

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 943 639**

51 Int. Cl.:

H05K 1/02 (2006.01)

G06F 7/58 (2006.01)

G06F 21/86 (2013.01)

G09C 1/00 (2006.01)

H04L 9/08 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **06.03.2018** **PCT/GB2018/050569**

87 Fecha y número de publicación internacional: **27.09.2018** **WO18172731**

96 Fecha de presentación y número de la solicitud europea: **06.03.2018** **E 18711631 (4)**

97 Fecha y número de publicación de la concesión europea: **01.03.2023** **EP 3603352**

54 Título: **Dispositivo electrónico antimanipulación**

30 Prioridad:

20.03.2017 GB 201704392

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

15.06.2023

73 Titular/es:

BLUESKYTEC LTD (100.0%)
One New Street
Wells, Somerset BA5 2LA, GB

72 Inventor/es:

MOBLEY, CHRISTOPHER

74 Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

ES 2 943 639 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

Dispositivo electrónico antimanipulación

5 La presente invención se refiere en general a dispositivos o conjuntos electrónicos antimanipulación, para su uso con placas de circuito integrado, para evitar, disuadir y/o indicar la manipulación no autorizada con respecto a las mismas.

10 Los dispositivos electrónicos antimanipulación son conocidos en la técnica y se utilizan principalmente para proteger información y/o tecnología en circuitos integrados o módulos de múltiples chips en placas de circuito impreso. Tales dispositivos son importantes, no solo para proteger la información ya almacenada en el sistema electrónico, sino también para evitar que un tercero instale malware tal como virus, gusanos o programas similares en el dispositivo. Por ejemplo, es deseable proteger ciertos elementos de dispositivos utilizados en transacciones financieras, tales como dispositivos de punto de venta o cajeros automáticos, en donde la información obtenida de tales dispositivos puede usarse con fines delictivos. También existe un deseo creciente de proteger los dispositivos IoT, tales como los dispositivos inteligentes en hogares y empresas, o las redes que pueden estar conectadas a Internet, para que no se infecten con malware. Hay muchos tipos diferentes de dispositivos electrónicos antimanipulación, que ofrecen diferentes niveles de seguridad. Algunos métodos proporcionan simplemente una alerta o notificación de que el dispositivo ha sido manipulado. Otros se configurarán para destruir/eliminar la información/electrónica protegida en caso de que se detecte una manipulación no autorizada.

20 Un método antimanipulación conocido de este tipo comprende colocar un revestimiento o sello sobre un componente o región particular de una placa de circuito. La patente de EE. UU. n.º 2004/0222014 describe, por ejemplo, un método en donde se proporciona un revestimiento de malla sobre un conjunto de circuito, teniendo el revestimiento de malla una firma única generada por radiactividad (partículas α). Un módulo de detección obtiene una imagen de la firma y se puede concluir la manipulación si se identifica una perturbación en la firma. Los espacios en la malla pueden incluir componentes eléctricos para borrar códigos de circuito para destruir la funcionalidad y el valor de la matriz protegida si se altera el revestimiento de la malla.

30 El documento US2008073491 (D2) describe un sistema de recinto antimanipulación que comprende un medio óptico; al menos un sensor fotosensible configurado para medir al menos una característica de una onda de luz transmitida en el medio óptico; al menos un circuito lógico acoplado a, el al menos, un sensor fotosensible, configurado el al menos un circuito lógico para iniciar medidas de seguridad cuando cambia la al menos una característica de la onda de luz; un recinto acoplado al medio óptico y configurado para encerrar el medio óptico, el al menos un sensor fotosensible y el al menos un circuito lógico; y una pluralidad de postes de fijación configurados para acoplarse a una placa de circuito impreso, en donde al menos uno de la pluralidad de postes de fijación está acoplado también al medio óptico.

40 El documento US2008278217 (D3) describe un sistema que comprende una placa de circuito y un dispositivo de circuito integrado montado en la placa de circuito por medio de un contacto externo, y que comprende un dispositivo antimanipulación que se puede conectar al contacto externo para conmutar el dispositivo de circuito integrado un modo seguro tras la aplicación de un estado eléctrico predeterminado en el contacto externo.

45 El documento US2001033012 (D4) describe un dispositivo de circuito integrado que comprende: un circuito que utiliza cifrado; y una capa de empaquetado de encapsulación; en donde el circuito responde a al menos un parámetro físico del encapsulado para aplicar el cifrado y/o el descifrado mediante la lectura de la clave del mismo, de forma que la manipulación del encapsulado para obtener acceso al circuito hace que el cifrado y/o el descifrado fallen.

