(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 577 685**

(51) Int. CI.:

G07F 19/00 (2006.01)
G07G 3/00 (2006.01)
G08B 29/04 (2006.01)
G08B 13/196 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.10.2011 E 11186780 (0)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2016 EP 2455925**

(54) Título: **Procedimiento y dispositivo para la defensa de intentos de manipulación en un sistema de cámara**

(30) Prioridad:

17.11.2010 DE 102010060624

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.07.2016

(73) Titular/es:

WINCOR NIXDORF INTERNATIONAL GMBH (100.0%)
Heinz-Nixdorf-Ring 1
33106 Paderborn, DE

(72) Inventor/es:

PRIESTERJAHN, DR. STEFFEN;
LE, DINH KHOI y
DRICHEL, ALEXANDER

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y dispositivo para la defensa de intentos de manipulación en un sistema de cámara

La invención se refiere a un procedimiento para la defensa de intentos de manipulación en un sistema de cámara de acuerdo con el preámbulo de la reivindicación 1 y a un dispositivo que trabaja de acuerdo con el sistema así como a un terminal de autoservicio equipado con él. La invención se refiere especialmente a un procedimiento así como a un dispositivo para la defensa de intentos de manipulación en un sistema de cámara, en el que desde una cámara instalada en un terminal de autoservicio se generan datos de imágenes y se transmiten a través de una conexión a un dispositivo que recibe los datos de imágenes, en el que la cámara detecta una zona de registro, que cubre una zona de mando a supervisar del terminal de autoservicio.

Se conoce que los terminales de autoservicio, como por ejemplo cajeros automáticos, no en pocas ocasiones están expuestos a manipulaciones por extraños, que colocan instalaciones de mando reproducidas, en particular superestructuras de teclados, para leer al mismo tiempo o bien registrar ilegalmente datos sensibles, como por ejemplo PIN y/o datos de tarjeta magnéticas y similares durante el manejo a través el cliente. Con la ayuda de los datos registrados, los extraños o bien criminales pueden copiar las tarjetas el cliente y utilizarlas con el PIN leído, para sacar dinero de las cuentas del cliente. Para reconocer las manipulaciones en tales terminales de autoservicio, se emplean con frecuencia cámaras, que supervisan la zona de mando del terminal de autoservicio y los elementos de mando que se encuentran allí, como por ejemplo el teclado, para poder reconocer si se manipula en el teclado o en otros elementos de mando a través de extraños. Las cámaras suministran datos de imágenes, que son transmitidos, en general, a través de una conexión de cable, a un dispositivo receptor, como por ejemplo a un PC instalado en el terminal de autoservicio, para ser evaluados allí localmente o, en cambio, para ser transmitidos entonces a continuación a través de un sistema de supervisión remota en adelante a una central. Recientemente se ha mostrado que también las cámaras o bien sistemas de cámaras propiamente dichos son utilizados por los criminales, para realizar intentos de manipulación en el terminal de autoservicio. Especialmente los criminales tratan de desviar directamente los datos de imágenes registrados por la cámara de supervisión o bien los datos transmitidos (la llamada “derivación de la cámara”) para detectar ilegalmente de esta manera durante una entrada del teclado del cliente la entrada del PIN.

En el documento DE 10 2009 018 321 A1 se publica un terminal de autoservicio (terminal-SB) con una disposición de cámara, que presenta varias cámaras, que están montadas en la zona próxima del campo de mando el terminal-SB y detectan allí diferentes elementos, como por ejemplo teclado, bandeja de salida de dinero, ranura de entrada de tarjetas, para reconocer intentos de manipulación en el terminal-SB. Al menos una cámara está instalada en el terminal-SB y un dispositivo conectado con la cámara está configurado como un ordenador, que está integrado en el terminal-SB. Desde la cámara respectiva se generan datos de imágenes y se transmiten a través de una conexión al dispositivo receptor de datos, detectando la cámara una zona de registro, que cubre una zona de mando a supervisar del terminal-SB- También se pueden detectar actuaciones extrañas sobre el sistema de cámara, como por ejemplo la cobertura de una cámara, verificando que aparecen diferencias de claridad entre las tomas de imágenes de varias cámaras.

