sensor, en particular cuando dependen de la contribución de varios ledes. Esto es especialmente útil si se utilizan en paralelo varias versiones de guías de luz. En ese caso, la distribución de la luz es distinta dependiendo de la guía de luz, y será difícil que un "espía" la reemplace con otra guía de luz (distinta diferencia mínima de definición, o de acumulación de polvo, etc.).

5.4. Arquitectura simplificada de un módulo de detección de intrusión

Se describe, en relación con las Figuras 5 y 6, un ejemplo de sistema de detección de intrusión, que comprende medios para ejecutar el método descrito en lo que antecede (en particular, medios 51 de cálculo y comparación, medios 52 de detección de intrusión y medios 53 de generación de alarma).

Así, tal como se ilustra en la Figura 5, un sistema 500 o módulo 500 de este tipo, integrado por ejemplo en el circuito impreso de un dispositivo electrónico, comprende al menos un sensor óptico (C1) conectado a al menos un módulo de seguridad (MS) del dispositivo electrónico, estando configurados el sensor óptico y el módulo de seguridad para detectar una variación de la intensidad lumínica medida por el sensor óptico con respecto a una intensidad lumínica de referencia asociada con al menos una fuente luminosa predeterminada (SL1) dentro del dispositivo electrónico, siendo la variación de la intensidad lumínica representativa de un riesgo de intrusión en el dispositivo electrónico.

Se describe ahora, en relación con la Figura 6, este sistema 500, también denominado módulo de detección.

Por ejemplo, el módulo comprende una memoria 61 constituida por una memoria intermedia, una unidad 62 de procesamiento equipada, por ejemplo, con un microprocesador y controlada por el programa informático 63, que implementa un método de detección de intrusión según los diversos modos de realización descritos en lo que antecede.

Se cargan al principio en una memoria, por ejemplo, las instrucciones de código del programa informático 63 antes de ser ejecutadas por el procesador de la unidad 62 de procesamiento. La unidad 62 de procesamiento recibe como entrada, por ejemplo, un valor medido de intensidad lumínica (por ejemplo, una medida de luminancia) y al menos un valor de intensidad lumínica (por ejemplo, una medida de luminancia) de referencia. El microprocesador de la unidad 62 de procesamiento ejecuta los pasos del método de detección de intrusión, de acuerdo con las instrucciones del programa informático 63, para generar una alarma.

Cabe señalar que los valores de intensidad medidos, así como los valores de referencia, se almacenan en una zona de memoria protegida, para evitar que un "espía" pueda explotar esos datos.

REIVINDICACIONES

1. Sistema de detección de una intrusión en un dispositivo electrónico, comprendiendo dicho sistema al menos un sensor óptico (C1) conectado a al menos un módulo de seguridad (MS) de dicho dispositivo electrónico, estando configurados dicho sensor óptico y dicho módulo de seguridad para detectar una variación de la intensidad lumínica medida por dicho sensor óptico con respecto a una intensidad lumínica de referencia asociada con al menos una fuente luminosa predeterminada (SL1) dentro de dicho dispositivo electrónico, al menos una fuente luminosa (SL1) esta que proporciona la retroiluminación del teclado y/o de la ranura de inserción de tarjeta de dicho dispositivo electrónico, siendo dicha variación de la intensidad lumínica representativa de un riesgo de intrusión en dicho dispositivo electrónico,
y comprendiendo dicho dispositivo electrónico al menos un módulo de seguridad (MS) y medios para transmitir hacia al menos dicha fuente luminosa al menos una señal aleatoria de encendido/apagado o una señal aleatoria de variación, teniendo en cuenta dicha detección óptica implementada por dicho sensor óptico y dicho módulo de seguridad la señal aleatoria transmitida.

2. Sistema de detección de una intrusión según la reivindicación 1, **caracterizado por que** dicho al menos un sensor pertenece al grupo que comprende al menos:

- una fotorresistencia;
- un fotodiodo;
- un sensor tipo DTC.

3. Sistema de detección de una intrusión según la reivindicación 1, **caracterizado por que** dicha al menos una fuente luminosa predeterminada corresponde a un diodo electroluminiscente.

4. Sistema de detección de una intrusión según la reivindicación 1, **caracterizado por que** dicho al menos un sensor óptico está implantado en dicho dispositivo electrónico en una ubicación elegida en función de al menos un criterio perteneciente al grupo que comprende:

- una contribución de al menos una fuente luminosa predeterminada dentro de dicho dispositivo electrónico;
- un gradiente de luminancia alrededor de dicha ubicación;
- una contribución de una fuente luminosa externa a dicho dispositivo electrónico.

