(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 600 30 739 T2** 2007.09.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 210 695 B1**
(21) Deutsches Aktenzeichen: **600 30 739.5**
(86) PCT-Aktenzeichen: **PCT/SE00/01472**
(96) Europäisches Aktenzeichen: **00 948 465.0**
(87) PCT-Veröffentlichungs-Nr.: **WO 2001/011577**
(86) PCT-Anmeldetag: **11.07.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **15.02.2001**
(97) Erstveröffentlichung durch das EPA: **05.06.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **13.09.2006**
(47) Veröffentlichungstag im Patentblatt: **06.09.2007**

(51) Int Cl.[8]: ***G07F 7/10*** (2006.01)
G06F 12/14 (2006.01)
G06K 19/073 (2006.01)

(30) Unionspriorität:

9902846	**06.08.1999**	**SE**
150438 P	**24.08.1999**	**US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Precise Biometrics AB, Lund, SE

(72) Erfinder:
WIEBE, Linus, S-211 56 Malmö, SE

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, 80538 München

(54) Bezeichnung: **ÜBERPRÜFUNG DER ZUGANGSBERECHTIGUNG**

Beschreibung

ÜBERPRÜFUNG DER ZUGANGSBERECHTIGUNG

Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft ein System zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen auf Basis von biometrischen Daten. Die Erfindung betrifft außerdem einen Datenträger, eine Verarbeitungseinheit und ein Verfahren zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen, die auf einem Datenträger gespeichert sind, auf Basis von biometrischen Daten.

Hintergrund der Erfindung

[0002] Der Zugang zu Informationen, zu einem Raum oder Ähnlichem muss in vielen Fällen auf bestimmte Einzelpersonen beschränkt werden. Dies gilt zum Beispiel, wenn elektronische Geldtransaktionen über das Internet erfolgen, wenn in einem Krankenhaus der Zugang zu Krankenakten zu beschränken ist oder wenn lediglich bestimmte Einzelpersonen an einem Arbeitsplatz Zugang zu bestimmten Informationen oder bestimmten Räumen haben dürfen.

[0003] Zu diesem Zweck wird oft von dem Gebrauch gemacht, was als intelligente Karten oder Chip-Karten bezeichnet wird. Eine Chip-Karte kann als eine Karte in der Größe einer Kundenkarte beschrieben werden, die einen eingebauten Prozessor oder eine Signalverarbeitungseinrichtung, einen Speicher und eine Kommunikationsschnittstelle aufweist. Vertrauliche Informationen sind auf allen Chip-Karten gespeichert, die in den vorgenannten Kontexten verwendet werden. Die vertraulichen Informationen bestehen aus einem oder mehreren Teilen. Ein erster Teil der vertraulichen Informationen ist eine sogenannte Schablone, die auf jeder Chip-Karte gespeichert ist, und kann als vorab gespeicherte Bezugsinformationen zu dem Benutzer der Karte beschrieben werden. Mit diesen Bezugsinformationen wird dann jedes Mal, wenn der Benutzer seine Berechtigung zum Benutzen der Karte verifizieren möchte, ein Vergleich durchgeführt. Die Schablone ist des Weiteren die einzige vertrauliche Information, die auf der Chip-Karte verfügbar sein muss, wenn sie als reine „Schlüsselkarte" verwendet werden soll und um ein „Ja" oder „Nein" zum Beispiel für physischen Zugang zu einem Raum zu erzeugen.

[0004] Ein zweiter Teil der vertraulichen Informationen ist auf Karten verfügbar, die nicht als „Schlüsselkarten", sondern als absolutere Informationsträger verwendet werden. Der zweite Teil der vertraulichen Informationen besteht dann aus Rechnerdateien, die Daten des Typs enthalten können, der mit Hilfe von Einführung angegeben wird und zu dem nur der Kartenbenutzer Zugang hat. Wenn der Kartenbenutzer verifizieren möchte, dass er die Zugangsberechtigung zu den vertraulichen Informationen, die in den Rechnerdateien auf der Chip-Karte gespeichert sind, hat, platziert er die Karte in einem Endgerät und gibt einen PIN-Code (PIN = Personal Identification Number) ein. Der PIN-Code ist auf 16 Byte beschränkt und besteht normalerweise aus vier Ziffern zwischen Null und Neun, die mit der Schablone, die auf der Karte gespeichert ist, abgeglichen werden. Wenn der PIN-Code der Schablone entspricht, „wird die Karte entriegelt", d. h. der Benutzer erhält Zugang zu den Rechnerdateien, die die vertraulichen Informationen enthalten. Dies unterscheidet sich von dem Fall, bei dem die Karte als eine reine „Schlüsselkarte" verwendet wird und lediglich ein „Ja" oder „Nein" in Reaktion auf das Abgleichen mit der Schablone erzeugt wird.

[0005] PIN-Codes werden derzeit in vielen Situationen verwendet und viele Leute empfinden es als schwierig, sich eine Reihe von unterschiedlichen PIN-Codes zu merken. Daher entscheiden sich viele Leute dafür, denselben PIN-Code in einer Reihe von unterschiedlichen Situationen zu verwenden, wodurch die Sicherheit herabgesetzt wird. Aus diesem Grund und im Hinblick auf weiter steigende Sicherheit wurden alternative Lösungen vorgelegt, bei denen ein Benutzer stattdessen sich selbst mit Hilfe von biometrischen Informationen identifiziert. Mit biometrischen Informationen sind Informationen gemeint, die für den Benutzer körperbezogen und personenspezifisch sind und die, im Kontext der vorliegenden Erfindung, aus dem Muster der Finger des Benutzers bestehen. Ein Verfahren, bei dem ein Benutzer sich selbst mit Hilfe von biometrischen Informationen identifiziert, läuft nach dem Stand der Technik typischerweise wie folgt ab: Der Benutzer platziert seine Chip-Karte in einem Endgerät und einen Finger auf einem Sensor, der ein digitales Bild, d. h. eine digitale Darstellung, seines Fingers erzeugt. Das digitale Bild des Fingers geht weiter zu einem externen Prozessor, zum Beispiel ein Personalcomputer, wo es vorverarbeitet wird. Bei dem Vorverarbeiten wird die Menge an Informationen in dem Bild so verringert, dass zum Beispiel ein binarisiertes Bild oder Teile eines binarisierten Bildes erzeugt werden. Ein entsprechendes vorverarbeitetes Bild wurde als eine Schablone auf der Karte gespeichert. Der externe Prozessor sammelt die Schablone von der Karte und vergleicht dies mit dem vorverarbeiteten Bild des Fingers. Bei Entsprechung sendet der externe Prozessor einen PIN-Code zu der Karte. Dieser PIN-Code agiert als ein Schlüssel und gewährt Zugang zu den vertraulichen Informationen, die in dem Speicher der Karte gespeichert sind. Wenn die Schablone und die vorverarbeiteten Bildinformationen nicht einander entsprechen, wird kein PIN-Code gesendet und der Benutzer kann nicht auf die Rechnerdateien mit den vertraulichen Informationen auf der Karte zugreifen.