El documento WO 2010/001282 A1 describe un procedimiento y un dispositivo para la defensa de intentos de manipulación en sistemas de cámaras en general. A tal fin se propone integrar en la carcasa una estera de armazón de hardware segura (“secure hardware mesh”), que está constituida por alambre conductores ultrafinos (“ultra thin conducting wires”), que están conectaos con entidades de semiconductores basada en transistor (“transistor based semi-conducting entities”) y de esta manera representan una configuración unívoca, cuyo cálculo con la ayuda de un algoritmo-Hash de seguridad conduce a una signatura unívoca. Esta signatura se utiliza para la seguridad de la transmisión de datos de imágenes de la cámara, en particular utilizando una PKI (Public Key Infrastructure). Cada intervención física, como por ejemplo la rotura de la estera de armadura, conduce a una modificación de la configuración y modifica la signatura calculada. De esta manera se pueden reconocer con seguridad manipulaciones que se realizan en forma de intervenciones físicas. Allí no se establece una referencia para la defensa de intentos de manipulación en terminales de autoservicio supervisados por cámara.

En el documento US 2005 / 0226338 A1 se describe un sistema de detección antirrobo basado en cámara, en el que los datos de imágenes son transmitidos desde al menos una cámara a través de un canal de transmisión o bien de comunicación hacia una primera memoria de datos. Adicionalmente, está prevista una segunda memoria, que es con preferencia una memoria tampón anular, para registrar los datos desde la primera memoria como copia de datos, cuando un sistema de supervisión reconoce que la al memos una cámara no transmite ya datos de imágenes a través del canal de comunicación. Tampoco aquí se establece ninguna relación con la defensa de intentos de manipulación en terminales de autoservicio supervisados con cámara.

En el documento DE 10 2009 018322 A1 se publica un terminal de autoservicio (terminal-SB) con una cámara para el reconocimiento de intentos de manipulación en el terminal-SB. La cámara está montada en una sección de carcasa, que rodea el campo de mando del terminal-SB, de manera que la cámara está instalada de tal manera que detecta al menos dos de los elementos previstos en el campo de mando, como por ejemplo teclado y bandeja de

salida de dinero, para reconocer de manera unívoca eventuales superestructuras colocadas e intentos de manipulación o bien de desescoriado similares.

Para cerrar los huecos de seguridad mencionados al principio en terminales de autoservicio supervisados con cámara, se propone en el documento DE 10 2008 039 689 A1 bloquear selectivamente la actividad de una cámara de supervisión, siendo desactivada la cámara, por ejemplo, cuando se introduce una tarjeta de cliente en el lector de tarjetas durante un cierto periodo de tiempo, de manera que una entrada de PIN realizada entonces a través el cliente no es registrada al mismo tiempo. De esta manera, se anular cualquier intento de manipulación, para "extraer" el sistema de cámara. Con esta solución conocida se mejora ya claramente la seguridad contra intentos de manipulación. Sin embargo, esta medida de seguridad solamente interviene cuando se puede asegurar que se realiza la desactivación de la cámara durante la entrada del PIN. Por lo tanto, existe la necesidad de mejorar adicionalmente esta solución.

De acuerdo con ello, el cometido de la presente invención es solucionar de manera ventajosa los inconvenientes que resultan del estado de la técnica. En particular, deben proponerse procedimientos y dispositivos, que son adecuados para la defensa de intentos de manipulación en sistemas de cámaras, en los que se generan datos de imágenes por una cámara instalada en un terminal de autoservicio y se transmiten adicionalmente.

El cometido se soluciona por medio de un procedimiento con las características de la reivindicación 1, así como por medio de un dispositivo, un terminal de autoservicio y un sistema de cámara con las características según una de las reivindicaciones secundarias.

