(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 455 925 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
23.05.2012 Patentblatt 2012/21

(51) Int Cl.:
G07F 19/00 *(2006.01)* ***G07G 3/00*** *(2006.01)*

(21) Anmeldenummer: **11186780.0**

(22) Anmeldetag: **26.10.2011**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME

(30) Priorität: **17.11.2010 DE 102010060624**

(71) Anmelder: **Wincor Nixdorf International GmbH**
33106 Paderborn (DE)

(72) Erfinder:
- **Priesterjahn, Dr. Steffen**
  33100 Paderborn (DE)
- **Le, Dr. Dinh Khoi**
  33102 Paderborn (DE)
- **Drichel, Alexander**
  33613 Bielefeld (DE)

(74) Vertreter: **2K Patentanwälte Blasberg Kewitz & Reichel**
Partnerschaft
Corneliusstraße 18
60325 Frankfurt a. M. (DE)

(54) **Verfahren und Vorrichtung zur Abwehr von Manipulationsversuchen an einem Kamera-System**

(57) Vorgeschlagen werden ein Verfahren und eine Vorrichtung (PC) zur Abwehr von Manipulationsversuchen an einem Kamera-System (SYS), bei dem von einer an einem Selbstbedienungs-Terminal (ATM) installierten Kamera (CAM) Bilddaten (VD) erzeugt und über eine Verbindung (CBL) an eine die Bilddaten (VD) empfangende Vorrichtung übertragen werden, die auch in die Vorrichtung (PC) zur Abwehr von Manipulationsversuchen integriert sein kann, wobei die Kamera (CAM) einen Aufnahmebereich erfasst, der einen zu überwachenden Bedienbereich (B) des Selbstbedienungs-Terminals (ATM) abdeckt. Die Vorrichtung (PC) kann eine Fremdeinwirkung auf das Kamera-System (SYS) detektieren, wie z.B. ein "Anzapfen" der Kamera (CAM), indem sie prüft, ob eine technische Zustandsänderung innerhalb des Kamera-Systems (SYS) auftritt und ggf. das Selbstbedienungs-Terminal (ATM) außer Betrieb nimmt und/oder einen Alarm auslöst.

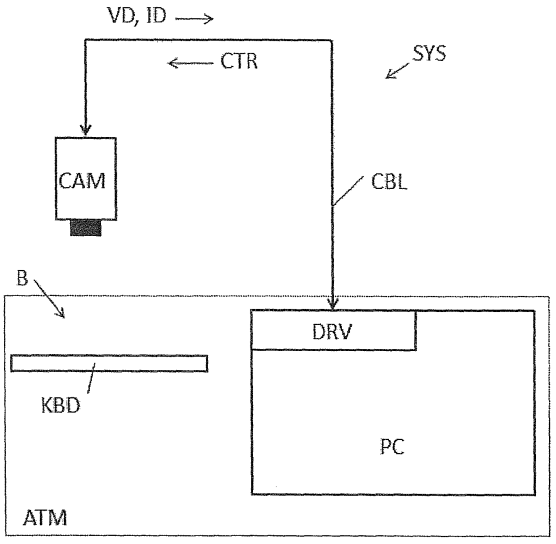

Fig. 1

EP 2 455 925 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Abwehr von Manipulationsversuchen an einem Kamera-System nach dem Oberbegriff des Anspruchs 1 und eine nach dem System arbeitende Vorrichtung sowie ein damit ausgestattetes Selbstbedienungs-Terminal. Die Erfindung betrifft insbesondere ein Verfahren sowie eine Vorrichtung zur Abwehr von Manipulationsversuchen an einem Kamera-System, bei dem von einer an einem Selbstbedienungs-Terminal installierten Kamera Bilddaten erzeugt und über eine Verbindung an eine die Bilddaten empfangende Vorrichtung übertragen werden, wobei die Kamera ein Aufnahmebereich erfasst, der einen zu überwachenden Bedienungsbereich des Selbstbedienungs-Terminals abdeckt.

