

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 984 174**

51 Int. Cl.:

G07D 5/00 (2006.01)

G07D 7/00 (2006.01)

G07D 7/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.11.2013** **PCT/GB2013/053080**

87 Fecha y número de publicación internacional: **05.06.2014** **WO14083319**

96 Fecha de presentación y número de la solicitud europea: **22.11.2013** **E 13796144 (7)**

97 Fecha y número de publicación de la concesión europea: **19.06.2024** **EP 2926322**

54 Título: **Prevención del fraude**

30 Prioridad:

29.11.2012 GB 201221504

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

29.10.2024

73 Titular/es:

CRANE PAYMENT INNOVATIONS LIMITED
(100.0%)
Coin House, New Coin Street
Royton, Oldham OL2 6JZ, GB

72 Inventor/es:

HADLEY, ALEX

74 Agente/Representante:

SÁEZ MAESO, Ana

ES 2 984 174 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Prevención del fraude

Campo

5 Esta invención se refiere a la prevención del fraude mediante la detección de intentos de fraude en un aparato de pago. En particular, pero no exclusivamente, la invención se refiere a monitorear uno o más sensores de monedas para verificar el correcto funcionamiento.

Antecedentes

10 En un esfuerzo por provocar fraudulentamente que un aparato de pago pague más dinero del que debería, un estafador puede intentar cegar un sensor de monedas en una salida de monedas del aparato para evitar que el aparato registre que se están dispensando monedas y, por lo tanto, provocar que el aparato de pago continúe liberando monedas en la salida de monedas.

15 La publicación de patente de Estados Unidos No. US 4,579,217 presenta un validador de monedas electrónico que comprende un sensor (10) inductivo de monedas que produce una respuesta predeterminada a una moneda válida y un circuito (18, 20) equivalente de moneda que puede conmutarse mediante un interruptor (14, 16) en conexión operativa con el sensor para producir un efecto en el sensor de monedas similar al de una moneda pero con la moneda ausente, y un comparador (26) para comparar las respuestas de los dos sensores. La publicación de solicitud de patente internacional No. WO 02/077932 A1 presenta un dispositivo de discriminación de monedas que dispone de un electrodo (5) sensor y un oscilador (13). El oscilador está acoplado al electrodo sensor. El oscilador genera una señal de salida con una frecuencia (f_{vco}) que se puede controlar capacitivamente. Un detector (15-20) de frecuencia detecta una desviación de frecuencia (f) en la
20 señal de salida del oscilador, provocada por una variación en la capacitancia (C_m) en el electrodo sensor cuando se sitúa una moneda (1) cerca del electrodo sensor. Un dispositivo (23) de procesamiento determina el espesor de la moneda a partir de la desviación de frecuencia (f). El dispositivo discriminador de monedas está dispuesto de manera que la variación de capacitancia (C_m) se produce entre el electrodo (5) sensor y una
25 superficie de la moneda (1).

Resumen

La invención se define en las reivindicaciones 1-21.

30 Se proporciona un aparato de prevención de fraude para un aparato de pago de monedas, que comprende un sensor de monedas que comprende un oscilador eléctrico para detectar monedas en una trayectoria de salida de monedas; y al menos un controlador configurado para provocar un cambio esperado en una frecuencia de oscilación del sensor y para verificar si la frecuencia de oscilación ha cambiado como se esperaba, en donde, si el al menos un controlador no puede verificar que la frecuencia de oscilación del sensor ha cambiado como se esperaba, el al menos un controlador está configurado para provocar que se genere una señal de alarma para provocar que el aparato de pago de monedas cese las operaciones de pago.

35 El controlador puede configurarse para provocar el cambio esperado en la frecuencia de oscilación alterando una propiedad de un circuito oscilador en el sensor.

El controlador puede configurarse para provocar el cambio esperado en la frecuencia de oscilación alterando la configuración de un componente del sensor.

40 La alteración de la configuración del componente del sensor puede comprender alterar la configuración de uno o más elementos de sincronización en el sensor.

La alteración de la configuración del componente del sensor puede comprender agregar selectivamente al menos un componente de circuito al sensor.

La alteración de la configuración del componente del sensor puede comprender eliminar selectivamente al menos un componente del circuito del sensor.

45 La alteración de la configuración del componente del sensor puede comprender variar selectivamente el funcionamiento de al menos un componente del circuito en el sensor.

El al menos un componente del circuito puede comprender un componente capacitivo.

El al menos un componente del circuito puede comprender una resistencia eléctrica.

El al menos un componente del circuito puede comprender un componente eléctricamente inductivo.

El al menos un componente del circuito puede tener un valor en un amplio rango de tolerancia predeterminado, tal como más amplio que el promedio.

5 El controlador puede configurarse para verificar si la frecuencia de oscilación ha cambiado como se esperaba determinando una frecuencia de oscilación real del sensor y comparando la frecuencia real con una frecuencia esperada.

El controlador puede configurarse para determinar la frecuencia de oscilación esperada a partir de una configuración de componentes del sensor.

El controlador puede configurarse para medir la frecuencia de oscilación real a partir de una señal de salida del sensor.

10 El controlador puede configurarse para verificar si la frecuencia de oscilación ha cambiado como se esperaba, buscando en un perfil de frecuencia medido del sensor una coincidencia con un cambio esperado.

El controlador puede configurarse para determinar un cambio esperado en la frecuencia de oscilación a partir de un cambio real en una configuración de componente del sensor.

15 El controlador puede configurarse para provocar el cambio esperado en la frecuencia de oscilación y verificar si la frecuencia de oscilación ha cambiado como se esperaba en respuesta al transcurso de un período de tiempo predeterminado, la detección de un evento predeterminado o la aparición de un evento de tiempo generado aleatoriamente.

20 Si el controlador determina que la frecuencia de oscilación no ha cambiado como se esperaba, el controlador está configurado para responder provocando que se genere una señal de alarma. El sensor puede configurarse para detectar objetos en una primera ubicación en una trayectoria de monedas del aparato de pago, un sensor separado se puede configurar para detectar objetos en una segunda ubicación en la trayectoria de las monedas del aparato de pago; y el al menos un controlador puede configurarse para comparar las detecciones en la primera y segunda ubicaciones y verificar si el resultado de la comparación es el esperado.

El sensor separado puede ser un sensor óptico.

25 Como alternativa, el sensor separado puede ser un sensor de infrarrojos o ultravioleta.

El resultado de la comparación puede comprender una dirección en la que un objeto se ha movido en la trayectoria de la moneda.

El resultado de la comparación puede comprender un intervalo de tiempo entre las detecciones en la primera y la segunda ubicación.

30 El sensor de monedas puede comprender un elemento sensor de monedas cuyas características eléctricas se ven afectadas por el efecto eléctrico del paso de una moneda.

También se proporciona un aparato de pago de monedas que comprende el aparato de prevención de fraude.

35 También se proporciona un método de detección de un fraude en un aparato de pago de monedas, que comprende provocar, mediante al menos un controlador, un cambio esperado en una frecuencia de oscilación de un sensor de monedas de detección de monedas en el aparato de pago; verificar, mediante al menos un controlador, si la frecuencia de oscilación ha cambiado como se esperaba; y si al menos un controlador falla al verificar que la frecuencia de oscilación del sensor ha cambiado como se esperaba, provocar, por parte del al menos un controlador, que se genere una señal de alarma para provocar que el aparato de pago cese las operaciones de pago.

40 El método puede comprender provocar el cambio esperado en la frecuencia de oscilación alterando una propiedad de un circuito oscilador en el sensor.

