(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 399 419**

(51) Int. CI.:

G07G 3/00 (2006.01)
G07F 19/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.03.2000 E 00302587 (1)**

(97) Fecha y número de publicación de la concesión europea: **02.01.2013 EP 1043704**

(54) Título: **Terminal de autoservicio**

(30) Prioridad:

06.04.1999 GB 9907639

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.04.2013

(73) Titular/es:

NCR INTERNATIONAL, INC. (100.0%)
3097 SATELLITE BLVD.
DULUTH, GA 30096, US

(72) Inventor/es:

MAIR, JOHN;
SHARP, GORDON DOIG y
RUSSELL, DOUGLAS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Terminal de autoservicio

La presente invención se refiere principalmente a terminales de autoservicio (SST), tales como cajeros automáticos (ATM); y, en particular, a un SST que incorpora una disposición de prevención de fraude. Otros aspectos de la invención se refieren a la prevención y detección de interferencia o manipulación no autorizadas con dispositivos de captura de datos.

Los SST, tales como los cajeros automáticos (ATM), se usan de manera generalizada y cada vez más para llevar a cabo muchas transacciones diarias que no requieren supervisión humana. En el caso de ATM, una de las transacciones ejecutadas más frecuentemente es la retirada de efectivo de una cuenta bancaria, aunque otras transacciones pueden implicar una transferencia electrónica de fondos entre cuentas, pagos de facturas, o simplemente obtener una indicación de un saldo de cuenta o un “miniextracto” que proporciona detalles de transacciones recientes.

Para usar un ATM convencional, en primer lugar se requiere que un usuario inserte una tarjeta de banda magnética en una ranura de lector de tarjetas en el frontal del ATM, sirviendo la tarjeta como testigo de identificación; al presentar la tarjeta el usuario está alegando una identidad particular. El usuario debe confirmar entonces su identidad, por ejemplo, introduciendo un número de identificación personal (PIN) asociado con la tarjeta, pero que sólo el usuario conoce. El PIN se introduce en un teclado numérico incorporado en el ATM.

Pueden usarse asimismo medios de confirmación de identidad alternativos o adicionales; por ejemplo, un usuario puede colocar su palma o dedo en un escáner electrónico, permitiendo una comparación entre la palma o huella dactilar y una muestra almacenada de la huella del usuario. De manera similar, pueden emplearse una cámara o escáner asociados con un procesador apropiado para comparar el patrón de iris del usuario u otro identificador biométrico con una plantilla almacenada.

Por tanto, si un usuario no autorizado desea acceder a una cuenta de un individuo y, por tanto, realizar retiradas no autorizadas de fondos, es necesario obtener tanto la tarjeta del individuo, como llegar a conocer el PIN apropiado u otros medios usados para confirmar la identidad del usuario.

Aunque la obtención de una tarjeta de un usuario sin su conocimiento puede ser relativamente fácil para un carterista, se han usado varias técnicas elaboradas con el fin de llegar a conocer el PIN de un individuo. Una de estas técnicas implica colocar un teclado numérico falso superpuesto encima del teclado numérico de ATM, teclado numérico falso que está conectado a una grabadora. Cuando un usuario introduce su PIN, el teclado numérico falso transmite la presión de las pulsaciones de las teclas al teclado numérico de ATM inferior, de modo que el usuario no percibe nada sospechoso, e introduce su PIN en el teclado numérico falso. En otras disposiciones menos sofisticadas, puede emplearse un teclado numérico falso que no puede transferir presión al teclado numérico de ATM, de manera que el usuario no podrá usar el ATM; los usuarios “introducirán” su PIN en el teclado numérico falso, pero el ATM no responderá y rechazará finalmente la tarjeta del usuario. Sin embargo, es más probable que se detecte esta forma de teclado numérico falso ya que los usuarios pueden sospechar y examinar el ATM más detenidamente e identificar el teclado numérico falso, o pueden notificar el “fallo” inmediatamente al operario de ATM.

