(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 605 241**

(51) Int. CI.:

G06F 21/86 (2013.01)
G06F 21/83 (2013.01)
G06K 7/00 (2006.01)
G06Q 20/34 (2012.01)
G07F 7/08 (2006.01)
G07F 7/10 (2006.01)
H05K 5/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.07.2009 PCT/FR2009/051404**

(87) Fecha y número de publicación internacional: **21.01.2010 WO10007314**

(96) Fecha de presentación y número de la solicitud europea: **15.07.2009 E 09737060 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2313844**

(54) Título: **Dispositivo y procedimiento de protección de un sistema electrónico contra un acceso no autorizado**

(30) Prioridad:

17.07.2008 FR 0854862

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2017

(73) Titular/es:

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

(72) Inventor/es:

LACROIX, PIERRE

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

DESCRIPCIÓN

Dispositivo y procedimiento de protección de un sistema electrónico contra un acceso no autorizado

Campo de la invención

La presente invención se refiere a un dispositivo y un procedimiento de protección de un sistema electrónico contra un acceso no autorizado.

Exposición de la técnica anterior

Ciertos sistemas electrónicos, por ejemplo los terminales de pago electrónico, comprenden un circuito impreso contenido en una caja. Pueden soldarse unos componentes electrónicos sobre las dos caras del circuito impreso o estar eléctricamente conectados al circuito impreso. Se trata, por ejemplo de microprocesadores, de un conector de tarjeta de memoria, una pantalla de presentación, etc.

Las reglas de seguridad editadas por los organismos de autorización imponen generalmente prever unos dispositivos de protección que permitan impedir el acceso a ciertos componentes electrónicos fijos al circuito impreso, por ejemplo los microprocesadores.

Un primer ejemplo de dispositivo de protección adaptado a un terminal de pago electrónico corresponde a unas teclas ficticias previstas a la altura de una membrana que forma el teclado del terminal. Una tecla ficticia se une al resto de la membrana mediante un borde periférico, como con una tecla clásica, pero no es visible desde el exterior del terminal.

Cuando la caja del terminal se cierra, la tecla ficticia está presionada permanentemente por la caja de manera que llega a apoyarse contra el circuito impreso. En este caso, la tecla ficticia cierra un interruptor previsto a la altura del circuito integrado. El cierre del interruptor se detecta por un circuito de tratamiento no representado. Cuando un individuo intenta abrir la caja para acceder a su contenido, la tecla ficticia ya no queda presionada por la caja y es repuesta por la acción del reborde hacia la posición de reposo lo que implica la apertura del interruptor asociado. El circuito de tratamiento está adaptado para detectar esta apertura, indicando que ha tenido lugar una apertura no autorizada de la caja.

Otro ejemplo de dispositivo de protección adaptado a un terminal de pago electrónico corresponde a un dispositivo de rejilla. Un dispositivo de protección de ese tipo corresponde, por ejemplo, a un circuito flexible que incluye un apilado de películas flexibles y aislantes que contienen una o varias pistas conductoras, por ejemplo de cobre. Las pistas forman unas líneas de seguridad dispuestas en zigzag y unidas al circuito de tratamiento. El circuito de tratamiento está adaptado para determinar si la línea de seguridad ha sido interrumpida, la interrupción de una línea de seguridad corresponde a un acceso no autorizado al circuito impreso.

Cada uno de los ejemplos de dispositivos de protección descritos anteriormente presenta unos inconvenientes. En efecto, en el caso de los dispositivos de protección de teclas ficticias, un usuario podría, sin abrir la caja y eliminando, por ejemplo mediante raspado, recorte, mecanizado, fresado, etc., una parte de la membrana del teclado, acceder a las pistas metálicas del circuito impreso y por tanto a unas informaciones contenidas en el circuito impreso sin que se detecte ningún acceso no autorizado. Otro inconveniente en un dispositivo de protección de teclas ficticias es que puede detectarse un acceso no autorizado de manera errónea durante un desplazamiento de una tecla ficticia en el caso de que la caja del sistema electrónico se someta a un choque. Además, para un dispositivo de protección de rejillas, un usuario podría conseguir desplazar, al menos en parte, el circuito flexible del dispositivo de rejilla sin interrumpir las pistas conductoras que contiene y de ese modo acceder a las pistas metálicas del circuito impreso sin que se detecte ningún acceso no autorizado.

El documento XP-310027733 divulga un sistema de protección de un circuito impreso que utiliza un captador capacitivo y un sistema de detección de variaciones de la capacidad de una pista conductora.

El documento US-6983378-B1 divulga un sistema de detección de intrusión en una caja que contiene unas informaciones sensibles en el que a continuación de una variación de la capacidad de una pista conductora se suprimen las informaciones sensibles.

Resumen de la invención

La presente invención se dirige a un dispositivo de protección de un sistema electrónico, contra los accesos no autorizados a un circuito electrónico contenido en la caja del sistema electrónico, que sea difícil de neutralizar.

