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

(11) **EP 2 321 806 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
28.10.2015 Patentblatt 2015/44

(21) Anmeldenummer: **09782032.8**

(22) Anmeldetag: **20.08.2009**

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

(86) Internationale Anmeldenummer:
PCT/EP2009/060774

(87) Internationale Veröffentlichungsnummer:
WO 2010/023153 (04.03.2010 Gazette 2010/09)

(54) **VERFAHREN UND VORRICHTUNG ZUR ABWEHR VON LAUSCHVERSUCHEN BEI DER BILDDATEN-ÜBERTRAGUNG AN EINEM SELBSTBEDIENUNGSTERMINAL**

METHOD AND DEVICE FOR DEFLECTING EAVESDROPPING ATTEMPTS IN IMAGE DATA TRANSFER AT A SELF-SERVICE TERMINAL

PROCÉDÉ ET DISPOSITIF CONTRE LES TENTATIVES D'INTRUSION LORS DE LA TRANSMISSION DE DONNÉES D'IMAGE SUR UN TERMINAL EN LIBRE-SERVICE

(84) Benannte Vertragsstaaten:
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 SE SI SK SM TR

(30) Priorität: **26.08.2008 DE 102008039689**

(43) Veröffentlichungstag der Anmeldung:
18.05.2011 Patentblatt 2011/20

(73) Patentinhaber: **Wincor Nixdorf International GmbH**
33106 Paderborn (DE)

(72) Erfinder:
- **VON DER LIPPE, Carsten**
  Paderborn 33106 (DE)
- **LE, Dinh Khoi**
  Paderborn 33106 (DE)

(56) Entgegenhaltungen:
EP-A- 1 914 694 US-B1- 6 731 778

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 2 321 806 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Abwehr von Lauschversuchen bei der Übertragung von Bilddaten, die aus Bildsignalen gewonnen werden, die von einer an einem Selbstbedienungsterminal installierten Kamera erzeugt werden gemäß dem Oberbegriff des Anspruchs 1. Ebenso betrifft die Erfindung eine das Verfahren ausführende Vorrichtung sowie ein damit ausgestattetes Selbstbedienungsterminal gemäß dem Oberbegriff eines der nebengeordneten Ansprüche.

[0002] Die Erfindung betrifft insbesondere ein Verfahren und eine Vorrichtung zur Abwehr von Lauschversuchen bei der Bilddaten-Übertragung an einem Selbstbedienungsterminal, das als Geldautomat ausgebildet ist, wobei eine Kamera einen Aufnahmebereich erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungsterminals bzw. des Geldautomaten abdeckt.

[0003] US 6 731 778 B1 offenbart eine Aufnahme- bzw. Fotografier-Vorrichtung für eine Transaktions-Verarbeitungseinheit, insbesondre einen Geldautomaten. Die Vorrichtung wird in und/oder an dem Geldautomaten installiert, um eine den Automaten benutzende Person zu beobachten und deren Gesicht und/oder Körper zu erfassen, damit festgestellt werden kann, ob diese Person falsche bzw. kriminelle Handlungen vornimmt. Dazu ist die Fotografier-Vorrichtung mit einem Mittel ausgestattet, welches den Feldwinkel der Kamera auf eine Vielzahl von zu fotografierenden Stellen aufteilt. Dieses Mittel kann z.B. durch einen Spiegel (s. Fig. 1 Element "18") realisiert werden, der es ermöglicht, das Gesicht und den Körper der Person in einer einzigen Aufnahme zu erfassen.

[0004] Die EP 1 914 694 A 2 befasst sich auch mit der Überwachung von Manipulationsversuchen an einem Geldautomaten oder sonstigem selbstbedienungsgerät ; allerdings geht es dort um das Problem, eine Datenübertragung, die eine Codierung betrifft, vor Ausspähen zu sichern. Dazu wird vorgeschlagen, die Datenübertragung der Codierung drahtlos, vorzugsweise verschlüsselt durchzuführen (s. dort Abs. [0014] und [0019]) oder auf bestimmte Zeitabschnitte zu beschränken (s. [0018]).

[0005] Es ist bekannt, Selbstbedienungsterminals, insbesondere Geldautomaten, durch eine Kameraüberwachung abzusichern, um kriminelle Vorgänge, wie insbesondere Sachbeschädigungen und/oder Manipulationen an den Terminals, festzustellen sowie Bildmaterial als Beweis- und Analysematerial aufzunehmen. Dazu wird mindestens eine Kamera an dem jeweiligen Selbstbedienungsterminal installiert. Diese mindestens eine Kamera liefert dann fortlaufend Bildsignale, aus denen üblicherweise digitale Bilddaten gewonnen werden, die an einen Bilddatenspeicher und entfernten Rechner bzw. Server übertragen werden, um dort ausgewertet zu werden. Insbesondere Terminals in Gestalt von Geldautomaten sind Gegenstand solcher Kameraüberwachungen. Eine typische Manipulation an Geldautomaten ist das Anbringen von sogenannten Skimming-Vorrichtungen. Hierbei werden von Tätern nachgebaute Tastaturen und/oder Kartenleser im Bedienbereich des Geldautomaten angebracht, um somit an sensitive Daten, insbesondere Kartendaten und PINs zu gelangen. In letzter Zeit haben sich Angriffsszenarien in Form von Lauschangriffen bzw. Abhörversuchen gehäuft, bei denen die Täter sich Zugang zu den von der Kamera erzeugten Bildsignalen bzw. den daraus gewonnenen Bilddaten verschaffen wollen, in dem sie die Übertragung dieser Bildsignale bzw. Bilddaten an den entsprechenden Übertragungsleitungen abgreifen (sog. "Abzapfen"). Ist ein solcher Lauschangriff erfolgreich, so kann der Täter aus den abgehörten Bildinformationen Rückschlüsse auf die von einem Kunden eingegebene PIN schließen sowie ggf. auch die Kartendaten beim Einführen der Karte in den Kartenschlitz ablesen. Somit kann der Täter ohne Einsatz von speziellen Skimming-Vorrichtungen an die sensitiven Daten gelangen.

[0006] Aufgabe der Erfindung ist es demnach, ein Verfahren und eine Vorrichtung zur effektiven Abwehr von Lauschversuchen bei der Bilddatenübertragung an einen Selbstbedienungsterminal vorzuschlagen. Insbesondere sollen ein Verfahren, eine Vorrichtung und ein damit ausgestattetes Bedienungsterminal vorgeschlagen werden, die die Bilddatenübertragung gegen derartige Lauschversuche absichern und schützen.