Una vez que se ha introducido el PIN del usuario en el teclado numérico falso y el usuario ha abandonado el ATM, el teclado numérico puede extraerse del ATM y recuperarse el PIN. El usuario no autorizado puede sustraer entonces la tarjeta del usuario, y combinar ésta con el PIN para llevar a cabo transacciones no autorizadas. Puede usarse una técnica algo similar con sensores biométricos tales como lectores de huellas dactilares o palmares: se superpone un escáner falso en el escáner verdadero, y pueden registrarse las características de la huella dactilar o huella palmar del usuario. Luego, pueden reproducirse las características registradas y usarse la reproducción para “engañar” al escáner haciéndolo creer que el usuario autorizado está presente.

Entre los objetos de las realizaciones de la presente invención está proporcionar un SST que reduce los riesgos de que se produzcan tales fraudes. Adicionalmente entre los objetos de las realizaciones de la presente invención está proporcionar un SST que alerte al operario de SST con respecto a una interferencia no autorizada con un SST.

El documento DE 196 05 102 A I da a conocer un terminal de autoservicio y un método de funcionamiento del mismo tal como se detalla en el preámbulo de las reivindicaciones independientes en el presente documento.

Según un primer aspecto de la presente invención, se proporciona un terminal de autoservicio (SST) que comprende: un dispositivo de captura de datos; un emisor; un detector; y medios para producir una señal de alarma si el detector no recibe emisiones del emisor, en el que el dispositivo de captura de datos, el emisor y el detector están dispuestos de manera que un objeto en las proximidades del dispositivo de captura de datos obstruirá el

trayecto de emisiones del emisor al detector; y caracterizado porque los medios producen una señal de alarma sólo si el detector no recibe emisiones del emisor durante un intervalo predeterminado.

En otros aspectos de la presente invención, puede proporcionarse un sistema para la incorporación en un SST existente.

El dispositivo de captura de datos puede ser un teclado numérico, un escáner de huellas dactilares, un escáner de iris o similar. En un SST de este tipo si, por ejemplo, se coloca un teclado numérico falso encima del teclado numérico de SST, el teclado numérico falso interrumpirá el trayecto de emisiones entre el emisor y el detector, y se detectará la presencia del teclado numérico falso.

Preferiblemente, el emisor y el detector utilizan radiación electromagnética; y lo más preferiblemente radiación infrarroja. La radiación infrarroja es invisible para los humanos, y la presencia de un sistema de monitorización de este tipo no resultaría evidente para los usuarios. Pueden usarse asimismo sistemas emisores-detectores adicionales o alternativos empleando, por ejemplo, ondas de radio, microondas, radiación ultravioleta o sistemas de radiación no electromagnética tales como ultrasonido. Puede resultar conveniente combinar dos o más sistemas diferentes en un único SST, de manera que si un malhechor estuviera al tanto de un sistema, y adoptara medidas para asegurarse de que, por ejemplo, la radiación infrarroja no se bloquea por un teclado numérico falso, la radiación ultravioleta todavía podría bloquearse, y, por tanto, el teclado numérico falso se detectaría de todas formas.

Preferiblemente, al menos una parte del dispositivo de captura de datos es transparente a las emisiones del emisor. Esto permite, por ejemplo, ocultar el emisor debajo de un teclado numérico, con el detector encima; o viceversa. Alternativamente, el dispositivo de captura de datos puede estar en un rebaje en el frontal del SST, y el emisor y el detector montarse en lados opuestos del rebaje encima del dispositivo de captura de datos.

Convenientemente, la parte transparente del dispositivo de captura de datos comprende al menos una ventana en una superficie del dispositivo de captura de datos, y lo más preferiblemente, una pluralidad de ventanas. Estas ventanas pueden estar en las teclas de un teclado numérico, o el área de palma de un escáner de palma y garantizar que un elemento falso superpuesto obscurezca al menos una ventana si el elemento falso superpuesto va a capturar los datos necesarios.