[0006] Selbst dann, wenn Biometrie verwendet wird, so dass der Benutzer keinen PIN-Code verwenden muss, wird immer noch ein PIN-Code in der letzten Stufe des Verifizierungsprozesses gesendet, da dieser PIN-Code für das „Entriegeln" spezifischer Dateien auf der Chip-Karte, die vertrauliche Informationen enthalten, erforderlich ist. Daher muss der PIN-Code entweder in der Software für die Anwendung, die mit der Karte kommuniziert, oder in einer Hardware in der Einheit, in der die Karte gelesen und geschrieben wird, festcodiert sein. Folglich wird trotz der Verwendung von Biometrie keine signifikante Steigerung der Sicherheit erreicht, da immer noch ein Risiko besteht, dass jemand auf die Rechnerdateien mit vertraulichen Informationen auf der Karte zugreift, indem der PIN-Code zu der Karte gesendet wird.

[0007] Außerdem müssen in dem Fall, bei dem die einzige Handlung der Chip-Karte darin besteht, ein Ja oder Nein zu erzeugen, die Informationen auf der Karte verschlüsselt werden, um garantieren zu können, dass das Ja/Nein, das gesendet wird, für jede Karte oder Sendung eindeutig ist. Dies verursacht dieselben Probleme wie oben beschrieben, da der Schlüssel für Verschlüsselung irgendwo gespeichert werden muss.

[0008] Ein weiteres Problem besteht darin, dass die Schablone, mit der der Abgleich erfolgt, von der Karte in den externen Prozessor, in dem der Vergleich mit den biometrischen Daten des Benutzers stattfindet, eingelesen werden muss. Erstens ist dies ein Sicherheitsrisiko und zweitens gibt es Richtlinien, die in manchen Ländern von Computersicherheitsbehörden herausgegeben wurden, in denen empfohlen wird, dass eine biometrische Schablone niemals die Chip-Karte verlassen sollte.

[0009] Eine Lösung der vorgenannten Probleme wird in dem schwedischen Patent Nr. 8101707-1 dargestellt, das einen Datenträger des Kundenkartentyps offenbart, der mit Verifizierungsausrüstung ausgestattet ist, die einen Sensor umfasst, auf den ein Benutzer einen seiner Finger platziert. Der Sensor zeichnet Papillarlinieninformationen von dem Finger des Benutzers auf und berechnet eine Identifizierungsbitfolge, die mit einer zuvor gespeicherten Bezugsbitfolge verglichen wird. Wenn die Bittfolgen miteinander übereinstimmen, wird ein Annahmesignal erzeugt, das eine Anzeigeeinrichtung oder eine Verbindungseinrichtung aktivieren kann, die den Datenträger verwendbar macht.

[0010] Auch wenn diese Lösung die Verwendung von PIN-Codes beseitigt und die Schablone jederzeit auf der Karte bleiben lässt, bleiben weiterhin bestimmte Nachteile bestehen. Zum Beispiel ist es relativ kostspielig, die Karte für eine große Anzahl von Benutzern allgemein verwendbar zu machen, da sie eine große Anzahl von Bauteilen enthält und speziell hergestellt werden muss. Auf Grund der großen Anzahl von Bauteilen und der Tatsache, dass alle Operationen auf der Karte ausgeführt werden, steigt außerdem die Wahrscheinlichkeit, dass die Karte Störungen unterliegt. Des Weiteren ist es schwierig, den Sensor auf der Karte gegen äußere mechanische Wirkung zu schützen.

[0011] EP-0 864 996 A2 offenbart einige unterschiedliche merkmalbasierte Fingerabdruck-Abgleichalgorithmen, bei denen Merkmalwerte als registrierte Daten in einem Speicher einer tragbaren Elektronikvorrichtung gespeichert werden und bei denen Merkmale eines eingegebenen Fingerabdrucks zu der tragbaren Elektronikvorrichtung gesendet werden und darin mit den registrierten Daten abgeglichen werden.

[0012] DE-198 11 332 A1 offenbart einen merkmalbasierten Fingerabdruck-Abgleichalgorithmus, bei dem die Position (x-, y-Koordinaten) jedes Merkmals von einer Chip-Karte zu einer Verarbeitungsvorrichtung gesendet wird und wobei die Verarbeitungsvorrichtung antwortet, indem sie für jedes Merkmal einen Typindikator sendet, der in der Chip-Karte zum Vergleich mit dem gespeicherten Typindikator des jeweiligen Merkmals verwendet wird.

Zusammenfassung der Erfindung

[0013] Eine Aufgabe der vorliegenden Erfindung besteht daher darin, die vorgenannten Probleme zu umgehen oder wenigstens zu mildem und ein alternatives System zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen bereitzustellen.

[0014] Nach der Erfindung wird diese Aufgabe durch ein System, einen tragbaren Datenträger, eine Verarbeitungseinheit und Verfahren erfüllt, die die Merkmale aufweisen, die in angehängten Nebenansprüchen definiert werden, wobei bevorzugte Ausführungen in angehängten Unteransprüchen dargelegt werden.

[0015] Die Erfindung wird durch den jeweiligen Nebenanspruch definiert.

[0016] Der Ausdruck „vertrauliche Informationen" ist in einem sehr breiten Sinn auszulegen. Die vertraulichen Informationen können Informationen, die auf dem eigentlichen Datenträger in der Form von Rechnerdateien gespeichert sind; ein „Schlüssel", der die Verwendung des Datenträgers ermöglicht, um zum Beispiel eine Tür eines Raums zu öffnen und dem Benutzer physischen Zugang zu Informationen eines Typs zu gewähren, der nicht zu denen gehört, die auf dem eigentlichen Datenträger gespeichert werden können; und unterschiedliche Typen sogenannter digitaler Zertifikate sein. Mit biometrischen Daten sind Daten gemeint, die eine personenspezifische Cha-

rakteristik einer Einzelperson darstellen. Beispiele für solche Daten können das Muster der Finger der Einzelperson sein. Der Datenträger, auf dem die vertraulichen Informationen gespeichert sind, kann in einer großen Anzahl unterschiedlicher Ausführungen bestehen. Die einzigen gemeinsamen Merkmale, die zwischen den unterschiedlichen Ausführungen erforderlich sind, bestehen darin, dass er einen Speicher, eine Signalverarbeitungseinrichtung, wie einen Prozessor, ein feldprogrammierbares Gate-Array (FPGA) oder einen anwendungsspezifischer Schaltkreis (ASIC), und eine Kommunikationseinrichtung, mit deren Hilfe er mit einer externen Verarbeitungseinheit kommunizieren kann, enthalten sollte. Damit der Datenträger in so vielen Situationen wie möglich verwendet werden kann, ist es wichtig, dass er tragbar ist, d. h. dass ein Benutzer in der Lage sein sollte, den Datenträger auf eine einfache Weise zu tragen, ohne zusätzliche Hilfen zu benötigen.

[0017] Nach der Erfindung soll der Datenträger daher zusammen mit einer Verarbeitungseinheit verwendet werden, die eine Signalverarbeitungseinrichtung enthält, die dazu eingerichtet ist, aktuelle biometrische Daten der Person vorzuverarbeiten, die bei einer bestimmten Gelegenheit den Datenträger zusammen mit der Verarbeitungseinheit verwendet, um Zugang zu den vertraulichen Informationen zu erhalten. Die Bezeichnung Vorverarbeitung wird hier somit in einem weiten Sinn verwendet und soll alle Typen von Signalverarbeitung an den aktuellen biometrischen Daten umfassen, die zum Zweck haben, eine ausreichende Menge an Informationen aus den biometrischen Daten zu extrahieren, um einen sicheren Vergleich mit vorgespeicherten biometrischen Bezugsdaten in dem Speicher des Datenträgers durchführen zu können. Die Signalverarbeitungseinrichtung des Datenträgers ist des Weiteren zum Durchführen dieses Vergleichs eingerichtet. Mit aktuellen biometrischen Daten ist gemeint, dass der Benutzer die biometrischen Daten dem System bei jeder Gelegenheit vorlegen muss, wenn er Zugang zu den vertraulichen Informationen erhalten möchte.