Otro objeto de la presente invención se dirige un dispositivo de protección poco sensible a los choques.

Un objeto de un modo de realización de la presente invención es proponer un sistema de protección configurable por producto o familia de productos.

Con este fin, un aspecto de la presente invención prevé un sistema electrónico que incluye un circuito impreso contenido en una caja. El sistema comprende un dispositivo de protección que comprende:

unas pistas conductoras soportadas por el circuito impreso y teniendo cada una un extremo libre y que se extiende a la altura del circuito impreso;
un primer circuito integrado conectado a las pistas conductoras y adaptado para detectar una variación de la capacidad vista por cada pista conductora; y
un segundo circuito integrado, eventualmente coincidente con el primer circuito integrado, que comprende una memoria configurable para seleccionar ciertas de las pistas conductoras. El segundo circuito integrado está adaptado para determinar que ha tenido lugar un acceso autorizado o no autorizado a partir de la detección de la variación de la capacidad vista por al menos una de las pistas conductoras seleccionadas.

Según un modo de realización de la invención, la configuración de la memoria es diferente de un sistema a otro o de una familia de sistemas a otra.

Según un modo de realización de la invención el trazado de dichas pistas conductoras está fuera de la verticalidad de los componentes soportados por el circuito impreso.

Según un modo de realización de la invención, el circuito impreso es rígido, comprendiendo el sistema electrónico un componente electrónico unido al circuito impreso mediante un circuito impreso flexible, extendiéndose al menos una de dichas pistas conductoras a la altura del circuito impreso flexible.

Según un modo de realización de la invención, algunas de dichas pistas conductoras están aisladas eléctricamente entre sí y al menos dos de dichas pistas conductoras se solapan y/o son adyacentes a la altura de una parte del circuito impreso.

Según un modo de realización de la invención, el primer circuito integrado está unido al segundo circuito integrado mediante un enlace serie.

Otro aspecto de la presente invención prevé un procedimiento de determinación de un acceso no autorizado a un circuito impreso contenido en una caja de un sistema electrónico. El procedimiento comprende las siguientes etapas:

prever unas pistas conductoras que tengan cada una un extremo libre y que se extiendan al menos a la altura del circuito impreso, un primer circuito integrado conectado a las pistas conductoras y un segundo circuito integrado, eventualmente coincidente con el primer circuito integrado, que comprende una memoria;
almacenar en la memoria unos parámetros de selección de ciertas de las pistas conductoras;
disponer el primer circuito integrado para detectar, para cada pista conductora, si la capacidad vista por la pista conductora varía; y
disponer el segundo circuito integrado para determinar que ha tenido lugar un acceso autorizado o no autorizado a partir de la detección de la variación de la capacidad vista por al menos una de las pistas conductoras seleccionadas.

Según un modo de realización de la invención, a cada pista conductora corresponde un identificador. El procedimiento consiste en disponer el primer circuito integrado para transmitir al segundo circuito integrado el identificador de la pista conductora para la que se ha detectado la variación de la capacidad.

Según un modo de realización de la invención, los parámetros comprenden al menos una lista de identificadores de al menos ciertas pistas conductoras. El segundo circuito integrado determina que ha tenido lugar un acceso autorizado o no autorizado si el identificador de la pista para la que se ha detectado la variación de la capacidad pertenece a la lista.

Según un modo de realización de la invención, los parámetros comprenden al menos una operación lógica que utiliza los identificadores de al menos ciertas de las pistas conductoras. El segundo circuito integrado determina que ha tenido lugar un acceso autorizado o no autorizado si se detectan unas variaciones de capacidad para las pistas conductoras asociadas a dichos identificadores y si se verifica la operación lógica.

Según un modo de realización de la invención se almacenan varios juegos de parámetros en la memoria. El procedimiento consiste en proporcionar al segundo circuito integrado una señal de selección de un juego de parámetros entre dichos juegos de parámetros, siendo utilizado dicho juego de parámetros seleccionado por el segundo circuito integrado para determinar que ha tenido lugar un acceso autorizado o no autorizado.

Según un modo de realización de la invención, la selección de las pistas conductoras difiere según el sistema o según la familia de sistemas.

Según un modo de realización de la invención, el procedimiento comprende, además, las siguientes etapas:

determinar unos valores de calibrado a partir de un circuito impreso de referencia;
realizar una operación de calibrado del primer circuito integrado del circuito impreso a partir de dichos valores de calibrado; y
disponer el primer circuito integrado para emitir una señal de anomalía en el caso de que se detecte una variación de la capacidad vista por al menos una de las pistas conductoras.