El método puede comprender provocar el cambio esperado en la frecuencia de oscilación alterando la configuración de un componente del sensor.

45 La alteración de la configuración del componente del sensor puede comprender alterar una configuración de al menos un componente de sincronización en el sensor.

La alteración de la configuración del componente del sensor puede comprender eliminar o agregar selectivamente al menos un componente del circuito de o al sensor.

La alteración de la configuración del componente del sensor puede comprender variar selectivamente el funcionamiento de al menos un componente del circuito en el sensor.

El al menos un componente del circuito puede tener un valor en un rango de tolerancia predeterminado que es más amplio que el promedio.

El método puede comprender verificar si la frecuencia de oscilación ha cambiado como se esperaba determinando una frecuencia de oscilación real del sensor y comparando la frecuencia real con una frecuencia esperada.

También se proporciona un método para fabricar una pluralidad de aparatos de prevención de fraude, que comprende seleccionar componentes de circuito de amplia tolerancia para usar en los sensores de manera que haga que diferentes sensores oscilen en diferentes rangos de frecuencias preestablecidas. Este método no es según las reivindicaciones 1-21.

Breve descripción de las figuras.

A continuación se describirán modos de realización de la invención, únicamente con fines de ejemplo, con referencia a las figuras adjuntas en las que:

La figura 1 es una ilustración esquemática de un aparato de pago de monedas que comprende un aparato de prevención de fraude;

la figura 2 es un diagrama esquemático de un circuito sensor de monedas, cuya frecuencia de oscilación esperada puede alterarse para verificar su correcto funcionamiento;

la figura 3 es un diagrama esquemático de otro circuito sensor de monedas, cuya frecuencia de oscilación esperada puede alterarse para verificar su correcto funcionamiento;

la figura 4 es un diagrama esquemático de otro circuito sensor de monedas, cuya frecuencia de oscilación esperada puede alterarse para verificar su correcto funcionamiento;

la figura 5 es una ilustración esquemática de la región de salida de monedas de un aparato de pago en el que un sensor óptico y un sensor oscilante están configurados para detectar la presencia de monedas y otros objetos; y

la figura 6 es un diagrama de flujo de un método de detección de ataques de fraude en un aparato de pago monetario.

Descripción detallada

A continuación se describe un aparato 1 de prevención de fraude de un aparato 2 de pago monetario. El aparato 1 de prevención de fraude está configurado para realizar operaciones de verificación, cuyos resultados son indicativos de si el aparato 2 de pago está funcionando correctamente. El funcionamiento incorrecto del aparato 2 de pago puede ser indicativo de un ataque de fraude al aparato 2 de pago, tal como un ataque en el que un estafador intenta hacer que el aparato 2 de pago pague monedas que de otro modo no pagaría si funcionara correctamente.

Las operaciones de verificación que se realizan por el aparato 1 de prevención de fraude pueden comprender verificar que uno o más sensores 3, que están configurados para detectar monedas a medida que se pagan a través de una salida 4 de monedas del aparato 2 de pago, estén funcionando correctamente. Con referencia a la figura 1, el(los) sensor(es) 3 puede(n) estar ubicado(s) en o adyacente(s) a una trayectoria 5 de salida de monedas que dirige las monedas liberadas desde el almacenamiento de monedas 6 del aparato 2 de pago a la salida 4 de monedas desde la cual las monedas están disponibles para su recogida. Un ejemplo de almacenamiento de monedas adecuado es una tolva 6 de monedas que dispensa monedas de forma selectiva y que se puede controlar a la salida 4 de monedas a través de la trayectoria 5 de salida de monedas. Durante un funcionamiento correcto, los sensores 3 están configurados para detectar la presencia de monedas a medida que las monedas pasan por los sensores 3 en la trayectoria 5 de salida de monedas y para generar señales que indican que las monedas han sido detectadas. De esta manera, el aparato 2 de pago de monedas es capaz de registrar y contar las monedas en la salida 4 de monedas y por tanto determinar cuándo dejar de dispensar monedas en la trayectoria 5 de salida de monedas.

El aparato 1 de prevención de fraude verifica que los sensores 3 estén funcionando correctamente monitorizando las señales generadas por los sensores 3 y comprobando que las señales sean las esperadas. Si las señales no son las esperadas, el aparato 1 de prevención de fraude puede configurarse para emitir una señal de alarma para indicar que el aparato 2 de pago está bajo un ataque de fraude. El aparato de pago 2 puede configurarse para responder a la señal de alarma cesando sus operaciones de pago.

El aparato 1 de prevención de fraude y el aparato 2 de pago monetario en el que está comprendido el aparato 1 de prevención de fraude pueden operar bajo el control de un único controlador electrónico, o una pluralidad de controladores electrónicos, cada uno de los cuales controla el funcionamiento de ambos aparatos. Por ejemplo, los aparatos 1, 2 pueden implementarse como una única unidad en la que el(los) controlador(es)

puede(n) configurarse para controlar todas las funciones del aparato 2 de pago, incluidas las del aparato 1 de prevención de fraude.

Alternativamente, el aparato 1 de prevención de fraude y el aparato 2 de pago monetario pueden operar bajo el control de controladores electrónicos separados dedicados, cada uno de los cuales controla las operaciones de solo uno de los dos aparatos 1, 2.

El aparato 1 de prevención de fraude comprende un sensor 3a para detectar monedas en la trayectoria 5 de salida de monedas del aparato 2 de pago. El sensor 3a comprende un oscilador, tal como un circuito oscilador eléctrico, que oscila a una frecuencia que depende de las características de un elemento 7 detector de monedas acoplado al sensor 3a. El elemento 7 detector de monedas tiene características eléctricas que varían temporalmente por el efecto eléctrico de las monedas a medida que las monedas se mueven a lo largo de la trayectoria 5 de salida de monedas, como se describe a continuación.

Puede usarse cualquier circuito oscilador adecuado. Ejemplos incluyen circuitos osciladores en los que el elemento 7 detector de monedas es un elemento 7 eléctricamente inductivo, como en los circuitos osciladores LC y RL. El elemento 7 eléctricamente inductivo puede comprender una o más bobinas eléctricamente inductivas u otros devanados.

Otro ejemplo es un circuito oscilador en el que el elemento 7 detector de monedas es un elemento 7 capacitivo, como en los circuitos osciladores RC. El elemento 7 capacitivo puede comprender uno o más condensadores.

En las figuras 2 a 4 se ilustran ejemplos específicos del sensor 3a. En estas figuras, el sensor 3a comprende un oscilador de LC relajación en el que el elemento 7 detector de monedas es un elemento inductivo.

El oscilador se puede implementar usando un disparador Schmitt inversor, que puede comprender una pluralidad de componentes de circuito discreto conectados, que comprende, por ejemplo, un comparador (por ejemplo, que comprende un transistor) y una pluralidad de resistencias, o un circuito integrado (IC) como se muestra en las figuras 2 a 4.

El elemento 7 detector de monedas está conectado en el oscilador de modo que el sensor 3a oscile a una frecuencia que depende de las características eléctricas del elemento 7 detector y que varía con ellas. Por ejemplo, si el elemento 7 detector comprende un inductor 7 como se ilustra en las figuras 2 a 4, el sensor 3a está configurado para oscilar a una frecuencia que depende de la inductancia del inductor 7.

Como se describirá a continuación, el aparato 1 de prevención de fraude está configurado para variar deliberadamente la frecuencia de oscilación base esperada del sensor 3a, por ejemplo alterando la configuración de un componente en el sensor 3a, para permitir la detección de ataques de fraude.