[0002] Es ist bekannt, dass Selbstbedienungs-Terminals, wie etwa Geldautomaten, nicht selten der Manipulation durch Fremde ausgesetzt sind, welche nachgebaute Bedieneinrichtungen, insbesondere Tastaturüberbauten, anbringen, um sensitive Daten, wie z.B. PIN und/oder Kartendaten von Magnetkarten und dergleichen, bei der Bedienung durch den Kunden widerrechtlich mitzulesen bzw. abzugreifen. Anhand der abgegriffenen Daten können die Fremden bzw. Kriminellen die Kundenkarten nachbilden und mit der ausgelesenen PIN nutzen, um beispielsweise Geld von dem Konto des Kunden abzuheben. Um die Manipulationen an solchen Selbstbedienungs-Terminals zu erkennen, werden häufig Kameras eingesetzt, die den Bedienbereich des Selbstbedienungs-Terminals und dortige Bedienelemente, wie z.B. die Tastatur, überwachen, um erkennen zu können, wann an der Tastatur oder an anderen Bedienungselementen durch Fremde manipuliert wird. Die Kameras liefern Bilddaten, die in der Regel über eine Kabelverbindung an eine empfangende Vorrichtung, wie z.B. an einen in dem Selbstbedienungs-Terminal installierten PC, übertragen werden, um dort lokal ausgewertet zu werden oder aber um dann anschließend über ein Fernüberwachungssystem weiter an eine Zentrale übertragen zu werden. Es hat sich neuerdings gezeigt, dass auch die Kameras bzw. Kamera-Systeme selbst von den Kriminellen benutzt werden, um Manipulationsversuche an dem Selbstbedienungs-Terminal durchzuführen. Insbesondere versuchen die Kriminellen, die von der Überwachungs-Kamera aufgenommenen Bilddaten bzw. die übertragenen Bilddaten direkt abzuzweigen (sog. "Anzapfen der Kamera"), um somit bei einer Tastatureingabe des Kunden die Eingabe der PIN widerrechtlich zu erfassen.

[0003] Um derartige Sicherheitslücken zu schließen, wird in der DE 10 2008 039 689 A1 vorgeschlagen, die Aktivität einer Überwachungs-Kamera gezielt zu blockieren, indem beispielsweise bei Einführung einer Kundenkarten in den Kartenleser die Kamera für einen gewissen Zeitraum deaktiviert wird, sodass eine dann durchgeführte PIN-Eingabe durch den Kunden nicht mit aufgenommen wird. Somit geht jeder Manipulationsversuch, das Kamera-System "anzuzapfen" in Leere. Mit dieser bekannten Lösung wird somit die Sicherheit gegen Manipulationsversuche bereits deutlich verbessert. Allerdings greift diese Sicherheitsmaßnahme nur dann, wenn sichergestellt werden kann, dass die Deaktivierung der Kamera während der PIN-Eingabe erfolgt. Daher besteht der Bedarf, auch diese Lösung weiter verbessern.

[0004] Demnach ist es Aufgabe der vorliegenden Erfindung, die sich aus dem Stand der Technik ergebenden Nachteile in vorteilhafter Weise zu überwinden. Insbesondere sollen ein Verfahren und Vorrichtungen vorgeschlagen werden, die zur Abwehr von Manipulationsversuchen an Kamera-Systemen geeignet sind, bei denen von einer an einem Selbstbedienungs-Terminal installierten Kamera Bilddaten erzeugt und weiter übertragen werden.

[0005] Die Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Anspruchs 1, sowie durch eine Vorrichtung, ein Selbstbedienungs-Terminal und ein Kamera-System mit den Merkmalen nach einem der nebengeordneten Ansprüche.

[0006] Demnach wird zur Abwehr von Manipulationsversuchen an einem Kamera-System vorgeschlagen, dass eine Fremdeinwirkung auf das Kamera-System detektiert wird, indem eine Vorrichtung, insbesondere die mit der Kamera verbundene Vorrichtung, prüft, ob eine technische Zustandsänderung innerhalb des Kamera-Systems auftritt.

[0007] Vorzugsweise handelt es sich bei der Vorrichtung um eine Vorrichtung, die die von der Kamera erzeugten Bilddaten empfängt und bspw. in einem Computer bzw. PC integriert ist, der in dem Selbstbedienungs-Terminals integriert ist.

[0008] Demnach wird vorgeschlagen, technische Zustandsänderungen innerhalb des Kamera-Systems selbst zu überprüfen bzw. zu überwachen, um somit festzustellen, ob eine Fremdeinwirkung an dem Kamera-System, d.h. an der Kamera und/oder an der die Bilddaten übertragenden Verbindung, aufgetreten ist. Beispielsweise wird geprüft, ob eine technische Zustandsänderung an der Kamera, an einem Anschluss der Kamera zur Verbindung und/oder an der Verbindung selbst auftritt. Es wird also erkannt, ob eine Fremdeinwirkung bzw. Fremdsteuerung der Kamera und/oder des Kamera-Systems vorliegt, um dann ggf. einen Alarm auszulösen oder das Selbstbedienungs-Terminal außer Betrieb zu nehmen.