De acuerdo con ello, se propone para la defensa de intentos de manipulación en un sistema de cámara que se detecte la actuación extraña sobre el sistema de cámara, verificando un dispositivo conectado con la cámara si aparece una modificación del estado técnico dentro del sistema de cámara, verificando el dispositivo si la cámara es desactivada a través de actuación extraña; y verificando si un controlador de aparatos instalado en el sistema de cámara como parte del dispositivo, que controla la cámara, no tiene acceso a la cámara, por que un controlador de otro ordenador controla la cámara; y/o verificando si se reciben datos de imágenes desde el dispositivo, aunque no se solicita por el dispositivo la emisión de datos de imágenes.

De acuerdo con ello, se propone verificar o bien supervisar modificaciones del estado técnico dentro del propio sistema de cámara, para establecer de esta manera si una actuación extraña ha aparecido en el sistema de cámara, es decir, en la cámara y/o en la conexión que transmite los datos de imágenes.

Por ejemplo, se verifica si aparece una modificación del estado técnico en la cámara, en un enchufe de la cámara para la conexión y/o en la propia conexión. Por lo tanto, se reconoce si existe una actuación extraña o bien un control extraño de la cámara y/o el sistema de cámara, para disparar entonces, dado el caso, una alarma o poner fuera de servicio el terminal de autoservicio.

De acuerdo con la invención se verifica a tal fin si la cámara ha sido desactivada a través de actuación extraña. De esta manera debe reconocerse especialmente si la cámara de supervisión ha sido manipulada, por ejemplo, a través de toma fraudulenta o corte del cable de la cámara, de manera que se pude partir de que los datos de la imagen son tomados directamente, es decir, sin transmisión al PC. De forma alternativa o complementaria a ello, se verifica también si la propia conexión ha sido influencia por actuación extraña, estando configurada la conexión especialmente como una conexión de cable. De esta manera se puede establecer con exactitud si ha sido manipulada la conexión de cable.

La invención se puede configurar también como se representa en adelante, de tal manera que se verifica una identificación consultable por la cámara. De esta manera se puede establecer si la cámara de supervisión propiamente dicha o bien el tipo de cámara previsto está o no conectado con el PC. Si éste no es el caso, se habla de que existe una manipulación de la cámara, por ejemplo por que se ha conectado en el sistema otra cámara de mando a distancia controlable a distancia por criminales.

La invención también se puede configurar de manera ventajosa para verificar al menos un parámetro de conexión típico para la cámara. En este caso se trata especialmente de parámetros para la conexión de la cámara en la conexión de cable, como por ejemplo resistencia de la línea, tensión, nivel de la señal durante la transmisión de la imagen y similares. De esta manera, se puede establecer también que probablemente ha sido conectado otro tipo de cámara y/o existe una toma fraudulenta de la transmisión de imágenes.

Por lo demás, según la invención se verifica si controlador de aparatos instalado en el sistema de cámara, que controla la cámara, tiene acceso a la cámara. En efecto, si éste no es el caso, entonces esto puede ser un indicio de que la cámara es controlada por el controlador de otro ordenador. Con otras palabras: el evento o bien el estado "la cámara reconoce, pero no tiene acceso" alude aquí a una actuación extraña.

Además, se puede verificar si se reciben datos de imágenes por el dispositivo, aunque no se solicite la emisión de datos de imágenes desde éste. De esta modo se puede establecer que la cámara instalada muy posiblemente es

controlada desde fuera o bien es disparada desde fuera, lo que representa de nuevo un indicio de una manipulación.

La invención forma una aportación especialmente ventajosa a la desactivación controlada por evento ya conocida de la cámara (durante la lectura de tarjetas y la entrada de PIN), siendo desactivado con preferencia todo el terminal-SB cuando se detecta la aparición de una actuación extraña sobre el sistema de cámara. De esta manera se puede excluir muy rápidamente que se pueda eludir una desactivación controlada por evento de la cámara, tal como se propone en el estado de la técnica, a través de la actuación extraña.

Éstas y otras ventajas se deducen también a partir de las reivindicaciones dependientes.