Con referencia a las figuras 1 a 4, el sensor 3a, y en particular el elemento 7 detector de monedas mencionado anteriormente, está ubicado en las proximidades de la trayectoria 5 de salida de monedas del aparato 2 de pago de manera que las monedas que se mueven a lo largo de la trayectoria 5 de salida hacia la salida 4 de monedas efectúa un cambio detectable en las características eléctricas, tales como la inductancia o capacitancia, del elemento 7 detector. Por lo tanto, cuando el aparato 2 de pago dispensa una moneda a lo largo de la trayectoria 5 de salida, la frecuencia de oscilación del sensor 3a se altera temporalmente, de una manera que está relacionada con las propiedades de la moneda, por el efecto electromagnético de la moneda que pasa por el elemento 7 detector.

El sensor 3a está configurado para generar una señal de salida que es proporcional y/o indicativa de su frecuencia de oscilación. Se debería esperar que esta señal de salida del sensor 3a, en el funcionamiento correcto del sensor 3a, refleje alteraciones en las características eléctricas del elemento 7 detector y, por tanto, la presencia de monedas en la trayectoria 5 de salida de monedas. Por ejemplo, se puede observar un pico, representativo de un cambio en las características eléctricas del elemento 7, en la señal de salida del sensor 3a cuando una moneda pasa por el elemento 7 detector en su trayectoria hacia la salida 4 de monedas.

La señal de salida puede comprender una señal de voltaje de salida del sensor 3a, como se muestra en las figuras 2 a 4, y por tanto puede oscilar a la misma frecuencia que el sensor 3a.

El aparato 2 de pago puede configurarse para determinar el valor de la(s) moneda(s) a partir de las características del(de los) cambio(s) correspondiente(s) en la señal de salida y para contar la(s) moneda(s) en la salida 4 de monedas. De este modo, el aparato 2 puede determinar cuándo se ha dispensado el valor requerido de monedas y evitar pagar en exceso. El sensor 3a puede, por ejemplo, configurarse para alimentar la señal de salida del sensor 3a a un controlador electrónico del aparato 2 de pago. El controlador está configurado para analizar la señal, por ejemplo comparando las características de la señal con las características conocidas de las monedas almacenadas en una memoria del aparato 2, para determinar cuándo se ha dispensado el valor correcto de monedas para un pago particular. Al hacerlo, el controlador puede configurarse para provocar que se cierre una salida del almacenamiento 6 de monedas, que alimenta la trayectoria 5 de salida de monedas, y por lo tanto evitar el pago en exceso. Alternativamente, el aparato 2

puede configurarse sólo para verificar que se haya dispensado el número esperado de monedas, en lugar de comprobar también adicionalmente el valor de las monedas dispensadas. Esto puede requerir menos componentes del circuito.

Si el sensor 3a no funciona correctamente, de modo que la señal de salida alimentada al controlador indica que se han dispensado menos monedas o un valor menor a la salida 4 de monedas de lo que realmente es el caso, el controlador puede ser inducido a error al dispensar más monedas de las necesarias en la trayectoria 5 de salida de monedas y, por tanto, pagar en exceso el pago en un intento de contar el valor correcto de las monedas en la salida 4 de monedas. Un caso en el que el sensor 3a puede no funcionar correctamente es si es sobrecargado de manera fraudulenta por una forma de onda generada externamente que oculta los cambios en la señal de salida que normalmente serían provocados por monedas que pasan por el elemento 7 detector en su camino desde el almacenamiento 6 de monedas a la salida 4 de monedas. Por ejemplo, el sensor 3a podría ser sobrecargado a una frecuencia similar a la que indica que no hay ninguna moneda presente en la trayectoria 5 de salida de monedas. Alternativamente, las características eléctricas del elemento 7 detector podrían alterarse insertando un objeto extraño en la trayectoria 5 de salida de monedas desde el exterior del aparato 2 de pago.

En estas circunstancias, las monedas pueden pasar el elemento 7 detector del sensor 3a en su camino hacia la salida 4 de monedas sin provocar los efectos correspondientes en la señal de salida del sensor 3a y, por lo tanto, sin ser registradas y contadas por el controlador.

El aparato 1 de prevención de fraude está configurado para detectar dichos actos fraudulentos verificando que el sensor 3a esté funcionando correctamente. Por ejemplo, el sensor 3a puede configurarse para alimentar su señal de salida a un controlador 8 electrónico del aparato 1 de prevención de fraude, mostrado en la figura 1, que está configurado para provocar que se lleve a cabo una operación de verificación del sensor en relación con el sensor 3a. El controlador 8 puede comprender uno o más procesadores 9 que, funcionando bajo el control de instrucciones legibles por ordenador, por ejemplo comprendidas en un código de programa informático almacenado en una memoria 10 del aparato 1 de prevención de fraude o en cualquier otro lugar del aparato 2 de pago, están configurados para realizar la operación de verificación.

La operación de verificación para el sensor 3a comprende provocar un cambio en la frecuencia de oscilación esperada del sensor 3a y posteriormente comprobar que la frecuencia de oscilación ha cambiado como se esperaba. El cambio en la frecuencia de oscilación esperada del sensor 3a puede deberse a la alteración de la configuración del componente del oscilador. Por ejemplo, como se describirá con más detalle a continuación, la alteración de la configuración de los componentes del oscilador puede comprender modificar uno o más componentes del circuito, tal como conmutar uno o más componentes del circuito dentro o fuera del circuito del oscilador, para alterar las propiedades del circuito. Los componentes que son modificados, por ejemplo, conmutados dentro y/o fuera del circuito, pueden ser componentes de sincronización del oscilador, tales como condensadores y/o resistencias, o componentes del inversor, como se explica a continuación.

Con referencia a las figuras 2 y 3, un ejemplo comprende alterar la capacitancia de un circuito oscilador de relajación LC en el sensor 3a en una cantidad conocida y verificar posteriormente que la frecuencia de oscilación del sensor 3a ha cambiado como se esperaría después del cambio conocido en la capacitancia. La capacitancia se puede alterar reemplazando, agregando y/o quitando componentes capacitivos hacia/desde el circuito oscilador. Para facilitar esto, el sensor 3a puede acoplarse selectivamente a una pluralidad de condensadores 11 que el controlador 8 puede conmutar selectivamente dentro y fuera del oscilador LC de relajación.

Más específicamente, la pluralidad de condensadores 11 puede acoplarse al oscilador LC de relajación a través de uno o más interruptores 12 electrónicos, tales como uno o más transistores 12a, 12b, que pueden ser accionados por el controlador 8 para conmutar selectivamente cada uno de los condensadores 11 dentro o fuera del circuito oscilador para variar su capacitancia. En la figura 2 se ilustra un ejemplo, en el que una pluralidad de interruptores 12, cada uno de los cuales que comprende un transistor 12a, 12b, están configurados para conmutar selectivamente uno o más de la pluralidad de condensadores 11 dentro y fuera de un circuito LC oscilador bajo el control del controlador 8.

El controlador 8 abre y cierra los interruptores 12 suministrando señales de control a los interruptores 12. Por ejemplo, la figura 2 ilustra cómo cada uno de los transistores 12a, 12b mencionados anteriormente puede acoplarse independientemente al controlador 8 del aparato 1 de prevención de fraude mediante un acoplamiento de comunicación adecuado de modo que se puedan aplicar señales de control, tales como señales de voltaje adecuadas, por el controlador 8 para hacer que los transistores 12a, 12b conmuten independientemente cada condensador 11 dentro o fuera del circuito oscilador.