[0009] In einem Ausführungsbeispiel der Erfindung wird hierzu geprüft, ob die Kamera durch Fremdeinwirkung deaktiviert wurde. Damit soll insbesondere erkannt werden, ob die Überwachungs-Kamera bspw. durch Abziehen oder Durchtrennen des Kamerakabels manipuliert wurde, sodass davon ausgegangen werden kann, dass die Bilddaten direkt, d.h. ohne Übertragung an den PC, abgegriffen werden. Alternativ oder ergänzend dazu wird auch geprüft, ob die Verbindung selbst durch Fremdeinwirkung beeinflusst wurde, wobei die Verbindung insbesondere als eine Kabelverbindung ausgebildet ist. So-

mit kann auch durch diese Maßnahme genau festgestellt werden, ob an der Kabelverbindung manipuliert wurde.

[0010] Die Erfindung kann auch dergestalt weiter ausgebildet werden, dass eine von der Kamera abfragbare Kennung geprüft wird. Dadurch kann festgestellt werden, ob die eigentliche Überwachungs-Kamera bzw. der vorgesehene Kameratyp mit dem PC verbunden ist oder nicht. Ist dies nicht der Fall, so spricht vieles dafür, dass eine Manipulation der Kamera vorliegt, indem bspw. eine andere von dem Kriminellen fremdsteuerbare Kamera an das System angeschlossen wurde.

[0011] Auch kann die Erfindung in vorteilhafter Weise dadurch weiter ausgebildet werden, dass mindestens ein für die Kamera typischer Anschlussparamenter geprüft wird. Hierbei handelt es sich insbesondere um Parameter für den Anschluss der Kamera an die Kabelverbindung, wie bspw. Leitungswiderstand, Spannung, Signalpegel bei der Bildübertragung und dergleichen. Hiermit kann auch festgestellt werden, dass wahrscheinlich ein anderer Kameratyp angeschlossen wurde und/oder eine Anzapfung der Bildübertragung vorliegt.

[0012] Des Weiteren kann geprüft werden, ob ein in dem Kamera-System installierter Gerätetreiber, der die Kamera ansteuert, Zugriff auf die Kamera hat. Ist dies nämlich nicht der Fall, so kann dies ein Indiz dafür sein, dass die Kamera von dem Treiber eines anderen Computers angesteuert wird. Mit anderen Worten: Das Ereignis bzw. der Zustand "Kamera erkannt, aber kein Zugriff" deutet hier auf eine Fremdeinwirkung hin.

[0013] Außerdem kann geprüft werden, ob Bilddaten von der Vorrichtung empfangen werden, obwohl von dieser das Senden von Bilddaten nicht angefordert wird. Dadurch kann festgestellt werden, dass die installierte Kamera wohlmöglich fremd-gesteuert bzw. fremd-getriggert wird, was wiederum Indiz für eine Manipulation darstellt.

[0014] Die Erfindung bildet einen besonders vorteilhaften Beitrag zu der bereits bekannten ereignisgesteuerten Deaktivierung der Kamera (während des Kartenlesens und der PIN-Eingabe), indem vorzugsweise das ganze SB-Terminal dann deaktiviert wird, wenn das Auftreten einer Fremdeinwirkung auf das Kamera-System detektiert wird. Dadurch kann sehr schnell ausgeschlossen werden, dass eine ereignisgesteuerte Deaktivierung der Kamera, sowie im Stand der Technik vorgeschlagen, durch Fremdeinwirkung umgangen werden kann.

[0015] Diese und weitere Vorteile ergeben sich auch aus den Unteransprüchen.

[0016] Im Weiteren wird die Erfindung näher anhand eines Ausführungsbeispiels und der beiliegenden Zeichnungen beschrieben, wobei die Zeichnungen folgende schematische Darstellung wiedergeben:

Fig. 1 zeigt den Aufbau eines Kamera-Systems mit einer erfindungsgemäßen Vorrichtung zur Abwehr von Manipulationsversuchen;

Fig. 2 zeigt ein Flussdiagramm für das erfindungsgemäße Verfahren zur Abwehr von Manipulationsversuchen an dem gezeigten Kamera-System.