Por lo demás, se describe la invención en detalle con la ayuda de un ejemplo de realización y de los dibujos adjuntos, reproduciendo los dibujos la siguiente representación esquemática:

La figura 1 muestra la estructura de un sistema de cámara con un dispositivo según la invención para la defensa de intentos de manipulación.

La figura 2 muestra un diagrama de flujo para el procedimiento según la invención para la defensa de intentos de manipulación en el sistema de cámara mostrado.

La figura 1 muestra una representación esquemática con el sistema de cámara SYS que está constituido por varios elementos y un dispositivo PC, que está conectado con el sistema de cámara SYS y que está configurado aquí también para la defensa de intentos de manipulación. El dispositivo PC corresponde en el ejemplo mostrado a un ordenador personal el terminal de autoservicio, que se designa, por lo demás, también de forma abreviada Terminal-SB y representa en el presente ejemplo un cajero automático. El sistema de cámara SYS comprende esencialmente una cámara CAM, que emite a través de una conexión, aquí conexión de cable CBL, datos de imágenes CD al dispositivo PC. La cámara comprende una zona, que detecta la zona de mando B del terminal-SB ATM o bien una parte del mismo. En el presente caso se trata a este respecto del teclado KBD.

En el dispositivo PC se trata de aquel ordenador personal, que está integrado en el terminal-SB y que controla los ciclos durante el manejo el terminal-SB, como por ejemplo la entrada de tarjetas, entrada del teclado, la transmisión de datos sensibles (datos de tarjetas, PIN) a un sistema central, la activación a través de una pantalla de imágenes de mando, la liberación y la realización de una salida de dinero en efectivo, etc. El dispositivo o bien el ordenador personal PC controla, entre otras cosas, también un controlador de aparatos DRV o bien controlador de cámara, que controla de nuevo la cámara CAM, para posibilitar el registro y la transmisión de datos de imágenes VD. En particular, el registro y la transmisión de los datos de imágenes se realizan también aquí controlados por evento, lo que se indica a través del signo de referencia CTR, que corresponde a una señal de control o bien de disparo emitida por el controlador de la cámara DRV a la cámara.

Además de los datos de imágenes VD registrados por la cámara se transmiten también otros datos desde la cámara CAM hacia el dispositivo o bien el ordenador personal PC, como por ejemplo la identificación o bien el número de identificación ID de la cámara CAM.

Los módulos y los elementos representados aquí son adecuados de acuerdo con ello para realizar el procedimiento propuesto por el estado de la técnica para el registro controlado por evento de datos de imágenes de la cámara. Además, aquí especialmente el dispositivo o bien el ordenador personal PC son adecuados para realizar el procedimiento descrito todavía en detalle a continuación para la defensa de intentos de manipulación en los sistemas de cámaras SYS representados aquí. De esta manera, se crea el ordenador personal PC representado en la figura 1 para detectar actuación extraña sobre el sistema de cámara SYS, verificando si aparece una modificación del estado técnico dentro el sistema de cámara, es decir, si se ha manipulado la propia cámara CAM y/o la conexión CBL o bien el controlador de la cámara DRV.

El procedimiento 100 realizado por el dispositivo o bien el ordenador personal PC se explica ahora en detalle con la ayuda de la figura 2. En una primera etapa 110 se verifica si aparece una modificación del estado técnico entro del sistema de cámara VD. A tal fin, se verifica en una etapa parcial 111 especialmente si la cámara ha sido desactivada a través de actuación externa. De manera alternativa o adicional a ello, en una etapa parcial 112 se verifica una identificación consultable por la cámara (ver ID en la figura 1). De esta manera, se puede establecer si la cámara CAM del sistema de cámara ha sido retirada, ha sido desactivada o ha sido sustituida por una cámara de otro tipo.