Se apreciará que en implementaciones alternativas del oscilador, los componentes de sincronización distintos de los condensadores 11 podrían conmutarse selectivamente dentro o fuera del circuito oscilador de la misma manera que se describió anteriormente para provocar un cambio en la frecuencia de oscilación esperada del

sensor 3a. Por ejemplo, si se usa un oscilador RL o RC, los componentes resistivos tales como resistencias pueden conmutarse selectivamente dentro y fuera del oscilador bajo el control del controlador 8.

Adicional o alternativamente, se puede provocar un cambio en la frecuencia de oscilación esperada del sensor 3a alterando la configuración de los componentes del inversor del sensor. Por ejemplo, con referencia a la figura 4, uno o más componentes de circuito discretos, tales como una o más resistencias, pueden conectarse o desconectarse del inversor para variar los umbrales de conmutación del inversor y, por lo tanto, variar la frecuencia de oscilación del sensor 3a.

Adicional o alternativamente, los cambios en la frecuencia de oscilación esperada del sensor 3a pueden ser provocados mediante la conmutación de elementos sensores de monedas adicionales 7 dentro o fuera del circuito oscilador. Por ejemplo, el circuito puede comprender una pluralidad de elementos inductivos o capacitivos 7, conectados en serie o en paralelo, que pueden conmutarse selectivamente, individual o colectivamente, dentro o fuera del circuito para variar la frecuencia de oscilación del sensor 3a.

Con referencia a las figuras 3 y 4, como alternativa al uso de los interruptores 12 expuestos anteriormente y mostrados en la figura 2, los componentes del circuito pueden conmutarse dentro y fuera del circuito oscilador mediante señales de voltaje de control aplicadas directamente a los componentes desde el controlador 8. Esto puede reducir el número de componentes necesarios en el circuito oscilador.

El controlador 8 puede configurarse para cambiar la frecuencia base esperada del oscilador, por ejemplo alterando la configuración del componente del oscilador en una de las formas descritas anteriormente, en respuesta al transcurso de períodos de tiempo preestablecidos. El controlador 8 puede configurarse para generar aleatoriamente la nueva configuración de componentes, de modo que la nueva frecuencia de oscilación esperada también se genere aleatoriamente. El controlador 8 puede alterar adicional o alternativamente la frecuencia base esperada del oscilador en momentos generados aleatoriamente, o en respuesta a eventos particulares. Por ejemplo, el controlador 8 puede configurarse para alterar la configuración del oscilador a intervalos de tiempo regulares, como cada diez milisegundos, con el fin de variar la frecuencia de oscilación esperada del sensor 3a. Se apreciará que se puede utilizar cualquier número preestablecido de milisegundos. Adicional o alternativamente, el controlador 8 puede configurarse para alterar la frecuencia base esperada del oscilador en respuesta al transcurso de un período de tiempo relativamente largo desde que el sensor 3a detectó una moneda por última vez o en respuesta a otros eventos similares que son consistentes con la manipulación de forma fraudulenta del sensor 3a. El controlador 8 puede configurarse para generar aleatoriamente una nueva configuración de componentes para el oscilador inmediatamente antes de provocar una transición a una nueva configuración.

El controlador 8 siempre conoce la configuración exacta de los componentes del oscilador y, por lo tanto, el controlador 8 siempre puede determinar la frecuencia de oscilación esperada del sensor 3a y comparar la frecuencia de oscilación esperada con la frecuencia de oscilación medida para verificar el funcionamiento correcto. El controlador 8 almacena la configuración en la memoria 10 del aparato 1 de prevención de fraude o en otro lugar del aparato 2 de pago.

Como se mencionó anteriormente, habiendo alterado la configuración del sensor 3a para esperar un cambio en su frecuencia de oscilación, el controlador 8 del aparato 1 de prevención de fraude está configurado para verificar que la frecuencia de oscilación del sensor 3a ha cambiado como se esperaba. El controlador 8 puede configurarse para realizar estas verificaciones a los mismos intervalos regulares que las alteraciones en la configuración del sensor.

El controlador 8 puede configurarse para predecir la nueva frecuencia de oscilación esperada del sensor 3a calculando matemáticamente la frecuencia basándose en la configuración de componentes conocida del oscilador. Por ejemplo, si se usa un oscilador LC de relajación, el controlador 8 está configurado para predecir la nueva frecuencia de oscilación esperada del sensor inductivo 3a calculando matemáticamente la frecuencia basándose en la capacitancia conocida del oscilador LC de relajación en su nueva configuración y otros parámetros conocidos del circuito oscilador, incluidos los del elemento 7 detector inductivo. Posteriormente, el controlador 8 puede configurarse para medir la frecuencia de oscilación real del sensor 3a para comprobar si la frecuencia medida cae dentro de un margen predeterminado de la frecuencia prevista. La medición de frecuencia tiene lugar antes de que el controlador 8 haga que el oscilador pase a otra nueva configuración de componente y, por tanto, a otra nueva frecuencia de oscilación esperada, momento en el cual se puede repetir el proceso de verificación. El tamaño del margen predeterminado, denominado inmediatamente a continuación rango aceptable predeterminado, puede tener en cuenta, o representar, márgenes de error asociados con las frecuencias predichas y/o medidas.

Si las frecuencias operativas previstas y reales del sensor 3a están ambas dentro del rango aceptable predeterminado, el controlador 8 puede configurarse para verificar positivamente que el sensor 3a esté funcionando correctamente. Por el contrario, si las frecuencias operativas previstas y reales no están dentro del rango predeterminado, el controlador 8 puede fallar al verificar que el sensor 3a está funcionando

correctamente, o puede tomar una determinación positiva de que no lo está, provocando por tanto la señal de alarma mencionada para que se genere previamente.

La fabricación de una pluralidad de aparatos 1 de prevención de fraude puede comprender variar los valores de los componentes en el sensor 3a de un aparato 1 al siguiente para garantizar que los sensores 3a de diferentes aparatos 1 no oscilen a las mismas frecuencias base. Por ejemplo, los valores de los componentes de sincronización en el circuito oscilador, tales como las capacitancias de los condensadores individuales 11 mostrados en las figuras 2 y 3 o las resistencias de las resistencias individuales, pueden variarse de un aparato 1 al siguiente. Alternativamente, los valores de los componentes discretos en el inversor pueden variarse de un aparato 1 al siguiente. Esta acción garantiza que las diversas configuraciones posibles del oscilador, y por tanto las frecuencias de oscilación, de cada sensor 3a sean diferentes y, por tanto, provoque una variación significativa a través de la pluralidad de aparatos 1 fabricados. El resultado es que no hay frecuencias de oscilación predefinidas en las que se sabe que todos los sensores 3a asociados con la pluralidad de aparatos de prevención de fraude funcionan correctamente y, como tales, en el improbable caso de que un estafador fuera capaz de sobrecargar con éxito o manipular fraudulentamente de otro modo un sensor particular 3a como se describió anteriormente, el estafador no podría manipular fraudulentamente otro sensor 3a de la misma manera debido a la diferencia en las frecuencias operativas entre los sensores 3a.

La variación en los valores de los componentes, tales como valores de condensadores o resistencias, de un aparato 1 al siguiente se puede lograr seleccionando los componentes para un aparato 1 particular de uno o más grupos constituidos por componentes con un gran número de valores declarados diferentes (por ejemplo, capacitancias o resistencias) y/o utilizando componentes que tengan amplias tolerancias.