50 La técnica anterior adicional incluye (D1) Anónimo, "Alpha Radiation Visualizer | Inventgeek", Internet, (20060625), páginas 1 - 16, URL: <http://www.inventgeek.com/alpha-radiation-visualizer/>, (20180523), XP055477591 - que describe un proyecto que utiliza el CCD integrado en una cámara web USB como medio para interactuar con la radiación alfa.

55 Existe un deseo continuo de un dispositivo electrónico antimanipulación mejorado que evite la ingeniería inversa de cualquier dispositivo electrónico protegido por el mismo, y también proporcione que una protección mejorada contra la manipulación física, al mismo tiempo que minimiza cualquier peso, tamaño, coste, complejidad y/o consumo de energía adicionales que a menudo se añaden a las placas de circuito mediante dispositivos antimanipulación convencionales.

Las realizaciones de la presente invención buscan abordar al menos algunos de estos problemas y, según un primer aspecto de la invención, se proporciona:

60 Un conjunto antimanipulación que comprende:

- una placa de circuito impreso provista de una capa uniforme que rodea uno o más componentes electrónicos, sobre la placa de circuito impreso que se va a proteger; y

– un recipiente que tiene paredes laterales, un primer extremo cerrado y un segundo extremo opuesto abierto, estando el recipiente montado en dicho segundo extremo abierto, sobre la capa uniforme, sobre dicho uno o más componentes electrónicos, para formar una cavidad sellada alrededor de dicho uno o más componentes electrónicos;

5 – una fuente aleatoria cuántica de partículas radiactivas montada, o provista de otro modo, sobre una superficie interna del primer extremo cerrado de dicho recipiente;

10 – un sensor de imagen, montado en la placa de circuito impreso, para capturar fotogramas de imagen dentro de dicha cavidad sellada, durante su uso, en donde dicho sensor de imagen comprende una región detectora que define una matriz de píxeles; y

15 – un procesador, proporcionado en la placa de circuito impreso, para recibir dichos fotogramas de imagen capturados, monitorear dichos fotogramas de imagen para detectar cambios en la distribución estadística de píxeles activos y, en el caso de que la distribución estadística de píxeles activos indique la presencia de una característica en un fotograma de imagen, generar una alerta de manipulación.

El sensor de imagen es sensible a la radiación ionizante y, en respuesta a las partículas radiactivas, se produce la ionización y se genera una carga. Como resultado, los píxeles afectados generarán un valor de datos representativo de una escala de grises o un valor de profundidad de color, lo que indica píxeles 'activos'. Durante el funcionamiento normal, la distribución estadística de píxeles activos en un fotograma de imagen y su intensidad serán estadísticamente aleatorias sin características discernibles. Si se produce una manipulación (por ejemplo, si el recipiente se extrae o se daña), la distribución de píxeles activos se volverá estadísticamente significativa y aparecerán 'características' en las imágenes. El procesador puede, por ejemplo, configurarse para realizar un proceso de extracción de características en las imágenes capturadas por el sensor de imágenes. En una realización ilustrativa, el procesador puede utilizar el análisis rápido de Fourier para transformar cada imagen del dominio espacial al dominio de la frecuencia, en donde una característica aparecería como un 'pico' en la traza resultante. Se puede utilizar un clasificador de aprendizaje para detectar la presencia de un cambio estadísticamente significativo de este tipo y hacer que se genere una alerta de manipulación en consecuencia. Una 'característica' en este contexto puede comprender un punto de píxeles de alta intensidad o una línea o forma de píxeles de alta intensidad, por ejemplo.

30 Ventajosamente, la fuente radioactiva puede ser una fuente de partículas α . La fuente radiactiva puede ser opcionalmente Americio-241.

35 Según una realización ilustrativa, el recipiente puede estar formado de metal, tal como cobre.

En una realización ilustrativa de la presente invención, el sensor de imagen puede ser una cámara que tiene una región fotorreceptora que comprende una pluralidad de píxeles, y puede configurarse para generar y capturar periódicamente imágenes dentro de la cavidad sellada, siendo cada imagen representativa de los píxeles que impactan en las partículas radiactivas de la región fotorreceptora, y comprendiendo una matriz respectiva de valores de escala de grises o de profundidad de color.