También en una etapa parcial 113 se puede verificar un parámetro de conexión típico para la cámara, como por ejemplo la conexión de la línea para la conexión del cable CBL. Además, en una etapa parcial 115 se puede verificar si la conexión CBL propiamente dicha ha sido influenciada por actuación externa o ha sido separada. En este caso, se puede tratar, por ejemplo, de la separación de la conexión de cable CBL y/o de la toma fraudulenta de la misma, lo que puede tener de nuevo repercusiones sobre determinados parámetros como por ejemplo el nivel de la señal y similar.

En una etapa 120 se verifica entonces si un controlador de aparatos instalados en el sistema de cámara, aquí el

controlador de la cámara DRV, tiene todavía acceso a la cámara CAM (ver también la figura 1).

Si éste no es el caso, esto alude a una manipulación del sistema de cámara. A continuación se verifica en una etapa 125 si los datos de imágenes VD son recibidos por el dispositivo PC, aunque no sea solicitada por este dispositivo PC la emisión de datos de imágenes (ver la señal de disparo CTR en la figura 1). En efecto, si éste fuera el caso, entonces también en este caso hay que partir de que existe una manipulación el sistema de cámara.

Si se establece en una de las etapas parciales 111 a 115 mencionadas anteriormente o bien en las etapas 120 y/o 125 que existe una manipulación del sistema de cámara, entonces se pone el terminal-SB ATM en una etapa 150 fuera de servicio y/o se dispara una alarma. El sistema de cámara SYS descrito aquí con el dispositivo PC previsto (ver la figura 1), no sólo es adecuado para controlar una o varias cámaras controladas por evento, para contrarrestar un intento de manipulación en el Terminal-SB, sino que es adecuado también para detectar intentos de manipulación en el propio sistema de cámara y contrarrestarlos efectivamente, desactivando, dado el caso, efectivamente el terminal-SB y/o disparando una alarma. En efecto, los ensayos con tales sistemas han mostrado que una desactivación controlada por evento de la cámara por sí sola no siempre es suficiente para garantizar una seguridad suficiente contra ensayos de manipulación de toda la instalación (terminal-SB y sistema de cámara). Puesto que por medio de los sistemas hasta ahora no se ha podido establecer si la cámara ha sido activada o bien controlada a distancia sin permiso durante una entrada en el teclado y de esta manera han sido espiadas imágenes por la entrada de la identificación (PIN) a pesar de las medidas de seguridad prevista y han sido transmitidas a terceros.

Con el dispositivo PC propuesto aquí se asegura ahora que también intentos de manipulación en el sistema de cámara propiamente dicho son reconocidos de manera inmediata y segura y, dado el caso se inician contramedidas (desconexión el terminal-SB y/o disparo de alarma). De este modo resulta un nivel de seguridad claramente elevado para todo el sistema.

La presente invención ha sido descrita en el ejemplo de un cajero automático, pero se puede aplicar a cualquier tipo de terminal de autoservicio y, por lo tanto, no está limitado a la forma de realización descrita concreta.

REIVINDICACIONES

1.- Procedimiento (100) para la defensa de intentos de manipulación en un sistema de cámara (SYS), en el que desde una cámara (CAM) se generan datos de imágenes (VD) y a transmiten a través de una conexión (CBL) a un dispositivo (PC) receptor de los datos de imágenes (VD), en el que la cámara (CAM) se instala en un terminal de autoservicio (ATM), en el que el dispositivo (PC) está configurado como un ordenador, que se integra en el terminal de autoservicio (ATM), en el que la cámara (CAM) detecta una zona de registro, que cubre una zona de mando (B) a supervisar del terminal de autoservicio (ATM), y en el que se detecta una actuación extraña sobre el sistema de cámara (SYS), caracterizado por que se detecta la actuación extraña sobre el sistema de cámara (SYS), verificando (110) si aparece una modificación del estado técnico dentro del sistema de cámara (SYS), en el que a través del dispositivo (PC) se verifica (111) si la cámara (CAM) es desactivada a través de la actuación extraña y se verifica (120), si un controlador de aparatos (DRV) instalado en el sistema de cámara (SYS) como parte del dispositivo (PC), que controla la cámara (CAM) no tiene acceso a la cámara (CAM), por que la cámara es controlada por un controlador de otro ordenador; y/o se verifica (125) si se reciben datos de imágenes (VD) desde el dispositivo (PC), aunque no se solicite desde el dispositivo (PC) la emisión de datos de imágenes.