Una alternativa a variar la configuración de los componentes del circuito oscilador es que el controlador 8 corte la alimentación al oscilador y verifique que la señal de salida del sensor 3a refleje esto como se esperaría. Si la señal de salida no varía como se esperaba, el controlador 8 está configurado para advertir de un ataque de fraude al aparato 2 como se describió anteriormente.

La figura 5 muestra una ubicación de ejemplo de un sensor óptico 3b, junto con el sensor 3a oscilante descrito anteriormente, para detectar monedas en la trayectoria 5 de salida de monedas del aparato 2 de pago. El sensor óptico 3b comprende uno o más emisores 13 ópticos, tales como uno o más LED 13, y uno o más detectores 14 ópticos, tales como uno o más fototransistores 14. Los emisores 13 ópticos están configurados para emitir luz en la dirección de los detectores 14 ópticos de modo que los detectores 14 detecten la luz emitida cuando la trayectoria óptica entre los emisores 13 y los detectores 14 no esté bloqueada.

Los emisores 13 ópticos y los detectores 14 están ubicados en las proximidades de la trayectoria 5 de salida de monedas en ubicaciones que hacen que las monedas que se desplazan a la salida 4 de monedas a través de la trayectoria 5 de salida de monedas bloqueen la trayectoria óptica entre el(los) emisor(es) 13 y el(los) detector(es) 14. Por ejemplo, un emisor 13 y un detector 14 correspondiente en la trayectoria óptica del emisor 13 pueden estar ubicados en lados opuestos de la trayectoria 5 de salida de monedas o de la salida 4 de monedas.

El sensor 3b óptico está acoplado comunicativamente al controlador 8 del aparato 1 de prevención de fraude y el controlador 8 está configurado para monitorear el estado del sensor 3b óptico con el fin de detectar monedas que se dispensan desde el almacenamiento 6 de monedas a la salida 4 de monedas. Más específicamente, una señal de salida del sensor óptico 3b indica al controlador 8 si la trayectoria óptica entre el(los) emisor(es) 13 y el(los) detector(es) 14 mencionados anteriormente está bloqueado. La señal de salida del sensor 3b óptico también indica el momento en el que se bloqueó la trayectoria óptica del sensor 3b. Por ejemplo, la señal de salida puede indicar los momentos en los que comenzó y terminó el bloqueo o la interrupción de la trayectoria óptica del sensor 3b, y también la duración durante la cual la trayectoria óptica estuvo bloqueada. Una indicación similar también está presente en la señal de salida del sensor 3a oscilante descrito anteriormente.

El sensor 3a oscilante y el sensor 3b óptico pueden estar físicamente separados en la trayectoria 5 de salida de monedas por una distancia predeterminada de modo que una moneda que se mueve a lo largo de la trayectoria 5 de salida de monedas hasta la salida 4 de monedas es detectada primero por el sensor 3a oscilante y posteriormente detectada por el sensor 3b óptico. Se apreciará que los sensores 3a, 3b podrían ubicarse alternativamente de manera que la moneda sea detectada primero por el sensor 3b óptico y posteriormente por el sensor 3a oscilante.

El orden en el que los sensores 3a, 3b detectan la moneda permite que el aparato 1 de prevención de fraude determine la dirección en la que se mueven las monedas a lo largo de la trayectoria 5 de salida de monedas. Por ejemplo, si se realiza una primera detección mediante el sensor 3a que está ubicado más lejos de la salida 4 de monedas y se realiza una segunda detección posterior mediante el sensor 3b que está ubicado más cerca de la salida 4 de monedas, el controlador 8 puede determinar que el objeto se ha movido desde el almacenamiento 6 de monedas hasta la salida 4 de monedas como sería de esperar durante el dispensado de monedas. El orden de detección también permite que el aparato 1 determine la dirección en la que se mueven objetos extraños, tales como dispositivos de manipulación de sensores fraudulentos inductivos, en la trayectoria

5 de la moneda y, por tanto, identifique un potencial ataque de fraude mediante la identificación de un evento inesperado.

Si el orden indicado por los sensores 3a, 3b no es el esperado, por ejemplo porque una comparación de las señales de salida del sensor indica que el sensor 3b que está ubicado más cerca de la salida 4 de monedas detectó el objeto antes que el sensor 3a que está ubicado más lejos de la salida 4 de monedas, entonces el controlador 8 puede determinar que se ha insertado un objeto en la trayectoria 5 de salida de monedas desde el exterior del aparato 2 de pago. Dicha determinación es indicativa de un ataque de fraude, tal como un intento de insertar un dispositivo para manipular la frecuencia de oscilación del sensor 3a oscilante como se describió anteriormente, y puede provocar que el controlador 8 genere la señal de alarma mencionada anteriormente.

Además de indicar la dirección en la que los objetos (por ejemplo, monedas) se han movido a lo largo de la trayectoria 5 de salida de monedas, una comparación de las señales de salida del sensor también permite al controlador 8 determinar el intervalo de tiempo entre el objeto que es detectado por los sensores 3a, 3b. El controlador 8 puede configurarse para comparar estos intervalos de tiempo medidos con los que se esperarían en el funcionamiento normal del aparato 2. Por ejemplo, el controlador 8 puede configurarse para comparar un intervalo de tiempo medido entre un objeto que pasa primero por el sensor 3a oscilante y posteriormente por el sensor 3b óptico con un intervalo de tiempo esperado que se almacena en una memoria del aparato 1 de prevención de fraude. El intervalo de tiempo esperado puede derivarse de la velocidad esperada de una moneda en la salida 5 de monedas en condiciones de funcionamiento normales y de la distancia conocida entre los sensores 3a, 3b. Adicional o alternativamente, el intervalo de tiempo esperado puede basarse en mediciones de configuración realizadas durante la fabricación del aparato 2.

Un intervalo de tiempo medido que no coincide estrechamente con el intervalo de tiempo esperado correspondiente almacenado en la memoria es indicativo de un ataque de fraude al aparato 2 de pago y puede provocar que el controlador 8 genere la señal de alarma mencionada anteriormente.

A continuación se detalla un método para prevenir el fraude, de acuerdo con los aparatos y operaciones descritos anteriormente, en relación con la figura 6.

En una primera etapa S1, el controlador 8 del aparato 1 de prevención de fraude está configurado para detectar un evento de activación que indica que se debe cambiar la frecuencia de funcionamiento del sensor 3a oscilante. El evento de activación puede ser el transcurso de un período de tiempo predeterminado desde un evento anterior, o la detección o aparición de un evento particular como se describió anteriormente. En una segunda etapa S2 del método, el controlador 8 está configurado para provocar el cambio en la frecuencia de funcionamiento del sensor 3a, por ejemplo alterando la configuración del circuito oscilador. En una tercera etapa S3 del método, el controlador 8 del aparato 1 de prevención de fraude está configurado para comprobar si la frecuencia operativa del sensor 3a ha cambiado como se esperaba y, si no lo ha hecho, puede configurarse para provocar que se genere una señal de alarma de fraude.

En una cuarta etapa S4, en respuesta a la detección de un objeto en la trayectoria 5 de salida de monedas por uno o ambos de los sensores 3a, 3b de monedas ubicados por separado, el controlador 8 está configurado para determinar la dirección en la que el objeto se ha movido a lo largo de la trayectoria 5 de salida determinando el orden en el que el objeto fue detectado por los sensores 3a, 3b. Si la dirección de desplazamiento no es la esperada, el controlador 8 puede configurarse para provocar que se genere la señal de alarma de fraude.