[0007] Gelöst wird die Aufgabe durch ein Verfahren mit den Merkmalen des Anspruchs 1 sowie durch eine Vorrichtung bzw. ein Selbstbedienungsterminal mit den Merkmalen der nebengeordneten Ansprüche 10 und 12.

[0008] Demnach wird vorgeschlagen, dass am Selbstbedienungsterminal, insbesondere in dem Aufnahmebereich der Kamera, aber auch außerhalb davon auftretende Ereignisse erkannt werden, und dass in Abhängigkeit von mindestens einem erkannten Ereignis, das einer sensitiven Bedienung des Selbstbedienungsterminals entspricht, die Erzeugung der Bildsignale an der Kamera und/oder die nachfolgende Übertragung der Bildsignale bzw. der daraus gewonnenen Bilddaten so gesteuert wird, dass die Erzeugung sensitiver Bildsignale und/oder die Übertragung sensitiver Bilddaten unterbunden wird. Demnach wird ein Ereignis erkannt, das beispielsweise die Betätigung der Tastatur und/oder das Einführen einer Karte in den Kartenschlitz darstellt, um dann davon abhängig die Erzeugung bzw. Übertragung der Bildsignale und/oder Bilddaten zu steuern. Deshalb kann selbst bei einem erfolgreichen Abzapfen von Leitungen und Übertragungsstrecken, verhindert werden, dass entsprechende sensitive Bildsignale bzw. Bilddaten überhaupt erzeugt bzw. übertragen werden. Einem Täter, dem es eventuell gelingen sollte, die Kamerasignale bzw. die daraus abgeleiteten Bilddaten abzugreifen, wird somit keinen Zugriff auf sensitive Bildsignale bzw. Bilddaten erhalten können.

[0009] Erfindungsgemäß wird auch eine das Verfahren ausführende Vorrichtung vorgeschlagen, die im Aufnahmebereich der Kamera auftretende Ereignisse mittels Auswertung der Bildsignale, der Bilddaten und/oder

von Sensorsignalen erkennt, und die in Abhängigkeit davon die Erzeugung und/oder Übertragung der Bildsignale bzw. Bilddaten steuert.

[0010] Außerdem wird ein mit einer solchen Vorrichtung ausgestattetes Selbstbedienungsterminal vorgeschlagen, das insbesondere als Geldautomat ausgebildet sein kann.

[0011] Die Unterbrechung der Erzeugung bzw. Übertragung von Bildsignalen/daten kann zeitgesteuert zumindest solange erfolgen, wie das sensitive Ereignis erkannt wird. Wiederum alternativ dazu werden in den gewonnenen Bilddaten zumindest Teilbilddaten ausgeblendet oder durch künstlich erzeugte Daten ersetzt, wenn zumindest ein Ereignis erkannt wird. In diesem Zusammenhang handelt es sich vorzugsweise um solche Teilbilddaten, die sich auf mindestens einen Teilbereich des Aufnahmebereiches beziehen, insbesondere sich auf einen ersten und zweiten Teilbereich beziehen, der eine Tastatur bzw. einen Kartenschlitz im Bedienbereich des Selbstbedienungsterminals abdeckt.

[0012] Die Ereignisse, die insbesondere im Bedienungsbereich innerhalb des Kamera-Aufnahmebereichs oder auch außerhalb davon erkannt werden, sind z.B. Bedienung einer Tastatur bzw. Einführen einer Karte. Die Ereignisse im Kamera-Aufnahmebereich können durch Auswertung der Bildsignale und/oder der Bilddaten erkannt werden. Dies kann in der erfindungsgemäßen Vorrichtung erfolgen. Alternativ dazu oder auch zusätzlich dazu können die Ereignisse durch Auswertung von mindestens einem Sensorsignal erkannt werden, das von einem Sensor zur Überwachung eines Bedienelementes im Bedienbereich des Selbstbedienungsterminals, auch außerhalb des Kamera-Aufnahmebereiches erzeugt wird. Außerdem können Ereignisse, wie z.B. das Einführen einer Karte, aus dem aktuellen Zustand des Selbstbedienungsterminals abgeleitet werden, insbesondere durch Abfrage bzw. Ablesen von Prozesszuständen bzw. Zustandsautomaten (state machines) oder dergleichen. Entsprechende Signale können dann an die erfindungsgemäße Vorrichtung gesendet werden.

[0013] Die Erfindung und die sich daraus ergebenden Vorteile werden nachfolgend von einem Ausführungsbeispiel und unter Bezugnahme auf die beiliegenden schematischen Zeichnungen beschrieben:

Fig. 1 zeigt schematisch den Bedienbereich eines Selbstbedienungsterminals und eine den Bedienbereich überwachende Kamera;

Fig. 2 zeigt in Form eines Blockschaltbildes Komponenten der Vorrichtung zur Abwehr von Lauschversuchen bei der Bilddaten-Übertragung; und

Fig. 3 zeigt das Ablaufdiagramm eines erfindungsgemäßen Verfahrens zur Abwehr von Lauschversuchen bei der Bilddaten-Übertragung.

[0014] Die Fig. 1 zeigt den Bedienbereich eines Selbstbedienungsterminals, das hier als Geldautomat ATM ausgebildet ist, wobei der Bedienbereich u.a. folgende Bedienelemente aufweist: eine Tastatur KBD zur Eingabe von Ziffern, insbesondere PIN-Nummern, mehrere Funktionstasten BTN, insbesondere zur Bestätigung von gemachten Tastatur-Eingaben, einen Bildschirm MON zur Darstellung von Bedieninformationen und einen Kartenschlitz SLT zum Einführen von Karten, insbesondere von Bankkarten. Außerdem weist der Bedienbereich noch weitere Felder, wie z.B. Schilder und Beschriftungen LBL auf. Durch mindestens eine am Bedienbereich angeordnete Kamera CAM wird der Bedienbereich überwacht, wobei die Kamera CAM einen Aufnahmebereich A0 aufweist, der den gesamten Bedienbereich abdeckt.