Opcionalmente, la región de sensor puede ser una superficie detectora de semiconductor de óxido de metal complementario (CMOS), aunque se puede usar un dispositivo acoplado de carga (CCD) o, de hecho, cualquier otro sensor de imagen adecuado, sensible a la radiación ionizante y no ionizante.

45 En una realización ilustrativa, el conjunto puede comprender además una fuente de alimentación montada dentro del recipiente y acoplada eléctricamente al procesador y al sensor de imagen.

50 El conjunto de recipiente, fuente radiactiva y sensor de imagen tiene otro uso/ventaja exclusivo, ya que puede usarse como parte de un generador de números aleatorios.

Por tanto, en un ejemplo que no forma parte de la invención reivindicada, se proporciona un generador de números aleatorios que comprende un recipiente sellado dentro del que se monta una fuente aleatoria cuántica de partículas radiactivas y un sensor de imagen que comprende una región de sensor en la forma de una matriz de píxeles, comprendiendo además el generador de números aleatorios un procesador para recibir, desde dicho sensor de imagen, fotogramas de imagen capturados desde dentro de dicho recipiente sellado representativos de los píxeles activos, comprendiendo cada conjunto de datos de imagen capturado una matriz de valores de escala de grises o de profundidad de color con respecto a dicha matriz de píxeles, y para combinar, con respecto a cada conjunto de datos de imágenes capturadas, dichos valores respectivos de escala de grises o de profundidad de color para generar un solo número respectivo.

60 Los números, así generados, serán completamente aleatorios porque la distribución estadística de píxeles activos en cada fotograma de imagen y su intensidad (representada por los valores de escala de grises/profundidad de color) serán estadísticamente aleatorios. Estos números aleatorios se pueden alimentar a un módulo criptográfico, en la misma placa de circuito o incluso en otro lugar, para su uso en uno de varios procesadores criptográficos que requieren el uso de números verdaderamente aleatorios.

Estos y otros aspectos de la presente invención resultarán evidentes a partir de la siguiente descripción específica, en que las realizaciones de la presente invención se describen únicamente a modo de ejemplo y con referencia a los dibujos acompañantes, en donde:

la Figura 1 es una vista lateral esquemática de un dispositivo antimanipulación según una realización ilustrativa de la presente invención;

la Figura 2 es una vista esquemática en perspectiva superior del dispositivo antimanipulación de la Figura 1; y

la Figura 3 es un diagrama esquemático de una placa de circuito impreso (PCB) con el dispositivo de la Figura 1.

Haciendo referencia a las Figuras 1 a 3 de los dibujos, un conjunto antimanipulación según una realización ilustrativa de la presente invención comprende una caja o lata 10 que tiene paredes laterales, una pared superior y un extremo inferior abierto. En la realización ilustrativa ilustrada, la caja/lata 10 tiene una sección transversal lateral generalmente cuadrada o rectangular. Sin embargo, la presente invención no pretende necesariamente limitarse a este respecto, y la caja/lata 10 podría, por ejemplo, ser generalmente cilíndrica, con una sección transversal lateral generalmente circular. La caja/lata 10 está configurada para montarse sobre uno o más componentes 13 en una placa de circuito impreso (PCB) 15, para proporcionar funcionalidad antimanipulación a ese/esos componente(s) 13. La PCB 15 está provista de una capa uniforme (ininterrumpida) 21, por ejemplo, de cobre que rodea el uno o más componentes que se van a proteger, y la caja/lata 10 se monta, en el extremo abierto (inferior) sobre la capa 21 para formar una cavidad sellada 11 alrededor del uno o más componentes 13. La capa 21 forma por tanto un límite antimanipulación alrededor del uno o más componentes 13 que se van a proteger, y la caja/lata 10 se suelda sobre la capa límite 21 para formar una cavidad sellada alrededor del uno o más componentes 13. Se apreciará que los términos direccionales tales como 'superior', 'inferior', 'más abajo', 'vertical', 'lateral', etc. se refieren al conjunto descrito cuando está orientado para su uso, es decir, cuando la PCB 15 está horizontal y generalmente paralela al suelo. Sin embargo, se apreciará que, en algunas aplicaciones, la PCB 15 puede no estar necesariamente orientada de esa forma, alterando por tanto la orientación del conjunto antimanipulación asociado.