Breve descripción de los dibujos

Estos objetos, características y ventajas, así como otros se expondrán en detalle en la descripción que sigue de modos de realización particulares realizada a título no limitativo en relación con las figuras adjuntas entre las que:

La figura 1 representa, de manera esquemática, un terminal de pago electrónico;
la figura 2 es una vista desde arriba esquemática de un circuito impreso del terminal de la figura 1 que comprende un dispositivo de protección según un ejemplo de realización de la invención;
las figuras 3 y 4 son unas secciones parciales y esquemáticas del circuito impreso de la figura 2; y
las figuras 5 y 6 ilustran, bajo la forma de esquemas de bloques, unas etapas de ejemplos de procedimientos de utilización del dispositivo de protección de la figura 2.

Descripción detallada

Por razones de claridad, los mismos elementos se han designado por las mismas referencias en las diferentes figuras. Además, solo se describirán los elementos necesarios para la comprensión de la invención.

La figura 1 representa, de manera esquemática, un ejemplo de realización de un sistema electrónico 10, por ejemplo un terminal de pago electrónico. El terminal 10 comprende una caja 12 constituida por una parte superior de caja 14 unida a una parte inferior de caja 16. Se prevén unas aberturas 17 en la parte superior de la caja 14 para una pantalla de presentación 18 y unas teclas 20 que pertenecen, por ejemplo, a un teclado. Además, se prevé una abertura 21 en la caja 12 para permitir la introducción de tarjetas de memoria, por ejemplo unas tarjetas bancarias, no representadas.

La figura 2 es una vista desde arriba esquemática de un ejemplo de realización de circuito impreso 30 contenido en la caja 12 y provisto de un dispositivo de protección 32 según un ejemplo de realización de la invención.

Las figuras 3 y 4 representan unas secciones transversales esquemáticas del circuito impreso 30 de la figura 2 según dos ejemplos de realización del circuito impreso 30.

En el ejemplo de realización representado en la figura 3, el circuito impreso 30 está constituido por un soporte 34 rígido y aislante que comprende dos caras opuestas 36 y 38. Se disponen unas pistas conductoras 40, por ejemplo de cobre, sobre la cara 36 y se disponen unas pistas conductoras 42, por ejemplo de cobre, sobre la cara 38. Puede preverse una capa de un barniz de protección sobre cada cara 36, 38. Unas vías 44 que atraviesan el soporte 34 unen ciertas pistas 40 a unas pistas 42.

En el ejemplo de realización representado en la figura 4, el sustrato 30 corresponde a una estructura multicapa que comprende una capa de base rígida y aislante 46 recubierta con una capa aislante secundaria 48. Se prevén unas pistas conductoras 50, por ejemplo de cobre, sobre la capa de base 46 y se recubren por la capa secundaria 48. Se disponen unas pistas conductoras 52 sobre la capa aislante secundaria 48. Unas vías 54 que atraviesan la capa secundaria 48 unen ciertas pistas conductoras 52 a unas pistas 50.

En la figura 2, se han representado de manera esquemática mediante unos rectángulos unos componentes 56 fijos al circuito impreso 30. Además, la pantalla 18 puede fijarse al circuito impreso 30 por medio de un circuito impreso flexible 58, o circuito flexible, cuyos extremos se conectan a la pantalla 18 y al circuito impreso 30 por medio de conectores 60, 62. Las pistas conductoras del circuito impreso 30 que participan en el funcionamiento clásico del terminal 10 no se representan.

El dispositivo de protección 32 comprende un captador de posición capacitivo 70 (sensor) unido a un circuito de protección contra un acceso no autorizado 71 (µP) mediante un enlace 72, por ejemplo un enlace serie. El captador 70 corresponde, por ejemplo, a un circuito integrado de la familia CY8C20x34 comercializado bajo la denominación CapSense por la sociedad Cypress Semiconductor Corporation.

El captador 70 se conecta a unas pistas conductoras 74 soportadas por el circuito impreso 30 y preferentemente repartidas sobre éste en función de las zonas a proteger. Las pistas 74 están aisladas unas de otras y cada pista 74 comprende un extremo libre. Preferentemente, las pistas 74 se extienden sustancialmente sobre la totalidad del circuito impreso 30, fuera de la verticalidad de los componentes. En particular, ciertas pistas conductoras 74 pueden extenderse a la altura del circuito flexible 58. Se han representado en la figura 2 en trazos continuos y en trazos

discontinuos unas pistas conductoras 74 de dos niveles diferentes. A título de ejemplo, cuando se realiza el circuito impreso 30 según el ejemplo de realización representado en la figura 3, las pistas conductoras 74 de trazo continuo corresponden a unas pistas 40 y las pistas conductoras 74 en trazos de puntos corresponden a unas pistas 42. Cuando el circuito impreso 30 se realiza según el ejemplo de realización representado en la figura 4, las pistas conductoras 74 de trazo continuo corresponden a unas pistas 52 y las pistas conductoras 74 de trazos de puntos corresponden a unas pistas conductoras 50. Puede preverse un plano de masa a la altura del circuito impreso 30 rodeando cada pista conductora 74 o ciertas de entre ellas y conectado al captador 70.