[0015] Beispielsweise wird nun mittels des nachfolgend beschriebenen Verfahrens und der entsprechenden Vorrichtung bei der Übertragung der Bildsignale bzw. Bilddaten eine Ausblendung bestimmter Teilbereiche A1 und/oder A2 durchgeführt, wenn ein sensitives Ereignis erkannt wird, das z.B. der Eingabe von PIN-Nummern oder dem Einführen einer Karte entspricht. Die ausgeblendeten Teilbereiche A1 und A2 beziehen sich insbesondere auf sensitive Bereiche des Aufnahmebereiches A0, hier z.B. auf den Bereich A1, der die Tastatur KBD abdeckt, sowie auf den Bereich A2, der den Kartenschlitz SLT abdeckt. Anhand der Fig. 2 und 3 wird nun das erfindungsgemäße Verfahren und die danach arbeitende Vorrichtung näher beschrieben:

[0016] Die Fig. 2 zeigt in Form eines Blockschaltbildes den Aufbau einer Vorrichtung, die insbesondere als Detektionseinheit DET ausgebildet ist, und zumindest mit einer Bildverarbeitungseinheit PRC verbunden ist, die von der Kamera CAM erzeugte Bildsignale Sa empfängt und diese verarbeitet. Die Bildverarbeitungseinheit PRC erzeugt aus den Bildsignalen Sa entsprechende digitale Bilddaten Sb und überträgt diese beispielsweise an eine Speichereinrichtung MEM. Diese Speichereinrichtung kann in einem von dem Selbstbedienungsterminal entfernten Server angeordnet sein. Zwischen der Kamera CAM und der Bildverarbeitungseinheit PRC befindet sich eine erste Verbindung Ca, über die die Bildsignale übertragen werden. Diese Verbindung Ca ist beispielsweise eine analoge Verbindung in Form eines Koaxialkabels, das entsprechende Bildsignale in Form von Videosignalen von der Kamera an die Bildverarbeitungseinheit überträgt. Vorzugsweise werden die Kamera CAM und die Bildverarbeitungseinheit PRC in einem Modul MD integriert, damit Dritte keinen direkten Zugriff auf die Verbindung Ca haben, um dort Abhörversuche vorzunehmen.

[0017] Zwischen der Bildverarbeitungseinheit PRC und dem externen Speicher MEM befindet sich eine zweite Verbindung Cb, über die die erzeugten digitalen Bilddaten Sb oder die erfindungsgemäß im Falle eines sensitiven Ereignisses veränderten digitalen Bilddaten Sb' übertragen werden. Diese Verbindung Cb stellt somit eine sichere digitale Datenübertragungsverbindung dar, die z.B. über Daten- oder Kommunikationsnetze, wie z.

B. IP-Verbindungen, bis zu entfernten Rechnern (Servern) reichen kann. Die übertragenen Bilddaten Sb bzw. Sb' werden dann empfangsseitig in dem dortigen Speicher MEM zwischengespeichert und dann einer Datenanzeige und/oder Auswertung zugeführt, um die von der Kamera erfassten Bilder auszuwerten.

[0018] Insbesondere diese zweite Verbindung Cb bietet einen potenziellen Angriffspunkt für Lauschangriffe, indem Dritte versuchen, diese Verbindung anzuzapfen. Zu Abwehr wird nun zumindest die Übertragung der digitalen Bilddaten Sb bzw. Sb' derart gesteuert, dass keine Bilddaten übertragen werden, die sensitive Vorgänge bzw. Ereignisse, wie z.B. Tastatureingaben oder das Einführen einer Bankkarte wiedergeben könnten. Die Steuerung erfolgt nach dem Verfahren, das anhand der Fig. 3 nachfolgend näher beschrieben wird.

[0019] Die Fig. 3 zeigt das Ablaufdiagramm für ein Verfahren 100 mit den Schritten 110 bis 130. In einem ersten Schritt führt die Kamera CAM Bildaufnahmen durch und erzeugt entsprechende Bildsignale Sa (siehe auch Fig. 1 und 2). Aus diesen analogen Bildsignalen werden digitale Bilddaten Sb in der Bildverarbeitungseinheit PRC erzeugt. Danach wird in einem Schritt 120 durch Auswertung der erzeugten Bilddaten festgestellt, ob ein Ereignis vorliegt, das die Bedienung von sensitiven Bereichen im Bedienbereich betreffen könnte. Beispielsweise wird anhand der Auswertung der Bilddaten Sb erkannt, dass eine Person die Tastatur KBD im Bedienbereich des Bankautomaten ATM bedient. Außerdem kann auch erkannt werden, ob eine Person eine Bankkarte in den Kartenschlitz SLT einführt. Ist dies der Fall, so folgt in einem Schritt 121 die Erzeugung eines Auslösesignals bzw. Triggers TR (siehe Fig. 2) der die Erzeugung bzw. Übertragung der Bilddaten dahingehend steuert, dass zumindest Teilbilddaten ausgeblendet bzw. ersetzt werden, die die genannten sensitiven Bildbereiche A1 bzw. A2 betreffen.

[0020] In einem nachfolgenden Schritt 122 werden dann die Bilddaten Sb' übertragen, wobei die sensitiven Bilddaten durch künstlich erzeugte Daten (Dummy-Daten) ersetzt worden sind. In einem nachfolgenden Schritt 130 erfolgt dann die Übertragung der veränderten Bilddaten Sb' über die zweite Verbindung Cb.

[0021] Wurde im Schritt 120 jedoch festgestellt, dass kein Ereignis vorliegt, so erfolgt entsprechend dem Schritt 130 eine Übertragung der Original-Bilddaten Sb, d.h. der unveränderten Bilddaten. Durch diese Maßnahme wird erreicht, dass nach wie vor eine sichere Überwachung des Selbstbedienungsterminals bzw. Bankautomaten ATM durchgeführt werden kann, dass aber im Falle von Ereignissen, die sensitiv sind, entsprechende Bilddaten nicht erzeugt bzw. nicht übertragen werden.

[0022] In einer einfachen Ausführung kann für den Fall, dass ein sensitives Ereignis erkannt wird, die Vorrichtung DET auch einen Auslöser bzw. Trigger TR* erzeugen, der die Kamera CAM direkt ansteuert, um die Erzeugung des Bildsignals Sa gänzlich zu unterbinden. In diesem Fall wird also die komplette Bildaufnahme unterdrückt.

[0023] Das Erkennen von Ereignissen kann nicht nur durch Auswertung der Bildsignale Sa bzw. der daraus gewonnenen Bilddaten Sb erfolgen, sondern kann alternativ oder zusätzlich dazu auch anhand von Sensorsignalen erfolgen. In diesem Falle ist die Vorrichtung DET mit Sensoren verbunden, die an den sensitiven Bedienelementen, wie z.B. der Tastatur KBD und/oder dem Kartenschlitz SLT angebracht sind. Der Sensor kann im einfachen Fall auch die jeweilige Taste der Tastatur selbst oder einen Detektor am Eingang des Kartenschlitzes SLT sein.