En una quinta etapa S5 del método, el controlador 8 está configurado para determinar si un intervalo de tiempo medido entre el objeto que es detectado independientemente por los sensores 3a, 3b de monedas es el que se esperaría para una moneda que se dispensa desde el almacenamiento de monedas 6 bajo condiciones normales de funcionamiento. Si el intervalo de tiempo no es el esperado, el controlador 8 puede configurarse para provocar que se genere la señal de alarma de fraude.

Se apreciará que se pueden realizar diversas modificaciones a la implementación descrita anteriormente y mostrada en las figuras sin apartarse del alcance de las reivindicaciones adjuntas. Por ejemplo, aunque el oscilador ilustrado en las figuras es para un sensor de modulación de frecuencia (FM), el sensor 3a oscilante podría comprender alternativamente un sensor de FM y un sensor de modulación de amplitud (AM) como una capa adicional de seguridad. En tal implementación, una señal AM demodulada proporcionaría una señal analógica al controlador 8 que es responsable de provocar cambios en la frecuencia de oscilación esperada del sensor 3a. El controlador 8 estaría configurado para determinar cambios en las señales de FM y AM emitidas por el sensor 3a y para verificar que los cambios, por ejemplo desde un valor predeterminado, sean en una sola dirección hasta que se reciba una señal de pico, seguida de cambios en la dirección opuesta, por ejemplo, volviendo al valor predeterminado. Los valores de pico en las señales de salida pueden ocurrir cuando la moneda está ubicada centralmente o adyacente al elemento 7 detector de monedas. Los cambios en la dirección de la señal que ocurren en un momento inesperado, tal como uno que no corresponde a la desviación máxima de la señal del valor predeterminado, pueden ser indicativos de un ataque de fraude.

El controlador 8 también puede configurarse para determinar la magnitud de las desviaciones de la señal de pico y para verificar que las magnitudes caen dentro de los límites esperados, que pueden almacenarse en la memoria 10.

Un diseño de circuito de factor de alta calidad garantiza una variación relativamente grande en la señal AM para un pequeño cambio en la frecuencia de oscilación del sensor 3a y, por lo tanto, establece una variable adicional que un posible estafador debe intentar manipular al realizar un ataque de fraude. Un diseño de este tipo también proporcionaría un alto nivel de variación en las características de funcionamiento (por ejemplo, frecuencia) del sensor 3a para cambios relativamente pequeños en los valores de los componentes, aumentando por tanto la complejidad y la dificultad para manipular con éxito una pluralidad de sensores 3a de la misma manera.

Se apreciará que los modos de realización y las alternativas descritas anteriormente se pueden usar de manera separada o en combinación. También se apreciará que alternativas que no se han expuesto explícitamente anteriormente están dentro del alcance de la invención. Por ejemplo, como se describe brevemente, aunque el circuito oscilador se describe anteriormente principalmente en relación con un oscilador LC, alternativamente se podrían usar otros tipos de oscilador. Las frecuencias de oscilación de dichos osciladores alternativos se pueden variar alterando la configuración de los componentes del oscilador de manera similar a los ejemplos de LC. Un ejemplo específico de un oscilador alternativo es un oscilador RL o RC, en el que se varía un valor de resistencia del circuito bajo el control del controlador 8 para provocar un cambio en la frecuencia de oscilación del sensor 3a. Los componentes resistivos, tales como una o más resistencias, se pueden encender y apagar del circuito de manera similar a los componentes capacitivos para alterar la frecuencia de oscilación. En particular, la operación de verificación para el sensor 3a oscilante puede comprender alterar la resistencia de un oscilador RL o RC en el sensor 3a en una cantidad conocida y verificar posteriormente que la frecuencia de oscilación del sensor 3a ha cambiado como se esperaría siguiendo el cambio en la resistencia conocida. La resistencia se puede alterar reemplazando, agregando y/o quitando componentes resistivos hacia/desde el circuito oscilador. Para facilitar esto, el sensor 3a puede acoplarse selectivamente a una pluralidad de resistencias que el controlador 8 puede conmutar selectivamente dentro y fuera del oscilador, por ejemplo usando uno o más interruptores 12 como se describió anteriormente o aplicando señales de control a los componentes desde el controlador 8.

También se apreciará que los componentes específicos y los valores de los componentes ilustrados en las figuras 2 a 4 se pueden reemplazar con componentes y valores de los componentes alternativos para lograr los mismos efectos que los circuitos ilustrados.

Además, como alternativa a conmutar componentes dentro o fuera del oscilador, como se describió anteriormente, el controlador 8 puede configurarse para ajustar los valores de componentes variables en el oscilador, tales como una o más resistencias variables, con el fin de alterar la frecuencia de oscilación del sensor 3a.

REIVINDICACIONES

1. Un aparato (1) de prevención de fraude para un aparato (2) de pago de monedas, que comprende:
un sensor (3) de monedas que comprende un oscilador eléctrico de detección de monedas en una trayectoria de salida de monedas; y
5 al menos un controlador (8) configurado para provocar un cambio esperado en una frecuencia de oscilación del sensor y para verificar si la frecuencia de oscilación ha cambiado como se esperaba;
en donde, si al menos un controlador falla al verificar que la frecuencia de oscilación del sensor haya cambiado como se esperaba, al menos un controlador está configurado para provocar que se genere una señal de alarma para provocar que el aparato de pago de monedas cese las operaciones de pago.
- 10 2. Un aparato según la reivindicación 1, en donde el controlador está configurado para provocar el cambio esperado en la frecuencia de oscilación alterando una propiedad de un circuito oscilador en el sensor.
3. Un aparato según la reivindicación 1 o 2, en donde el controlador está configurado para provocar el cambio esperado en la frecuencia de oscilación alterando la configuración de un componente del sensor.
4. Un aparato según la reivindicación 3, en donde la alteración de la configuración del componente comprende:
15 alterar la configuración de uno o más elementos de sincronización en el sensor; y/o
añadir selectivamente al menos un componente de circuito al sensor; y/o
retirar selectivamente al menos un componente del circuito del sensor; y/o
variar selectivamente el funcionamiento de al menos un componente del circuito en el sensor.
- 20 5. Un aparato según la reivindicación 4, en donde al menos un componente del circuito comprende un componente capacitivo y/o una resistencia eléctrica y/o un componente eléctricamente inductivo.
6. Un aparato según cualquiera de las reivindicaciones anteriores, en donde el controlador está configurado para verificar si la frecuencia de oscilación ha cambiado como se esperaba determinando una frecuencia de oscilación real del sensor y comparando la frecuencia real con una frecuencia esperada.
- 25 7. Un aparato según la reivindicación 6, en donde el controlador está configurado para determinar la frecuencia de oscilación esperada a partir de una configuración de componentes del sensor.
8. Un aparato según la reivindicación 6 o 7, en donde el controlador está configurado para medir la frecuencia de oscilación real a partir de una señal de salida del sensor.
9. Un aparato según cualquiera de las reivindicaciones 6 a 8, en donde el controlador está configurado para verificar si la frecuencia de oscilación ha cambiado como se esperaba, buscando en un perfil de frecuencia medido del sensor una coincidencia con un cambio esperado.
- 30 10. Un aparato según cualquiera de las reivindicaciones anteriores, en donde el controlador está configurado para determinar un cambio esperado en la frecuencia de oscilación a partir de un cambio real en una configuración de componente del sensor.
11. Un aparato según cualquiera de las reivindicaciones anteriores, en donde el controlador está configurado para provocar el cambio esperado en la frecuencia de oscilación y verificar si la frecuencia de oscilación ha cambiado como se esperaba en respuesta al transcurso de un período de tiempo predeterminado, la detección de un evento predeterminado o la aparición de un evento temporal generado aleatoriamente.
12. Un aparato según cualquiera de las reivindicaciones anteriores, en donde:
40 el sensor está configurado para detectar objetos en una primera ubicación en una trayectoria de monedas del aparato de pago;
un sensor separado está configurado para detectar objetos en una segunda ubicación en la trayectoria de monedas del aparato de pago; y
el al menos un controlador está configurado para comparar las detecciones en la primera y segunda ubicaciones y verificar si el resultado de la comparación es el esperado.
- 45 13. Un aparato según la reivindicación 12, en donde el sensor separado es un sensor óptico.
14. Un aparato según la reivindicación 12 o 13, en donde el resultado de la comparación comprende:
una dirección en la que un objeto se ha movido en la trayectoria de la moneda; y/o
un intervalo de tiempo entre las detecciones en la primera y la segunda ubicaciones.