Cuando una vía 44 o 54 une dos pistas en unos niveles diferentes, al menos una de ellas tiene un extremo libre. Se puede considerar por tanto que se trata de la misma pista realizada en varios niveles y que tiene un extremo libre.

Pueden intercambiarse unos datos entre el circuito de protección 71 y un sistema externo al terminal 10 por medio de un enlace 78, por ejemplo un enlace serie o paralelo. Pueden intercambiarse unos datos entre el captador 70 y un sistema externo al terminal 10 por medio de los enlaces 72, 78, y del circuito 71.

A título de ejemplo, el captador 70 está adaptado para detectar, para cada pista conductora 74, que ha tenido lugar una variación de la capacidad vista por la pista conductora 74 y para proporcionar, en este caso, al circuito de protección 71, mediante el enlace 72, una señal de anomalía representativa de un identificador de la pista conductora 74 para la que se ha detectado una variación de capacidad. El captador 70 puede verificar de manera sucesiva, pista 74 tras pista 74, si la capacidad vista por cada pista 74 no ha variado. A título de ejemplo, el captador 70 proporciona una señal de anomalía asociada a una pista 74 dada cuando la diferencia (en valor absoluto) entre la capacidad vista por la pista conductora 74 y un valor de referencia es superior a un umbral. Se describe una descripción más detallada de un ejemplo de funcionamiento del captador 70 en las notas de explicación AN 2393 y AN 14459 proporcionadas por la sociedad Cypress Semiconductor Corporation.

Cuando un individuo intenta acceder al circuito impreso 30, por ejemplo por medio de herramientas, la presencia de la herramienta en la proximidad del circuito impreso 30 implica una variación de la capacidad vista por al menos una de las pistas conductoras 74 adyacentes a la herramienta, lo que se detectará por el captador 70. La variación de capacidad puede obtenerse sin que la herramienta esté en contacto con el circuito impreso 30. La detección de la variación de capacidad de las pistas 74 permite por tanto detectar que ha tenido lugar un acceso en la caja 12.

Puede realizarse una operación de calibración del captador 70 para fijar, para cada pista conductora 74, el valor de referencia de capacidad y el umbral de comparación. Se describe una descripción más detallada de un ejemplo de operación de calibración del captador 70 en la nota de explicación AN 42137 proporcionada por la sociedad Cypress Semiconductor Corporation. La operación de calibración puede realizarse conectando un sistema externo al captador 70 por medio de los enlaces 72, 78 y del circuito 71.

El circuito de protección 71 está adaptado para determinar si ha tenido lugar un acceso no autorizado al interior de la caja 12 a partir de las señales de anomalía proporcionadas por el captador 70. Cuando el circuito 71 determina que ha tenido lugar un acceso no autorizado, puede ordenar la detención del terminal de pago 10, el borrado de datos sensibles almacenados en el terminal de pago 10, etc.

En el presente ejemplo de realización, el circuito de detección 71 comprende una memoria 80 (MEM) en la que se almacenan varios juegos de condiciones o de parámetros. Cada juego de condiciones corresponde a un conjunto de condiciones a partir de los que el circuito 71 determina si ha tenido lugar un acceso autorizado o no autorizado cuando recibe una o varias señales de anomalía proporcionadas por el captador 70. En un instante dado, el circuito de protección 71 no utiliza más que uno de los juegos de condiciones. Los juegos de condiciones pueden modificarse mediante un sistema externo conectado al terminal de pago 10 por medio del enlace 78. A título de ejemplo, un juego de condiciones puede comprender una lista de los identificadores de las pistas conductoras 74 que deben tenerse en cuenta para la detección de un acceso no autorizado. En este caso, el circuito 71 no determina que ha tenido lugar un acceso no autorizado más que si recibe la señal de anomalía correspondiente a un identificador que pertenece a la lista. Según otro ejemplo, una condición puede corresponder a una operación lógica que une unos identificadores de las pistas 74. Cuando el circuito de protección 71 recibe sucesivamente las señales de anomalía asociadas a diferentes pistas 74, determina que ha tenido lugar un acceso no autorizado solamente si se verifica la operación lógica que une los identificadores de estas pistas.

La utilización de juegos de condiciones permite delimitar, de manera simple y modulable, unas zonas del circuito impreso 30, a las que se desea impedir el acceso, unas zonas para las que se desea autorizar el acceso incluso si las pistas conductoras 74 se extienden sobre la casi totalidad del circuito impreso 30. La delimitación de la zona del circuito impreso 30 a la que se desea autorizar el acceso puede obtenerse mediante una condición que indica al circuito 71 no detectar un acceso no autorizado en el caso de que el captador 70 transmita sucesivamente unas señales de anomalía correspondientes a un conjunto determinado de pistas 74. A título de ejemplo, en el caso en el que el juego de condiciones indica que debe determinarse un acceso no autorizado salvo en el caso en el que el captador 70 transmita unas señales de anomalía correspondientes a las pistas P1 y P2, esto significa que el acceso no está autorizado para el conjunto de las partes del circuito impreso 30 a la altura de las que se extienden las pistas conductoras 74 con excepción de la parte del circuito impreso 30 en la proximidad del cruce entre las pistas P1 y P2.