Convenientemente, el emisor está montado directamente bajo el dispositivo de captura de datos, y el detector está montado encima del dispositivo de captura de datos. Alternativamente, puede usarse la disposición inversa.

Preferiblemente, el emisor emite una serie codificada de impulsos u otra forma de señal codificada o encriptada; el uso de una señal codificada hará más difícil imitar la señal emitida. El código utilizado puede variarse con el tiempo, o puede determinarse por la naturaleza de la transacción anterior, o alguna otra condición. Esta complejidad añadida reducirá la probabilidad de que un individuo no autorizado determine la naturaleza del código y use ese conocimiento para eludir el sistema de detección.

Preferiblemente, los medios para producir una señal de alarma sólo producen una señal de alarma si el detector no recibe emisiones del emisor durante un intervalo predeterminado; en el transcurso normal de uso del SST, habrá obstrucciones en el trayecto del emisor al detector cuando, por ejemplo, una mano del usuario acciona el dispositivo de captura de datos. El intervalo puede seleccionarse para adaptarse a interrupciones de la detección de emisiones tal como se esperaría que sucediera durante el uso normal del SST. Sin embargo, interrupciones continuas más largas, tal como se producirían si se realizara un intento de cubrir el dispositivo de captura de datos con un dispositivo falso, darán como resultado la producción de una señal de alarma.

Los medios para producir una señal de alarma pueden adoptar cualquier forma apropiada, por ejemplo, un comparador para comparar señales emitidas por el emisor con señales recibidas por el detector, o una conmutación sencilla que se activa cuando no se introduce ninguna señal en el detector.

Preferiblemente, se proporciona el SST junto con una alarma, estando la alarma lo más preferiblemente alejada del SST, con lo cual al detectar una obstrucción cerca del dispositivo de captura de datos puede alertarse a una persona autorizada. El SST puede apagarse cuando se produce una señal de alarma, para impedir el uso del terminal mientras existe un riesgo de actividad fraudulenta. Alternativamente, o además, el SST puede programarse o disponerse de otro modo para iniciar otra acción, por ejemplo puede activarse una cámara en el SST para grabar la escena y ayudar a identificar a la persona que ha colocado el elemento falso superpuesto sobre el dispositivo de captura de datos, o la cámara puede permitir a una persona autorizada ver el frontal del terminal desde una ubicación alejada y determinar si se requiere una acción inmediata. Por ejemplo, el operario puede determinar que la señal de alarma se ha generado debido a una situación que no es una amenaza para la seguridad, por ejemplo, la cartera de un usuario, un envoltorio de alimentos u otro artículo que se haya dejado sobre un teclado numérico de ATM.

Según un aspecto adicional de la presente invención, se proporciona un método para detectar un intento de fraude en un terminal de autoservicio (SST), comprendiendo el método las etapas de: proporcionar un emisor y un detector dispuestos con respecto a un dispositivo de captura de datos de un SST; monitorizar la recepción de emisiones del emisor por el receptor para permitir la detección de objetos colocados en las proximidades del dispositivo de captura de datos y obstruir el trayecto de emisiones del emisor al detector y caracterizado porque los medios para producir una señal de alarma sólo producen una señal de alarma si el detector no recibe emisiones del emisor durante un intervalo predeterminado.

En este aspecto de la invención, el dispositivo de captura puede ser un dispositivo de captura de datos o un dispositivo de captura de testigos para capturar un testigo de identificación, tal como una tarjeta de banda magnética o una tarjeta inteligente.

Ahora se describirán éstos y otros aspectos de la presente invención, sólo a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

la figura 1 muestra una vista en perspectiva del frontal de un cajero automático (ATM) convencional;

la figura 2 muestra una sección transversal esquemática de un frontal de un ATM que incluye una disposición de detección de fraude según una primera realización de la presente invención; y

la figura 3 muestra una sección transversal esquemática de un frontal de un ATM que incluye una disposición de detección de fraude según una segunda realización de la presente invención.

