(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 576 228**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/83 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.10.2012 E 12778351 (2)**

(97) Fecha y número de publicación de la concesión europea: **16.03.2016 EP 2774069**

(54) Título: **Procedimiento y dispositivo de gestión de una matriz de teclas, con protección contra un dispositivo espía activo, producto programa de ordenador y medio de almacenamiento correspondientes**

(30) Prioridad:

04.11.2011 FR 1160022

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.07.2016

(73) Titular/es:

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

(72) Inventor/es:

BELLAHCENE, MOHAMMED;
BENOIT, OLIVIER y
DELORME, JEAN-JACQUES

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento y dispositivo de gestión de una matriz de teclas, con protección contra un dispositivo espía activo, producto programa de ordenador y medio de almacenamiento correspondientes

1. Campo de la invención

El campo de la invención es el de los teclados matriciales, es decir, de los teclados que comprenden una matriz de teclas que permite a un usuario introducir caracteres (letras, dígitos, símbolos...).

Más concretamente, la invención se refiere a una técnica de gestión segura de tal matriz de teclas mediante un dispositivo (por ejemplo, un procesador), con el fin de determinar la o las teclas pulsadas por el usuario. Esta técnica también recibe el nombre de “rutina de exploración del teclado” (o “keyboard scan routine” en inglés).

La invención es de especial aplicación, aunque no exclusiva, en el teclado de un terminal punto de venta que permite el pago de compras de bienes y de servicios. El teclado permite, en este caso, la introducción de los importes de las transacciones por parte del vendedor, así como la introducción de los códigos confidenciales (códigos PIN, por “Personal Identity Number” en inglés) por parte de los clientes.

La invención no queda limitada a un tipo particular de teclado, y es de aplicación cualesquiera que sean el número y la índole de las teclas del teclado (teclas numéricas, teclas de función...).

2. Antecedentes tecnológicos

La figura 1 presenta un ejemplo de teclado numérico que comprende una matriz de teclas unida a un procesador 10. En este ejemplo, la matriz de teclas comprende diez teclas (asociadas a los dígitos 0 a 9), cuatro filas (referenciadas con LIG0 a LIG3) y tres columnas (referenciadas con COL0 a COL2). Cada tecla, cuando es pulsada, permite cortocircuitar una fila y una columna de la matriz. Por ejemplo, la tecla asociada al dígito 6, cuando es pulsada, permite cortocircuitar la fila LIG1 y la columna COL1.

La técnica convencional de gestión de una matriz de teclas consiste, para el procesador 10, en efectuar varias iteraciones sucesivas de una fase de exploración. La figura 2 ilustra dos iteraciones sucesivas (referenciadas con T_n y T_{n+1}). Cada iteración de la fase de exploración comprende las siguientes etapas, para cada una de las filas LIG0 a LIG3 tratadas sucesivamente:

- escritura de un valor lógico predeterminado (nivel lógico “0” en el ejemplo de la figura 2) en la fila; y
- para cada columna COL0 a COL2, lectura de un valor lógico en la columna para determinar si la columna está en cortocircuito con la fila, mediante comparación entre el valor lógico leído y el valor lógico predeterminado.

Dicho de otro modo, el procesador, cuando ejecuta una iteración de la fase de exploración, escribe en las filas una por una, y lee en las columnas simultáneamente. Así, el procesador puede detectar que se ha pulsado una única tecla, o bien que se han pulsado varias teclas simultáneamente.

En el ejemplo de la figura 2 y más adelante en la descripción, la escritura en las filas y la lectura en las columnas se efectúan en un nivel lógico “0”, asumiendo que las filas y las columnas se hallan por defecto al valor lógico “1”. Sin embargo, está claro que el principio sigue siendo el mismo si se invierte la utilización de los niveles lógicos “0” y “1” (es decir, si la escritura en las filas y la lectura en las columnas se efectúan en el nivel lógico “1”, asumiendo que las filas y las columnas se hallan por defecto al valor lógico “0”).

Se considera que la anterior formulación, que está basada en una matriz de teclas (matriz M) y las nociones de escrituras sucesivas en las filas de esta matriz M y de lecturas simultáneas en las columnas de esta matriz M, es genérica. En efecto, existe una alternativa consistente en escribir sucesivamente en las columnas de esta matriz M y en leer simultáneamente en las filas de esta matriz M. Pero esta alternativa puede ser tratada según la anterior formulación, si se considera una nueva matriz M’ en la que las filas se corresponden con las columnas de la matriz M y las columnas se corresponden con las filas de la matriz M.

En el ejemplo de la figura 2, se asume que es pulsada la tecla 6. Por lo tanto, el procesador detecta un cortocircuito entre la fila LIG1 y la columna COL1, por donde deduce que se ha pulsado la tecla 6 situada en la intersección entre esta fila LG1 y esta columna COL1.

Existe la necesidad de hacer segura la técnica convencional de gestión de una matriz de teclas (es decir, la rutina convencional de exploración de teclado).

Se hace alusión a esta problemática en el documento de patente FR 2599525, que indica que existe un riesgo de que personas malintencionadas traten de interceptar un código confidencial en el momento en que este pasa del teclado a unos medios a propósito para el análisis matricial del teclado, por fila y columna. Más adelante en la descripción, estos medios también reciben el nombre de dispositivo de gestión de la matriz de teclas, o también, procesador. El documento FR 2599525 puntualiza que el conocimiento de la forma de onda de las señales de

análisis del teclado permite a un dispositivo espía pasivo llegar de inmediato hasta cualquier información confidencial ingresada en el teclado. Al dispositivo espía pasivo, para espiar el teclado, le bastan unos pocos empalmes (mediante sondas) sobre las filas y columnas de la matriz de teclas del teclado. El espionaje de las señales presentes en las filas y las columnas de la matriz se puede efectuar asimismo mediante análisis de las radiaciones electromagnéticas (o EMA, por "ElectroMagnetic Analysis" en inglés). Por el contrario, se asume que las señales que circulan en el interior del dispositivo de gestión de la matriz de teclas son relativamente complejas, lo cual dificulta su utilización para averiguar la información confidencial ingresada en el teclado. De ahí que, en el documento FR 2599525, el dispositivo de gestión de la matriz de teclas recibe el nombre de "módulo protegido".

Con el fin de mejorar la seguridad del teclado, el documento FR 2599525 propone una implementación, mediante el dispositivo de gestión de la matriz de teclas ("módulo protegido"), de contramedidas orientadas a obstaculizar la posibilidad de interceptación de cualquier información confidencial ingresada en el teclado (código confidencial, por ejemplo) mediante espionaje del estado de las filas y columnas de la matriz de teclas del teclado.

Más concretamente, la técnica que propone el documento FR 2599525 combina:

- un primer mecanismo de simulación: el módulo protegido está dotado de enlaces bidireccionales hacia algunas al menos de las columnas y filas del teclado, y el módulo protegido incluye medios para simular falsos accionamientos de teclas, aplicándose algunos al menos de los impulsos de interrogación al mismo tiempo a al menos una fila y al menos una columna;

- un mecanismo de verdadero barrido del teclado: el módulo protegido barre el teclado tecla por tecla, sondeando cada vez una fila o una columna llamada "realmente analizada", que no recibe el impulso de interrogación (con origen en el módulo protegido). En este barrido verdadero, se propone asimismo una simulación complementaria cuando el módulo protegido se encuentra en presencia de una no transferencia del comienzo del impulso de interrogación a la columna o fila analizada (es decir, no accionamiento de una o varias teclas barridas): el módulo protegido responde entonces a esta condición aplicando a la columna o fila analizada un impulso ficticio que finaliza con el impulso de interrogación (retrasándose, en cambio, ligeramente su comienzo con relación al comienzo del impulso de interrogación, habida cuenta del tiempo de decisión necesario para el módulo protegido);

- un segundo mecanismo de simulación: el módulo protegido no efectúa ninguna verdadera interrogación de una tecla escogida, durante un tiempo predeterminado correspondiente al tiempo normal de accionamiento de una tecla, y, durante el mismo tiempo, origina una falsa respuesta asignable a esa tecla escogida.

Se proponen dos formas de realización de estos mecanismos: en la primera, el módulo protegido está dotado de enlaces bidireccionales hacia todas las columnas del teclado; en la segunda, el módulo protegido está dotado de enlaces bidireccionales hacia todas las filas y todas las columnas del teclado.

Aunque permita mejorar la seguridad del teclado frente a un dispositivo espía pasivo, la técnica del documento FR 2599525 no es óptima. Y es que propone contramedidas durante cada iteración de la fase de exploración, pero no aborda el refuerzo de la seguridad del teclado durante cada margen de tiempo entre dos iteraciones sucesivas de la fase de exploración efectuadas por el procesador (este margen de tiempo se denomina "margen de tiempo intermedio" más adelante en la descripción).

Ahora bien, en un contexto tal como el representado en la figura 3, existe un riesgo de espionaje del teclado durante el margen de tiempo intermedio (referenciado con IT) si un dispositivo espía activo 11 se empalma mediante sondas a las filas y columnas de la matriz de teclas del teclado. En efecto, tal como se ilustra en la figura 4, el dispositivo espía activo 11 puede (a diferencia de un dispositivo espía pasivo) espiar el teclado, salvando las contramedidas, si él mismo efectúa una iteración de la fase de exploración (esta iteración, con escritura en las filas y lectura en las columnas, está simbolizada por la flecha referenciada con 41 en la figura 4), durante el margen de tiempo intermedio IT (es decir, entre dos iteraciones sucesivas T_n y T_{n+1} de la fase de exploración efectuadas por el procesador 10).