La caja/lata 10 está ventajosamente formada por un metal duro, tal como cobre, que es muy resistente al daño, deterioro y deformación, además de ser capaz de bloquear partículas radiactivas, particularmente, partículas α y β con una pared relativamente fina. Sin embargo, un experto en la materia apreciará que se podrían utilizar materiales alternativos, y no se pretende que la presente invención esté necesariamente limitada a este respecto.

Se monta una fuente cuántica 12 de radiación, o se proporciona de otro modo en la superficie interior de la pared superior de la caja/lata 10. En una realización preferida, la fuente radiactiva se selecciona para producir una fuente aleatoria constante de partículas α , puesto que las partículas α tienen un alcance corto y se bloquean con relativa facilidad con capas finas de material, incluso papel, de tal forma que las paredes de la caja/lata 10 puede hacerse relativamente muy finas de tal forma que se minimice el peso/coste adicional añadido a la PCB por el conjunto antimanipulación. Una fuente radiactiva adecuada 12 de este tipo podría ser Americio 241, que es conocido para su uso en detectores de humo y similares, se considera relativamente seguro para los seres humanos cuando se manipula adecuadamente y tiene una vida media relativamente larga. Sin embargo, no se pretende que la presente invención esté necesariamente limitada en este aspecto y otras fuentes radiactivas adecuadas serán evidentes para un experto en la materia. De hecho, se podría utilizar una fuente radiactiva que emita partículas β , pero es posible que las paredes de la caja/lata 10 deban hacerse más gruesas (aproximadamente 2 mm de espesor para partículas β hasta una energía de 4 MeV) por razones de seguridad, por lo que se aumenta el peso y el coste del conjunto.

Un sensor 14 de imagen se monta en la PCB 15, dentro de la cavidad 11, y se ubica por lo general debajo de la fuente radiactiva 12 con la región detectora del mismo orientada hacia la fuente radiactiva 12. El sensor 14 puede ser una cámara, tal como una cámara CMOS o una cámara de dispositivo acoplado por carga (CCD) con la lente extraída, aunque se puede usar cualquier detector sensible a la radiación ionizante y la presente invención no pretende necesariamente limitarse a este respecto. El sensor de imagen comprende una matriz de M por N píxeles. Durante su uso, la fuente radiactiva 12 emite partículas radiactivas 16 que llenan y están contenidas dentro de la cavidad 11. Cuando una partícula 16 golpea un píxel del sensor de imagen, provoca un cambio en la energía, lo que genera una carga en el píxel, haciéndolo 'activo'. Esta carga, y su intensidad, normalmente se cuantifica en términos de un valor de escala de grises o de profundidad de color correspondiente, y cada conjunto de píxeles activos se emite en forma de un fotograma de imagen respectivo. Debido a que el movimiento de las partículas 16 dentro de la cavidad sellada 11 se ajusta al movimiento browniano, es un proceso aleatorio donde las partículas individuales 16 experimentan interacciones aleatorias entre sí. Por tanto, cada imagen capturada (es decir, patrón de valores de escala de grises o de color) es completamente aleatoria y nunca se repetirá (estadísticamente) (hasta el nivel de digitalización de la cámara). Por tanto, una cámara VGA produce 640×480 píxeles, con una escala de grises o profundidad de color de 16 bits, lo que brinda más de 20 mil millones de imágenes posibles, mientras que una cámara XGA produce 1024×768 píxeles con una escala de grises o profundidad de color de 24 bits, lo que brinda más de 13 millones de millones imágenes posibles.

Las imágenes se capturan periódicamente dentro de la cavidad sellada 11, y la matriz resultante de valores de escala de grises o de píxeles de color de cada fotograma capturado se pueden usar para generar un número aleatorio usando cualquier combinación adecuada de los valores capturados. Por ejemplo, los valores de píxeles capturados pueden simplemente multiplicarse o sumarse, aunque otros algoritmos adecuados serán evidentes para un experto en la materia. Independientemente de la forma en que los valores representativos de un fotograma de imagen capturado se combinen para generar un valor, se generará una serie de tales números a lo largo del tiempo, y se puede alimentar a un módulo criptográfico separado para su uso en uno de un número de procesos criptográficos que requieren el uso de números aleatorios.