2.- Procedimiento (100) de acuerdo con la reivindicación 1, caracterizado por que se verifica si aparece una modificación del estado técnico de la cámara (CAM), en una conexión de la cámara (CAM) a la conexión (CBL) y/o en la conexión (CBL).

3.- Procedimiento (100) de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se verifica una identificación (ID) consultable por la cámara (CAM).

4.- Procedimiento (100) de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se verifica (113) al menos un parámetro de conexión típico para la cámara (CAM).

5.- Procedimiento (100) de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se verifica si la conexión (CBL) está influenciada o separada (115) por la actuación exterior, en el que la conexión está configurada especialmente como una conexión de cable (CBL).

6.- Procedimiento (100) de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el terminal de autoservicio (ATM) se pone fuera de servicio y/o se emite una alarma (150) cuando se detecta la aparición de una actuación extraña sobre la disposición de cámara (SYS).

7.- Dispositivo (PC) para la defensa de intentos de manipulación en un sistema de cámara (SYS), en el que desde una cámara (CAM) se generan datos de imágenes (VD) y se transmiten a través de una conexión (CBL) al dispositivo (PC) receptor de los datos de imágenes (VD), en el que la cámara (CAM) está instalada en un terminal de autoservicio (ATM), en el que el dispositivo (PC) está configurado como un ordenador, que se integra en el terminal de autoservicio (ATM), en el que la cámara (CAM) detecta una zona de registro (A), que cubre una zona de mando a supervisar del terminal de autoservicio (ATM), y en el que el dispositivo (PC) detecta una actuación extraña sobre el sistema de cámara (SYS), caracterizado por que el dispositivo (PC) detecta la actuación extraña sobre el sistema de cámara (SYS), verificando el dispositivo (PC) si aparece una modificación del estado técnico dentro del sistema de cámara (SYS), en el que el dispositivo (PC) verifica (111) si la cámara (CAM) es desactivada a través de la actuación extraña; y se verifica (120), si un controlador de aparatos (DRV) instalado en el sistema de cámara (SYS) como parte del dispositivo (PC), que controla la cámara (CAM), no tiene acceso a la cámara (CAM), por que un controlador de otro ordenador controla la cámara; y/o verifica (125) si son recibidos datos de imágenes (VD) por el dispositivo (PC), aunque no se solicite desde el dispositivo (PC) la emisión de datos de imágenes.

8.- Terminal de autoservicio (ATM) con un dispositivo (PC) según la reivindicación 7.

9.- Sistema de cámara (SYS) con un dispositivo (PC) según la reivindicación 7.