En referencia en primer lugar a la figura 1, se muestra el frontal de un cajero automático (ATM) convencional. El ATM 10 comprende varios elementos para la interacción con un usuario, que incluyen una ranura 12 de lector de tarjeta magnética, en la que el usuario inserta una tarjeta 14 de identificación; un dispositivo de recopilación de datos en forma de un teclado 16 numérico, en el que el usuario puede introducir su PIN u otros datos; una pantalla 18, en la que el ATM muestra mensajes para el usuario; y una ranura 20 de dispensación de efectivo, de la cual el usuario puede recoger billetes de banco u otros medios de valor.

Si va a cometerse un intento de fraude tal como se describió anteriormente, se coloca un teclado 21 numérico falso (figura 2) sobre el teclado 16 numérico, y se conecta a un dispositivo de monitorización (no mostrado). Cuando un usuario inserta su tarjeta 14 en la ranura 12, el ATM 10 muestra un mensaje en la pantalla 18, pidiendo que el usuario introduzca su PIN en el teclado 16 numérico. El usuario introduce entonces su PIN, a través del teclado 21 numérico falso; el teclado 21 numérico registra el PIN. Después de que se ha completado la transacción, un individuo no autorizado puede descargar el PIN del teclado 21 numérico falso. Si un cómplice roba satisfactoriamente la billetera del usuario y adquiere posesión de su tarjeta 14, el PIN puede usarse entonces para retirar fondos de la cuenta bancaria del usuario.

La figura 2 muestra una sección transversal esquemática de un frontal de un ATM 30, que incluye una disposición según una realización de la presente invención mediante la cual pueden detectarse tales intentos de fraude. Ubicado bajo el teclado 16 numérico hay un emisor 34 de infrarrojos, conectado a una fuente 36 de alimentación y a un codificador 38. Ubicado verticalmente por encima del emisor 34 en el frontal de ATM hay un detector 40 de infrarrojos, conectado a la fuente 36 de alimentación y a un decodificador 42. Tanto el codificador 38 como el decodificador 42 están enlazados a un comparador 44. En este ejemplo, el emisor 34 está situado bajo el teclado 16 numérico, que cuenta con partes transparentes a infrarrojos, de manera que el emisor 34 esté oculto. El detector 40 está oculto detrás de una pantalla 46 de monitor transparente a infrarrojos.

El emisor 34 emite señales codificadas a intervalos temporizados, señales que pasan a través del teclado 16 numérico al detector 40. Las señales detectadas se pasan al decodificador 42 que se comunica con el comparador 44 para confirmar que las señales detectadas corresponden a las emitidas por el emisor 34.

Si se coloca un teclado 21 numérico falso sobre el teclado 16 numérico de ATM, se interrumpen las señales del emisor 34 y no alcanzan el detector 40. Esta condición hace que el comparador 44 emita una señal de alarma para activar un circuito 48 de alarma y, por tanto, alertar al operario de ATM, y desactivar el ATM.

Para adaptarse al uso normal del ATM 30, el comparador 44 incorpora un retardo de tiempo que impide la emisión de una señal de alarma hasta que el detector 40 no haya recibido señales del emisor 34 durante un intervalo predeterminado. El intervalo se selecciona de manera que el uso del teclado 16 numérico por un usuario, que dará como resultado la interrupción de las señales que alcanzan al detector 40, no dará como resultado la emisión de señales de alarma espurias.

Resultará evidente para los expertos en la técnica que la realización de la invención tal como se describió anteriormente sirve para impedir intentos de fraude utilizando teclados falsos para obtener PIN de los usuarios.