Durante el funcionamiento normal, es decir, cuando no se ha producido manipulación, la distribución estadística de los píxeles activos en cada fotograma de imagen y su intensidad serán estadísticamente aleatorios, sin 'características' discernibles; en otras palabras, las imágenes son representativas de la emisión de la fuente aleatoria cuántica de partículas α (en este caso). Sin embargo, si se produce una manipulación tal que, por ejemplo, se rompa el sello del recipiente o se altere la fuente aleatoria contenida de partículas radiactivas, entonces comenzarán a aparecer características en los fotogramas de imagen que son estadísticamente significativas y, por lo tanto, indican una manipulación. Las 'características' en este contexto pueden ser un punto de píxeles de alta intensidad o una línea o forma de píxeles de alta intensidad, por ejemplo.

Se proporciona un procesador 18 en la PCB 15 para a) recibir las imágenes capturadas en forma de una matriz de valores de color/escala de grises y usar esos valores para generar un número aleatorio representativo; y b) monitorear las imágenes y, si se detectan características, generar una alerta de manipulación. Con este fin, el procesador 18 puede utilizar varios procesos diferentes de detección o extracción de 'características' y serán evidentes para un experto en la materia. Por ejemplo, el procesador 18 puede configurarse para transformar cada imagen del dominio espacial al dominio de frecuencia. Las características de una imagen aparecerán en el dominio de la frecuencia como 'picos'. Por lo tanto, se puede emplear un clasificador de aprendizaje dentro del procesador 18 para identificar 'picos' u otros eventos estadísticamente significativos en la traza de frecuencia y generar una alerta de manipulación si se identifica un evento de este tipo. El procesador 18 puede configurarse también para tener en cuenta cambios a más largo plazo en la distribución estadística y la intensidad a lo largo del tiempo, debido a una caída en la radiactividad debido a la desintegración radiactiva. Sin embargo, el Americio tiene una vida media de 432 años, por lo que no se espera que haya un cambio notable en la intensidad de un año a otro.

Volviendo a las Figuras 2 y 3 de los dibujos, la PCB 15 se ilustra sin la caja/lata 10 de cobre montada sobre la misma. Los dientes 19 que sobresalen hacia abajo en el extremo inferior (abierto) de la caja/lata 10 están alineados con los orificios 20 que se extienden dentro y/o a través de la PCB 15 (ilustrado mejor en la Figura 2). Los dientes 19 encajan en los orificios 20 y se pueden soldar allí, sellando así la caja 10 de cobre en la placa de circuito con los componentes relevantes sellados dentro de la cavidad 11. Haciendo referencia en particular a la Figura 3, se muestra una vista en planta de una PCB 15, incluyendo los orificios 20 para recibir los dientes 19 de la caja 10 de cobre. También se ilustra una pluralidad de otros componentes eléctricos y chips 26 que no deben ser protegidos por el dispositivo antimanipulación. Por lo tanto, la caja 10 de cobre se puede utilizar para proteger parte de una PCB 15 y los componentes eléctricos 13 que requieren protección ubicados en su interior.

Para alimentar el sensor 14 y el procesador 18, se puede proporcionar una batería 22 en la PCB 15 y contenerla dentro de la cavidad 11.

Por tanto, en la realización ilustrativa ilustrada, la batería y los componentes del dispositivo antimanipulación están todos contenidos dentro de la caja o lata 10. Además, el dispositivo puede estar eléctricamente aislado del resto de la PCB (excepto los componentes eléctricos 13). Esto es una ventaja adicional, ya que significa que el dispositivo antimanipulación está contenido de forma segura dentro de la caja 10 y no puede manipularse con el mismo, por ejemplo, no se puede interrumpir la fuente de alimentación ni retirar el procesador.

Este dispositivo protege un sistema electrónico de la manipulación por interferencias físicas, electromagnéticas y radiactivas. El concepto es tener una cavidad 11 físicamente segura que detecte el impacto mecánico, electromagnético y la radiación que incide sobre la cavidad 11 segura. Dentro de esta cavidad se ubicará la electrónica 13 que necesita seguridad. La funcionalidad del conjunto se puede resumir así: a) la cavidad 11 se forma soldando una caja/lata 10 de cobre a una PCB 15 con capas de cobre ininterrumpidas; b) la cavidad 11 se llena con partículas radiactivas 16 de una fuente radiactiva que produce preferiblemente predominantemente partículas α , tal como Americio-241 y una cámara captura imágenes dentro de la cavidad sellada 11; c) un procesador 18 lee los fotogramas de imagen, que comprenden una matriz de valores de escala de grises o de profundidad de color, y los procesa para eventos estadísticamente significativos; d) el procesador, ubicado dentro de la cavidad, generará una señal de alerta si se detecta una manipulación no autorizada. El procesador puede configurarse para borrar o destruir su contenido si se detecta una manipulación no autorizada.