3. Objetivos de la invención

La invención tiene como objetivo, en al menos una forma de realización, paliar estos diferentes inconvenientes del estado de la técnica.

Más concretamente, en al menos una forma de realización de la invención, es un objetivo proporcionar una técnica de gestión segura, mediante un dispositivo (por ejemplo, un procesador), de una matriz de teclas de un teclado.

Tiene asimismo como objetivo al menos una forma de realización de la invención proporcionar una técnica de este tipo que permita reducir, cuando no evitar, los riesgos de espionaje por un dispositivo espía activo capaz de efectuar él mismo una iteración de la fase de exploración.

Es otro objetivo de al menos una forma de realización de la invención proporcionar una técnica de este tipo que sea simple en su puesta en práctica y económica.

4. Explicación de la invención

En una forma particular de realización de la invención, se propone un procedimiento de gestión, mediante un dispositivo, de una matriz de teclas que comprende al menos una fila y al menos dos columnas, permitiendo cada tecla, cuando es pulsada, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el procedimiento al menos dos iteraciones de una fase de exploración que comprende las siguientes etapas para cada una de las filas tratadas sucesivamente:

- escritura de un valor lógico predeterminado en la fila; y
- para cada columna, lectura de un valor lógico en la columna para determinar si la columna está en cortocircuito con la fila, mediante comparación entre el valor lógico leído y el valor lógico predeterminado, durante al menos una parte de un margen de tiempo comprendido entre dos iteraciones sucesivas de la fase de exploración, el dispositivo efectúa al menos un mecanismo de protección perteneciente al grupo que comprende:
- un primer mecanismo de protección, consistente en leer un valor lógico en al menos una fila o columna, y detectar un intento de exploración ilícita en función del valor lógico leído;
- un segundo mecanismo de protección, consistente en escribir un valor lógico arbitrario, igual a o diferente del valor lógico predeterminado, en al menos una fila o columna, en orden a impedir un intento de exploración ilícita.

De este modo, el dispositivo de gestión de la matriz de teclas del teclado pone en práctica un mecanismo de protección (o una combinación de varios mecanismos de protección) que permite hacer seguro el teclado durante el margen de tiempo intermedio, situado entre dos iteraciones sucesivas de la fase de exploración efectuadas por el dispositivo de gestión. Los mecanismos primero y segundo no son de la misma naturaleza: uno está orientado a detectar un intento de exploración ilícita (de la matriz de teclas del teclado) por un dispositivo espía activo, en tanto que el otro está orientado a impedir tal intento de exploración ilícita.

Se considera que la anterior formulación, que está basada en una matriz de teclas (matriz M) y las nociones de escrituras sucesivas (durante T) en cada una de las filas de esta matriz M y de lecturas (durante T1) y escrituras (durante T2) en cada una de las columnas de esta matriz M, es genérica. En efecto, existe una alternativa consistente en escribir sucesivamente (durante T) en cada una de las columnas de esta matriz M y en leer (durante T1) y escribir (durante T2) en cada una de las filas de esta matriz M. Pero esta alternativa puede ser tratada según la anterior formulación, si se considera una nueva matriz M' en la que las filas se corresponden con las columnas de la matriz M y las columnas se corresponden con las filas de la matriz M.

De acuerdo con una primera puesta en práctica particular, en el primer mecanismo de protección, un intento de exploración ilícita es detectado si el valor lógico leído es el valor lógico predeterminado.

En esta primera puesta en práctica particular, el dispositivo de gestión de la matriz de teclas pretende detectar un intento de exploración ilícita por un dispositivo espía activo que escribe y lee niveles lógicos (típicamente, una señal posee un nivel lógico "0" si su tensión es inferior a un primer umbral, y posee un nivel lógico "1" si su tensión es superior a un segundo umbral).

De acuerdo con una característica particular, el dispositivo efectúa el primer mecanismo de protección durante todo el referido margen de tiempo.

De este modo, se hace seguro el teclado durante todo el referido margen de tiempo intermedio.

De acuerdo con una característica particular, el dispositivo efectúa el primer mecanismo de protección sobre todas las filas y columnas.

De esta manera, se mejora aún más el refuerzo de la seguridad del teclado.

De acuerdo con una segunda puesta en práctica particular, el dispositivo efectúa el segundo mecanismo de protección durante todo el referido margen de tiempo.

En esta segunda puesta en práctica particular, el dispositivo de gestión de la matriz de teclas pretende impedir un intento de exploración ilícita por un dispositivo espía activo que escribe y lee señalas analógicas no consideradas como niveles lógicos (típicamente, una señal analógica no posee un nivel lógico "0" si su tensión no es inferior a un primer umbral, y no posee un nivel lógico "1" si su tensión no es superior a un segundo umbral).

De acuerdo con una característica particular, el dispositivo efectúa el segundo mecanismo de protección sobre todas las filas y columnas.

De esta manera, se mejora aún más el refuerzo de la seguridad del teclado.

De acuerdo con una característica particular, el segundo mecanismo de protección consiste en escribir un valor lógico arbitrario que cambia dentro de dicho margen de tiempo y/o de un margen de tiempo intermedio a otro.

De este modo, se complica el aprendizaje por parte de un dispositivo espía.

De acuerdo con una característica particular, el cambio de valor lógico arbitrario, dentro de dicho margen de tiempo y/o de un margen de tiempo intermedio a otro, es aleatorio.

De este modo, se complica el aprendizaje por parte de un dispositivo espía.

De acuerdo con una tercera puesta en práctica particular, el dispositivo efectúa el segundo mecanismo de protección, sobre al menos una fila o columna dada, durante al menos una parte del margen de tiempo, salvo durante al menos un intervalo de tiempo de detección. Adicionalmente, durante cada intervalo de tiempo de detección, el dispositivo efectúa el primer mecanismo de protección, consistente en leer un valor lógico en dicha al menos una fila o columna dada, y detectar un intento de exploración ilícita si el valor lógico leído es diferente de dicho valor lógico arbitrario escrito por el segundo mecanismo antes de dicho intervalo de tiempo de detección, colocándose cada fila o columna, en la que escribe el dispositivo al efectuar el segundo mecanismo de protección, en un estado de baja impedancia, y colocándose cada fila o columna, en la que lee el dispositivo al efectuar el primer mecanismo de protección, en un estado de alta impedancia.

En esta tercera puesta en práctica particular, el dispositivo de gestión de la matriz de teclas pretende:

- durante el margen de tiempo intermedio, exceptuando el o los intervalos de tiempo de detección, impedir un intento de exploración ilícita por un dispositivo espía activo que escribe y lee señales analógicas no consideradas como niveles lógicos; y

- durante el o los intervalos de tiempo de detección, detectar un intento de exploración ilícita por un dispositivo espía activo que inyecta en las filas (de la matriz de teclas) corrientes suficientemente intensas como para generar una tensión medible analógicamente.

De acuerdo con una característica particular, el número y/o la posición y/o la duración del o los intervalo(s) de tiempo de detección varía(n) aleatoriamente de un margen de tiempo intermedio a otro.

De esta manera, se evita que un atacante sortee, por aprendizaje, el primer mecanismo de protección efectuado durante cada intervalo de tiempo de detección.

De acuerdo con una característica particular, el segundo mecanismo de protección consiste en escribir un valor lógico arbitrario que cambia dentro de dicho margen de tiempo y/o de un margen de tiempo intermedio a otro.

De este modo, se complica el aprendizaje por parte de un dispositivo espía.

De acuerdo con una característica particular, el cambio de valor lógico arbitrario, dentro de dicho margen de tiempo y/o de un margen de tiempo intermedio a otro, es aleatorio.

De este modo, se complica el aprendizaje por parte de un dispositivo espía.

De acuerdo con una característica particular, el dispositivo efectúa el segundo mecanismo de protección durante todo el referido margen de tiempo, salvo durante dicho al menos un intervalo de tiempo de detección, efectuando el dispositivo el primer mecanismo de protección durante cada intervalo de tiempo de detección.

De este modo, se hace seguro el teclado durante todo el referido margen de tiempo intermedio.

De acuerdo con una característica particular, el dispositivo efectúa los mecanismos de protección primero y segundo sobre todas las filas y columnas.

De esta manera, se mejora aún más el refuerzo de la seguridad del teclado.

En otra forma de realización de la invención, se propone un producto programa de ordenador que comprende instrucciones de código de programa para la puesta en práctica del aludido procedimiento (en una cualquiera de sus diferentes formas de realización) cuando dicho programa se ejecuta en un ordenador o un procesador.

En otra forma de realización de la invención, se propone un medio de almacenamiento legible por ordenador y no transitorio, que almacena un programa de ordenador que comprende un juego de instrucciones ejecutables por un ordenador o un procesador para llevar a la práctica el aludido procedimiento (en una cualquiera de sus diferentes formas de realización).