La misma división puede obtenerse previendo dos pistas conductoras 74 suficientemente próximas entre sí en la parte del circuito impreso 30 para la que se desea autorizar el acceso. Las pistas conductoras 74 pueden ser entonces del mismo “nivel”.

Una partición dada del circuito impreso 30 en zonas de acceso autorizado y zonas de acceso no autorizado corresponde a un juego de condiciones dado. Varios juegos de condiciones, correspondiente cada uno a una partición particular, pueden almacenarse en la memoria 80 del circuito de protección 71. El captador 70 utiliza en un instante dado un único juego de condiciones. La partición del circuito impreso 30 puede modificarse mediante la selección del juego de condiciones utilizado por el circuito 71.

Una partición del circuito impreso 30 en zonas de acceso autorizado y zonas de acceso no autorizado puede ser deseable en ciertos casos. Según un ejemplo, en funcionamiento, puede ser deseable autorizar un acceso a ciertas partes del circuito impreso 30 a un usuario del terminal 10. A título de ejemplo, un terminal 10 puede comprender una tarjeta de chips del tipo tarjeta SIM (del inglés Subscriber Identity Module) propiedad del usuario. Puede ser deseable entonces autorizar el cambio de la tarjeta SIM por el usuario. La presente invención permite, de manera ventajosa, adaptar el número y la posición de las zonas de acceso autorizado del terminal 10 en función de la configuración de funcionamiento del terminal 10. De ese modo, cuando el terminal 10 comprende una tarjeta SIM, el circuito 71 utiliza un juego de condiciones que autorizan un acceso a la tarjeta SIM mientras que cuando el terminal 10 no comprende una tarjeta SIM, el circuito 71 utiliza un juego de condiciones que no autorizan un acceso al emplazamiento del circuito impreso 30 que, en la configuración descrita anteriormente, está presente una tarjeta SIM. Según otro ejemplo, durante una operación de mantenimiento, es deseable permitir a un operario cualificado acceder a la totalidad o al menos a ciertas partes del circuito impreso 30.

La figura 5 representa, bajo la forma de un esquema de bloques, las etapas del procedimiento de utilización del circuito impreso 30 de la figura 2 según un ejemplo de realización de la invención.

En la etapa 90, se realiza la selección del modo de funcionamiento del circuito de protección 71. Esto corresponde a la selección del juego de condiciones almacenado en la memoria 80 a utilizar por el circuito 71. Esto puede obtenerse mediante la conexión de un sistema externo al terminal 10 por medio del enlace 78. Esto puede obtenerse igualmente por la introducción de un código particular por medio del teclado 20. El procedimiento se prosigue en la etapa 92.

En la etapa 92, en el curso del funcionamiento del terminal 10, el captador 70 verifica sucesivamente si la capacidad vista por cada pista conductora 74 varía. Cuando se detecta una variación de ese tipo, el captador 70 proporciona al circuito de protección 71 una señal de anomalía representativa del identificador de la pista conductora 74 para la que se ha realizado una detección. Un acceso al circuito 30 puede implicar la emisión sucesiva de varias señales de anomalía por el captador 70 asociadas a diferentes pistas conductoras 74. El procedimiento se prosigue en la etapa 94.

En la etapa 94, el circuito 71 determina si el acceso está autorizado o no a partir del juego de condiciones seleccionado y a partir de los identificadores de las pistas conductoras 74 para cada una de las cuales ha recibido una señal de anomalía. Si el acceso está autorizado, no se realiza ninguna acción y el procedimiento se prosigue al estado 92. Si el acceso no está autorizado, el procedimiento se prosigue a la etapa 96.

En la etapa 96, el circuito 71 realiza las etapas de protección del circuito impreso 30 durante la detección de un acceso no autorizado. Se trata, por ejemplo, de la detención del funcionamiento del terminal 10, del borrado de ciertos datos almacenados en unas memorias conectadas al circuito impreso 30, etc.

La figura 6 representa, en la forma de un esquema de bloques, las etapas del procedimiento de utilización del circuito impreso 30 según otro ejemplo de realización de la invención. Un procedimiento de ese tipo consiste en utilizar el dispositivo de protección 32 al final del montaje de los componentes electrónicos sobre el circuito impreso 30 para asegurarse de que todos los componentes electrónicos se han dispuesto correctamente. Permite de manera simple, sin equipo dedicado, verificar que el montaje del circuito impreso se ha desarrollado correctamente.

El procedimiento se inicia en la etapa 100, en la que se realiza una etapa de aprendizaje que consiste, para un circuito impreso 30 de referencia para el que se han colocado correctamente todos los componentes 56, en realizar una operación de calibración del captador 70 del circuito impreso 30 de referencia hasta que no se transmita ninguna señal de anomalía. Se almacenan los valores de los parámetros de calibración obtenidos al final de la calibración del circuito impreso de referencia. El procedimiento se prosigue a la etapa 102.