Los eventos estadísticamente significativos dentro de las imágenes (es decir, 'características') pueden ocurrir por varias razones. Si, por ejemplo, se rompe la caja/lata 10 donde no hay fotones para inundar el fotosensor, entonces se seguirá detectando la manipulación, ya que la cámara 14 se desplazará en posición relativa a la fuente radiactiva. Esto altera las estadísticas de imagen y el procesador lo detecta como una manipulación no autorizada y, por lo tanto,

generará la señal de alerta. Las emisiones de partículas de alta energía, tales como las que pueden emitir los microscopios electrónicos de barrido, u otras radiaciones (por ejemplo, rayos X) harán que la sensibilidad de la superficie del detector CMOS se altere y se aleje de la norma estadística de la cavidad sellada 11. Las partículas de alta energía causarán "puntos calientes" en la superficie del detector CMOS (es decir, altos valores de escala de grises o de profundidad de color constantes que no varían entre las imágenes) y, por tanto, alterarán las estadísticas de imagen. Cada uno de estos casos hace que el procesador detecte un cambio repentino y genere una señal de alerta.

Los expertos en la materia entenderán que se pueden realizar modificaciones y variaciones de la realización ilustrativa descrita en el presente documento sin apartarse del alcance de protección como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un conjunto antimanipulación que comprende:
 - 5 - una placa (15) de circuito impreso provista de una capa uniforme (21) que envuelve uno o más componentes electrónicos (13), sobre la placa (15) de circuito impreso que se va a proteger; y
 - un recipiente (10) que tiene paredes laterales, un primer extremo cerrado y un segundo extremo opuesto abierto, estando el recipiente (10) montado en dicho segundo extremo abierto, sobre la capa uniforme (21),
10 sobre dicho uno o más componentes electrónicos (13), para formar una cavidad sellada (11) alrededor de dicho uno o más componentes electrónicos (13);
 - una fuente aleatoria cuántica (12) de partículas radiactivas (16) montada, o provista de otro modo, sobre una
15 superficie interna del primer extremo cerrado de dicho recipiente (10);
 - un sensor (14) de imagen, montado en la placa (15) de circuito impreso, para capturar fotogramas de imagen dentro de dicha cavidad sellada (11), durante su uso, en donde dicho sensor (14) de imagen comprende una región detectora que define una matriz de píxeles; y
 - 20 - un procesador (18), proporcionado en la placa (15) de circuito impreso, para recibir dichos fotogramas de imagen capturados, monitorear dichos fotogramas de imagen para detectar cambios en la distribución estadística de píxeles activos y, en el caso de que la distribución estadística de píxeles activos indique la presencia de una característica en un fotograma de imagen, generar una alerta de manipulación.
- 25 2. Un conjunto antimanipulación según la reivindicación 1, en donde cada fotograma de imagen está representado por una matriz espacial de valores de escala de grises o de profundidad de color asociados con los respectivos píxeles activos.
3. Un conjunto antimanipulación según la reivindicación 2, en donde dicho procesador (18) está configurado
30 para, con respecto a cada uno de una pluralidad de fotogramas de imagen, generar un número aleatorio respectivo combinando dichos valores de escala de grises o de profundidad de color.
4. Un conjunto antimanipulación según cualquiera de las reivindicaciones anteriores, en donde dicha fuente radiactiva (12) genera partículas α .
- 35 5. Un conjunto antimanipulación según cualquiera de las reivindicaciones anteriores, en donde dicha fuente radiactiva (12) es Americio-241.
6. Un conjunto antimanipulación según cualquiera de las reivindicaciones anteriores, en donde dicho recipiente
40 (10) está formado por un metal, tal como cobre.
7. Un conjunto antimanipulación según cualquiera de las reivindicaciones anteriores, en donde dicho procesador (18) está configurado para realizar un proceso de extracción de características en dichos fotogramas de imagen y, en caso de que se detecte una característica en un fotograma de imagen, generar una alerta de
45 manipulación.
8. Un conjunto antimanipulación según la reivindicación 7, en donde dicho procesador (18) está configurado para transformar cada fotograma de imagen de un dominio espacial a un dominio de frecuencia y usar dicho dominio de frecuencia para realizar dicha técnica de extracción de características.
- 50 9. Un conjunto antimanipulación según la reivindicación 8, en donde dicho procesador (18) incluye un clasificador de aprendizaje configurado para identificar eventos estadísticamente significativos en dicho dominio de frecuencia y, en caso de que se identifique un evento estadísticamente significativo, generar una alerta de manipulación.
- 55 10. Un conjunto antimanipulación según cualquiera de las reivindicaciones anteriores, en donde dicha región detectora de dicho sensor (14) de imagen es una superficie detectora de semiconductor de óxido de metal complementario (CMOS) o un dispositivo acoplado de carga (CCD).
- 60 11. Un conjunto antimanipulación según cualquiera de las reivindicaciones anteriores, en donde el conjunto comprende además una fuente de alimentación montada dentro de dicho recipiente (10).