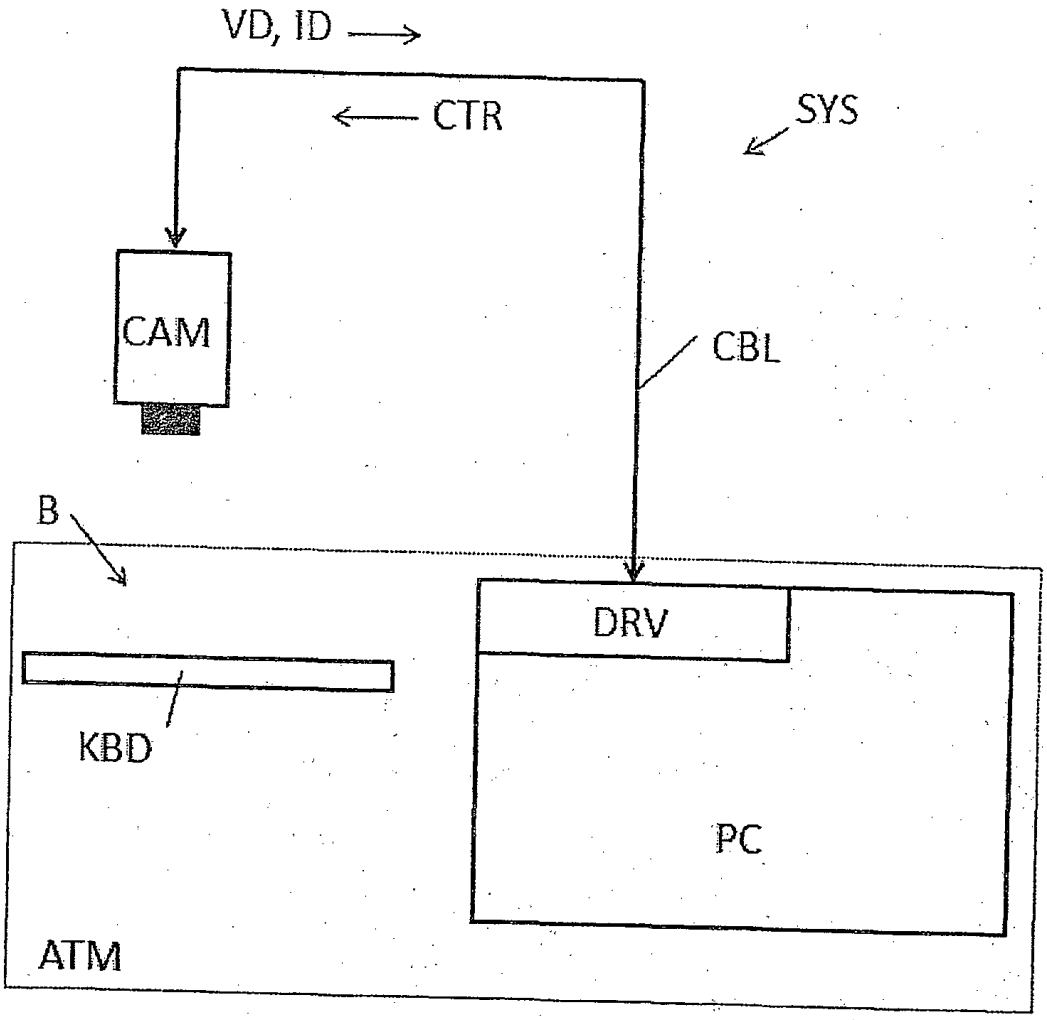

Fig. 1

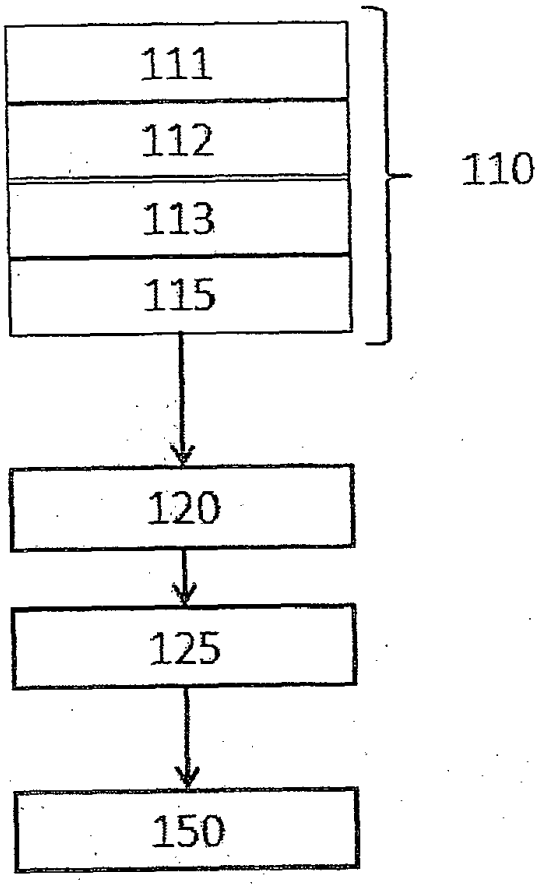

Fig. 2