[0018] Durch das Durchführen der Prüfung der Zugangsberechtigung auf dem Datenträger muss kein PIN-Code in der Verarbeitungseinheit erzeugt und zu dem Datenträger übertragen werden. Stattdessen werden die vorverarbeiteten biometrischen Daten übertragen, die viel schwieriger zu fälschen sind, da sie komplexer sind als ein gewöhnlicher PIN-Code.

[0019] Auf Grund der Vorverarbeitung in der externen Verarbeitungseinheit kann der Datenträger ein kostengünstiger Standardtyp sein, wie eine Java-Karte oder eine MULTOS-Karte, und muss nicht speziell hergestellt werden und eine große Anzahl von Bauteilen enthalten, wie dies bei dem Stand der Technik der Fall ist. Lediglich das Betriebssystem auf dem Datenträger hat Zugang zu den biometrischen Bezugsdaten und anderen vertraulichen Informationen, die darauf gespeichert sind. Dies impliziert außerdem, dass die biometrischen Bezugsdaten in dem Speicher des Datenträgers den Datenträger nicht verlassen müssen, um mit den vorverarbeiteten biometrischen Daten verglichen zu werden. Die endgültige Entscheidung, ob die Zugangsberechtigung zu den vertraulichen Informationen besteht oder nicht, wird somit durch das Betriebssystem auf dem eigentlichen Datenträger getroffen. Auch dies sorgt für eine weitere Steigerung der Sicherheit.

[0020] Nach einer bevorzugten Ausführung bestehen die vorverarbeiteten biometrischen Daten und die biometrischen Bezugsdaten aus digitalen Darstellungen eines personenspezifischen Parameters. Mit einer digitalen Darstellung eines personenspezifischen Parameters ist eine Aufzeichnung in digitaler Form einer körperbezogenen Charakteristik, die in gewisser Weise für eine Einzelperson eindeutig ist, gemeint. Ein Beispiel dafür ist ein digitales Bild des Musters an den Fingern der Einzelperson.

[0021] Die digitalen Darstellungen bestehen aus digitalen Bildern. Die digitalen Bilder können mit Hilfe eines optischen Sensors, eines kapazitiven Sensors oder auf eine andere Weise aufgezeichnet werden. Die Hauptsache ist, dass die personenspezifischen Informationen in dem digitalen Bild aufgezeichnet werden. Der Vorteil der Verwendung digitaler Bilder besteht darin, dass sie schnell und einfach aufgezeichnet werden können und auf unterschiedliche Weisen einfach verarbeitet werden können.

[0022] Wenn ein digitales Bild die digitale Darstellung bildet, ist die Signalverarbeitungseinrichtung der Verarbeitungseinheit vorteilhafterweise bei der Vorverarbeitung zum Durchführen einer Binarisierung des digitalen Bilds, das die aktuellen biometrischen Daten darstellt, eingerichtet. Jeder Bildpunkt in dem digitalen Bild, das die aktuellen biometrischen Daten darstellt, besitzt einen Farb- oder Graustufenwert. Das Binarisieren impliziert, dass die Farb- oder Graustufenwerte der Bildpunkte mit einem Schwellenwert verglichen werden. Ist der Wert des Bildpunktes größer als der Schwellenwert, wird er in Weiß umgewandelt, und wenn er kleiner als der Schwellenwert ist, wird er in Schwarz umgewandelt oder umgekehrt. Durch diese Binarisierung sinkt die Datenmenge in dem digitalen Bild signifikant, da Schwarz und Weiß jeweils durch lediglich ein Bit dargestellt werden können, statt durch eine größere Anzahl von Bits, die für einen Bildpunkt erforderlich ist, der grau ist oder eine andere Farbe aufweist. Gleichzeitig werden die Konturen des Bildes, die die für den Benutzer spezifischen biometrischen Daten darstellen, im Wesentlichen gewahrt. Der Schwellenwert, mit dem die Bildpunkte des digitalen Bildes verglichen werden, kann entweder für alle Bildpunkte derselbe sein oder zwischen unterschiedlichen Teilen des digitalen Bildes

variieren.

[0023] Der Zweck des Verringerns der Datenmenge in dem ursprünglichen digitalen Bild bei der Vorverarbeitung, wie oben beschrieben, besteht darin, ein digitales Bild zu erzielen, das eine ausreichende Datenmenge enthält, um einen sicheren Vergleich auf dem Datenträger zu ermöglichen. Gleichzeitig sollte dieser Vergleich nicht zu viel Zeit erfordern.

[0024] Bei einer bevorzugten Ausführung der Erfindung ist die Signalverarbeitungseinrichtung des Datenträgers zum Durchführen eines zweidimensionalen Vergleichs wenigstens eines Teilbereichs der biometrischen Bezugsdaten und wenigstens eines Teilbereichs der vorverarbeiteten biometrischen Daten eingerichtet. Mit einem zweidimensionalen Vergleich ist gemeint, dass die Signalverarbeitungseinrichtung direkt Bereiche der vorverarbeiteten biometrischen Daten und in den Bezugsdaten vergleicht. Als Folge muss weder ein Bezugspunkt noch eine ähnliche Hilfe bei dem Vergleich verwendet werden. Um den Zeitaufwand bei diesem Vergleich zu verringern, werden auf vorteilhafte Weise Teilbereiche der beiden Bilder genutzt. Ein Teilbereich des Bildes, das die digitalen Bezugsdaten enthält, wird schrittweise mit unterschiedlichen Teilbereichen des vorverarbeiteten Bildes verglichen, bis ausreichende Entsprechung zwischen den Teilbereichen erreicht ist. Nachfolgend werden zusätzliche Teilbereiche der Darstellung der digitalen Bezugsdaten mit den vorverarbeiteten biometrischen Bezugsdaten verglichen, bis ein vorgegebenes Vergleichskriterium erfüllt ist. Das Vergleichskriterium kann zwischen unterschiedlichen Anwendungen variieren, und wenn es nicht erfüllt wird, werden die biometrischen Bezugsdaten als den aktuellen biometrischen Daten nicht entsprechend erachtet. Die bei dem Vergleich verwendeten Teilbereiche können in Größe, Form und Position variieren. Wichtig ist dabei, dass sie so ausgewählt werden, dass die personenspezifischen Informationen in den Bereichen maximal sind.

[0025] Wenn die digitale Darstellung ein anderes Format als ein digitales Bild hat, unterscheiden sich die Vorverarbeitung und der Vergleich selbstverständlich von der Vorverarbeitung und dem Vergleich, die oben beschrieben wurden. Wie oben beschrieben, besteht jedoch der Zweck der Vorverarbeitung darin, die Datenmenge in der ursprünglichen digitalen Darstellung zu verringern, um eine digitale Darstellung zu erzielen, die eine ausreichende Datenmenge enthält, um einen sicheren Vergleich auf dem Datenträger zu ermöglichen.