En otra forma de realización de la invención, se propone un dispositivo de gestión de una matriz de teclas que comprende al menos una fila y al menos dos columnas, permitiendo cada tecla, cuando es pulsada, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el dispositivo unos medios de exploración adaptados para efectuar al menos dos iteraciones de una fase de exploración, comprendiendo los medios de exploración los siguientes medios, activados para cada una de las filas tratadas sucesivamente: medios de escritura de un valor lógico predeterminado en la fila; y medios de lectura de un valor lógico en cada columna para determinar si la

columna está en cortocircuito con la fila, mediante comparación entre el valor lógico leído y el valor lógico predeterminado. El dispositivo comprende, además, al menos un medio de protección activado durante al menos una parte de un margen de tiempo comprendido entre dos iteraciones sucesivas de la fase de exploración, perteneciendo dicho al menos un medio de protección al grupo que comprende:

- un primer medio de protección, que comprende medios de lectura de un valor lógico en al menos una fila o columna, y medios de detección de un intento de exploración ilícita en función del valor lógico leído;
- un segundo medio de protección, que comprende medios de escritura de un valor lógico arbitrario, igual a o diferente del valor lógico predeterminado, en al menos una fila o columna, en orden a impedir un intento de exploración ilícita.

Ventajosamente, el dispositivo de gestión de la matriz de teclas comprende medios de puesta en práctica de las etapas que efectúa en el procedimiento tal como se ha descrito anteriormente, en una cualquiera de sus diferentes formas de realización.

5. Lista de figuras

Otras características y ventajas de la invención se irán poniendo de manifiesto con la lectura de la descripción siguiente, dada a título de ejemplo indicativo y no limitativo, y de los dibujos que se acompañan, en los cuales:

la figura 1, ya descrita en relación con la técnica anterior, presenta un ejemplo de teclado numérico que comprende una matriz de teclas unida a un procesador;

la figura 2, ya descrita en relación con la técnica anterior, ilustra la técnica convencional de gestión de la matriz de teclas de la figura 1, en el caso en que se aprieta la tecla 6;

la figura 3, ya descrita en relación con la técnica anterior, presenta el empalme de un dispositivo espía activo sobre las filas y columnas de la matriz de teclas del teclado;

la figura 4, ya descrita en relación con la técnica anterior, ilustra el riesgo de espionaje del teclado durante el margen de tiempo intermedio por el dispositivo espía activo de la figura 3;

la figura 5 ilustra una primera forma de realización del procedimiento según la invención;

la figura 6 ilustra una respuesta defensiva a la primera forma de realización de la figura 5;

la figura 7 ilustra una segunda forma de realización del procedimiento según la invención;

la figura 8 ilustra una respuesta defensiva a la segunda forma de realización de la figura 7;

la figura 9 ilustra una tercera forma de realización del procedimiento según la invención; y

la figura 10 presenta la constitución de un dispositivo de gestión de una matriz de teclas de un teclado, según una forma particular de realización de la invención.

6. Descripción detallada

En interés de la simplificación, más adelante en la descripción se utiliza el ejemplo de teclado de la figura 1, con una matriz de teclas que comprende diez teclas (asociadas a los dígitos 0 a 9), cuatro filas (referenciadas con LIG0 a LIG3) y tres columnas (referenciadas con COL0 a COL2). Claro está que la técnica que a continuación se presenta, según diferentes formas de realización de la invención, no queda limitada a este ejemplo de teclado.

Cada una de las figuras 5 a 8 presenta los valores de las señales presentes en las filas LG0 a LG3 y las columnas COL0 a COL2, durante dos iteraciones sucesivas (referenciadas con T_n y T_{n+1}) de la fase de exploración, así como durante el margen de tiempo intermedio (referenciado con IT) situado entre estas dos iteraciones sucesivas. La figura 9 presenta los valores de las señales presentes en las filas LG0 a LG3 y las columnas COL0 a COL2, únicamente durante el margen de tiempo intermedio (referenciado con IT).

Más adelante en la descripción, se asume que los impulsos de interrogación poseen un nivel lógico “0”. Sin embargo, está claro que el principio de la invención sigue siendo el mismo si se invierte la utilización de los niveles lógicos “0” y “1”.

En relación con la figura 5, se pasa a presentar a continuación una primera forma de realización del procedimiento según la invención.

Se asume que, al igual que en el ejemplo de la figura 4, el dispositivo espía activo 11 espía el teclado efectuando él mismo una iteración de la fase de exploración (esta iteración, con escritura de un nivel lógico “0” (impulso de interrogación) en las filas y lectura en las columnas, está simbolizada por la flecha referenciada con 41), durante el margen de tiempo intermedio IT (es decir, entre dos iteraciones sucesivas T_n y T_{n+1} de la fase de exploración

efectuadas por el procesador 10).

La técnica que se propone en la primera forma de realización de la invención consiste, durante todo el margen de tiempo intermedio IT, en leer el valor lógico presente en cada una de las filas LG0 a LG3 y cada una de las columnas COL0 a COL2, y detectar un intento de exploración ilícita si el valor lógico leído (en al menos una de las filas y columnas) es el valor lógico “0” (nivel lógico de los impulsos de interrogación).

En el ejemplo de la figura 5, el procesador 10 detecta el flanco de bajada correspondiente al comienzo de la escritura, por parte del dispositivo espía activo 11, de un nivel lógico “0” (impulso de interrogación) en la fila LIG0. Esta detección está simbolizada por la flecha referenciada con 51. El procesador 10 deduce la existencia de un intento de exploración ilícita del teclado, de modo que se puede(n) poner en práctica cual(es)quier(a) acción(ones) oportuna(s) (por ejemplo, aseguramiento del aparato (puesta fuera de servicio), disparo de una alarma (mensaje, pitido, sirena...), borrado de información sensible, aviso a un dispositivo de vigilancia a efectos de intervención, etc.).

Esta primera forma de realización utiliza, por ejemplo, las posibilidades de interrupciones del procesador 10: entre dos iteraciones sucesivas T_n y T_{n+1} de la fase de exploración, el conjunto de las filas / columnas del teclado están colocadas en un “estado de entrada” (es decir, en un estado de lectura por el procesador 10) con interrupción ante un cambio de estado lógico. En caso de exploración ilícita por parte de un dispositivo espía activo 11, el procesador 10 detecta un cambio de nivel lógico por intermedio de su sistema de gestión de las interrupciones y memoriza un intento de exploración ilícita de teclado. Este mecanismo de protección por gestión de interrupción tan solo es posible en procesadores con entradas / salidas que tienen posibilidades de interrupciones.

En una variante, el procesador 10 explora permanentemente las filas y columnas para detectar un cambio de nivel lógico (esta variante es más consumidora de recursos del procesador).

En otra variante, el mecanismo de protección según la primera forma de realización tan solo se efectúa durante una parte del margen de tiempo intermedio IT.

En otra variante, el mecanismo de protección según la primera forma de realización tan solo se efectúa en cierta(s) fila(s) y/o cierta(s) columna(s).

La figura 6 ilustra una respuesta defensiva a la primera forma de realización de la figura 5. Esta respuesta defensiva consiste en utilizar un dispositivo espía activo analógico 11, es decir, un dispositivo espía activo con entradas analógicas, capaces de trabajar (en escritura y en lectura) con señales analógicas que no disparan interrupciones ni cambios de estado lógico (señales analógicas que no se consideran niveles lógicos “0”, debido a que permanecen en un nivel de tensión superior al umbral definitorio del nivel lógico “0”).

En la figura 6, la iteración de la fase de exploración efectuada por el dispositivo espía activo analógico 11 (con escritura en las filas y lectura en las columnas de señales analógicas que no disparan interrupciones ni cambios de estado lógico) está simbolizada por la flecha referenciada con 61.

Se pasa a presentar a continuación, en relación con la figura 7, una segunda forma de realización del procedimiento según la invención, que permite evitar la respuesta defensiva ilustrada en la figura 6.

La técnica que se propone en la segunda forma de realización de la invención consiste, durante todo el margen de tiempo intermedio IT, en escribir el valor lógico “0” en cada una de las filas LG0 a LG3 y cada una de las columnas COL0 a COL2 (nivel lógico de los impulsos de interrogación). Esta escritura en las filas y las columnas está simbolizada por la flecha referenciada con 71. Dicho de otro modo, el procesador 10 fuerza los niveles de las filas LG0 a LG3 y columnas COL0 a COL2 a un nivel lógico “0” (colocándose las filas y las columnas en un “estado de salida”, es decir, en un estado de escritura por el procesador 10). Para ello, el procesador 10 bloquea las filas y las columnas a masa.

En una variante, el procesador 10 fuerza los niveles de las filas LG0 a LG3 y columnas COL0 a COL2 a un nivel lógico “1”, durante todo el margen de tiempo intermedio IT.

En otra variante, el procesador 10 fuerza los niveles de las filas LG0 a LG3 y columnas COL0 a COL2 a un nivel lógico arbitrario que cambia (“0” ó “1”) de un margen de tiempo intermedio IT a otro. Este cambio es preferiblemente aleatorio, con el fin de complicar el aprendizaje por parte de un dispositivo espía.

En otra variante, el procesador 10 fuerza los niveles de las filas LG0 a LG3 y columnas COL0 a COL2 a un nivel lógico arbitrario que cambia (“0” ó “1”) dentro del margen de tiempo intermedio IT. Dicho de otro modo, el procesador 10 fuerza al nivel lógico “0” durante una o varias primeras porciones del margen de tiempo intermedio IT, y al nivel lógico “1” durante una o varias segundas porciones del margen de tiempo intermedio IT.