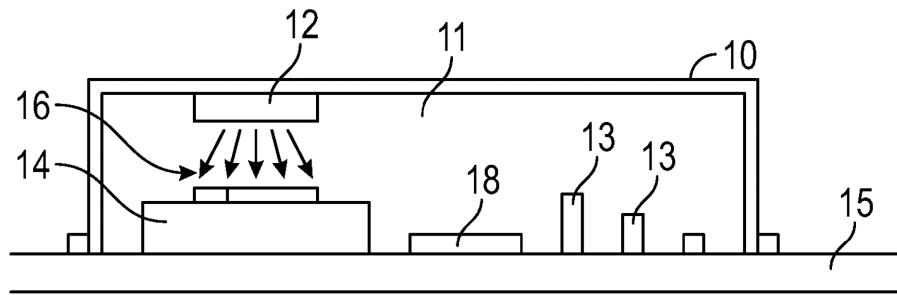


Figura 1

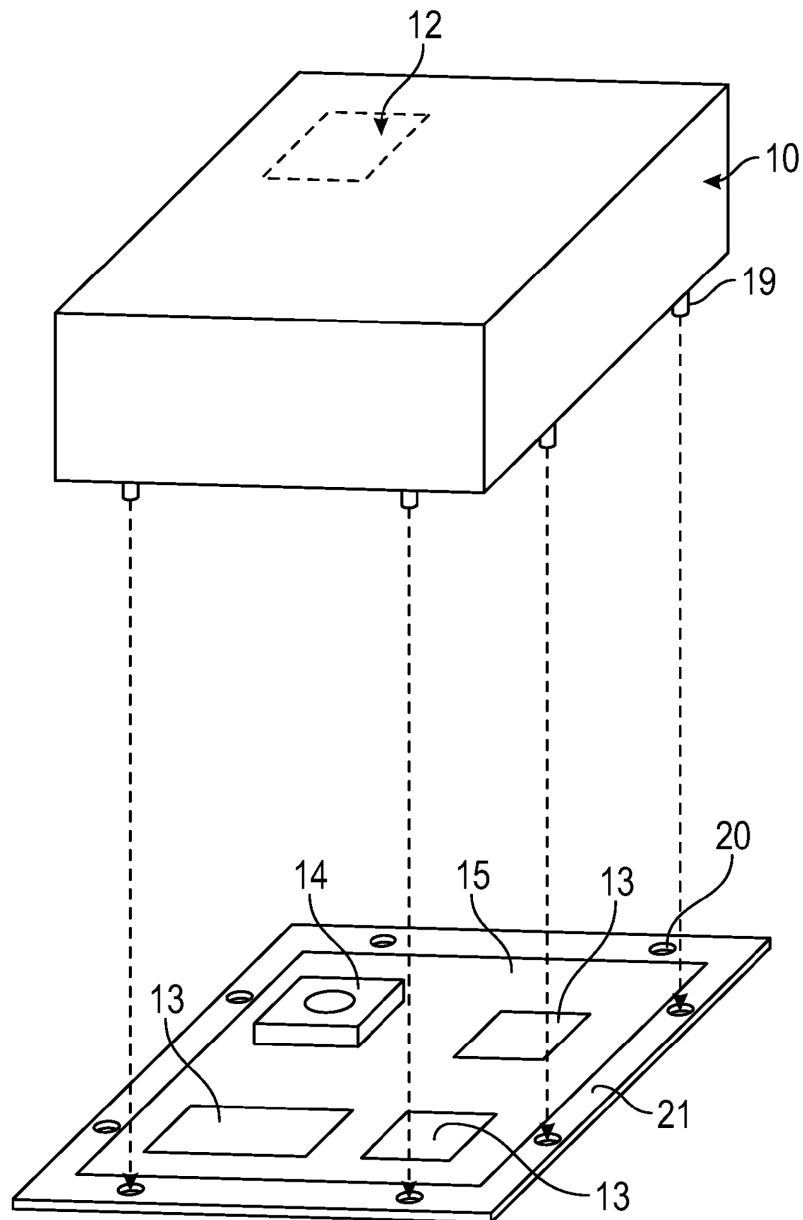