La figura 3 muestra una sección transversal esquemática de un frontal de un ATM 100, que incluye una disposición según una segunda realización de la presente invención mediante la cual puede detectarse un intento de fraude superponiendo un lector de tarjetas. Ubicado detrás de la ranura 12 de lector de tarjeta hay un detector 102 de infrarrojos, conectado a una fuente 104 de alimentación y a un codificador 106. Ubicado verticalmente encima del detector 102 en el frontal de ATM hay un emisor 108 de infrarrojos, conectado a una fuente 104 de alimentación y a un decodificador 110. Tanto el codificador 106 como el decodificador 110 están enlazados a un comparador 112. En este ejemplo el detector 102 está situado en el borde superior de la ranura 12 detrás de una parte 114 de frontal que es transparente a la radiación infrarroja, pero no es transparente a la luz visible, de manera que el detector 102 esté oculto de la vista de un usuario mediante la parte 114. El emisor 108 está oculto detrás de una pantalla 116 de monitor transparente a infrarrojos y emite radiación infrarroja en un ángulo amplio.

El emisor 108 emite señales codificadas a intervalos temporizados, señales que pasan a través de una parte 114 al detector 102. Las señales detectadas se pasan al decodificador 106 que se comunica con el comparador 112 para confirmar que las señales detectadas corresponden a las emitidas por el emisor 108.

Si se coloca una lámina 118 falsa (mostrada en la figura 3 mediante una línea discontinua) que tiene una ranura de lector de tarjetas falsa sobre la parte inferior del ATM, se interrumpen las señales del emisor 108 y no alcanzan el detector 102. Esta condición hace que el comparador 112 emita una señal de alarma para activar un circuito 120 de alarma y, por tanto, alertar al operario de ATM, y desactivar el ATM.

Para adaptarse al uso normal del ATM 100, el comparador 112 incorpora un retardo de tiempo que impide la emisión de una señal de alarma hasta que el detector 108 no haya recibido señales del emisor 102 durante un intervalo de tiempo predeterminado. El intervalo se selecciona de manera que el uso de la ranura 12 de lector de tarjetas por un usuario, que dará como resultado la interrupción de las señales que alcanzan el detector 108, no dará como resultado la emisión de señales de alarma espurias.

Resultará evidente que pueden realizarse diversas modificaciones y mejoras a las disposiciones descritas anteriormente sin apartarse del alcance de la invención. Por ejemplo, puede usarse cualquier forma adecuada de señal para detectar la presencia de un teclado no autorizado o similar, además de o como alternativa a emisiones infrarrojas. Además, puede variarse la ubicación relativa del emisor y del detector; o puede pasarse una señal a través de la superficie de un teclado numérico, en lugar de a través del teclado numérico. En otras realizaciones, el detector puede estar configurado para detectar reflexiones de señales emitidas desde el emisor, de modo que un objeto colocado en las proximidades del dispositivo de captura de datos refleje una señal emitida desde el emisor al detector. En una realización de este tipo, puede activarse una alarma si se detecta una señal reflejada durante más de un periodo de tiempo predeterminado. Otras realizaciones de la invención pueden tener un único emisor y múltiples detectores, de modo que los detectores pueden estar ubicados en el teclado numérico, ranura de lector de tarjetas, ranura de dispensador de efectivo y tales ubicaciones similares.

Pueden proporcionarse otras realizaciones de la invención para su uso junto con dispositivos de captura de datos distintos de los proporcionados en combinación con SST, por ejemplo, combinación de teclados numéricos de entrada o escáneres de huella palmar que se utilizan para abrir cerraduras para acceder a áreas seguras.

REIVINDICACIONES

1. Terminal de autoservicio (SST) que comprende: un dispositivo (16) de captura de datos; un emisor (34); un detector (40); y medios (44, 48) para producir una señal de alarma si el detector (40) no recibe emisiones del emisor (34), en el que el dispositivo (16) de captura de datos, el emisor (34) y el detector (40) están dispuestos de manera que un objeto (21) en las proximidades del dispositivo (16) de captura de datos obstruirá el trayecto de emisiones del emisor (34) al detector (40); y

caracterizado porque los medios (44, 48) producen una señal de alarma sólo si el detector (40) no recibe emisiones del emisor (34) durante un intervalo predeterminado.