En la etapa 102, cuando todos los componentes están fijos a un circuito impreso 30 a ensayar, se realiza una operación de calibración del captador 70 del circuito impreso 30 a ensayar a partir de los parámetros de calibración obtenidos en la etapa 100. El procedimiento se prosigue a la etapa 104.

En la etapa 104, cuando no se disponen correctamente ciertos componentes sobre el circuito impreso 30 a ensayar y/o cuando ciertos componentes previstos están ausentes, los valores de las capacidades vistas por las pistas

conductoras 74 adyacentes a los emplazamientos de los componentes fijos de manera incorrecta y/o faltantes son diferentes de los valores esperados. Esta diferencia se detecta por captador 70 que proporciona unas señales de anomalía. El procedimiento se prosigue a la etapa 106.

En la etapa 106, se realiza un análisis de las señales de anomalía proporcionadas por el captador 70 por medio de un sistema externo unido al captador 70 mediante los enlaces 72, 78 y el circuito 71. Este análisis conduce a la determinación de los componentes faltantes o montados de manera incorrecta.

El dispositivo de protección es configurable, por las informaciones contenidas en la memoria 80, para distinguir unos productos (o sistemas) o unas familias de productos (o familias de sistemas) unos de otras. De ese modo, la configuración de la memoria permite seleccionar las pistas cuya variación de capacidad es tenida en cuenta. Basándose en una misma estructura, se puede modificar por tanto la firma del circuito por simple configuración de la memoria 80. Esto hace todavía más difícil un eventual pirateado suprimiendo la reproducibilidad de un circuito a otro.

El hecho de no prever una pista en la verticalidad de los componentes no es perturbador en términos de seguridad y evita introducir unas capacidades parásitas en el funcionamiento de los circuitos.

Se han descrito unos modos de realización particulares de la presente invención. Surgirán para el experto en la materia diversas variantes y modificaciones. En particular, aunque en los ejemplos de realización descritos anteriormente, el circuito de protección 71 y el captador 70 se han descrito como los circuitos separados, es claro que estos dos circuitos podrían ser, al menos en parte, comunes. En particular, el almacenamiento y la utilización de los juegos de condiciones podrían realizarse por parte del captador 70.

REIVINDICACIONES

1. Sistema electrónico (10) que incluye un circuito impreso (30) contenido en una caja (12) y un dispositivo de protección (32), **caracterizado por que** el sistema electrónico incluye:

unas pistas conductoras (74, P1, P2) soportadas por el circuito impreso y teniendo cada una un extremo libre;
un primer circuito integrado (70) conectado a las pistas conductoras y adaptado para detectar una variación de la capacidad vista por cada pista conductora; y
un segundo circuito integrado (71), eventualmente coincidente con el primer circuito integrado, que comprende una memoria (80) configurable para seleccionar ciertas de las pistas conductoras, estando adaptado el segundo circuito integrado para determinar que ha tenido lugar un acceso autorizado o no autorizado a partir de la detección de la variación de la capacidad vista por al menos una de las pistas conductoras seleccionadas.

2. Sistema según la reivindicación 1, en el que la configuración de la memoria es diferente de un sistema a otro o de una familia de sistemas a otra.

3. Sistema según la reivindicación 1 o 2, en el que el trazado de dichas pistas conductoras (74, P1, P2) está fuera de la verticalidad de los componentes (56) soportados por el circuito impreso (30).

4. Sistema electrónico según una cualquiera de las reivindicaciones 1 a 3, en el que el circuito impreso (30) es rígido, comprendiendo el sistema electrónico (10) un componente electrónico (18) unido al circuito impreso mediante un circuito impreso flexible (58), extendiéndose al menos una de dichas pistas conductoras (74) a la altura del circuito impreso flexible.

5. Sistema electrónico según una cualquiera de las reivindicaciones 1 a 4, en el que dichas pistas conductoras (74, P1, P2) están aisladas eléctricamente entre sí y en el que al menos dos de dichas pistas conductoras se solapan y/o son adyacentes a la altura de una parte del circuito impreso (30).

6. Sistema electrónico según una cualquiera de las reivindicaciones 1 a 5, en el que el primer circuito integrado (71) está unido al segundo circuito integrado (70) mediante un enlace serie (72).

7. Procedimiento de determinación de un acceso no autorizado a un circuito impreso (30) contenido en una caja (12) de un sistema electrónico (10), caracterizado por que el procedimiento incluye las siguientes etapas:

prever unas pistas conductoras (74, P1, P2) que tengan cada una un extremo libre y que se extiendan al menos la altura del circuito impreso, un primer circuito integrado (70) conectado a las pistas conductoras y un segundo circuito integrado (71), eventualmente coincidente con el primer circuito integrado, que comprende una memoria (80);
almacenar en la memoria unos parámetros de selección de ciertas de las pistas conductoras;
disponer el primer circuito integrado para detectar, para cada pista conductora, si la capacidad vista por la pista conductora varía; y
disponer el segundo circuito integrado para determinar que ha tenido lugar un acceso autorizado o no autorizado a partir de la detección de la variación de la capacidad vista por al menos una de las pistas conductoras seleccionadas.