15. Un aparato según cualquiera de las reivindicaciones anteriores, en donde el sensor de monedas comprende un elemento detector de monedas cuyas características eléctricas se ven afectadas por el efecto eléctrico del paso de una moneda.
- 5 16. Un aparato (2) de pago de monedas que comprende un aparato (1) de prevención de fraude según cualquiera de las reivindicaciones anteriores.
17. Un método de detección de fraude en un aparato (2) de pago de monedas, que comprende:
provocar, mediante al menos un controlador, un cambio esperado en una frecuencia de oscilación de un sensor (3) de monedas para detectar monedas en el aparato de pago;
verificar, mediante al menos un controlador, si la frecuencia de oscilación del sensor ha cambiado como se
10 esperaba; y
si al menos un controlador falla al verificar que la frecuencia de oscilación del sensor ha cambiado como se esperaba, provocar, por parte del al menos un controlador, que se genere una señal de alarma para provocar que el aparato de pago cese las operaciones de pago.
- 15 18. Un método según la reivindicación 17, que comprende provocar el cambio esperado en la frecuencia de oscilación alterando una propiedad de un circuito oscilador en el sensor.
19. Un método según la reivindicación 17 o 18, que comprende provocar el cambio esperado en la frecuencia de oscilación alterando la configuración de un componente del sensor.
20. Un método según la reivindicación 19, en donde la alteración de la configuración del componente comprende:
20 alterar una configuración de al menos un componente de sincronización en el sensor; y/o
eliminar o añadir selectivamente al menos un componente del circuito de o al sensor; y/o
variar selectivamente el funcionamiento de al menos un componente del circuito en el sensor.
- 25 21. Un método según cualquiera de las reivindicaciones 17 a 20, que comprende verificar si la frecuencia de oscilación ha cambiado como se esperaba determinando una frecuencia de oscilación real del sensor y comparando la frecuencia real con una frecuencia esperada.