El cambio arbitrario de nivel lógico (de un margen de tiempo intermedio IT a otro y/o dentro del margen de tiempo intermedio IT) puede ser aleatorio, con el fin de complicar el aprendizaje por parte de un dispositivo espía.

En una variante, el mecanismo de protección según esta segunda forma de realización tan solo se efectúa durante una parte del margen de tiempo intermedio IT.

En otra variante, el mecanismo de protección según esta segunda forma de realización tan solo se efectúa en cierta(s) fila(s) y/o cierta(s) columna(s).

La figura 8 ilustra una respuesta defensiva a la segunda forma de realización de la figura 7.

Esta respuesta defensiva consiste en utilizar un dispositivo espía activo analógico 11, es decir, un dispositivo espía activo con entradas analógicas, capaz de inyectar en las filas LG0 a LG3 corrientes suficientemente intensas como para generar una tensión medible analógicamente. En efecto, es necesario inyectar una corriente suficientemente importante en una fila para obtener una tensión medible (es decir, en este caso concreto, una tensión débil pero no nula), teniendo presente que la impedancia de una fila colocada en un “estado de salida” (es decir, en escritura por el procesador 10) es pequeña (< 1 Ω).

En la figura 8, la flecha referenciada con 81 simboliza la iteración de la fase de exploración efectuada por el dispositivo espía activo analógico 11, con escritura en las filas (y lectura en las columnas) de señales resultantes de la inyección en las filas LG0 a LG3 de corrientes suficientemente intensas.

Se pasa a presentar a continuación, en relación con la figura 9, una tercera forma de realización del procedimiento según la invención, que permite evitar la respuesta defensiva ilustrada en la figura 8.

La técnica que se propone en la tercera forma de realización de la invención consiste en:

- poner en práctica un primer mecanismo durante todo el margen de tiempo intermedio IT, salvo durante al menos un intervalo de tiempo de detección. Este primer mecanismo es idéntico al mecanismo de protección según la segunda forma de realización, antes descrito en relación con la figura 7 (inclusive en las diferentes variantes, antes reseñadas, de esta segunda forma de realización); y
- poner en práctica un segundo mecanismo de protección durante cada intervalo de tiempo de detección, consistente en: leer el valor lógico presente en cada una de las filas LG0 a LG3 y cada una de las columnas COL0 a COL2, y detectar un intento de exploración ilícita si el valor lógico leído (en al menos una de las filas y columnas) es diferente del valor lógico arbitrario escrito por el segundo mecanismo antes de este intervalo de tiempo de detección. En el ejemplo de la figura 9, se escribe el valor lógico arbitrario “0” con el primer mecanismo y se detecta un intento de exploración ilícita con el segundo mecanismo si se lee el valor lógico “1”. Este segundo mecanismo de protección utiliza, por ejemplo, las posibilidades de interrupciones del procesador 10, o bien una detección permanente de un cambio de nivel lógico).

De este modo, al comienzo de cada intervalo de tiempo de detección (es decir, con el paso del primer al segundo mecanismo de protección), cada fila o columna pasa de un “estado de salida” de escasa impedancia (estado de escritura de un valor lógico arbitrario “0” ó “1” por el procesador 10) a un “estado de entrada” de gran impedancia (estado de lectura por el procesador 10). En la práctica, el cambio de impedancia es casi instantáneo (una instrucción de procesador). Esta variación de impedancia es suficientemente grande para que, si en una fila o una columna hay presencia de una intensa corriente, esto conlleva en esa fila o columna una tensión medible por el procesador 10. Según se ha explicado en relación con la figura 8, en una fila hay presencia de una intensa corriente si un dispositivo espía activo analógico 11 inyecta en esa fila esa intensa corriente. En una columna, hay presencia de una intensa corriente si esa columna está en cortocircuito con una fila en la que el dispositivo espía activo analógico 11 ha inyectado esa intensa corriente.

En el ejemplo de la figura 9, en el que, en interés de la simplificación, no hay más que un solo intervalo de tiempo de detección (correspondiente a la porción referenciada con P2 del margen de tiempo intermedio IT), el procesador pone en práctica el primer mecanismo (simbolizado por las flechas referenciadas con 91 y 93) durante las porciones referenciadas con P1 y P3 del margen de tiempo intermedio IT, y pone en práctica el segundo mecanismo (simbolizado por la flecha referenciada con 92) durante la porción referenciada con P2.

Con el fin de complicar el aprendizaje por parte del dispositivo espía, el procesador 10 hacer variar de manera aleatoria, de un margen de tiempo intermedio IT a otro, el número y/o la posición y/o la duración del o los intervalo(s) de tiempo de detección.

En una variante, el mecanismo de protección según esta tercera forma de realización tan solo se efectúa durante una parte del margen de tiempo intermedio IT.

En otra variante, el mecanismo de protección según esta tercera forma de realización tan solo se efectúa en cierta(s) fila(s) y/o cierta(s) columna(s).

La figura 10 presenta la constitución de un dispositivo 10 de gestión de una matriz de teclas de un teclado, según una forma particular de realización de la invención. Este dispositivo pone en práctica la técnica antes presentada (en una cualquiera de las formas de realización, presentadas en relación con las figuras 5 a 9).

En este ejemplo, el dispositivo comprende una memoria RAM 103 (por “Random Access Memory” en inglés), una unidad de proceso 101 (o CPU, por “Central Processing Unit” en inglés), equipada, por ejemplo, con un procesador y

pilotada por un programa almacenado en una memoria ROM 102 (por “Read Only Memory” en inglés). Con la inicialización, las instrucciones de código del programa se cargan, por ejemplo, en la memoria RAM 103 antes de ser ejecutadas por la unidad de proceso 101. La unidad de proceso 101 administra las señales en las filas y las columnas (LIG0 a LIG3 y COL0 a COL2 en este ejemplo) de la matriz de teclas del teclado, según las instrucciones del programa 102, con el fin de poner en práctica la técnica antes presentada (en una cualquiera de las formas de realización).

Esta figura 10 solo ilustra una manera particular, de entre varias posibles, de realizar la técnica antes presentada, en relación con las figuras 5 a 9. En efecto, la técnica de la invención se realiza indistintamente:

- en una máquina de cálculo reprogramable (un procesador o un microcontrolador, por ejemplo) que ejecuta un programa que comprende una secuencia de instrucciones, o
- en una máquina de cálculo especializada (por ejemplo, un conjunto de puertas lógicas tal como una FPGA o un ASIC, o cualquier otro módulo de soporte físico).

En caso de implantarse la invención en una máquina de cálculo reprogramable, el correspondiente programa (es decir, la secuencia de instrucciones) puede almacenarse en un medio de almacenamiento extraíble (tal como, por ejemplo, un disquete, un CD-ROM o un DVD-ROM) o no, siendo legible este medio de almacenamiento, parcial o totalmente, por un ordenador o un procesador.

REIVINDICACIONES

1. Procedimiento de gestión, mediante un dispositivo (10), de una matriz de teclas que comprende al menos una fila (LIG0 a LIG3) y al menos dos columnas (COL0 a COL2), permitiendo cada tecla, cuando es pulsada, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el procedimiento al menos dos iteraciones (T_n, T_{n+1}) de una fase de exploración que comprende las siguientes etapas para cada una de las filas tratadas sucesivamente:

- escritura de un valor lógico predeterminado en la fila; y
- para cada columna, lectura de un valor lógico en la columna para determinar si la columna está en cortocircuito con la fila, mediante comparación entre el valor lógico leído y el valor lógico predeterminado,

caracterizado por que, durante al menos una parte de un margen de tiempo (IT) comprendido entre dos iteraciones sucesivas (T_n, T_{n+1}) de la fase de exploración, el dispositivo efectúa:

- un primer mecanismo de protección (92), consistente en leer un valor lógico en al menos una fila o columna, y detectar un intento de exploración ilícita en función del valor lógico leído; y
- un segundo mecanismo de protección (91, 93), consistente en escribir un valor lógico arbitrario, igual a o diferente del valor lógico predeterminado, en al menos una fila o columna, en orden a impedir un intento de exploración ilícita;

por que el dispositivo efectúa el segundo mecanismo de protección (91, 93), sobre al menos una fila o columna dada, durante al menos una parte (P1, P3) del margen de tiempo (IT), salvo durante al menos un intervalo de tiempo de detección (P2), **por que**, durante cada intervalo de tiempo de detección, el dispositivo efectúa el primer mecanismo de protección (92), consistente en leer un valor lógico en dicha al menos una fila o columna dada, y detectar un intento de exploración ilícita si el valor lógico leído es diferente de dicho valor lógico arbitrario escrito por el segundo mecanismo antes de dicho intervalo de tiempo de detección,

por que cada fila o columna en la que escribe el dispositivo, antes de dicho intervalo de tiempo de detección, al efectuar el segundo mecanismo de protección, se coloca en un estado de baja impedancia,

por que cada fila o columna, en la que lee el dispositivo, durante dicho intervalo de tiempo de detección, al efectuar el primer mecanismo de protección, se coloca en un estado de alta impedancia, y **por que**, para dicha al menos una fila o columna dada, el comienzo del intervalo de tiempo de detección se corresponde con un paso de dicho estado de baja impedancia a dicho estado de alta impedancia, que conlleva una tensión medible por el dispositivo si en dicha al menos una fila o columna dada hay presencia de una corriente dimanada de un intento de exploración ilícita.