8. Procedimiento según la reivindicación 6, en el que a cada pista conductora (74, P1, P2) le corresponde un identificador, consistiendo el procedimiento en disponer el primer circuito integrado (71) para trasmitir al segundo circuito integrado (72) el identificador de la pista conductora para la que se ha detectado la variación de la capacidad.

9. Procedimiento según la reivindicación 8, en el que los parámetros comprenden al menos una lista de identificadores de al menos ciertas pistas conductoras (74, P1, P2), determinando el segundo circuito integrado que ha tenido lugar un acceso autorizado o no autorizado si el identificador de la pista para la que se ha detectado la variación de la capacidad pertenece a la lista.

10. Procedimiento según la reivindicación 8, en el que los parámetros comprenden al menos una operación lógica que implementa los identificadores de al menos ciertas de las pistas conductoras (74, P1, P2), determinando el segundo circuito integrado (71) que ha tenido lugar un acceso autorizado o no autorizado si se detectan unas variaciones de capacidad para las pistas conductoras asociadas a dichos identificadores y si se verifica la operación lógica.

11. Procedimiento según una cualquiera de las reivindicaciones 7 a 10, en el que se almacenan varios juegos de parámetros en la memoria (80), consistiendo el procedimiento en proporcionar al segundo circuito integrado (71) una señal de selección de un juego de parámetros entre dichos juegos de parámetros, siendo utilizado dicho juego de parámetros seleccionado por el segundo circuito integrado para determinar que ha tenido lugar un acceso autorizado o no autorizado.

12. Procedimiento según una cualquiera de las reivindicaciones 7 a 11, en el que la selección de las pistas conductoras difiere según el sistema o según la familia de sistemas.

13. Procedimiento según una cualquiera de las reivindicaciones 5 a 12, que comprende, además, las siguientes etapas:

determinar unos valores de calibrado a partir de un circuito impreso de referencia;
realizar una operación de calibrado del primer circuito integrado (70) del circuito impreso (30) a partir de dichos valores de calibrado; y
disponer el primer circuito integrado para emitir una señal de anomalía en el caso de que se detecte una variación de la capacidad vista por al menos una de las pistas conductoras (74, P1, P2).