5. Sistema de detección de una intrusión según la reivindicación 1, **caracterizado por que** comprende asimismo un filtro infrarrojo o ultravioleta aplicado sobre al menos una parte de la superficie a proteger de dicho dispositivo electrónico.

6. Método de detección de una intrusión en un dispositivo electrónico que emplea un sistema de detección según la reivindicación 1, comprendiendo el método un paso de detección óptica de una intrusión cuando al menos un valor absoluto de una diferencia entre:

- una intensidad lumínica medida por dicho al menos un sensor óptico y
- una intensidad lumínica de referencia

supera un umbral predeterminado,
y comprendiendo un paso de transmitir hacia al menos una de dichas fuentes luminosas internas de dicho dispositivo electrónico al menos una señal aleatoria de encendido/apagado o una señal aleatoria de variación, fuentes luminosas internas estas que proporcionan la retroiluminación del teclado y/o de la ranura de inserción de tarjeta de dicho dispositivo electrónico, y en que dicho paso de detección óptica tiene en cuenta la señal aleatoria transmitida.

7. Método de detección de una intrusión según la reivindicación 6, **caracterizado por que** dicho paso de detección óptica también tiene en cuenta un resultado de medida adicional de temperatura y/o de intensidad lumínica obtenido por otro sensor.

8. Método de detección de una intrusión según la reivindicación 6, **caracterizado por que** comprende un paso de generar una alarma cuando se detecta una intrusión durante dicho paso de detección óptica, siendo dicha alarma de un tipo perteneciente al grupo que comprende al menos:

- el paso de dicho dispositivo electrónico al modo "robo";
- la visualización de un mensaje de alarma en dicho dispositivo electrónico;
- una combinación de los tipos de alarma arriba indicados.

9. Método de detección de una intrusión según la reivindicación 6, **caracterizado por que** comprende un paso de almacenar al menos un valor de intensidad lumínica medido por al menos un sensor óptico.

10. Método de detección de una intrusión según la reivindicación 6, **caracterizado por que** comprende un paso de

comparar al menos un valor de intensidad lumínica medido por al menos un sensor con al menos un valor de intensidad lumínica previamente almacenado.

11. Método de detección de una intrusión según la reivindicación 6, **caracterizado por que** lo desencadena un suceso perteneciente al grupo que comprende al menos:

- la activación de las medidas de seguridad de dicho dispositivo electrónico;
- cualquier apagado de dicho dispositivo electrónico;
- cualquier reinicio de dicho dispositivo electrónico;
- periódicamente;
- antes de una transacción protegida;
- una combinación de al menos dos sucesos de los arriba indicados.

12. Dispositivo electrónico que comprende al menos un sistema de detección de una intrusión según la reivindicación 1 para implementar el método de detección de intrusión según la reivindicación 6.

13. Programa informático descargable desde una red de comunicaciones y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, programa informático que comprende instrucciones de código de programa para ejecutar un método según una cualquiera de las reivindicaciones 6 a 12 cuando este programa es ejecutado por un procesador.

14. Soporte de grabación legible por ordenador en el cual se ha grabado un programa informático que comprende instrucciones para ejecutar los pasos del método según una cualquiera de las reivindicaciones 6 a 12.