2. Procedimiento según la reivindicación 1, **caracterizado por que** el número y/o la posición y/o la duración del o los intervalo(s) de tiempo de detección varía(n) aleatoriamente de un margen de tiempo intermedio a otro.

3. Procedimiento según una cualquiera de las reivindicaciones 1 y 2, **caracterizado por que** el segundo mecanismo de protección consiste en escribir un valor lógico arbitrario que cambia dentro de dicho margen de tiempo y/o de un margen de tiempo intermedio a otro.

4. Procedimiento según la reivindicación 3, **caracterizado por que** el cambio arbitrario de valor lógico, dentro de dicho margen de tiempo y/o de un margen de tiempo intermedio a otro, es aleatorio.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** el dispositivo efectúa el segundo mecanismo de protección durante todo el referido margen de tiempo (IT), salvo durante dicho al menos un intervalo de tiempo de detección (P2), efectuando el dispositivo el primer mecanismo de protección durante cada intervalo de tiempo de detección.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, **caracterizado por que** el dispositivo efectúa los mecanismos de protección primero y segundo sobre todas las filas y columnas.

7. Producto programa de ordenador, que comprende instrucciones de código de programa para la puesta en práctica del procedimiento según al menos una de las reivindicaciones 1 a 6, cuando dicho programa se ejecuta en un ordenador o un procesador.

8. Medio de almacenamiento legible por ordenador y no transitorio, que almacena un programa de ordenador que comprende un juego de instrucciones ejecutables por un ordenador o un procesador para llevar a la práctica el procedimiento según al menos una de las reivindicaciones 1 a 6.

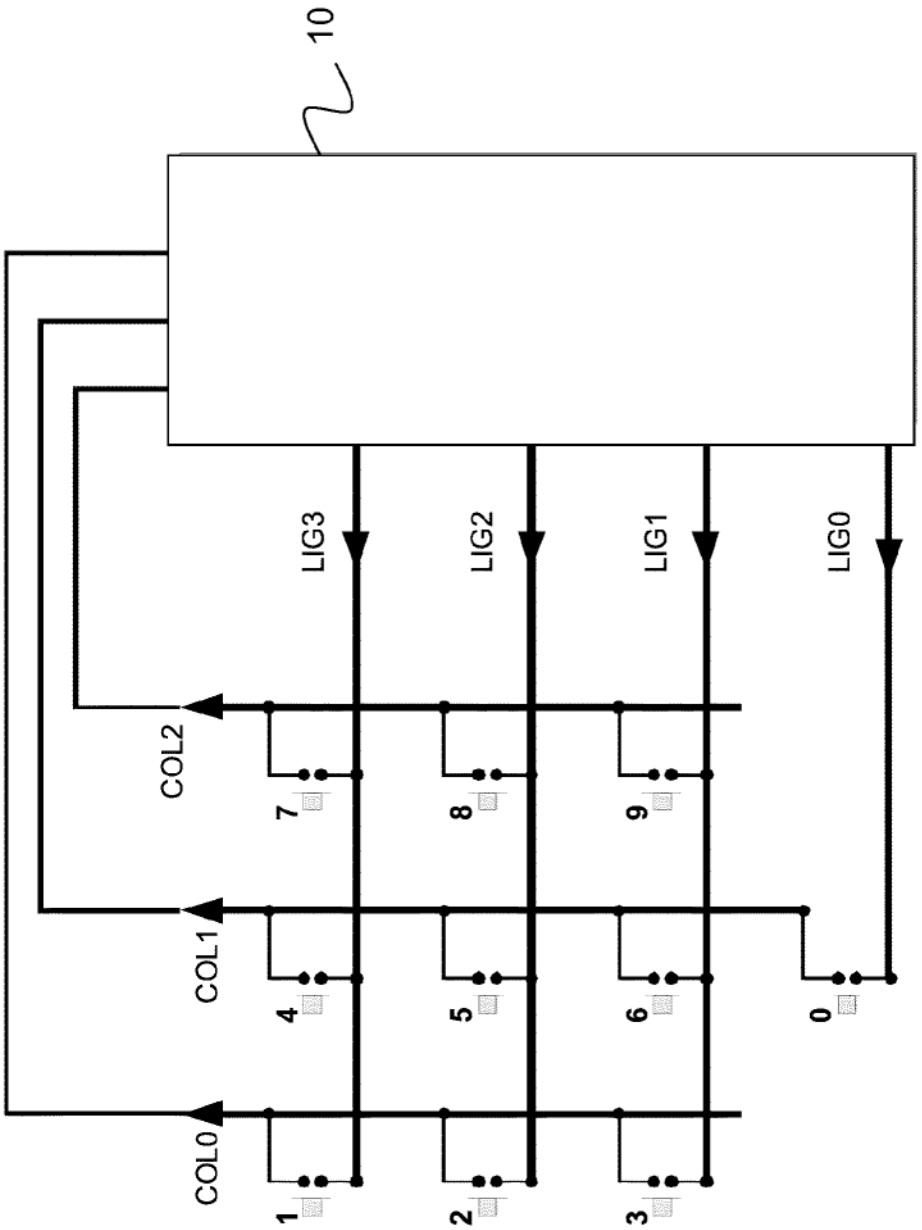

Figura 1

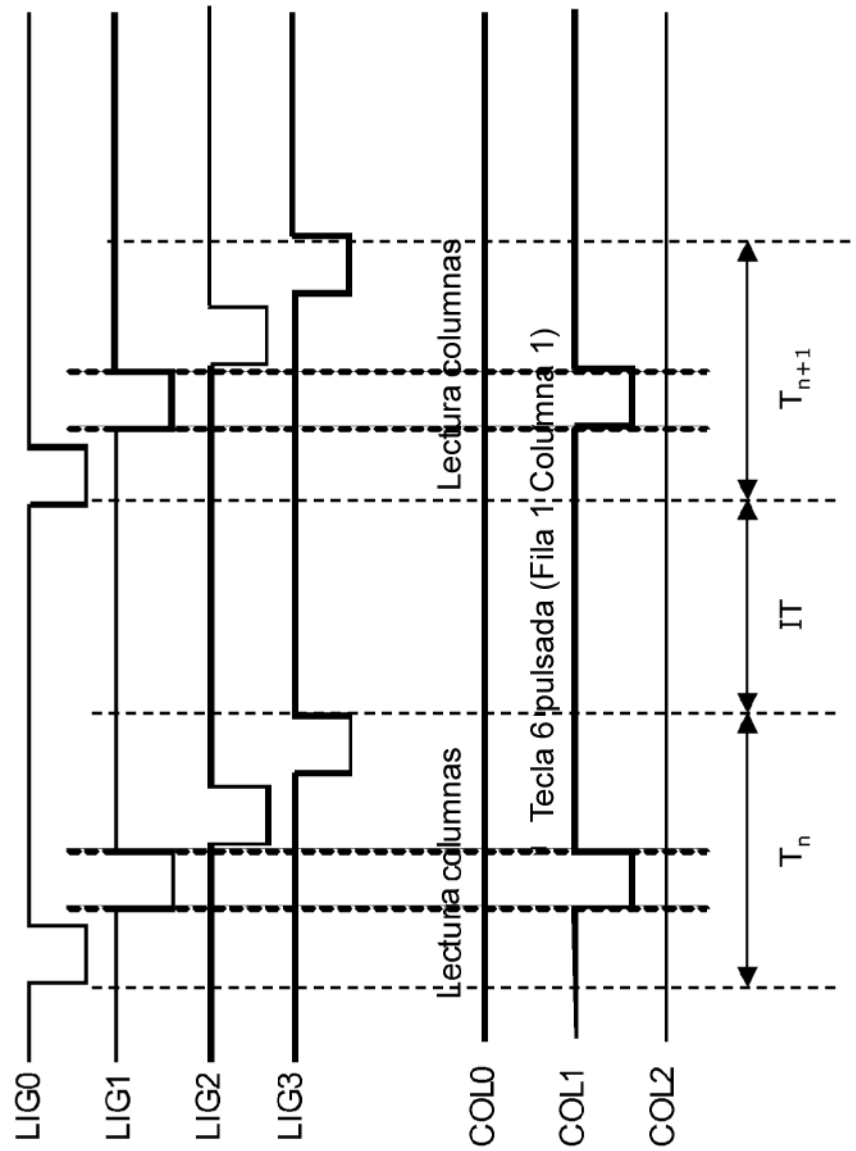
Escritura filas
Escritura filas
Lectura columnas
Lectura columnas
Tecla 6 pulsada (Fila 1 Columna 1)
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2
T_n
IT
T_{n+1}