Figura 2

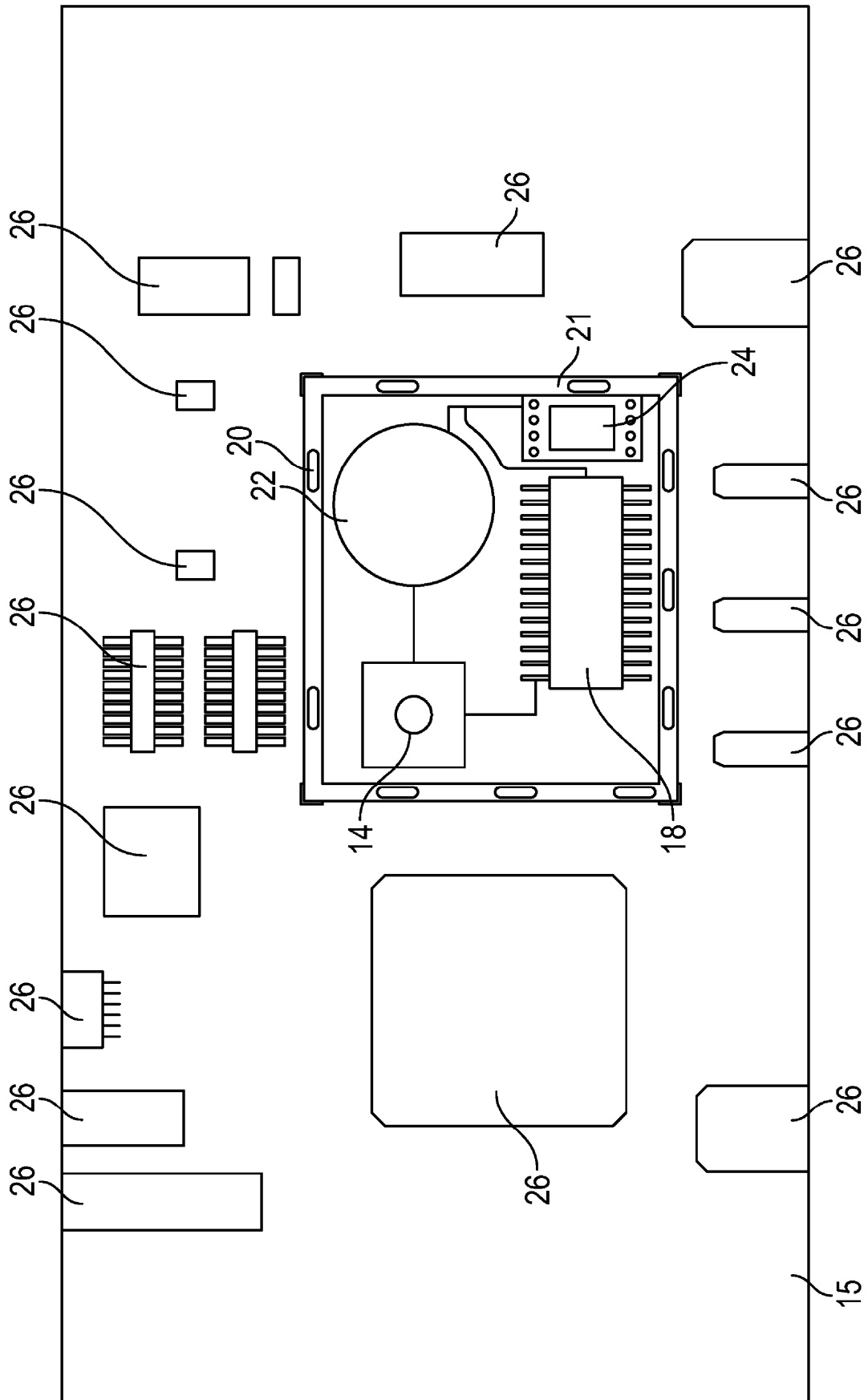


Figura 3