[0024] Als Kamera CAM kann eine Kamera üblicher Bauart eingesetzt werden, welche analoge oder digitale Bildaufnahmen durchführt. Die erste Verbindung Ca kann beispielsweise als Koaxialkabel für analoge Bildsignale oder beispielsweise als USB-Kabel für digitalisierte Bildsignale bzw. Bilddaten ausgeführt sein. Die Bildverarbeitung erfolgt in der Bildverarbeitungseinheit PRC, die beispielsweise als dedizierte Elektronik oder auch als Softwareprogramm, welches auf einem Personal Computer läuft, ausgeführt sein kann. Das verarbeitete Bild bzw. die gewonnenen Bilddaten werden dann über die zweite Verbindung Cb weitergeleitet zu dem Speicher MEM bzw. zu einem entfernten Rechner, insbesondere einem Server, der die Bilddaten weiter auswertet bzw. zur Anzeige bringt. Der Server befindet sich beispielsweise in einer Überwachungszentrale, die mehrere Selbstbedienungsterminals gleichzeitig überwacht.

[0025] Neben den bereits beschriebenen Maßnahmen können die übertragenen Bildsignale Sa bzw. Bilddaten Sb zusätzlich noch verschlüsselt werden, um gegen Lauschversuche Dritter noch stärker gesichert zu sein. Vorzugsweise bilden die Kamera CAM und die Bildverarbeitungseinheit PRC eine bauliche Einheit in Form eines Moduls MD. Wie oben beschrieben worden ist, werden in der Bildverarbeitung diejenigen Bereiche des Bildes ausgeblendet und/oder unkenntlich gemacht, aus welchen sich Rückschlüsse auf die PIN-Eingabe oder auf Kartendaten gewinnen lassen können. Die Veränderung der Bilddaten erfolgt beispielsweise, indem alle Pixel in den besagten Teilbereichen auf den gleichen Farb- und/oder Helligkeitswert gesetzt werden.

[0026] Die Steuerung der Erzeugung der Bildsignale bzw. Übertragung der Bilddaten kann zeitabhängig erfolgen, indem die beschriebene Ausblendung von Bilddaten nur zu solchen Zeitpunkten durchgeführt wird, wenn ein Ereignis erkannt wird. Somit wird sichergestellt, dass keine sensitiven bzw. kritischen Vorgänge, wie beispielsweise Eingaben von PIN-Nummern bzw. Einführen von Karten, aufgenommen und/oder übertragen werden. Die Festlegung der ausgeblendeten bzw. veränderten Teil-Bilddatenbereiche kann auch derart weiter ausgebildet werden, dass nur dezidierte Teilbereiche, wie etwa Schriftzüge und Ziffernangaben auf Bankkarten ausgeblendet bzw. überschrieben werden. Die Abwehr gegen Lauschversuche kann auch derart erfolgen, dass mittels eines Triggers die Bildaufnahme vollständig unterbrochen wird. Dies geschieht beispielsweise, sobald eine

Hand bzw. ein Finger sich über der Tastatur KBD befindet und somit auf den Vorgang einer PIN-Eingabe geschlossen werden kann. Das Erkennen einer solchen Situation kann durch Bilderkennungstechniken durchgeführt werden, mittels denen z.B. das Erscheinen von Hand bzw. Fingern im Aufnahmebereich, insbesondere im Bereich der Tastatur KBD, oder das Einführen einer Bankkarte in den Kartenschlitz SLT erkannt werden.

[0027] Weiterhin können zur Überprüfung, ob ein sensitives Ereignis vorliegt, neben Sensoren noch zusätzliche Informationen herangezogen werden, die in der Regel in einem Selbstbedienungsterminal vorhanden sind. Dies ist beispielsweise der aktuelle Status bezüglich des Zustandes des Selbstbedienungsterminals. So braucht beispielsweise die Hand bei der PIN-Eingabe nur dann im Bild maskiert zu werden, wenn auch tatsächlich eine PIN-Nummer eingegeben wird. Hingegen ist keine Maskierung erforderlich, wenn die Hand lediglich eine Menüsteuerung durchführt. Auch ist keine Maskierung erforderlich, solange sich eine Magnet- bzw. Chipkarte im System befindet.

[0028] Die vorgeschlagene Erfindung verhindert effektiv jeden Lauschangriff auf die Übertragung von Kamerasignalen bzw. Bilddaten an einem Selbstbedienungsterminal.

Bezugszeichenliste

[0029]

ATM	Selbstbedienungsterminal, hier als Geldautomat ausgebildet;
MON	Bildschirm
SLT	Kartenschlitz
KBD	Bedienelement in Gestalt einer Tastatur
BTN	Bedienelemente in Gestalt von Funktionstasten
LBL	Schild bzw. Beschriftung
CAM	Kamera zur Überwachung des ATM-Bedienbereichs
A0	Aufnahmebereich
A1, A2	sensitive Teilbereiche, die ausgeblendet bzw. maskiert werden
DET	Vorrichtung umfassend eine Detektionseinheit zum Erkennen sensitiver Ereignisse
PRC	Bildverarbeitungseinheit
MD	Modul mit CAM, PCR und DET
MEM	externe Speichereinrichtung (z.B. eines Servers)
TR, TR*	Steuersignale bzw. Trigger
Sa	analoges Bildsignal von CAM
Sb, Sb'	digitale Bilddaten von PRC aus dem Bildsignal Sa gewonnen
Ca, Cb	Verbindungen zur Bild-Übertragung

100 Verfahren zur Abwehr von Lauschversuchen mit Schritten 110 bis 130

Patentansprüche

1. verfahren (100) zur Abwehr von Lauschversuchen bei der Übertragung von Bilddaten (Sb), die aus Bildsignalen (Sa), die von einer an einem Selbstbedienungsterminal (ATM) installierten Kamera (CAM) erzeugt werden, gewonnen werden, wobei die Kamera (CAM) einen Aufnahmebereich (A0) erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungsterminals (ATM) abdeckt (110),
dadurch gekennzeichnet, dass
am Selbstbedienungsterminal (ATM) auftretende Ereignisse erkannt werden (120) und dass in Abhängigkeit von mindestens einem erkannten Ereignis,
das einer PIN-Eingabe oder Einführung einer karte bein Selbstbedienungsterminal entspricht, die Erzeugung der Bildsignale (Sa) und/oder die Übertragung der Bilddaten (Sb) so gesteuert wird (122, 130), dass die Erzeugung sensitiver Bildsignale und/oder die Übertragung sensitiver Bilddaten unterbunden wird.