[0026] Bei einer weiteren Ausführung ist die Signalverarbeitungseinrichtung des Datenträgers des Weiteren dazu eingerichtet, bei Entsprechung zwischen den vorverarbeiteten biometrischen Daten und den biometrischen Bezugsdaten zu bestimmen, welche Operationen die Verarbeitungseinheit an den vertraulichen Informationen durchführen darf. Sobald die vorverarbeiteten biometrischen Daten ein Mal von der Verarbeitungseinheit zu dem Datenträger übertragen wurden, führt die Signalverarbeitungseinrichtung des Datenträgers zuerst die Endprüfung durch, ohne die Signalverarbeitungseinrichtung der Verarbeitungseinheit zu beteiligen. Wenn bei dieser Prüfung festgestellt wird, dass die vorverarbeiteten biometrischen Daten und die biometrischen Bezugsdaten einander entsprechen, gewährt die Signalverarbeitungseinrichtung des Datenträgers der Verarbeitungseinheit bestimmte Berechtigungen in Bezug darauf, welche Operationen sie an den vertraulichen Informationen durchführen darf. Diese Operationen können zum Beispiel reines Lesen vertraulicher Informationen aus dem Speicher des Datenträgers, Durchführen von Änderungen an den bestehenden vertraulichen Informationen in dem Speicher des Datenträgers, Zuführen zusätzlicher vertraulicher Informationen zu dem Speicher des Datenträgers oder verschiedene Kombinationen der vorgenannten Operationen sein.

[0027] Bei der derzeit am stärksten bevorzugten Ausführung bestehen die aktuellen biometrischen Daten aus einem Fingerabdruck, der einen einfachen Aufzeichnungsprozess ermöglicht.

[0028] Nach einem anderen Aspekt enthält der Speicher des Datenträgers Merkmal-Bezugsdaten. Wenn ein niedrigeres Sicherheitsniveau und eine höhere Verifizierungsgeschwindigkeit gewünscht werden, können stattdessen Merkmaldaten verwendet werden, um die Berechtigung des Benutzers zum Verwenden der Karte zu verifizieren. Der Vergleich von Merkmalen bei Fingerabdrücken ist auf dem Gebiet wohlbekannt und dieser Verifizierungsprozess kann von einem Fachmann auf eine Weise konstruiert werden, die für die anstehende Anwendung geeignet ist.

[0029] Im Hinblick auf das Erhöhen der Verifizierungsgeschwindigkeit bei gleichzeitigem Wahren eines hohen Sicherheitsniveaus ist die Signalverarbeitungseinrichtung der Verarbeitungseinheit dazu eingerichtet, bei der Vorverarbeitung Merkmale von dem Fingerabdruck zu extrahieren und diese mit Merkmal-Bezugsdaten, die von dem Datenträger zu der Verarbeitungseinheit übertragen wurden, zu vergleichen. Als Folge kann die höhere Kapazität der Signalverarbeitungsvorrichtung in der Verarbeitungseinheit genutzt werden. Der Vergleich von Merkmaldaten, der bei der Vorverarbeitung durchgeführt wird, kann verschiedenen Zwecken dienen. Zum Beispiel ist es durch Vergleichen der Merkmale möglich, sowohl die Drehung als auch die Übersetzung des aktuellen Fingerabdrucks relativ zu dem Bezugsfingerabdruck zu bestimmen. Dies führt einerseits zu verbesserter Sicherheit und andererseits zu schnellerer

Verifizierung, da weniger Kombinationen von Drehung und Übersetzung auf dem Datenträger untersucht werden müssen. Zu diesem Verifizierungsprozess kann somit gesagt werden, dass er eine Art „Hybridabgleich" bildet, bei dem einerseits ein traditioneller Vergleich von Merkmaldaten von dem Fingerabdruck durchgeführt wird und andererseits ein zweidimensionaler Vergleich von Teilbereichen der digitalen Bilder durchgeführt wird.

[0030] Der Datenträger ist eine Standard-Chip-Karte, wie zum Beispiel eine Java- oder MULTOS-Karte, d. h. einfache, kostengünstige Datenträgertypen, die sich leicht an unterschiedliche Anwendungen anpassen lassen und von einem Benutzer leicht zu tragen sind. Daher kann eine Standard-Chip-Karte, die Daten zu einem bestimmten Benutzer enthält, in vielen unterschiedlichen Situationen verwendet werden, da sie einfach standardisiert ist und da das Betriebssystem auf der Karte die Dateien bearbeitet, so dass die Bearbeitung der Dateien von der Anwendung, für die die Karte verwendet wird, unabhängig ist, was bei Datenträgern nach dem Stand der Technik, wie oben beschrieben, nicht der Fall ist.

[0031] Nach einem anderen Aspekt der Erfindung umfasst sie einen tragbaren Datenträger mit einem Speicher, der vertrauliche Informationen enthält, einer Signalverarbeitungseinrichtung und einer Kommunikationseinrichtung. Die Kommunikationseinrichtung des Datenträgers ist dazu eingerichtet, vorverarbeitete biometrische Daten von einer Verarbeitungseinheit zu empfangen und selbige zu der Signalverarbeitungseinrichtung zu übertragen, die dazu eingerichtet ist, die empfangenen vorverarbeiteten biometrischen Daten mit biometrischen Bezugsdaten, die in dem Speicher gespeichert sind, zu vergleichen.

[0032] Somit ist der Datenträger zum Empfangen vorverarbeiteter biometrischer Daten eingerichtet. Die von dem Datenträger empfangenen Daten können unterschiedliche personenspezifische Parameter, wie zum Beispiel des oben beschriebenen Typs, darstellen und können unterschiedliche Formate aufweisen. Die empfangenen biometrischen Daten müssen ein Datentyp sein, der in einer Verarbeitungseinheit vorverarbeitet wird. Es reicht beispielsweise nicht aus, seinen Finger auf dem Datenträger zu platzieren, sondern die biometrischen Daten müssen in einem elektronisch lesbaren Format zugänglich sein. Das Vorverarbeiten kann jedoch mehr oder weniger umfangreich sein und das Format der vorverarbeiteten Daten kann, je nach anstehender Anwendung, in einem großen Umfang variieren. Der entscheidende Faktor dafür, welcher Typ von vorverarbeiteten Daten von dem Datenträger empfangen werden kann, besteht darin, dass sie von demselben Typ wie die in dem Speicher des Datenträgers gespeicherten biometrischen Bezugsdaten sein müssen und dass der Datenträger ausreichende Kapazität aufweisen muss, um wenigstens den Vergleich mit den biometrischen Daten, die in dem Speicher des Datenträgers gespeichert sind, durchführen zu können.

[0033] Bei dem Datenträger ist die Signalverarbeitungseinrichtung dazu eingerichtet, die vorverarbeiteten biometrischen Daten mit biometrischen Bezugsdaten zu vergleichen, indem digitale Darstellungen eines personenspezifischen Parameters verglichen werden. Der Vorteil der Verwendung digitaler Darstellungen ist aus der obigen Besprechung in Verbindung mit der Beschreibung des Systems offensichtlich. Die digitalen Darstellungen bestehen aus digitalen Bildern.