Figura 2

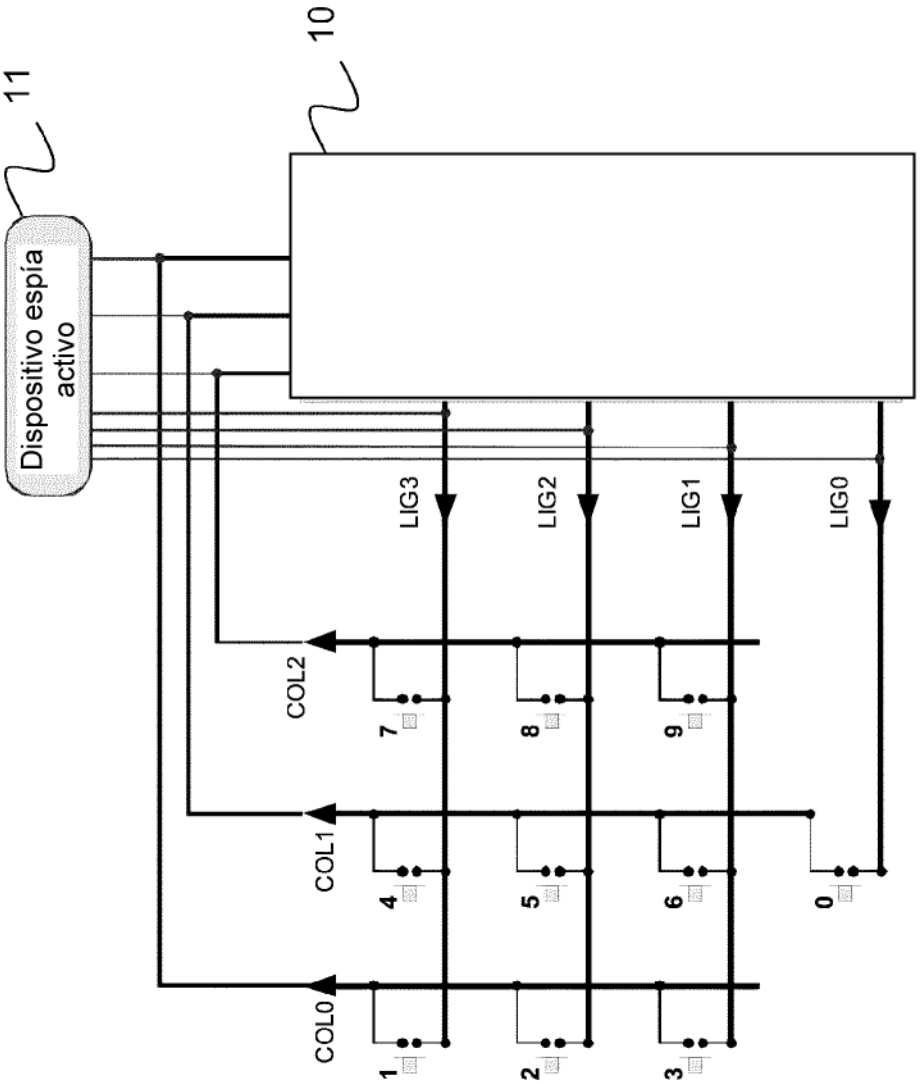
11
10
Dispositivo espía activo
LIG3
LIG2
LIG1
LIG0
COL2
COL1
COL0
7
8
9
4
5
6
0
1
2
3

Figura 3

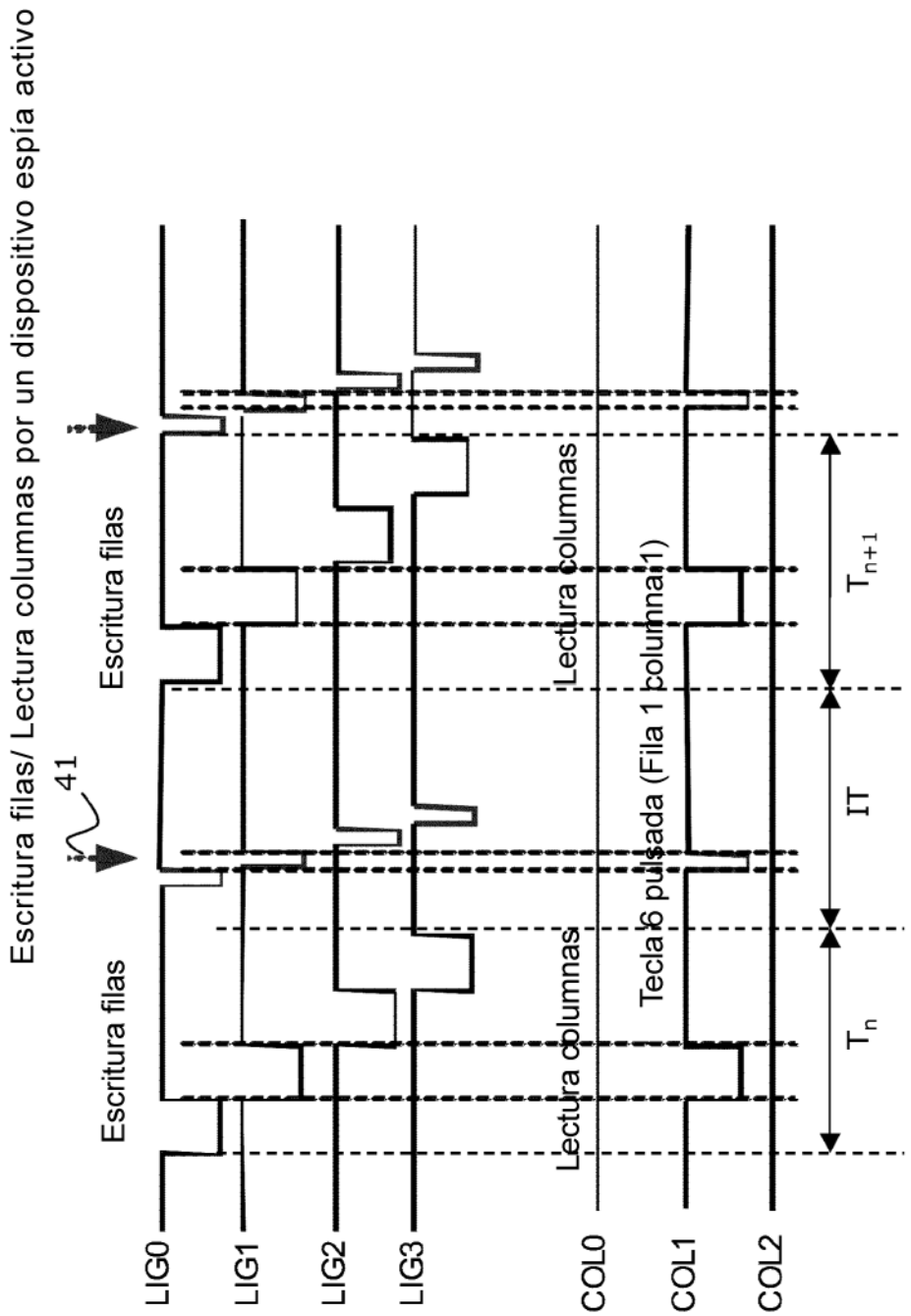
Escritura filas/ Lectura columnas por un dispositivo espía activo
41
Escritura filas
Escritura filas
Lectura columnas
Lectura columnas
Tecla 6 pulsada (Fila 1 columna 1)
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2
T_n
IT
T_{n+1}

Figura 4

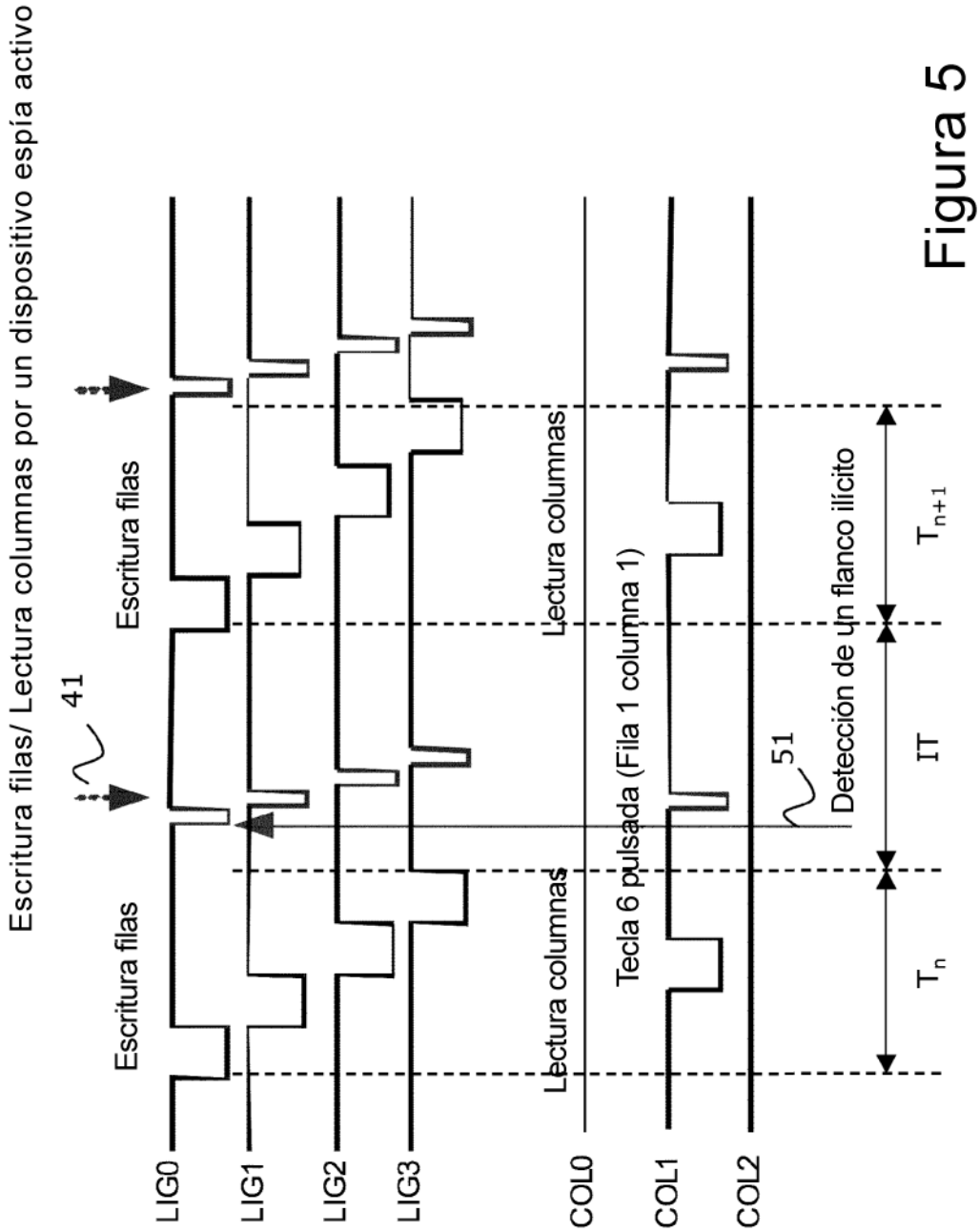
Escritura filas/ Lectura columnas por un dispositivo espía activo
41
Escritura filas
Escritura filas
Lectura columnas
Lectura columnas
Tecla 6 pulsada (Fila 1 columna 1)
51
Detección de un flanco ilícito
IT
T_n
T_{n+1}
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2