2. Verfahren (100) nach Anspruch 1, **dadurch gekennzeichnet, dass** am Selbstbedienungsterminal (ATM) im Bedienbereich, insbesondere im Aufnahmebereich (A0) der Kamera (CAM), und/oder außerhalb davon Ereignisse erkannt werden.

3. Verfahren (100) nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** als Ereignis, die Betätigung einer Tastatur (KBD) im Bedienbereich des Selbstbedienungsterminals (ATM) erkannt wird (120).

4. Verfahren (100) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichet, dass als Ereignis, das Einführen einer Karte in einen Kartenschlitz (SLT) im Bedienbereich des Selbstbedienungsterminals (ATM) erkannt wird (120).

5. Verfahren (100) nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** in den gewonnenen Bilddaten (Sb) zumindest Teilbilddaten (Sb') ausgeblendet oder durch künstlich erzeugte Daten ersetzt werden, wenn zumindest ein Ereignis erkannt wird.

6. Verfahren (100) nach Anspruch 5, **dadurch gekennzeichnet, dass** die Teilbilddaten (Sb') sich auf mindestens einen Teilbereich (A1, A2) des Aufnahmebereichs (A0) beziehen, insbesondere sich auf einen ersten und/oder zweiten Teilbereich (A1, A2) beziehen, der eine Tastatur (KBD) und/oder einen Kartenschlitz (SLT) im Bedienbereich des Selbstbedienungsterminals (ATM) abdeckt.

7. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Ereignisse durch Auswertung der Bildsignale (Sa) und/oder der Bilddaten (Sb) erkannt werden (120).

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Ereignisse durch Auswertung von mindestens einem Sensorsignal erkannt werden, das von einem Sensor zur Überwachung eines Bedienelementes (KBD, SLT) im Bedienbereich des Selbstbedienungsterminals (ATM) erzeugt wird.

9. Verfahren (100) nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** zur Steuerung der Erzeugung der Bildsignale (Sa) und/oder der Übertragung der Bilddaten (Sb) mindestens ein Auslösesignal (TR, TR*) erzeugt wird (121), wenn ein Ereignis erkannt wird.

10. Vorrichtung (DET) zur Abwehr von Lauschversuchen bei der Übertragung von Bilddaten (Sb), die aus Bildsignalen (Sa), die eine an einem Selbstbedienungsterminal (ATM) installierte Kamera (CAM) erzeugt, gewonnen werden, wobei die Kamera (CAM) einen Aufnahmebereich (A0) erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungsterminal (ATM) abdeckt (110), **dadurch gekennzeichnet, dass**
die Vorrichtung (DET) Signale über an dem Selbstbedienungsterminal (ATM) auftretende Ereignisse erhält und/oder im Aufnahmebereich (A0) auftretende Ereignisse mittels Auswertung der Bildsignale (Sa), der Bilddaten (Sb) und/oder von Sensorsignalen erkennt und in Abhängigkeit von mindestens einem erkannten Ereignis, das einer PIN-Eingabe oder Einführung einer karte bein selbstbedienungsterminal entspricht, die Erzeugung der Bildsignale (Sa) und/oder die Übertragung der Bilddaten (Sb) so steuert, dass die Erzeugung sensitiver Bildsignale und/oder die Übertragung sensitiver Bilddaten unterbunden wird.

11. Vorrichtung (DET) nach Anspruch 10, **dadurch gekennzeichnet, dass** die Vorrichtung (DET) mit der Kamera (CAM) und/oder mit einer Bildverarbeitungseinheit (PRC) verbunden ist, die aus den Bildsignalen (Sa) die Bilddaten (Sb) erzeugt oder ableitet.

12. Selbstbedienungsterminal (ATM) mit einer Vorrichtung (DET) zur Abwehr von Lauschversuchen bei der Übertragung von Bilddaten (Sb), die aus Bildsignalen (Sa), die eine an dem Selbstbedienungsterminal (ATM) installierte Kamera (CAM) erzeugt, gewonnen werden, wobei die Kamera (CAM) einen Aufnahmebereich (A0) erfasst, der einen zu überwachenden Bedienbereich des Selbstbedienungsterminal (ATM) abdeckt (110),
dadurch gekennzeichnet, dass
die Vorrichtung (DET) Signale über an dem Selbstbedienungsterminal (ATM) auftretende Ereignisse erhält und/oder im Aufnahmebereich (A0) auftretende Ereignisse mittels Auswertung der Bildsignale (Sa), der Bilddaten (Sb) und/oder von Sensorsignalen erkennt und in Abhängigkeit von mindestens einem erkannten Ereignis, das einer PIN-Eingabe oder Einführung einer karte bein Selbstbedienungsterminal entspricht, die Erzeugung der Bildsignale (Sa) und/oder die Übertragung der Bilddaten (Sb) so steuert, dass die Erzeugung sensitiver Bildsignale und/oder die Übertragung sensitiver Bilddaten unterbunden wird.

13. Selbstbedienungsterminal (ATM) nach Anspruch 12,
dadurch gekennzeichnet, dass das Selbstbedienungsterminal (ATM) eine mit der Kamera (CAM) über eine erste Verbindung (Ca) verbundene Bildverarbeitungseinheit (PRC) aufweist, die aus den Bildsignalen (Sa) die Bilddaten (Sb) erzeugt oder ableitet.

14. Selbstbedienungsterminal (ATM) nach Anspruch 13,
dadurch gekennzeichnet, dass die Bildverarbeitungseinheit (PRC) die Bilddaten (Sb) über eine zweite Verbindung (Cb) an einen internen oder externen Datenspeicher (MEM) überträgt.

15. Selbstbedienungsterminal (ATM) nach einem der Ansprüche 11 bis 13, **dadurch gekennzeichnet, dass** die Kamera (CAM) und die Bildverarbeitungseinheit (PRC) in einem Modul (MD) integriert sind.