2. SST según la reivindicación 1, en el que el dispositivo de captura de datos es un teclado (16) numérico.

3. SST según la reivindicación 1 ó 2, en el que el emisor (34) y el detector (40) funcionan usando radiación electromagnética.

4. SST según la reivindicación 3, en el que el emisor (34) y el detector (40) funcionan usando radiación infrarroja.

5. SST según cualquiera de las reivindicaciones anteriores, en el que al menos una parte del dispositivo (16) de captura de datos es transparente a emisiones del emisor (34).

6. SST según cualquiera de las reivindicaciones anteriores, en el que el emisor (34) emite una señal codificada.

7. SST según cualquiera de las reivindicaciones anteriores, que comprende además una alarma (48).

8. Método para detectar un intento de fraude en un terminal de autoservicio (SST), comprendiendo el método las etapas de: proporcionar un emisor (34) y un detector (40) dispuestos con respecto a un dispositivo (16) de captura de datos de un SST (30); monitorizar la recepción de emisiones del emisor (34) por el receptor (40) para permitir la detección de objetos (21) colocados en las proximidades del dispositivo (16) de captura de datos y obstruir el trayecto de emisiones del emisor (34) al detector (40) y caracterizado porque los medios (44, 48) para producir una señal de alarma sólo producen una señal de alarma si el detector (40) no recibe emisiones del emisor (34) durante un intervalo predeterminado.