[0034] Nach einem weiteren Aspekt der Erfindung umfasst sie eine Verarbeitungseinheit zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen, die auf einem tragbaren Datenträger gespeichert sind, wobei die Prüfung auf aktuellen biometrischen Daten einer Einzelperson basiert und die Verarbeitungseinheit einen Speicher, eine Signalverarbeitungseinrichtung und eine Kommunikationseinrichtung umfasst. Die Signalverarbeitungseinrichtung der Verarbeitungseinheit ist dazu eingerichtet, biometrische Daten der Einzelperson vorzuverarbeiten und dies über die Kommunikationseinrichtung zu dem Datenträger zu übertragen. Je nach Typ der aktuellen biometrischen Daten, die von der Einzelperson zugeführt werden, können eine Reihe unterschiedlicher Typen von Vorverarbeitung durchgeführt werden. Der Zweck besteht jedoch stets darin, die Menge an Informationen in den aufgezeichneten aktuellen biometrischen Daten zu verringern, um ihnen ein Format zu verleihen, das eine Übertragung zu dem Datenträger und einen endgültigen Vergleich auf demselben ermöglicht. Die Verarbeitungseinheit kann ein Typ von Einheit sein, die einen Speicher, eine Signalverarbeitungseinrichtung und eine Kommunikationseinrichtung aufweist, und besteht vorteilhafterweise aus einem Rechner.

[0035] Darüber hinaus kann die Verarbeitungseinheit mit einem Sensor ausgestattet sein, um aktuelle biometrische Daten der Einzelperson in der Form einer digitalen Darstellung, wie ein digitales Bild, aufzuzeichnen. Somit muss keine zusätzliche Ausrüstung mit der Verarbeitungseinheit verbunden werden, was bedeutet, dass das Aufzeichnen und Vorverarbeiten so integriert werden kann, dass der Prozess von der Aufzeichnung der biometrischen Daten des Benutzers bis einschließlich zu der Übertragung zu dem tragbaren Datenträger schnell ist. Des Weiteren erhöht sich außerdem die Sicherheit, da keine aktuellen biometrischen Daten zwischen einer speziellen Aufzeichnungseinheit und der Verarbeitungseinheit übertragen werden müssen. Der Sensor kann außerdem im Vergleich zu dem Fall, bei dem er auf dem eigentlichen Datenträger angeordnet ist, besser gegen mechanische Wirkung geschützt werden.

[0036] Die aktuellen biometrischen Daten sind ein Fingerabdruck und die Signalverarbeitungseinrichtung der Verarbeitungseinheit ist dazu eingerichtet, bei der Vorverarbeitung Merkmale aus dem Fingerabdruck zu extrahieren und diese mit Merkmal-Bezugsdaten zu vergleichen, die von dem Datenträger zu der Verarbeitungseinheit übertragen wurden. Der Zweck dieses Vergleichs von Merkmalen ist aus der obigen Besprechung in Verbindung mit dem System offensichtlich.

[0037] Nach einem letzten Aspekt der Erfindung umfasst sie ein Verfahren, um auf Basis von aktuellen biometrischen Daten einer Person die Zugangsberechtigung zu vertraulichen Informationen, die auf einem tragbaren Datenträger gespeichert sind, zu prüfen. Das Verfahren umfasst die folgenden Schritte:

– Vorverarbeiten der aktuellen biometrischen Daten in einer Verarbeitungseinheit;
– Übertragen der vorverarbeiteten biometrischen Daten zu dem Datenträger;
– Vergleichen der vorverarbeiteten biometrischen Daten mit biometrischen Bezugsdaten, die auf dem Datenträger gespeichert sind, auf dem Datenträger; und
– bei Entsprechung zwischen den vorverarbeiteten biometrischen Daten und den biometrischen Bezugsdaten Gewähren der Zugangsberechtigung zu den vertraulichen Informationen für die Person.

[0038] Bevorzugte Varianten dieses Verfahrens werden in den angehängten Verfahrensansprüchen dargestellt. Diese Verfahren führen zu denselben Vorteilen, die oben in der Besprechung des Systems, des Datenträgers und der Verarbeitungseinheit angegeben wurden.

Kurze Beschreibung der Zeichnungen

[0039] Die Erfindung wird nun mit Hilfe einer Ausführung unter Bezugnahme auf die beigefügten schematischen Zeichnungen ausführlicher beschrieben.

[0040] Fig. 1 ist eine schematische Zeichnung, die ein System nach der Erfindung zeigt;

[0041] Fig. 2 ist ein Blockdiagramm, das ein Verfahren nach der Erfindung zum Aufzeichnen biometrischer Bezugsdaten auf einem Datenträger zeigt;

[0042] Fig. 3 ist ein Blockdiagramm, das ein Verfahren nach der Erfindung zeigt, um die Zugangsberechtigung zu vertraulichen Informationen, die auf einem Datenträger gespeichert sind, zu prüfen.

Beschreibung

[0043] Fig. 1 ist eine schematische Ansicht eines Systems nach der Erfindung, bestehend aus einem Datenträger (**1**) in der Form einer Chip-Karte und einer Verarbeitungseinheit (**2**), die in diesem Fall ein Rechner ist. Die Chip-Karte (**1**) ist eine gewöhnliche Standard-Karte, wie zum Beispiel eine Java- oder MULTOS-Karte, und besitzt eine Kommunikationseinrichtung (**3**), die zum Kommunizieren mit einer Kommunikationseinrichtung (**4**) in dem Rechner (**2**) eingerichtet ist. Die Chip-Karte (**1**) besitzt des Weiteren eine Signalverarbeitungseinheit in der Form eines Prozessors (**5**) und einen Speicher (**6**). Der Speicher (**6**) enthält vertrauliche Informationen einerseits in der Form von Rechnerdateien, zu denen die Person, die das System verwendet, Zugang haben möchte, und andererseits in Form einer Schablone, die aus biometrischen Bezugsdaten des Benutzers besteht. Die Schablone besteht aus einer vorverarbeiteten digitalen Darstellung in der Form eines digitalen Bildes und es wird im Folgenden in Verbindung mit Fig. 2 beschrieben, wie dieses Bild erzeugt wird. Zusätzlich zu den vertraulichen Informationen und der Schablone enthält der Speicher (**6**) außerdem Software, die der Prozessor (**5**) zum Vergleichen des vorverarbeiteten Bildes der biometrischen Daten des Benutzers, die von dem Rechner (**2**) zu der Chip-Karte (**1**) übertragen wurden, und der Schablone verwendet.

[0044] Der Rechner (**2**) umfasst eine Signalverarbeitungseinrichtung oder einen Prozessor (**7**), der bei der Vorverarbeitung der biometrischen Daten des Benutzers verwendet wird. Die biometrischen Benutzerdaten werden mit Hilfe eines Sensors (**8**) aufgezeichnet, der bei dieser Ausführung aus einem kapazitiven Sensor besteht. Jedoch können auch andere bekannte Sensorentypen, die Fingerabdrücke aufzeichnen können, wie Wärmesensoren oder optische Sensoren, verwendet werden. Der Sensor (**8**) ist verbunden mit dem Prozessor (**7**) und mit einem Speicher (**10**), in dem Software für die Vorverarbeitung der biometrischen Daten gespeichert ist, die der Prozessor (**7**) ausführt. Der Rechner (**2**) umfasst außerdem Schaltungen (**11**) für externe Kommunikation mit anderen Einheiten. Die Kommunikation zwischen den unterschiedlichen Einheiten in dem Rechner (**2**) bzw. auf der Chip-Karte (**1**) erfolgt über einen Datenbus (nicht gezeigt).

[0045] Zum Durchführen eines Vergleichs auf der Karte (**1**) muss eine Schablone erzeugt werden, mit der die biometrischen Daten des Benutzers jedes Mal dann verglichen werden können, wenn eine Verifizierung der Zugangsberechtigung zu den vertraulichen Informationen auf der Karte (**1**) durchgeführt werden muss. Eine Beschreibung, wie dies gemacht wird, folgt im Folgenden.