16. Selbstbedienungsterminal (ATM) nach einem der Ansprüche 11 bis 14, **dadurch gekennzeichnet, dass** das Selbstbedienungsterminal als ein Geldautomat (ATM) ausgebildet ist, der einen Bedienbereich mit einer Tastatur (KBD) und/oder einem Kartenschlitz (SLT) aufweist.

Claims

1. Method (100) for protecting against eavesdropping attempts during the transmission of image data (Sb) that are obtained from image signals (Sa) that are produced by a camera (CAM) installed at a self-service terminal (ATM), wherein the camera (CAM) captures a recording area (A0) that covers (110) a user area, that is to be monitored, of the self-service terminal (ATM), **characterized in that** events taking place at the self-service terminal (ATM) are detected (120) and **in that**, on the basis of at least one detected event that corresponds to PIN input or inser-

tion of a card on the self-service terminal, the production of the image signals (Sa) and/or the transmission of the image data (Sb) is/are controlled (122, 130) such that the production of sensitive image signals and/or the transmission of sensitive image data is/are stopped.

2. Method (100) according to Claim 1, **characterized in that** events are detected at the self-service terminal (ATM) in the user area, particularly in the recording area (A0) of the camera (CAM), and/or outside thereof.

3. Method (100) according to Claim 1 or 2, **characterized in that** the event detected (120) is the operation of a keyboard (KBD) in the user area of the self-service terminal (ATM).

4. Method (100) according to one of Claims 1 to 3, **characterized in that** the event detected (120) is the insertion of a card into a card slot (SLT) in the user area of the self-service terminal (ATM).

5. Method (100) according to one of Claims 1 to 4, **characterized in that** at least image data elements (Sb') are hidden or are replaced by artificially produced data in the obtained image data (Sb) when at least one event is detected.

6. Method (100) according to Claim 5, **characterized in that** the image data elements (Sb') relate to at least one subarea (A1, A2) of the recording area (A0), particularly relate to a first and/or second subarea (A1, A2) that covers a keyboard (KBD) and/or a card slot (SLT) in the user area of the self-service terminal (ATM).

7. Method (100) according to one of the preceding claims, **characterized in that** the events are detected (120) by evaluating the image signals (Sa) and/or the image data (Sb).

8. Method according to one of the preceding claims, **characterized in that** the events are detected by evaluating at least one sensor signal that is produced by a sensor for monitoring a user element (KBD, SLT) in the user area of the self-service terminal (ATM).

9. Method (100) according to one of the preceding claims, **characterized in that** control of the production of the image signals (Sa) and/or of the transmission of the image data (Sb) involves at least one trigger signal (TR, TR*) being produced (121) when an event is detected.

10. Apparatus (DET) for protecting against eavesdropping attempts during the transmission of image data (Sb) that are obtained from image signals (Sa) that a camera (CAM) installed at a self-service terminal (ATM) produces, wherein the camera (CAM) captures a recording area (A0) that covers (110) a user area, that is to be monitored, of the self-service terminal (ATM), **characterized in that**
the apparatus (DET) receives signals about events taking place at the self-service terminal (ATM) and/or detects events taking place in the recording area (A0) by means of evaluation of the image signals (Sa), the image data (Sb) and/or sensor signals and, on the basis of at least one detected event that corresponds to PIN input or insertion of a card on the self-service terminal, controls the production of the image signals (Sa) and/or the transmission of the image data (Sb) such that the production of sensitive image signals and/or the transmission of sensitive image data is/are stopped.

11. Apparatus (DET) according to Claim 10, **characterized in that** the apparatus (DET) is connected to the camera (CAM) and/or to an image processing unit (PRC) that produces or derives the image data (Sb) from the image signals (Sa).

12. Self-service terminal (ATM) having an apparatus (DET) for protecting against eavesdropping attempts during the transmission of image data (Sb) that are obtained from image signals (Sa) that a camera (CAM) installed at the self-service terminal (ATM) produces, wherein the camera (CAM) captures a recording area (A0) that covers (110) a user area, that is to be monitored, of the self-service terminal (ATM), **characterized in that**
the apparatus (DET) receives signals about events taking place at the self-service terminal (ATM) and/or detects events taking place in the recording area (A0) by means of evaluation of the image signals (Sa), the image data (Sb) and/or sensor signals and, on the basis of at least one detected event that corresponds to pin input or insertion of a card on the self-service terminal, controls the production of the image signals (Sa) and/or the transmission of the image data (Sb) such that the production of sensitive image signals and/or the transmission of sensitive image data is/are stopped.

13. Self-service terminal (ATM) according to Claim 12, **characterized in that** the self-service terminal (ATM) has an image processing unit (PRC) that is connected to the camera (CAM) via a first connection (Ca) and that produces or derives the image data (Sb) from the image signals (Sa).

14. Self-service terminal (ATM) according to Claim 13, **characterized in that** the image processing unit (PRC) transmits the image data (Sb) to an internal or external data memory (MEM) via a second con-

nection (Cb).

15. Self-service terminal (ATM) according to one of Claims 11 to 13, **characterized in that** the camera (CAM) and the image processing unit (PRC) are integrated in one module (MD).

16. Self-service terminal (ATM) according to one of Claims 11 to 14, **characterized in that** the self-service terminal is in the form of an automated teller machine (ATM) that has a user area having a keyboard (KBD) and/or a card slot (SLT).

Revendications

1. Procédé (100) contre les tentatives d'intrusion lors de la transmission de données d'images (Sb) qui sont obtenues à partir de signaux d'images (Sa) générées par une caméra (CAM) installée sur un terminal en libre service (ATM), dans lequel la caméra (CAM) détecte une zone d'acquisition (A0) couvrant (110) une zone d'utilisation à surveiller du terminal en libre service (ATM),
caractérisé en ce que des événements se produisant sur le terminal en libre service (ATM) sont détectés (120) et **en ce que** la génération des signaux d'image (Sa) et/ou la transmission des données d'image (Sb) est commandée (122, 130) en fonction d'au moins un événement correspondant à la saisie d'un code PIN ou à l'introduction d'une carte sur le terminal en libre service, de manière à empêcher la génération de données d'images sensibles et/ou la transmission de données d'image sensibles.

2. Procédé (100) selon la revendication 1, **caractérisé en ce que** des événements peuvent être détectés sur le terminal en libre service (ATM) dans la zone d'utilisation, notamment dans la zone d'acquisition (A0) de la caméra (CAM) et/ou à l'extérieur de celle-ci.