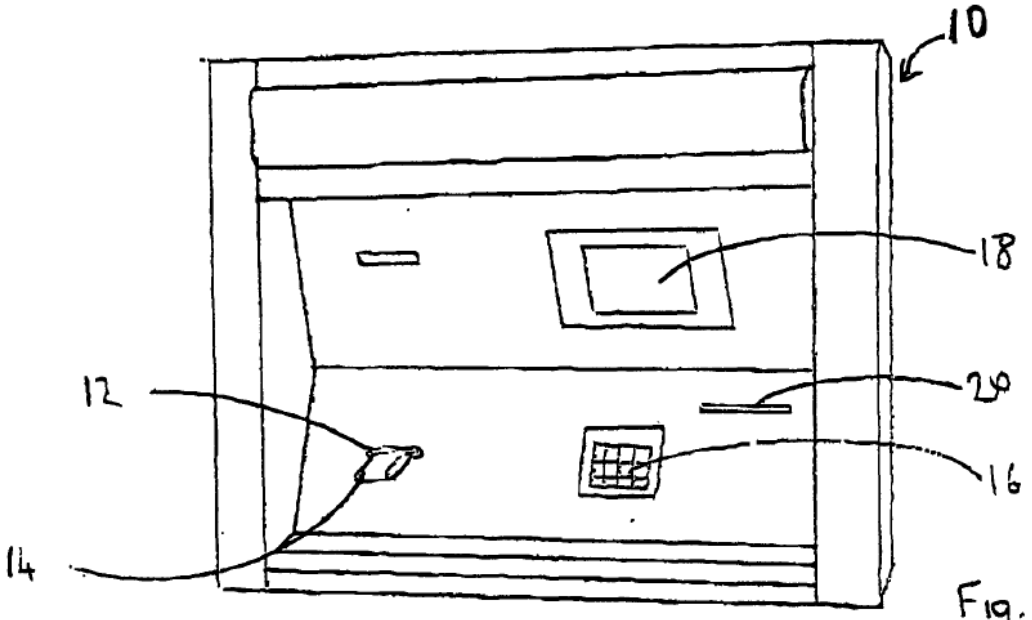

Fig. 1

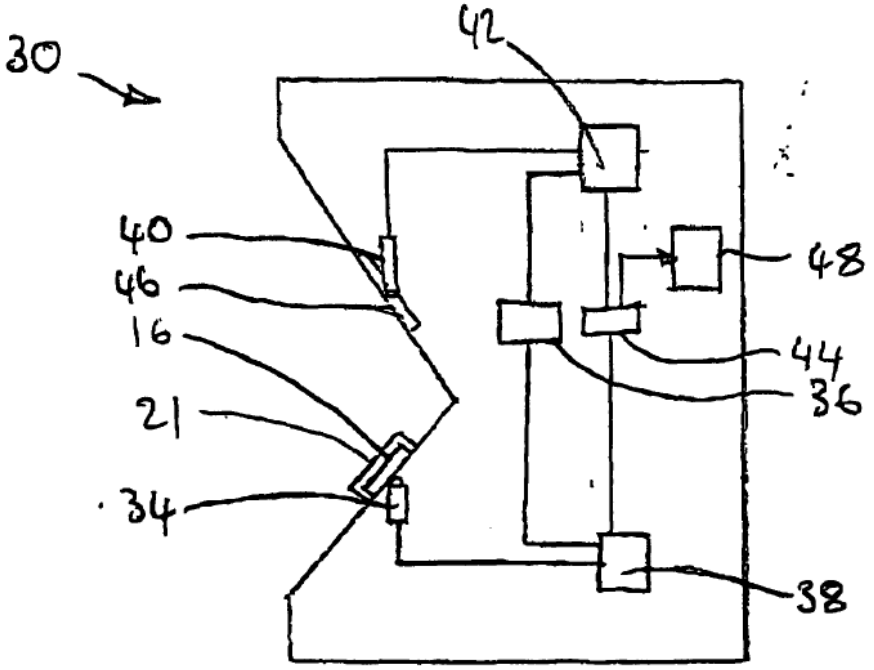

Fig. 2

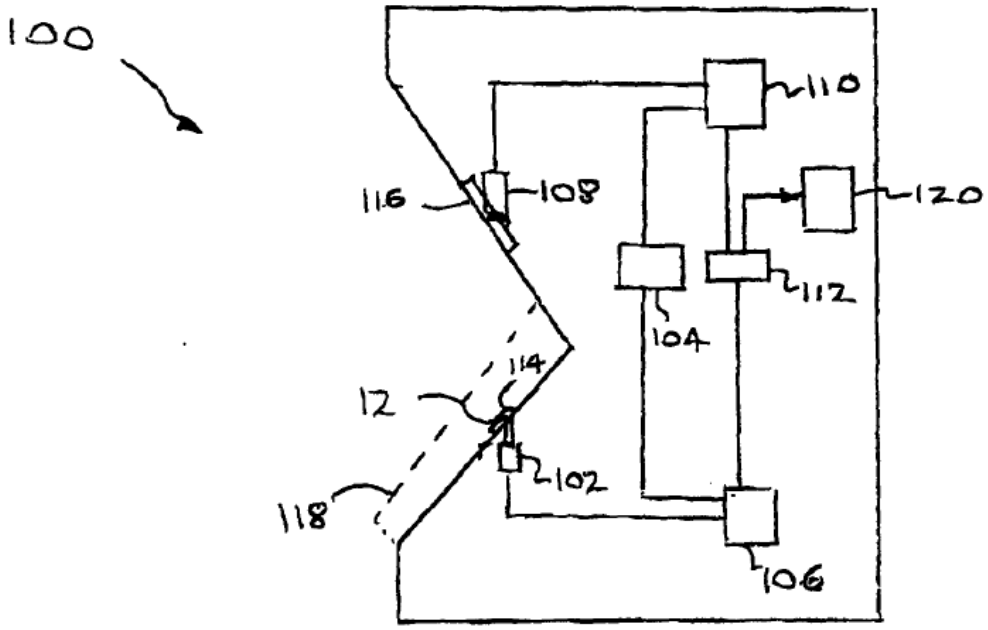

Fig 3