[0017] Die Fig. 1 zeigt eine schematische Darstellung mit den aus mehreren Elementen bestehenden Kamera-System SYS und einer Vorrichtung PC, die mit dem Kamera-System SYS verbunden ist und hier auch zur Abwehr von Manipulationsversuchen ausgebildet ist. Die Vorrichtung PC entspricht in dem gezeigten Beispiel einem Personal-Computer des Selbstbedienungs-Terminals, das im weiteren auch kurz SB-Terminal genannt wird und im vorliegenden Beispiel einen Geldautomaten darstellt. Das Kamera-System SYS umfasst im Wesentlichen eine Kamera CAM, die über eine Verbindung, hier Kabelverbindung CBL, Bilddaten CD an die Vorrichtung PC sendet. Die Kamera erfasst einen Bereich, der den Bedienbereich B des SB-Terminals ATM bzw. eines Teiles davon erfasst. Im vorliegenden Beispiel handelt es sich dabei um die Tastatur KBD.

[0018] Bei der Vorrichtung PC handelt es sich um denjenigen Personal-Computer, der in dem SB-Terminal integriert ist und die Abläufe während der Bedienung des SB-Terminals steuert, wie bspw. die Karteneingabe, Tastatureingabe, das Weiterleiten von sensitiven Daten (Kartendaten, PIN) an ein zentrales System, die Ansteuerung eines Bedienbildschirmes, die Freigabe und das Ausführung einer Bargeldausgabe usw.. Die Vorrichtung bzw. der Personal-Computer PC steuert unter anderem auch einen Gerätetreiber DRV bzw. Kameratreiber, der wiederrum die Kamera CAM ansteuert, um die Aufnahme und das Übertragen der Bilddaten VD zu ermöglichen. Insbesondere wird die Aufnahme und Übertragung der Bilddaten auch hier ereignisgesteuert durchgeführt, was durch das Bezugszeichen CTR angedeutet ist, welches einem von dem Kameratreiber DRV an die Kamera gesendeten Steuerungs- bzw. Triggersignal entspricht.

[0019] Neben den von der Kamera aufgenommenen Bilddaten VD werden auch weitere Daten von der Kamera CAM an die Vorrichtung bzw. den Personal-Computer PC übertragen, wie etwa die Kennung bzw. Identifikation-Nummer ID der Kamera CAM.

[0020] Die hier dargestellten Baugruppen und Elemente sind demnach geeignet, das im Stand der Technik vorgeschlagene Verfahren zur ereignisgesteuerten Aufnahme von Kamera-Bilddaten auszuführen. Darüber hinaus ist hier insbesondere die Vorrichtung bzw. der Personal-Computer PC geeignet, das im Nachfolgenden noch näher beschriebene Verfahren zur Abwehr von Manipulationsversuchen an den hier dargestellten Kamera-Systemen SYS auszuführen. Somit ist der in Fig. 1 dargestellte Personal-Computer PC beschaffen, Fremdeinwirkung auf das Kamera-System SYS zu detektieren, indem geprüft wird, ob eine technische Zustandsänderung innerhalb des Kamera-Systems auftritt, d.h. ob an der Kamera CAM selbst und/oder an der Verbindung CBL bzw. an dem Kameratreiber DRV manipuliert wurde.

[0021] Das von der Vorrichtung bzw. dem Personal-Computer PC durchgeführte Verfahren 100 wird nun anhand der Fig. 2 näher erläutert. In einem ersten Schritt 110. wird geprüft, ob eine technische Zustandsänderung innerhalb des Kamera-Systems VD auftritt. Dazu wird in einem Teilschritt 111 insbesondere geprüft, ob die Kamera durch Fremdeinwirkung deaktiviert wurde. Alternativ oder ergänzend dazu wird in einem Teilschritt 112 auf eine von der Kamera abfragbare Kennung (siehe ID in Fig. 1) hin geprüft. Dadurch kann festgestellt werden, ob die Kamera CAM des Kamera-System entfernt wurde, deaktiviert wurde oder durch eine Kamera eines anderen Typs ersetzt wurde.