3. Procédé (100) selon la revendication 1 ou 2, **caractérisé en ce que** l'actionnement d'un clavier (KBD) dans la zone d'utilisation du terminal en libre service (ATM) est détecté (120) en tant qu'événement.

4. Procédé (100) selon l'une quelconque des revendications 1 à 3, **caractérisé en ce que** l'introduction d'une carte dans une fente pour cartes (SLT) dans la zone d'utilisation du terminal en libre service (ATM) est détectée (120) en tant qu'événement.

5. Procédé (100) selon les revendications 1 à 4, **caractérisé en ce qu'**au moins des données d'images partielles (Sb') sont masquées ou sont remplacées par des données générées artificiellement lorsqu'au moins un événement est détecté dans les données d'images obtenues (Sb).

6. Procédé (100) selon la revendication 5, **caractérisé en ce que** les données d'images partielles (Sb') concernent au moins une zone partielle (A1, A2) de la zone d'acquisition (A0), et concernent plus particulièrement une première et/ou une seconde zone partielle (A1, A2) qui couvre un clavier (KBD) et/ou une fente pour cartes (SLT) dans la zone d'utilisation du terminal en libre service (ATM).

7. Procédé (100) selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les événements sont détectés (120) par évaluation des signaux d'images (Sa) et/ou des données d'images (Sb).

8. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les événements sont détectés par évaluation d'au moins un signal de capteur qui est généré par un capteur destiné à surveiller un événement d'utilisation (KBD, SLT) dans la zone d'utilisation du terminal en libre service (ATM) .

9. Procédé (100) selon l'une quelconque des revendications précédentes, **caractérisé en ce qu'**au moins un signal de déclenchement (TR, TR*) est généré (121) pour commander la génération des signaux d'images (Sa) et/ou la transmission des données d'images (Sb) lorsqu'un événement est détecté.

10. Dispositif (DET) contre les tentatives d'intrusion lors de la transmission de données d'images (Sb) qui sont obtenues à partir de signaux d'images (Sa) générés par une caméra (CAM) installée sur un terminal en libre service (ATM), dans lequel la caméra (CAM) détecte une zone d'acquisition (A0) couvrant (110) une zone d'utilisation à surveiller du terminal en libre service (ATM),
caractérisé en ce que le dispositif (DET) obtient des signaux concernant des événements se produisant sur le terminal en libre service (ATM) et/ou détecte des événements se produisant dans la zone d'acquisition (A0) par évaluation des signaux d'images (Sa), des données d'images (Sb) et/ou des signaux de capteurs et commande la génération de signaux d'images (Sa) et commande la transmission des données d'images (Sb) en fonction d'au moins un événement détecté correspondant à la saisie d'un code PIN ou à l'introduction d'une carte sur le terminal en libre service, de manière à empêcher la génération de signaux d'images sensibles et/ou la transmission de données d'images sensibles.

11. Dispositif (DET) selon la revendication 10, **caractérisé en ce que** le dispositif (DET) est connecté à la

caméra (CAM) et/ou à une unité de traitement d'image (PRC) qui génère ou déduit les données d'images (Sb) à partir des signaux d'images (Sa).

12. Terminal en libre service (ATM) comportant un dispositif (DET) contre les tentatives d'intrusion lors de la transmission de données d'images (Sb) qui sont obtenues à partir de signaux d'images (Sa) générés par une caméra (CAM) installée sur le terminal en libre service (ATM), dans lequel la caméra (CAM) détecte une zone d'acquisition (A0) qui couvre (110) une zone d'utilisation à surveiller du terminal en libre service (ATM),
caractérisé en ce que le dispositif (DET) obtient des signaux concernant des événements se produisant sur le terminal en libre service (ATM) et/ou détecte des événements se produisant dans la zone d'acquisition (A0) par évaluation des signaux d'images (Sa), des données d'images (Sb) et/ou de signaux de capteurs et commande la génération des signaux d'image (Sa) et/ou la transmission des données d'image (Sb) en fonction d'au moins un événement détecté qui correspond à une saisie de code PIN ou à l'introduction d'une carte sur le terminal en libre service, de manière à empêcher la génération de signaux d'images sensibles et/ou la transmission de données d'image sensibles.

13. Terminal en libre service (ATM) selon la revendication 12,
caractérisé en ce que le terminal en libre service (ATM) comprend une unité de traitement d'image (PRC) connectée à la caméra (CAM) par l'intermédiaire d'une première liaison (Ca), laquelle unité de traitement d'image génère ou déduit les données d'images (Sb) à partir des signaux d'images (Sa).

14. Terminal en libre service (ATM) selon la revendication 13,
caractérisé en ce que l'unité de traitement d'image (PRC) transmet les données d'images (Sb) par l'intermédiaire d'une seconde liaison (Cb) à une mémoire de données interne ou externe (MEM).

15. Terminal en libre service (ATM) selon l'une quelconque des revendications 11 à 13,
caractérisé en ce que la caméra (CAM) et l'unité de traitement d'image (PRC) sont intégrées dans un module (MD) .

16. Terminal en libre service (ATM) selon l'une quelconque des revendications 11 à 14,
caractérisé en ce que le terminal en libre service est réalisé sous la forme d'un distributeur automatique de billets (ATM) qui comprend une zone d'utilisation munie d'un clavier (KBD) et/ou d'une fente pour cartes (SLT).