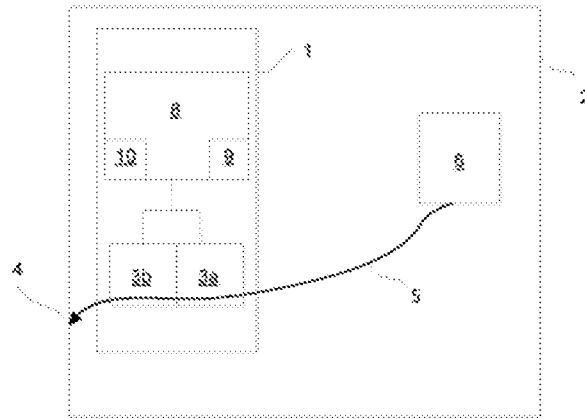


Fig. 1

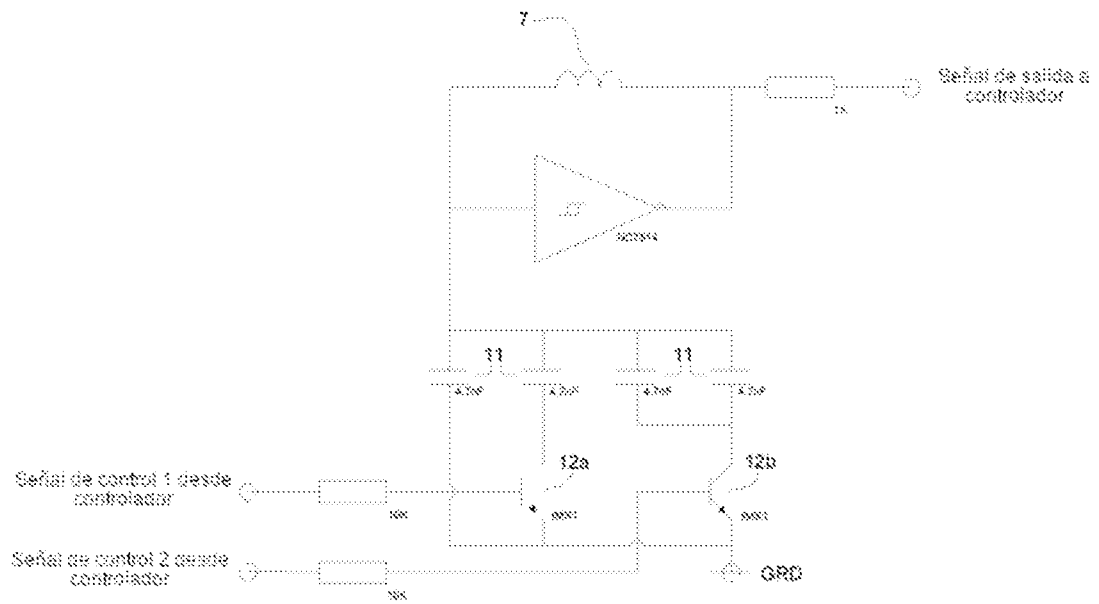


Fig. 2

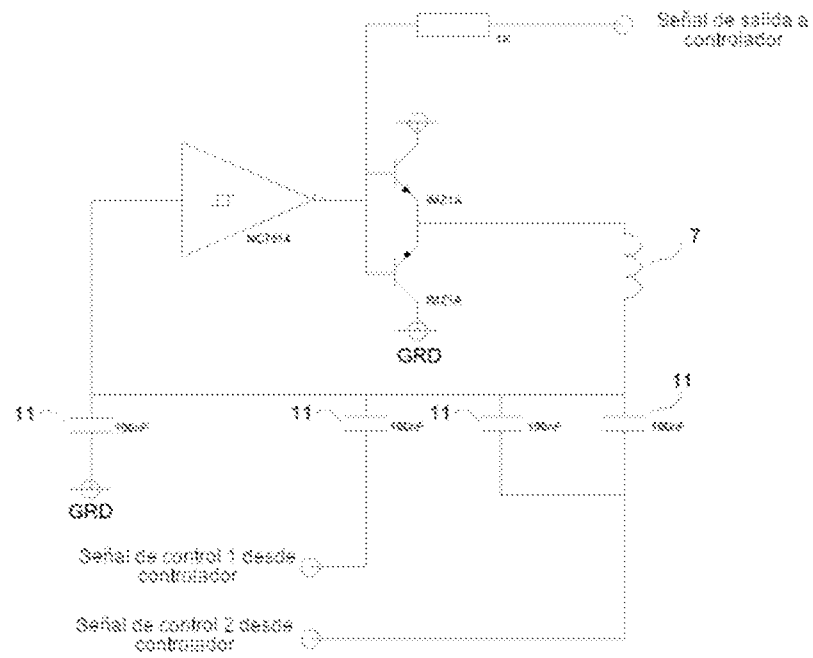


Fig. 3

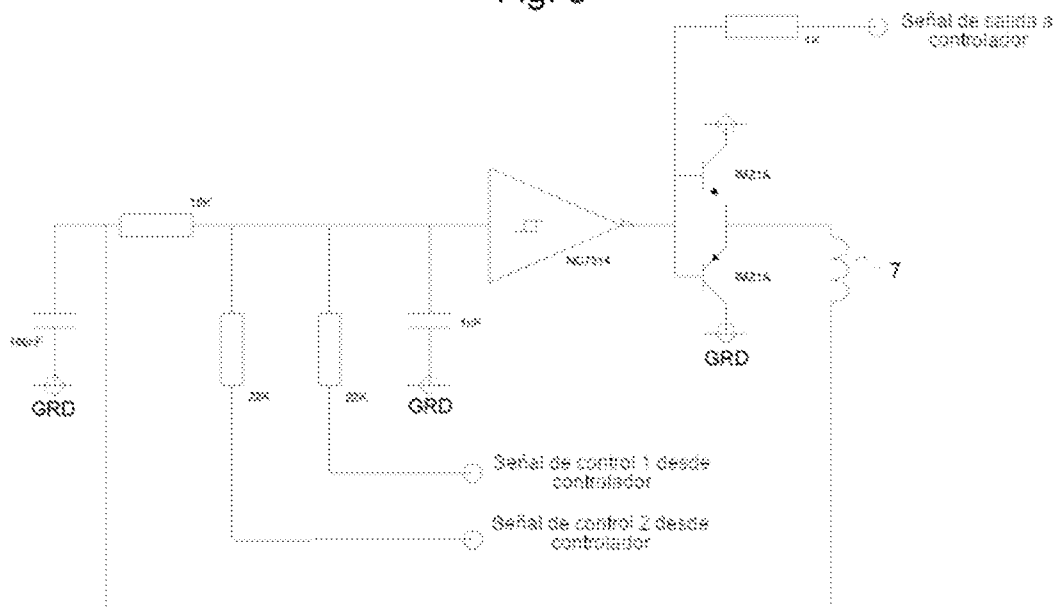


Fig. 4

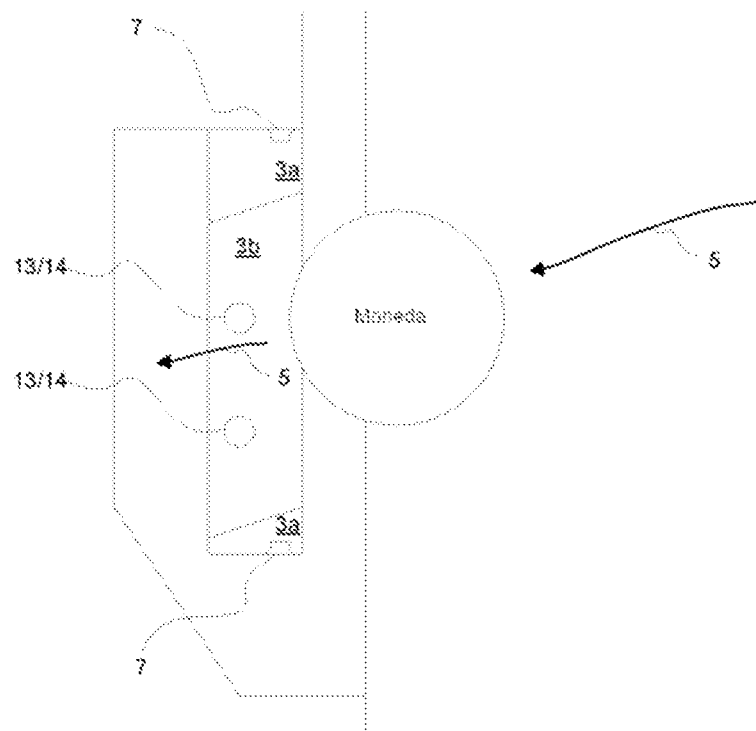


Fig. 5

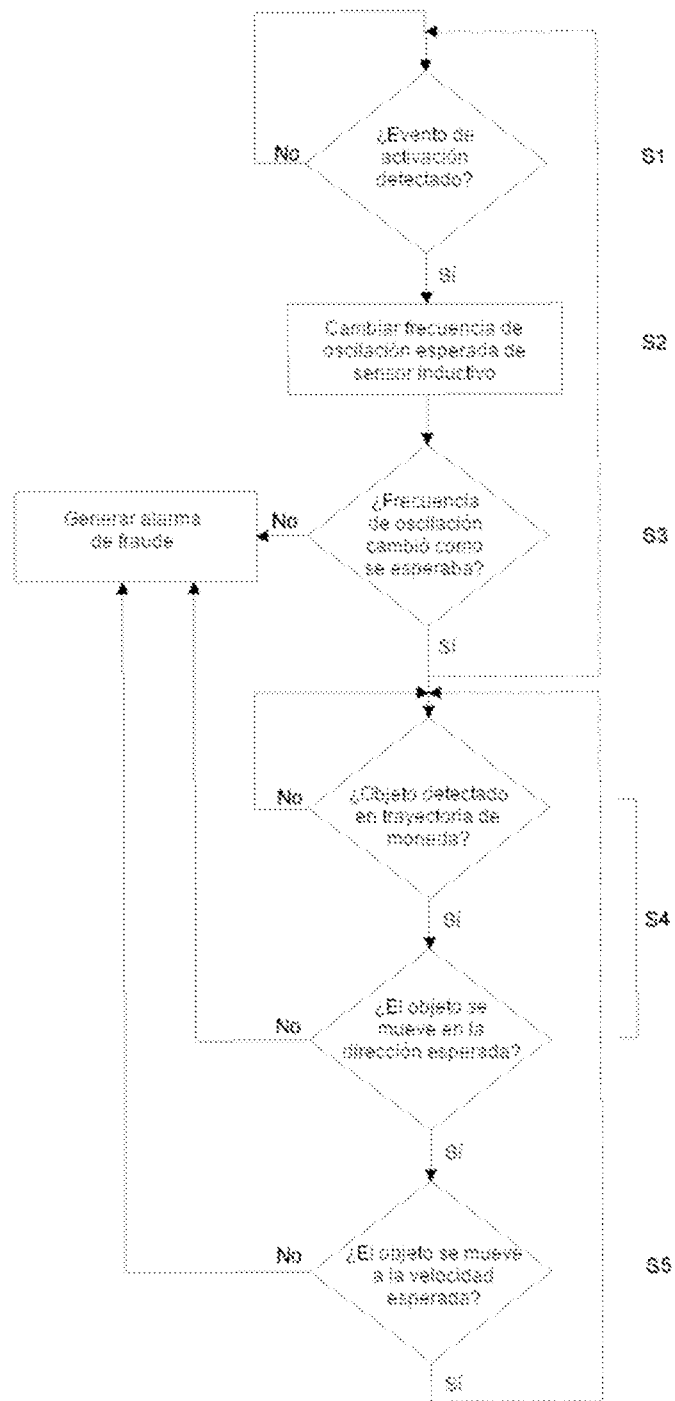


Fig. 6