[0046] Fig. 2 ist ein Blockdiagramm, das zeigt, wie eine Schablone und vertrauliche Informationen aufgezeichnet und auf dem Datenträger oder der Chip-Karte (**1**) gespeichert werden. In Schritt **20** wird

ein Bild des Fingers des Benutzers mit Hilfe des Sensors (**8**) in dem Rechner (**2**) aufgezeichnet. Das Ergebnis der Aufzeichnung ist ein digitales Bild in Graustufen, das den Fingerabdruck des Benutzers darstellt. In Schritt **21** wird dieses digitale Bild vorverarbeitet, um eine Schablone zu erzeugen. Diese Vorverarbeitung kann auf viele Weisen durchgeführt werden, wobei eine davon im Folgenden beschrieben wird.

[0047] Zuerst wird eine Prüfung der Bildqualität des Fingerabdrucks durchgeführt. Unter anderem wird geprüft, ob der Benutzer seinen Finger mit ausreichendem Druck auf den Sensor (**8**) aufgelegt hat, so dass Feuchtigkeit auf dem Finger des Benutzers es dem Sensor (**8**) nicht unmöglich gemacht hat, zwischen „Kämmen" und „Tälern" an dem Finger zu unterscheiden. Wenn die Qualität des Bildes unzureichend ist, wird der Benutzer aufgefordert, die Unzulänglichkeiten auf eine geeignete Weise zu korrigieren.

[0048] Wenn ein digitales Bild in Graustufen ausreichender Qualität durch den Sensor (**8**) aufgezeichnet wurde, erfolgt eine Binarisierung des Bildes. Die Binarisierung impliziert, dass die Bildpunkte des Bildes mit einem Graustufen-Schwellenwert verglichen werden. Die Bildpunkte, deren Wert kleiner als der Graustufen-Schwellenwert ist, werden in Weiß umgewandelt und diejenigen, deren Wert größer als der Graustufen-Schwellenwert ist, werden in Schwarz umgewandelt. Der Graustufen-Schwellenwert kann für das gesamte Bild derselbe sein oder zwischen unterschiedlichen Teilen des Bildes variieren. Der Binarisierungsalgorithmus kann des Weiteren verfeinert werden, so dass die Bildpunkte mit den Umgebungen verglichen werden, um zum Beispiel zu verhindern, dass einzelne Bildpunkte weiß sind, wenn alle umgebenden Bildpunkte schwarz sind. Diese Adaptierung ist von einem Fachmann leicht durchzuführen.

[0049] Nach der Binarisierung wird eine Anzahl von Bereichen des Bildes ausgewählt, um in der Form einer Schablone gespeichert zu werden. Einer der Bereiche wird ausgewählt, um ziemlich mittig in dem Bild positioniert zu werden, und die anderen, deren Anzahl normalerweise je nach dem gewünschtem Sicherheitsniveau zwischen vier und acht variiert, können variierende Positionen relativ zu dem mittigen Bereich haben. Die Größe der ausgewählten Bereiche beträgt in dieser Ausführung 48 × 48 Bildpunkte, kann jedoch leicht durch einen Fachmann nach den bestehenden Erfordernissen eingestellt werden. Die Größe und Position der verschiedenen Bereiche werden so ausgewählt, dass sie so viele personenspezifische Informationen umfassen wie möglich. Zum Beispiel sind Bereiche mit gekrümmten Linien von größerem Interesse als Bereiche mit geraden parallelen Linien.

[0050] Anschließend wird in Schritt **22** die Schablone von dem Rechner (**2**) über die Kommunikationsschaltungen (**3**, **4**) zu dem Speicher der Chip-Karte (**1**) übertragen. Wenn die Schablone übertragen wurde, können, in Schritt **23**, außerdem vertrauliche Informationen von dem Rechner (**2**) übertragen und in dem Speicher (**6**) der Chip-Karte (**1**) gespeichert werden, falls dies gewünscht wird. Das Aufzeichnen von Schablonen für den Karteninhaber wird lediglich ein Mal durchgeführt. Die vertraulichen Informationen können jedoch nötigenfalls ersetzt werden.

[0051] Fig. 3 zeigt einen Verifizierungsprozess, wenn ein Benutzer auf die vertraulichen Informationen, die auf der Chip-Karte (**1**) gespeichert sind, zugreifen möchte. Zuerst platziert er seine Chip-Karte (**1**) in einer Kartenlesevorrichtung entweder direkt in dem Rechner (**2**) oder in einer getrennten Kartenlesevorrichtung, die mit dem Rechner (**2**) kommuniziert. Er platziert dann seinen Finger auf dem Sensor (**8**) und es wird in Schritt **30** ein digitales Bild auf dieselbe Weise aufgezeichnet, wie oben beschrieben. Das Bild wird in dem Rechner (**2**) in Schritt **31** auf dieselbe Weise wie bei dem Aufzeichnen der Schablone vorverarbeitet, außer, dass keine Teilbereiche ausgewählt werden, so dass es ansonsten dasselbe Format wie die auf der Chip-Karte (**1**) gespeicherte Schablone aufweist. Anschließend wird das vorverarbeitete Bild über die Kommunikationsschaltungen (**3**, **4**) zu der Chip-Karte (**1**) übertragen, wo es mit der Schablone abgeglichen wird (Schritt **32**). Bei dem Abgleichen „streicht" der mittige Teilbereich der Schablone über das vorverarbeitete Bild und in jeder Position wird ein Vergleich Bildpunkt für Bildpunkt durchgeführt. Wenn ein Bildpunkt in der Schablone einem Bildpunkt in dem vorverarbeiteten Bild entspricht, wird ein vorgegebener Wert, zum Beispiel 1, zu einer Summe addiert. Wenn die Bildpunkte nicht entsprechen, wird die Summe nicht erhöht. Wenn der mittige Teilbereich der Schablone über das gesamte vorverarbeitete Bild gestrichen ist, wird eine Position erreicht, an der der mittige Teilbereich der Schablone einen Teilbereich des vorverarbeiteten Bildes am besten überlappt.

[0052] Nächstfolgend werden die verbleibenden Teilbereiche der Schablone mit dem anstehenden vorverarbeiteten Bild abgeglichen. Dieses Abgleichen ist weniger zeitaufwändig, da eine ungefähre Position der verbleibenden Teilbereiche bereits aus dem Aufzeichnungsvorgang für die Schablone bekannt ist. Wenn die Bildpunkte in den verbleibenden Teilbereichen der Schablone mit entsprechenden Bereichen des vorverarbeiteten Bildes verglichen wurden, wird ein Gesamtabgleichswert zwischen 0% (d. h. überhaupt keine Übereinstimmung) und 100% (d. h. genaue Übereinstimmung) erzielt. Dieser Abgleichswert wird mit einem vorbestimmten Schwellenwert verglichen (Schritt **33**). Eine umfassendere Beschreibung der Aufzeichnung von Schablonen und

der Verifizierung ist in der internationalen Patentanmeldung Nr. PCT/SE99/00553 des Anmelders zu finden.

[0053] Wenn der Grad der Entsprechung zwischen dem vorverarbeiteten Bild und der Schablone niedriger als der Schwellenwert ist, Schritt **33**, sendet die Chip-Karte in Schritt **34** ein Signal an den Rechner (**2**) zurück, der den Benutzerzugang zu den vertraulichen Informationen auf der Chip-Karte (**1**) verweigert, worauf der Prozess beendet wird. Wenn andererseits die Schablone und das vorverarbeitete Bild einander entsprechen, entriegelt der Prozessor (**5**) der Chip-Karte (**1**) die Dateien, die vertrauliche Informationen enthalten (Schritt **35**). Dann erhält der Rechner (**2**) Zugang zu diesen Informationen, Schritt **36**, und diese und andere vertrauliche Informationen können zwischen den beiden Einheiten ausgetauscht werden.