[0022] Auch kann in einem teilschritt 113 auf einen für die Kamera typischen Anschlussparameter, wie z.B. den Leitungsanschluss zur Kabelverbindung CBL, hin geprüft werden. Außerdem kann in einem Teilschritt 115 geprüft werden, ob die Verbindung CBL selbst durch Fremdeinwirkung beeinflusst oder getrennt wurde. Dabei kann es sich bspw. um das Durchtrennen der Kabelverbindung CBL handeln und/oder um das Anzapfen derselben, was wiederum Auswirkungen auf bestimmte Parameter, wie etwa Signalpegel und dergleichen haben kann.

[0023] In einem Schritt 120 wird dann geprüft, ob ein in dem Kamera-System installierter Gerätetreiber, hier der Kameratreiber DRV, noch Zugriff auf die Kamera CAM hat (siehe auch Fig. 1).

[0024] Ist dies nicht der Fall, so deutet dies auf eine Manipulation des Kamera-Systems hin. Danach wird in einem Schritt 125 geprüft, ob die Bilddaten VD von der Vorrichtung PC empfangen werden, obwohl von dieser Vorrichtung PC das Senden von Bilddaten nicht angefordert wird (siehe Triggersignal CTR in Fig. 1). Sollte dies nämlich der Fall sein, so ist auch in diesem Fall davon auszugehen, dass eine Manipulation des Kamera-Systems vorliegt.

[0025] Wird in einem der oben genannten Teilschritte 111 bis 115 bzw. Schritte 120 und/oder 125 festgestellt, dass eine Manipulation des Kamera-Systems vorliegt, so wird in einem Schritt 150 das SB-Terminal ATM außer Betrieb genommen und/oder es wird ein Alarm ausgelöst. Das hier beschriebene Kamera-System SYS mit der vorgesehenen Vorrichtung PC (siehe Fig. 1) ist nicht nur dafür geeignet, eine oder mehrere Kameras ereignisgesteuert anzusteuern, um einem Manipulationsversuch an dem SB-Terminal entgegenzuwirken, sondern ist auch dafür geeignet, Manipulationsversuche am Kamera-System selbst zu detektieren und diesen effektiv entgegenzuwirken, indem das SB-Terminal ggf. sofort deaktiviert wird und/oder ein Alarm ausgelöst wird. Versuche mit üblichen Systemen haben nämlich gezeigt, dass eine ereignisgesteuerte Deaktivierung der Kamera allein nicht immer genügt, um eine ausreichende Sicherheit gegen Manipulationsversuche des Gesamtanlage (SB-Terminal und Kamera-System) zu garantieren. Denn mittels der bisherigen Systeme konnte nicht festgestellt werden, ob die Kamera während einer Tastatureingabe unerlaubt aktiviert bzw. ferngesteuert wurde und somit Bilder von der Eingabe der Kennung (PIN) trotz vorgesehener Sicherheitsmaßnahmen abgehört und an einen Dritten geliefert wurden.

[0026] Mit der hier vorgeschlagenen Vorrichtung PC nun wird sichergestellt, dass auch Manipulationsversuche am Kamera-System selbst sofort und sicher erkannt werden und ggf. Gegenmaßnahmen (Abschalten des SB-Terminals und/oder Alarm-Auslösung) sofort ausgeführt bzw. eingeleitet werden. Somit ergibt sich ein deutlich erhöhtes Sicherheitsniveau für das Gesamtsystem.

[0027] Die vorliegende Erfindung wurde am Beispiel eines Geldautomaten beschrieben, ist aber auf jede Art von Selbstbedienungs-Terminals anwendbar und somit nicht auf die konkret beschriebene Ausführungsform beschränkt.

Patentansprüche

1. Verfahren (100) zur Abwehr von Manipulationsversuchen an einem Kamera-System (SYS), bei dem von einer an einem Selbstbedienungs-Terminal (ATM) installierten Kamera (CAM) Bilddaten (VD) erzeugt und über eine Verbindung (CBL) an eine die Bilddaten (VD) empfangende Vorrichtung (PC) übertragen werden, wobei die Kamera (CAM) einen Aufnahmebereich erfasst, der einen zu überwachenden Bedienbereich (B) des Selbstbedienungs-Terminals (ATM) abdeckt, **dadurch gekennzeichnet, dass** eine Fremdeinwirkung auf das Kamera-System (SYS) detektiert wird, indem geprüft wird (110), ob eine technische Zustandsänderung innerhalb des Kamera-Systems (SYS) auftritt.