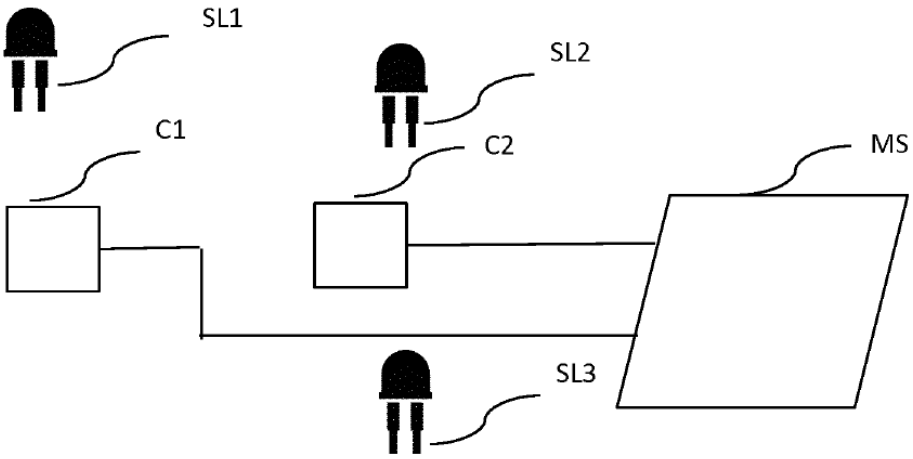

Figura 1

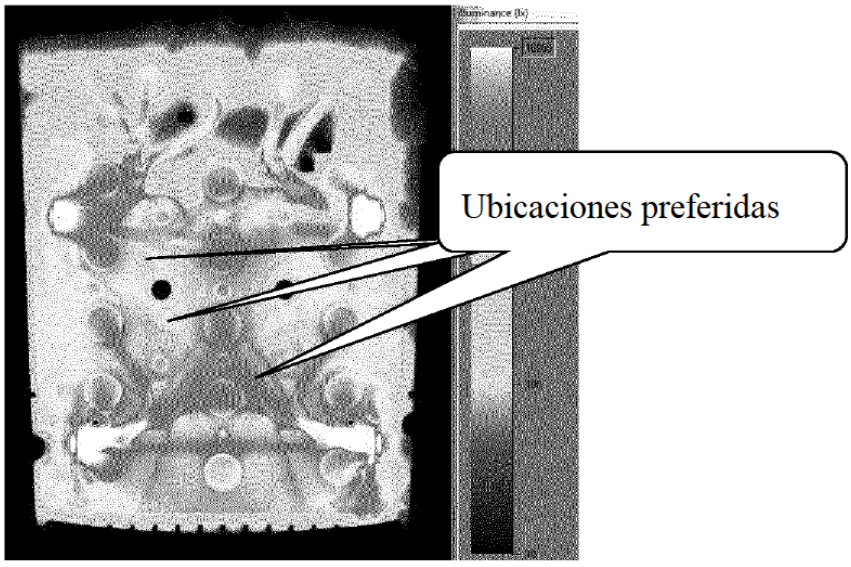

Figura 3

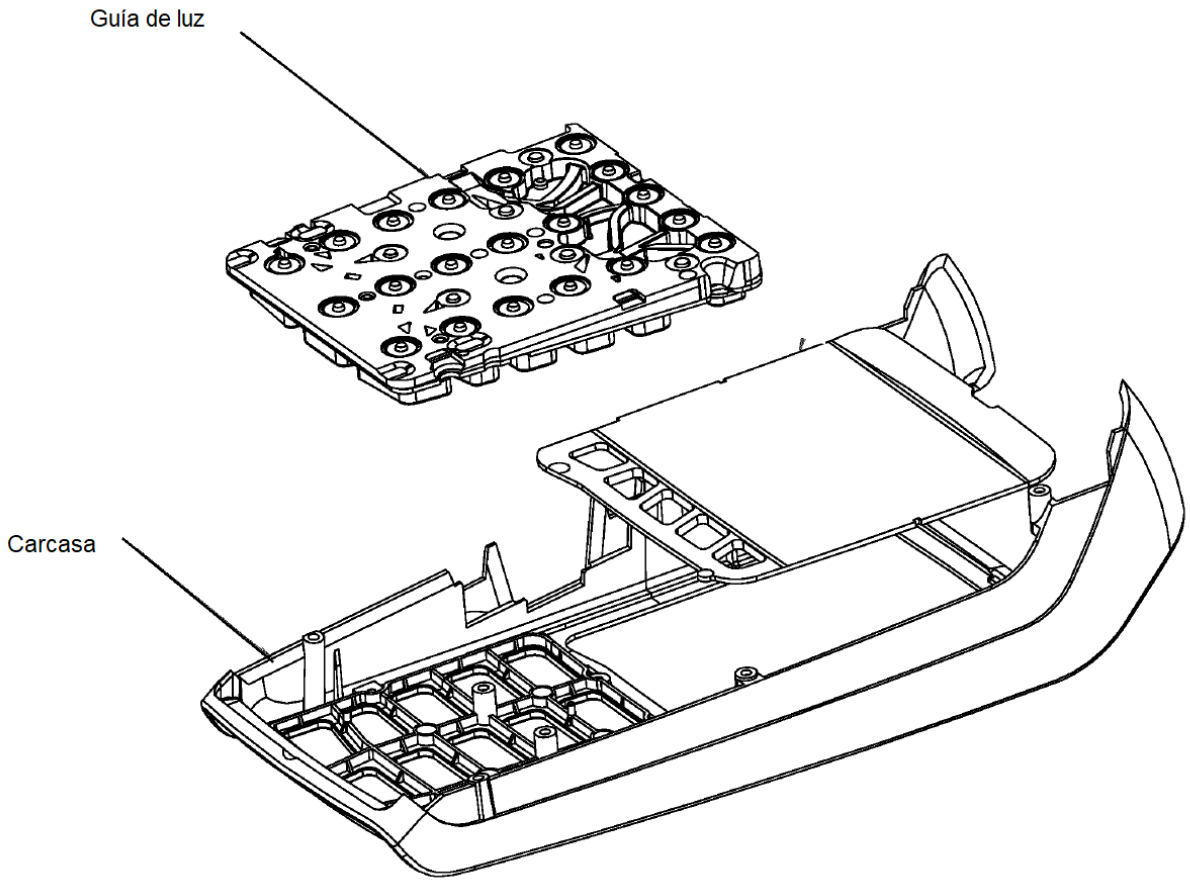

Figura 2