[0054] Auch wenn oben eine spezielle Ausführung der Erfindung beschrieben wurde, ist für Fachleute offensichtlich, dass angesichts der obigen Beschreibung viele Alternativen, Modifizierungen und Varianten machbar sind. Zum Beispiel kann ein Bezugspunkt bei der Verifizierung angeordnet werden, um einen schnelleren Vergleich zwischen den Bildern zu erreichen, und die Bereiche des Bildes, die zum Abgleichen ausgewählt werden, können auf der Basis anderer Kriterien als die oben beschriebenen ausgewählt werden. Daher gilt für die Erfindung, dass sie all diese Alternativen, Modifizierungen und Varianten umfasst, die in dem Umfang der angehängten Ansprüche liegen.

Patentansprüche

1. System zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen, wobei das Prüfen auf einem digitalen Bild eines Fingerabdrucks einer Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, basiert und das System Folgendes umfasst:
– einen tragbaren Datenträger (**1**), umfassend eine Signalverarbeitungseinrichtung (**5**), eine Kommunikationseinrichtung (**3**) und einen Speicher (**6**), der die vertraulichen Informationen, Merkmal-Bezugsdaten eines Fingerabdrucks einer Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, und Fingerabdruck-Bezugsdaten, d. h. ein digitales Bild wenigstens eines Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, enthält; und
– eine Verarbeitungseinheit (**2**), die dazu eingerichtet ist, das digitale Bild des Fingerabdrucks von der Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, zu empfangen, und einen Speicher (**10**), eine Signalverarbeitungseinrichtung (**7**) und eine Kommunikationseinrichtung (**4**) umfasst;
wobei die Signalverarbeitungseinrichtung (**7**) der Verarbeitungseinheit (**2**) dazu eingerichtet ist, das digitale Bild des Fingerabdrucks vorzuverarbeiten, wobei das Vorverarbeiten Extrahieren von Merkmalen aus dem digitalen Bild des Fingerabdrucks und Vergleichen dieser mit den Merkmal-Bezugsdaten umfasst, die von dem Datenträger zu der Verarbeitungseinheit übertragen wurden, und das vorverarbeitete digitale Bild des Fingerabdrucks mit Hilfe der Kommunikationseinrichtungen (**3**, **4**) zu der Signalverarbeitungseinrichtung (**5**) des Datenträgers (**1**) zu übertragen; und
wobei die Signalverarbeitungseinrichtung (**5**) des Datenträgers (**1**) dazu eingerichtet ist, das empfangene vorverarbeitete digitale Bild des Fingerabdrucks mit den Fingerabdruck-Bezugsdaten, die vorab in dem Speicher (**6**) des Datenträgers (**1**) gespeichert wurden, zu vergleichen, um zu bestimmen, ob die Zugangsberechtigung zu den vertraulichen Informationen besteht.

2. System nach Anspruch 1, wobei die Signalverarbeitungseinrichtung (**7**) der Verarbeitungseinheit (**2**) bei der Vorverarbeitung dazu eingerichtet ist, eine Binarisierung des digitalen Bildes des Fingerabdrucks durchzuführen.

3. System nach einem der vorhergehenden Ansprüche, wobei die Signalverarbeitungseinrichtung (**5**) des Datenträgers (**1**) dazu eingerichtet ist, einen zweidimensionalen Vergleich des wenigstens einen Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, und wenigstens eines Teilbereichs des vorverarbeiteten digitalen Bildes des Fingerabdrucks durchzuführen.

4. System nach einem der vorhergehenden Ansprüche, wobei die Signalverarbeitungseinrichtung (**5**) des Datenträgers (**1**) des Weiteren dazu eingerichtet ist, bei Entsprechung zwischen dem vorverarbeiteten digitalen Bild des Fingerabdrucks und den Fingerabdruck-Bezugsdaten zu bestimmen, welche Operationen die Verarbeitungseinheit (**2**) an den vertraulichen Informationen durchführen darf.

5. System nach einem der vorhergehenden Ansprüche, wobei der Datenträger (**1**) eine Chip-Karte ist.

6. System nach einem der vorhergehenden Ansprüche, wobei die Signalverarbeitungseinrichtung (**7**) der Verarbeitungseinheit (**2**) zum Bestimmen der Drehung sowie der Übersetzung des digitalen Bildes des Fingerabdrucks relativ zu den Fingerabdruck-Bezugsdaten eingerichtet ist.

7. Tragbarer Datenträger (**1**), umfassend eine Signalverarbeitungseinrichtung (**5**), eine Kommunikationseinrichtung (**3**) und einen Speicher (**6**), der ver-

trauliche Informationen, Merkmal-Bezugsdaten eines Fingerabdrucks einer Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, und Fingerabdruck-Bezugsdaten, d. h. ein digitales Bild wenigstens eines Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, enthält; wobei die Signalverarbeitungseinrichtung (**5**) dazu eingerichtet ist, die Merkmal-Bezugsdaten zu einer Verarbeitungseinheit (**2**) zu übertragen, um ein digitales Bild eines Fingerabdrucks für eine Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, vorzuverarbeiten; wobei die Kommunikationseinrichtung (**3**) dazu eingerichtet ist, das vorverarbeitete digitale Bild des Fingerabdrucks von der Verarbeitungseinheit (**2**) zu empfangen und selbiges zu der Signalverarbeitungseinrichtung (**5**) zu übertragen; und wobei die Signalverarbeitungseinrichtung (**5**) dazu eingerichtet ist, das empfangene vorverarbeitete digitale Bild des Fingerabdrucks mit den Fingerabdruck-Bezugsdaten, die in dem Speicher (**6**) gespeichert sind, zu vergleichen, um zu bestimmen, ob die Zugangsberechtigung zu den vertraulichen Informationen besteht.

8. Tragbarer Datenträger nach Anspruch 7, wobei die Signalverarbeitungseinrichtung (**5**) zum Durchführen eines zweidimensionalen Vergleichs des wenigstens einen Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, und wenigstens eines Teilbereichs des vorverarbeiteten digitalen Bildes des Fingerabdrucks eingerichtet ist.

9. Tragbarer Datenträger nach Anspruch 7 oder 8, wobei der Datenträger eine Chip-Karte ist.

10. Verarbeitungseinheit (**2**) zur Verwendung beim Prüfen der Zugangsberechtigung zu vertraulichen Informationen, die auf einem tragbaren Datenträger (**1**) gespeichert sind, wobei das Prüfen auf einem digitalen Bild eines Fingerabdrucks einer Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, basiert und die Verarbeitungseinheit (**2**), die zum Empfangen des digitalen Bildes des Fingerabdrucks eingerichtet ist, einen Speicher (**10**), eine Signalverarbeitungseinrichtung (**7**) und eine Kommunikationseinrichtung (**4**) umfasst; wobei die Signalverarbeitungseinrichtung (**7**) zum Vorverarbeiten des digitalen Bildes des Fingerabdrucks eingerichtet ist und das Vorverarbeiten umfasst, Merkmale aus dem digitalen Bild des Fingerabdrucks zu extrahieren und sie mit Merkmal-Bezugsdaten eines Fingerabdrucks einer Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, zu vergleichen, wobei die Merkmal-Bezugsdaten von einem Datenträger zu der Verarbeitungseinheit übertragen wurden, und das vorverarbeitete digitale Bild des Fingerabdrucks, das ein digitales Bild eines Fingerabdrucks der Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, umfasst, zu dem Datenträger zu übertragen, wo das vorverarbeitete digitale Bild des Fingerabdrucks mit auf dem Datenträger gespeicherten Fingerabdruck-Bezugsdaten, d. h. ein digitales Bild wenigstens eines Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, zu vergleichen ist, um zu bestimmen, ob die Zugangsberechtigung zu den vertraulichen Informationen besteht.