Figura 5

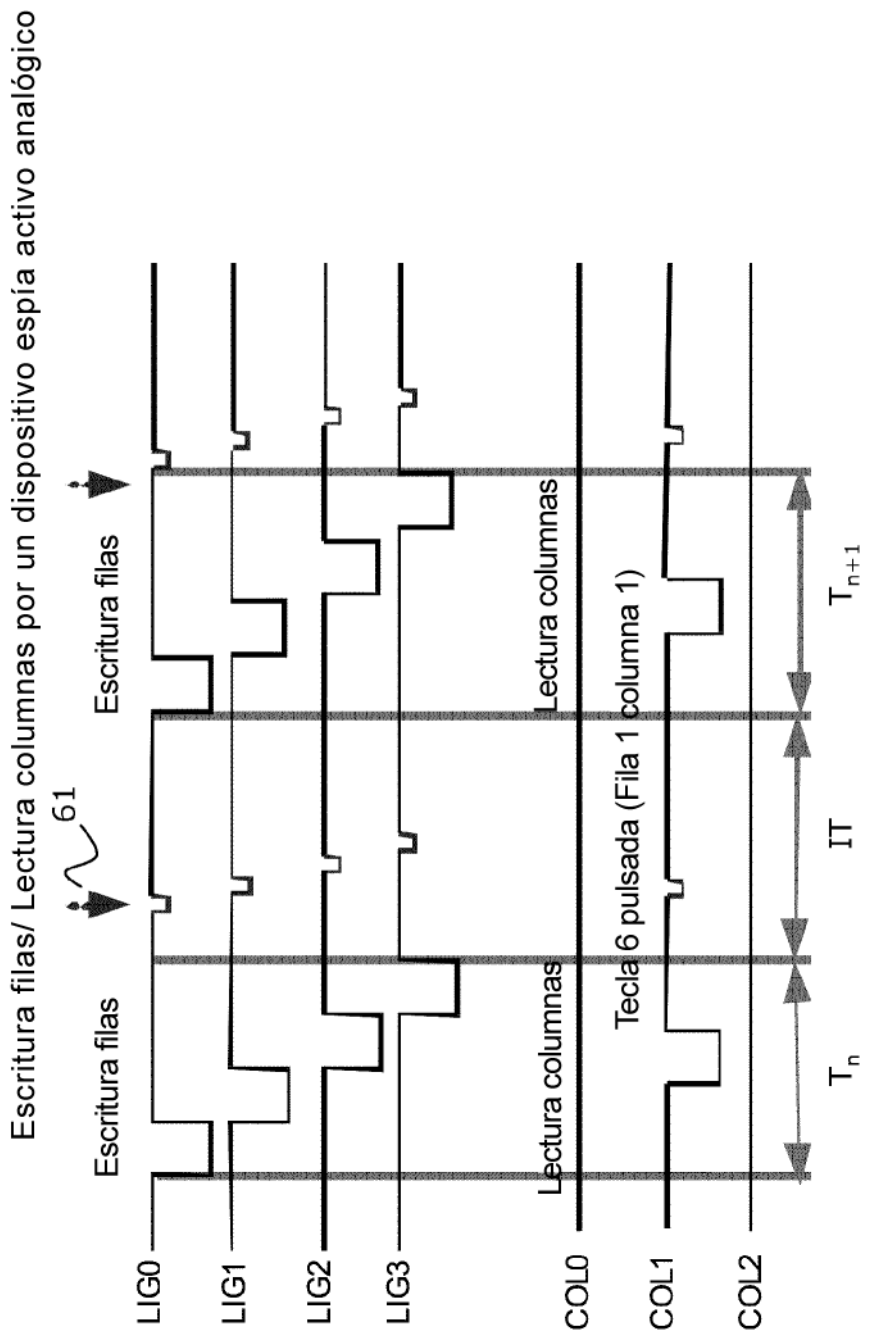
Escritura filas/ Lectura columnas por un dispositivo espía activo analógico
61
Escritura filas
Escritura filas
Lectura columnas
Lectura columnas
Tecla 6 pulsada (Fila 1 columna 1)
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2
T_n
IT
T_{n+1}

Figura 6

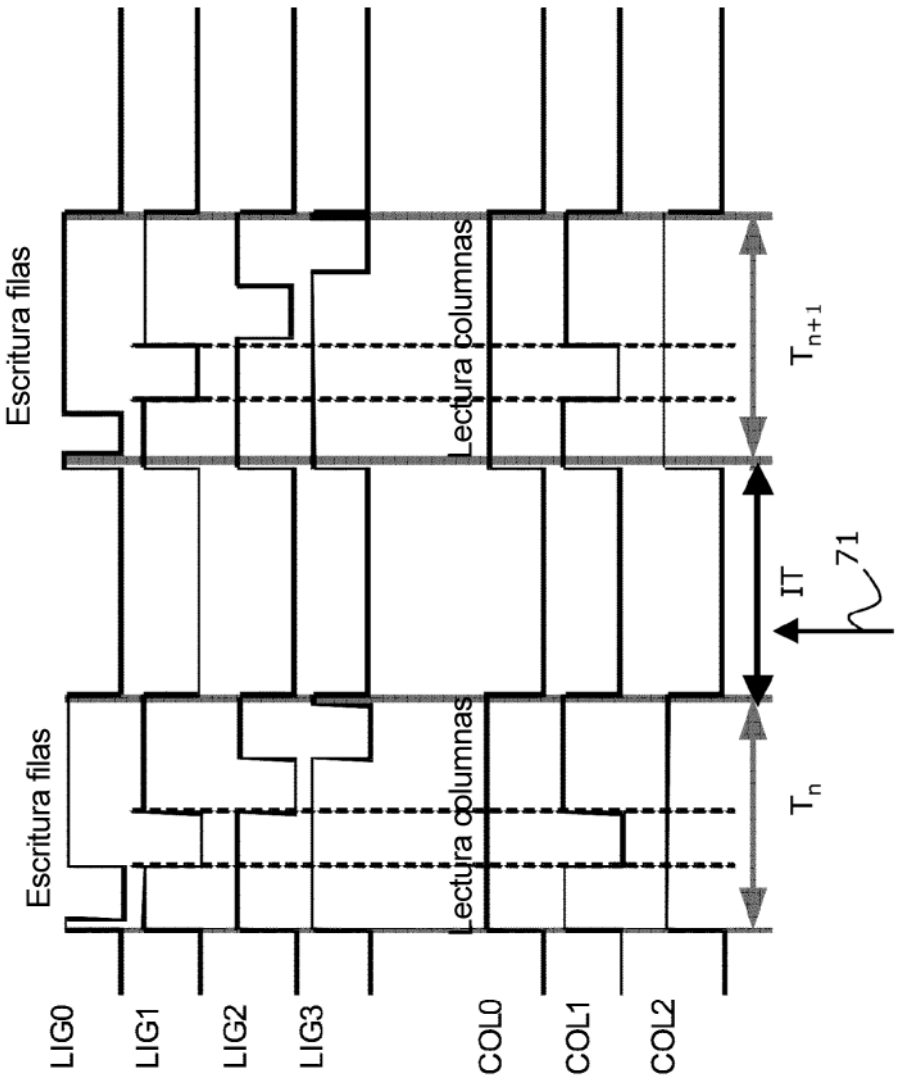
Escritura filas
Lectura columnas
Escritura filas
Lectura columnas
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2
T_n
T_{n+1}
IT
71
Escritura del valor lógico «0»
en las filas y las columnas