2. Verfahren (100) nach Anspruch 1, **dadurch gekennzeichnet, dass** geprüft wird, ob eine technische Zustandsänderung an der Kamera (CAM), an einem Anschluss der Kamera (CAM) zu der Verbindung (CBL) und/oder an der Verbindung (CBL) auftritt.

3. Verfahren (100) nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** geprüft wird (111), ob die Kamera (CAM) durch Fremdeinwirkung deaktiviert wird.

4. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** eine von der Kamera (CAM) abfragbare Kennung (ID) geprüft wird (112).

5. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** mindestens ein für die Kamera (CAM) typischer Anschluss-Parameter geprüft wird (113).

6. Verfahren (100) nach einem der vorhergehenden

Ansprüche, **dadurch gekennzeichnet, dass** geprüft wird, ob die Verbindung (CBL) durch Fremdeinwirkung beeinflusst oder getrennt wird (115), wobei die Verbindung insbesondere als eine Kabel-Verbindung (CBL) ausgebildet ist.

7. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** geprüft wird (120), ob ein in dem Kamera-System (SYS) installierter Gerätetreiber (DRV), der die Kamera (CAM) ansteuert, Zugriff auf die Kamera (CAM) hat.

8. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** geprüft wird (125), ob Bilddaten (VD) von der Vorrichtung (PC) empfangen werden, obwohl von der Vorrichtung (PC) das Senden von Bilddaten nicht angefordert wird.

9. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das Selbstbedienungs-Terminal (ATM) außer Betrieb genommen und/oder ein Alarm ausgelöst wird (150), wenn das Auftreten einer Fremdeinwirkung auf die Kamera-Anordnung (SYS) detektiert wird.

10. Vorrichtung (PC) zur Abwehr von Manipulationsversuchen an einem Kamera-System (SYS), bei dem von einer an einem Selbstbedienungs-Terminal (ATM) installierten Kamera (CAM) Bilddaten (VD) erzeugt und über eine Verbindung (CBL) an eine die Bilddaten (VD) empfangende Vorrichtung (PC) übertragen werden, wobei die Kamera (CAM) einen Aufnahmebereich (A) erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungs-Terminals (ATM) abdeckt, **dadurch gekennzeichnet, dass**
die Vorrichtung (PC) eine Fremdeinwirkung auf das Kamera-System (SYS) detektiert, indem die Vorrichtung (PC) prüft, ob eine technische Zustandsänderung innerhalb des Kamera-Systems (SYS) auftritt.

11. Vorrichtung (PC) nach Anspruch 10, **dadurch gekennzeichnet, dass** die Vorrichtung (PC) der die Bilddaten (VD) empfangenden Vorrichtung (PC) entspricht.

12. Vorrichtung (PC) nach Anspruch 10 oder 11, **dadurch gekennzeichnet, dass** die Vorrichtung als ein Computer, insbesondere Personal Computer (PC), ausgebildet ist, der in dem Selbstbedienungs-Terminal (ATM) integriert ist.

13. Selbstbedienungs-Terminal (ATM) mit einer Vorrichtung (PC) zur Abwehr von Manipulationsversuchen an einem Kamera-System (SYS), bei dem von einer an dem Selbstbedienungs-Terminal (ATM) installierten Kamera (CAM) Bilddaten (VD) erzeugt und über eine Verbindung (CBL) an eine die Bilddaten (VD) empfangende Vorrichtung (PC) übertragen werden, wobei die Kamera (CAM) einen Aufnahmebereich (A) erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungs-Terminals (ATM) abdeckt, **dadurch gekennzeichnet, dass**
die Vorrichtung (PC) eine Fremdeinwirkung auf das Kamera-System (SYS) detektiert, indem die Vorrichtung (PC) prüft, ob eine technische Zustandsänderung innerhalb des Kamera-Systems (SYS) auftritt.

14. Kamera-System (SYS) mit einer Vorrichtung (PC) zur Abwehr von Manipulationsversuchen an dem Kamera-System (SYS), bei dem von einer an einem Selbstbedienungs-Terminal (ATM) installierten Kamera (CAM) Bilddaten (VD) erzeugt und über eine Verbindung (CBL) an eine die Bilddaten (VD) empfangende Vorrichtung (PC) übertragen werden, wobei die Kamera (CAM) einen Aufnahmebereich (A) erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungs-Terminals (ATM) abdeckt, **dadurch gekennzeichnet, dass**
die Vorrichtung (PC) eine Fremdeinwirkung auf das Kamera-System (SYS) detektiert, indem die Vorrichtung (PC) prüft, ob eine technische Zustandsänderung innerhalb des Kamera-Systems (SYS) auftritt.