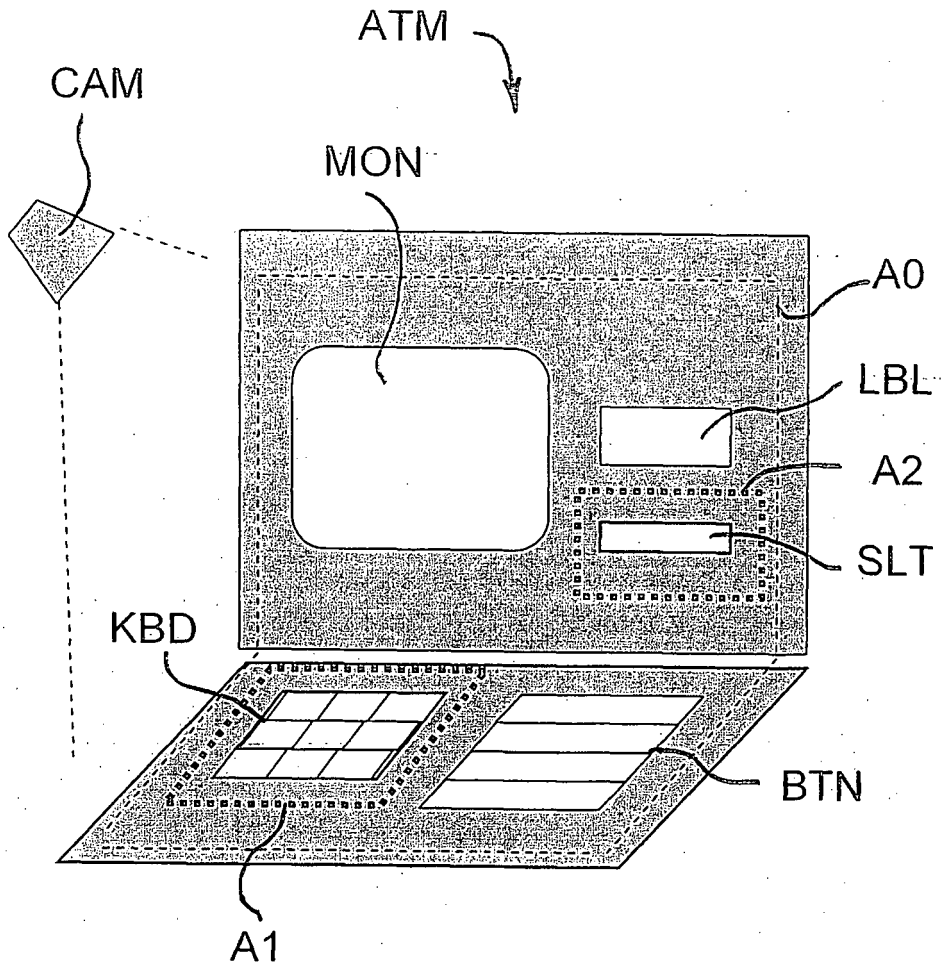

Fig. 1

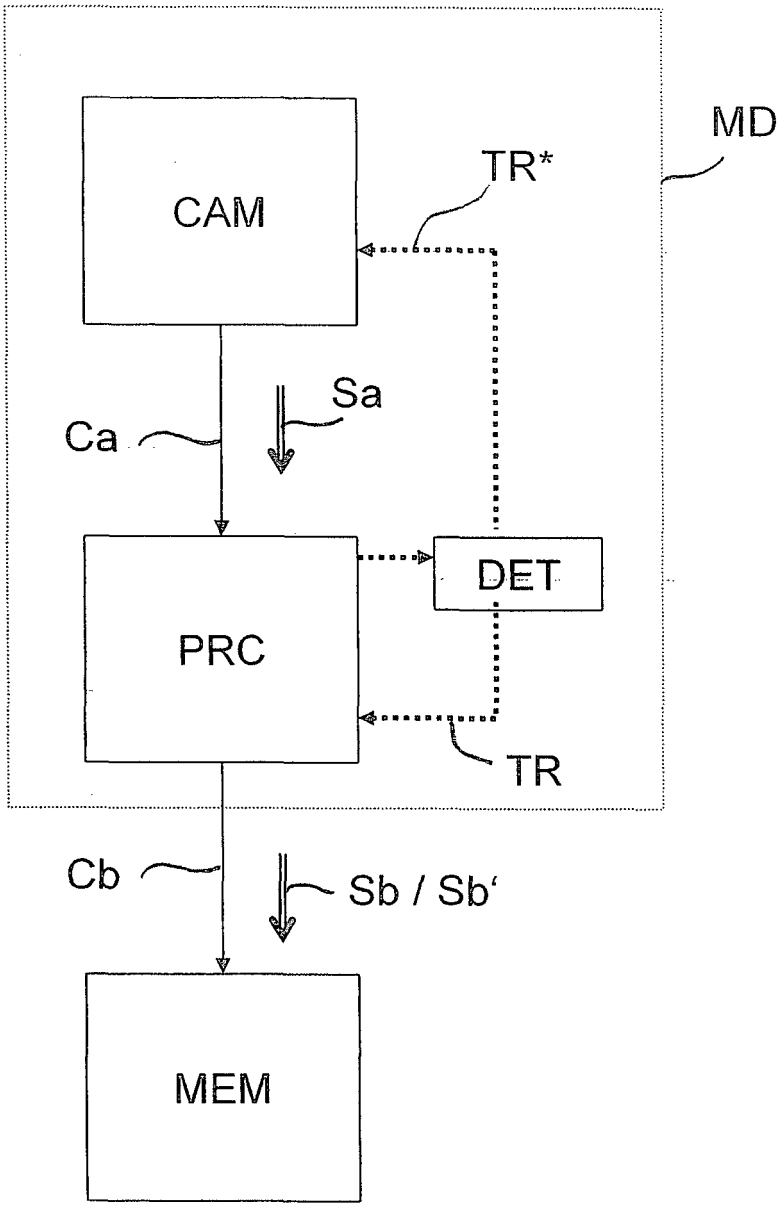

Fig. 2

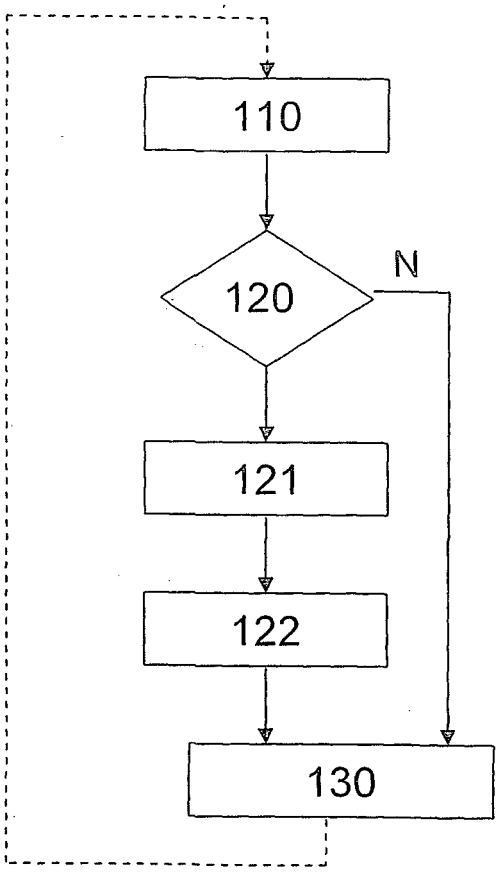

Fig. 3

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

- US 6731778 B1 **[0003]**
- EP 1914694 A2 **[0004]**