Figura 7

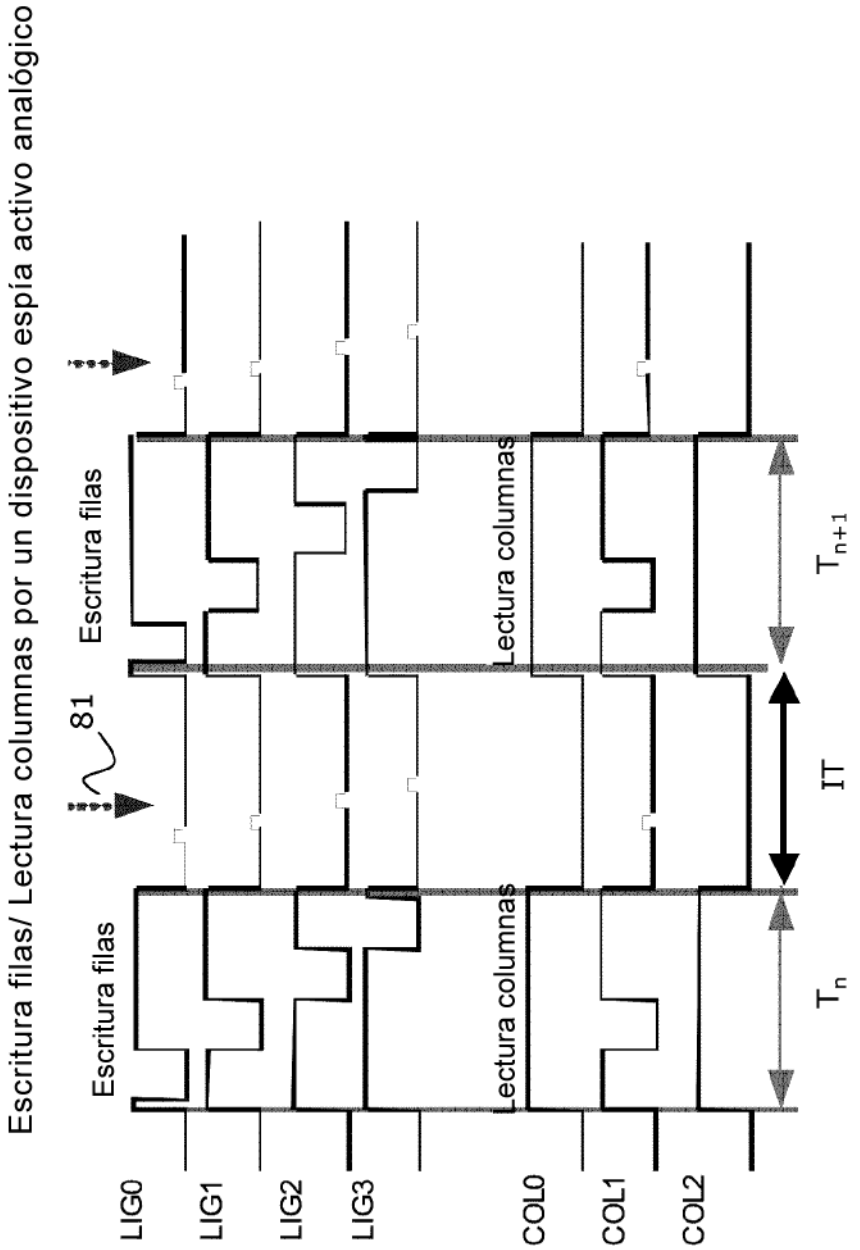
Escritura filas/ Lectura columnas por un dispositivo espía activo analógico
81
Escritura filas
Escritura filas
Lectura columnas
Lectura columnas
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2
T_n
IT
T_{n+1}

Figura 8

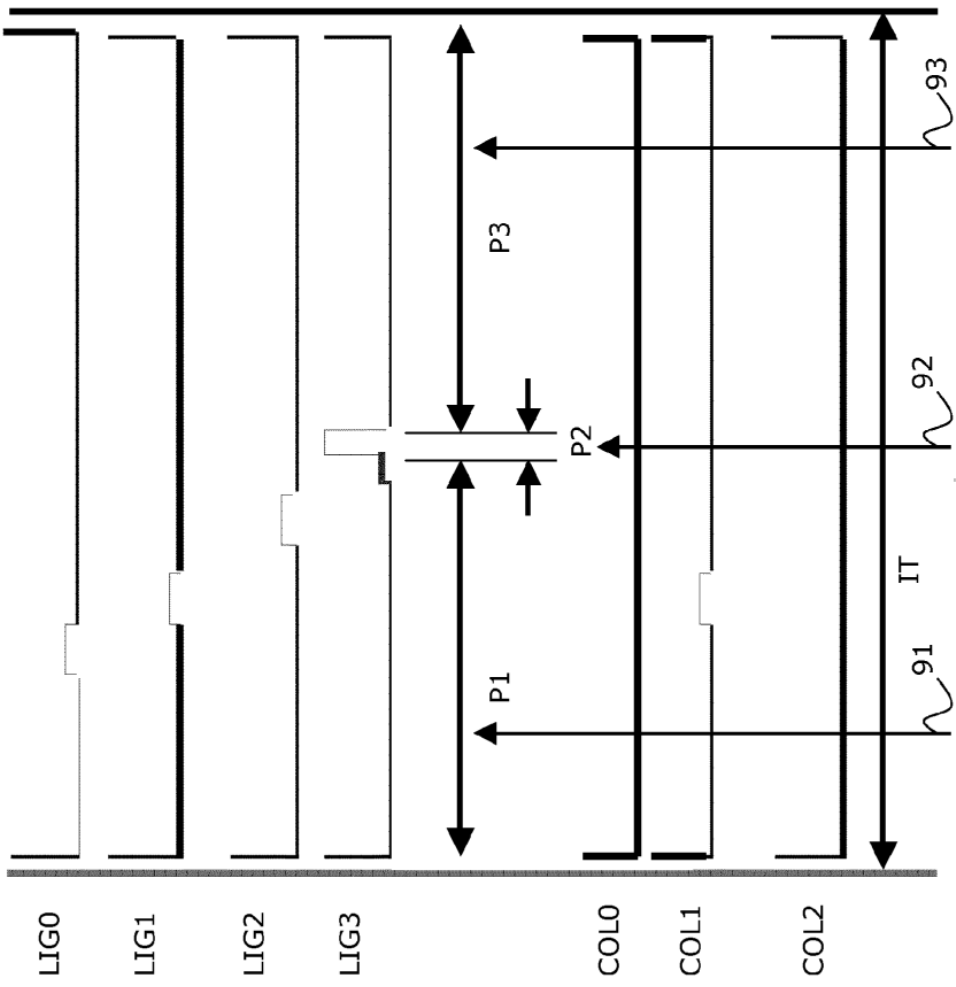
LIG0
LIG1
LIG2
LIG3
COL0
COL1
COL2
P1
P2
P3
IT
91
92
93
Escritura del valor lógico «0» en las filas y las columnas
Detección de un flanco ilícito
Escritura del valor lógico «0» en las filas y las columnas

Figura 9

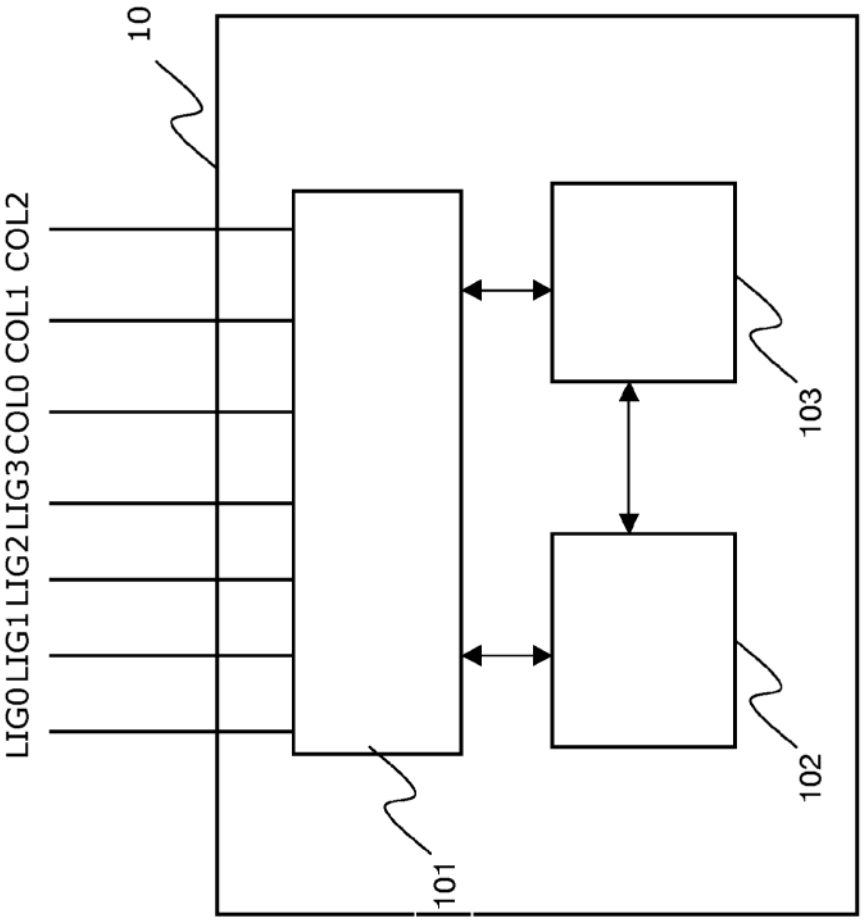

Figura 10