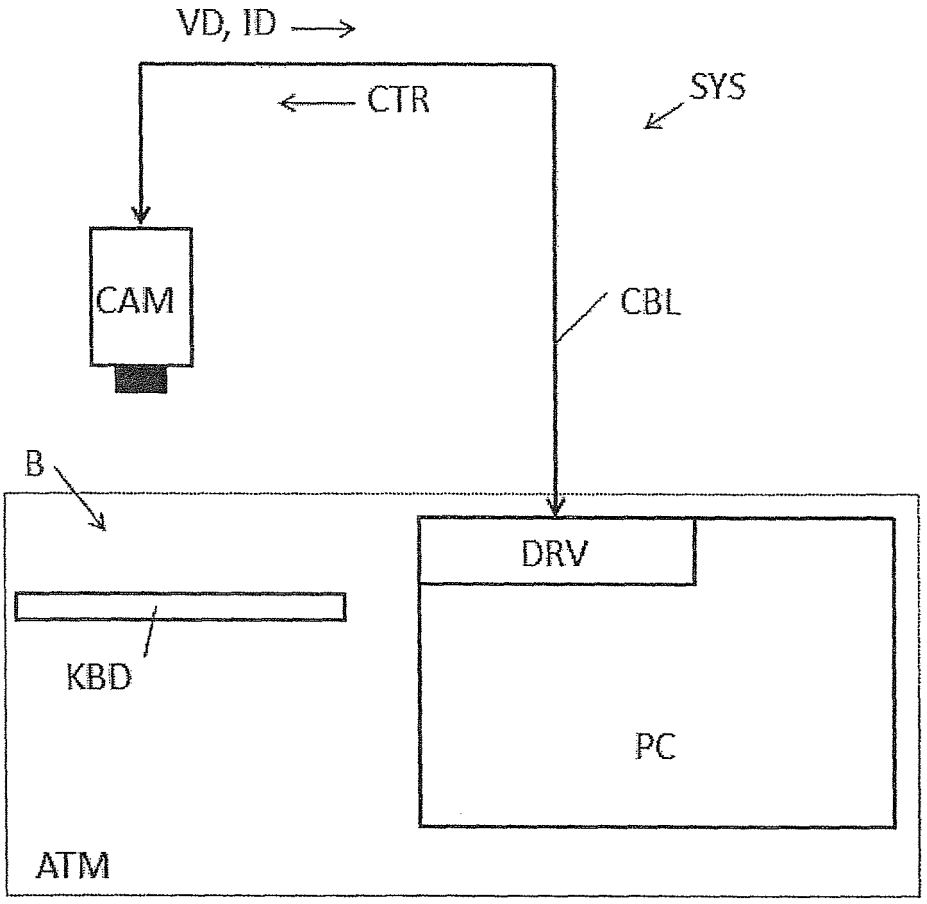

Fig. 1

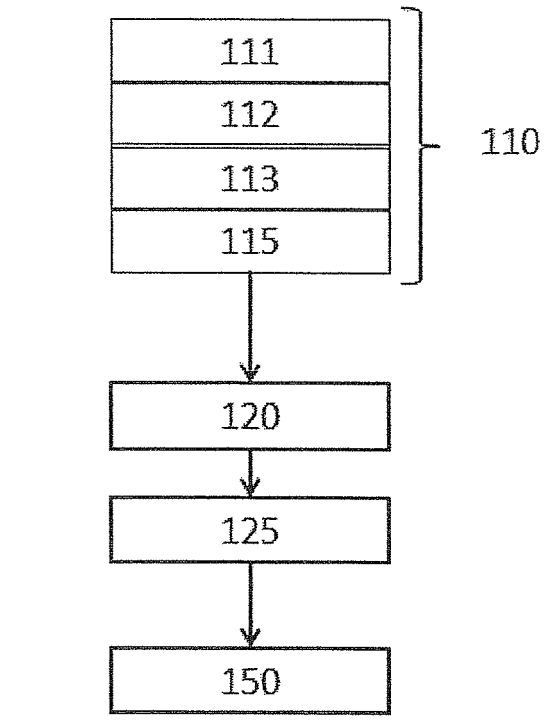

Fig. 2

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- DE 102008039689 A1 **[0003]**