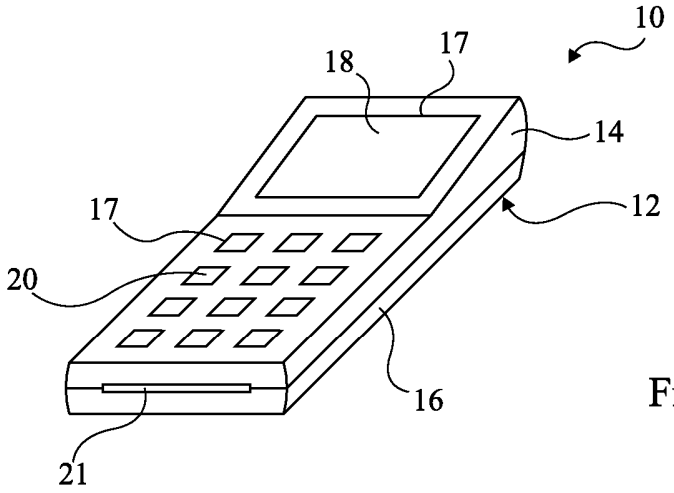
10
17
18
14
12
17
20
16
21

Fig 1

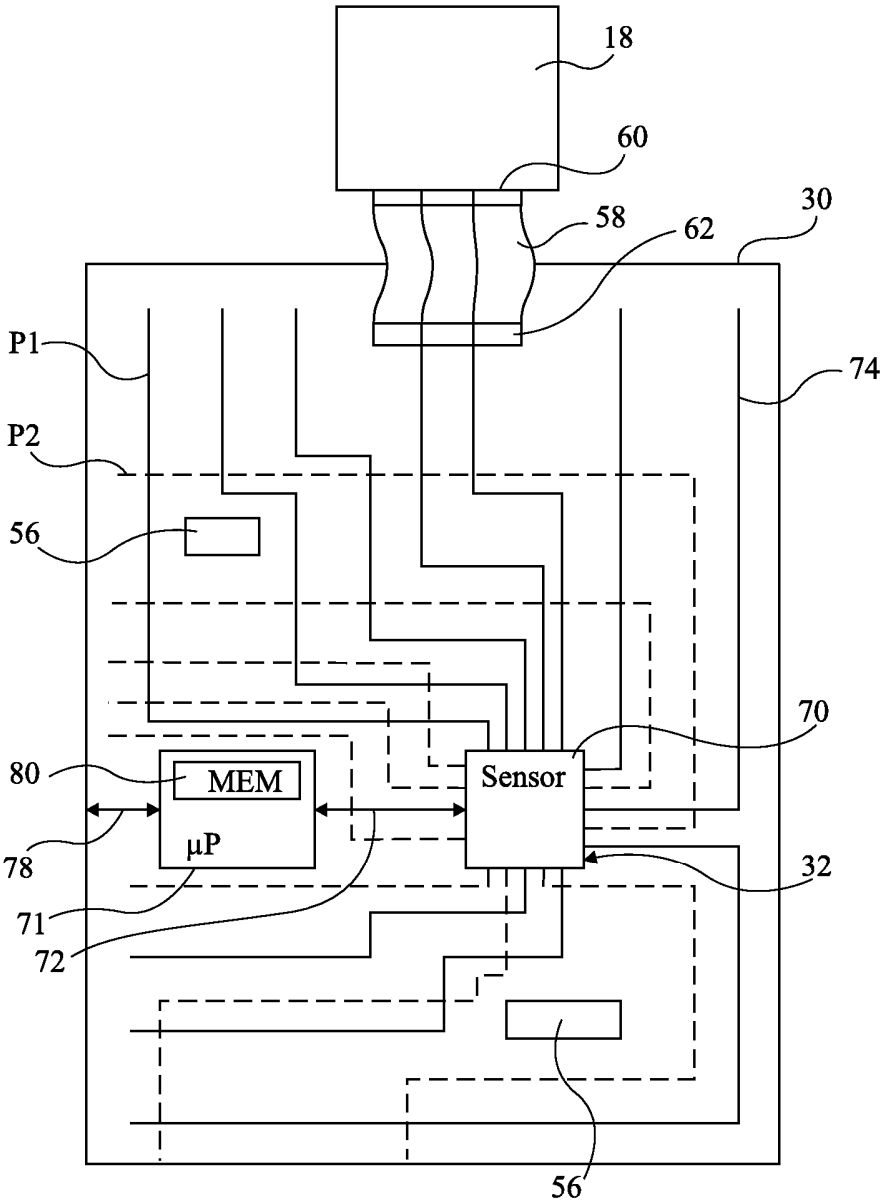
18
60
58
62
30
P1
74
P2
56
70
80
MEM
Sensor
μP
78
32
71
72
56

Fig 2

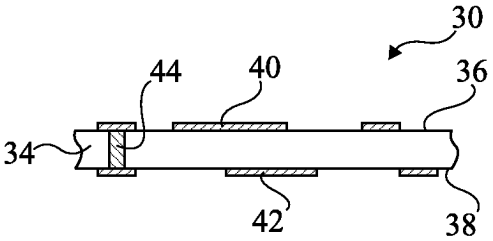

Fig 3

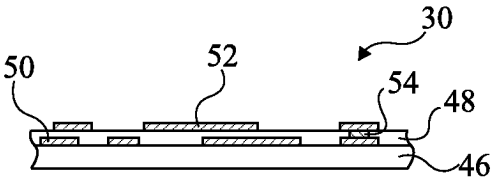

Fig 4

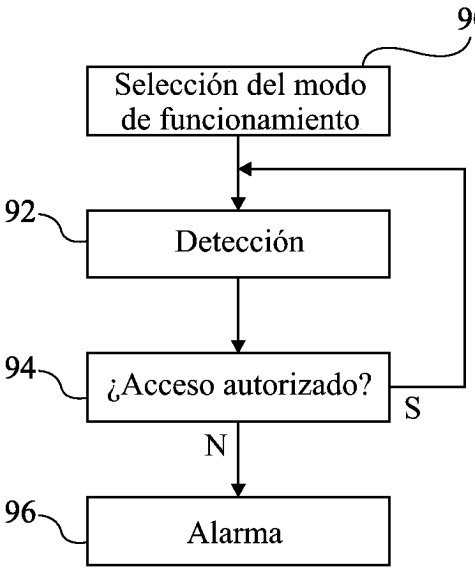

Fig 5

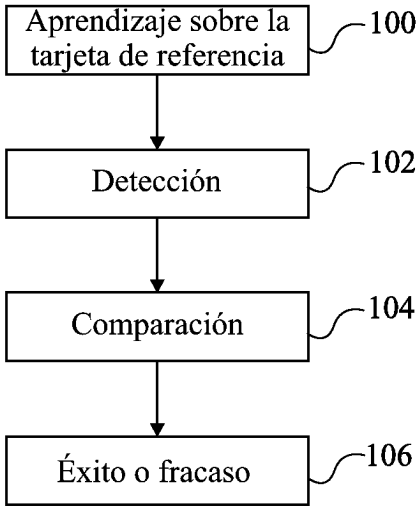

Fig 6