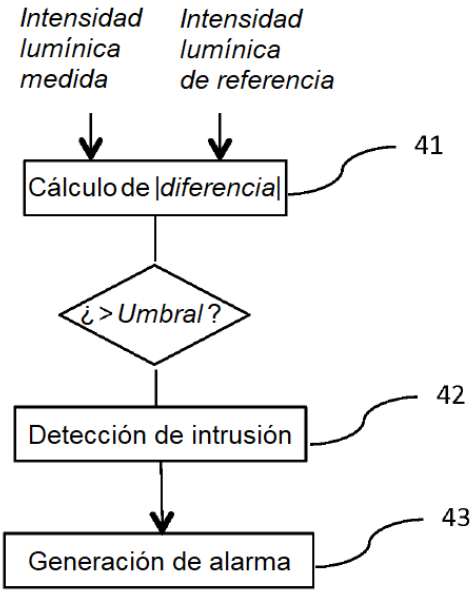

Figura 4

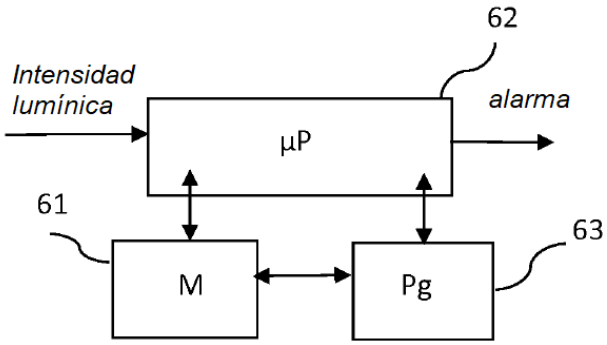

Figura 6

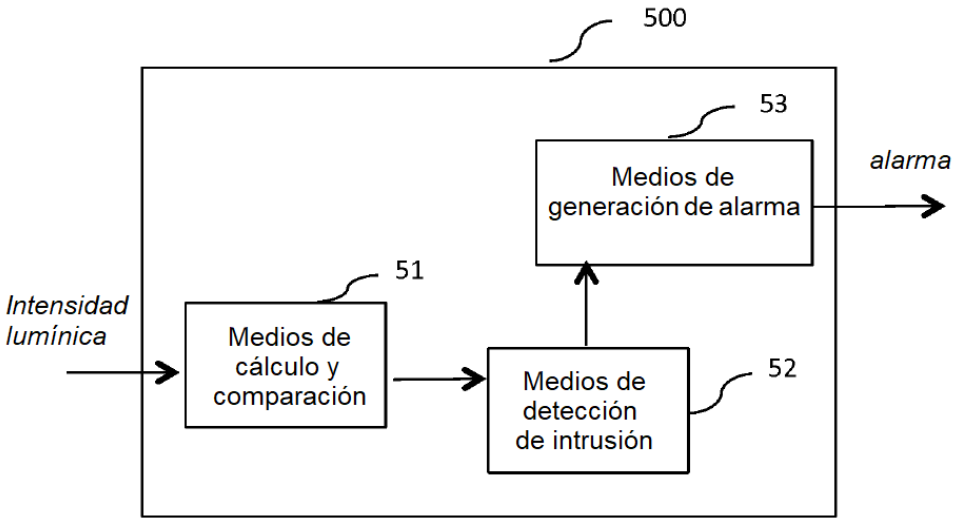

Figura 5