11. Verarbeitungseinheit (**2**) nach Anspruch 10, wobei die Signalverarbeitungseinrichtung (**7**) des Weiteren zum Durchführen von Operationen an den vertraulichen Informationen auf Basis von Berechtigungen, die der Verarbeitungseinheit (**2**) von dem Datenträger (**1**) zugewiesen werden, eingerichtet ist.

12. Verarbeitungseinheit (**2**) nach einem der vorhergehenden Ansprüche 10 bis 11, wobei die Verarbeitungseinheit (**2**) des Weiteren mit einem Sensor (**8**) ausgestattet ist, um das digitale Bild des Fingerabdrucks der Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, in der Form eines digitalen Bildes aufzuzeichnen.

13. Verarbeitungseinheit (**2**) nach Anspruch 12, wobei die Signalverarbeitungseinrichtung (**7**) bei der Vorverarbeitung dazu eingerichtet ist, eine Binarisierung des digitalen Bildes, das den Fingerabdruck darstellt, durchzuführen.

14. Verarbeitungseinheit nach einem der vorhergehenden Ansprüche 10 bis 13, wobei die Signalverarbeitungseinrichtung (**7**) zum Bestimmen der Drehung sowie der Übersetzung des digitalen Bildes des Fingerabdrucks relativ zu den Fingerabdruck-Bezugsdaten eingerichtet ist.

15. Verfahren zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen, die auf einem tragbaren Datenträger (**1**) gespeichert sind, wobei das Prüfen auf einem digitalen Bild eines Fingerabdrucks einer Person, deren Zugangsberechtigung zu vertraulichen Informationen zu prüfen ist, basiert, die folgenden Schritte umfassend:
– Empfangen des digitalen Bildes des Fingerabdrucks von der Person, deren Zugangsberechtigung zu vertraulichen Informationen zu prüfen ist, in einer Verarbeitungseinheit (**2**);
– Empfangen von Merkmal-Bezugsdaten eines Fingerabdrucks für eine Person, die die Zugangsberechtigung zu vertraulichen Informationen hat, von dem Datenträger (**1**) in der Verarbeitungseinheit (**2**);
– Vorverarbeiten des digitalen Bildes des Fingerabdrucks in der Verarbeitungseinheit (**2**), wobei das Vorverarbeiten Extrahieren von Merkmalen aus dem digitalen Bild des Fingerabdrucks und Vergleichen dieser mit den Merkmal-Bezugsdaten umfasst;
– Übertragen des vorverarbeiteten digitalen Bildes

des Fingerabdrucks von der Verarbeitungseinheit (**2**) zu dem Datenträger (**1**);
– Vergleichen des vorverarbeiteten digitalen Bildes des Fingerabdrucks mit Fingerabdruck-Bezugsdaten, die auf dem Datenträger (**1**) gespeichert sind und ein digitales Bild wenigstens eines Teilbereichs des Fingerabdrucks der Person, die eine Zugangsberechtigung zu den vertraulichen Informationen hat, umfassen, auf dem Datenträger (**1**); und
– bei Entsprechung zwischen dem vorverarbeiteten digitalen Bild des Fingerabdrucks und den Fingerabdruck-Bezugsdaten Gewähren von Zugang zu den vertraulichen Informationen.

16. Verfahren nach Anspruch 15, des Weiteren folgenden Schritt umfassend:
– Bestimmen mit Hilfe der Signalverarbeitungseinrichtung (**5**) des Datenträgers (**1**), welche Operationen die Verarbeitungseinheit (**2**) bei Entsprechung zwischen dem vorverarbeiteten digitalen Bild des Fingerabdrucks und den Fingerabdruck-Bezugsdaten an den vertraulichen Informationen durchführen darf.

17. Verfahren nach einem der Ansprüche 15 bis 16, des Weiteren folgenden Schritt umfassend:
– Aufzeichnen des digitalen Bildes des Fingerabdrucks der Person, deren Zugangsberechtigung zu den vertraulichen Informationen zu prüfen ist, mit Hilfe der Verarbeitungseinheit (**2**).

18. Verfahren nach einem der Ansprüche 15 bis 17, wobei der Schritt des Vergleichens des übertragenen vorverarbeiteten digitalen Bildes des Fingerabdrucks mit den Fingerabdruck-Bezugsdaten den Schritt des Vergleichens zweier digitaler Bilder umfasst.

19. Verfahren nach Anspruch 18, wobei der Schritt des Vorverarbeitens des digitalen Bildes des Fingerabdrucks in der Verarbeitungseinheit (**2**) den Schritt des Binarisierens des digitalen Bildes, das das digitale Bild des Fingerabdrucks darstellt, umfasst.

20. Verfahren nach einem der Ansprüche 15 bis 19, wobei der Schritt des Vergleichens des vorverarbeiteten digitalen Bildes des Fingerabdrucks mit Fingerabdruck-Bezugsdaten folgenden Schritt umfasst:
– Durchführen eines zweidimensionalen Vergleichs des wenigstens einen Teilbereichs des digitalen Bildes des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, und wenigstens eines Teilbereichs des vorverarbeiteten digitalen Bildes des Fingerabdrucks.

21. Verfahren nach einem der Ansprüche 15 bis 20, des Weiteren folgenden Schritt umfassend:
– Bestimmen, in der Verarbeitungseinheit (**2**), der Drehung sowie der Übersetzung des digitalen Bildes des Fingerabdrucks relativ zu den Fingerabdruck-Bezugsdaten.

22. Verfahren in einem tragbaren Datenträger (**1**) zum Prüfen der Zugangsberechtigung zu vertraulichen Informationen, die in einem Speicher des Datenträgers gespeichert sind, folgende Schritte umfassend:
– Übertragen von Merkmal-Bezugsdaten eines Fingerabdrucks einer Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, von dem Datenträger (**1**) zu einer Verarbeitungseinheit (**2**) zum Vorverarbeiten eines digitalen Bildes eines Fingerabdrucks von einer Person, deren Zugangsberechtigung zu den vertraulichen Daten zu prüfen ist;
– Empfangen des vorverarbeiteten digitalen Bildes des Fingerabdrucks von der Verarbeitungseinheit (**2**);
– Vergleichen des empfangenen vorverarbeiteten digitalen Bildes des Fingerabdrucks mit Fingerabdruck-Bezugsdaten, die in einem Speicher auf dem Datenträger gespeichert sind und ein digitales Bild wenigstens eines Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, umfassen; und
– Bestimmen, ob die Zugangsberechtigung zu den vertraulichen Informationen besteht.

23. Verfahren nach Anspruch 22, wobei der Schritt des Vergleichens das Durchführen eines zweidimensionalen Vergleichs des wenigstens einen Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, und wenigstens eines Teilbereichs des vorverarbeiteten digitalen Bildes des Fingerabdrucks umfasst.

24. Verfahren in einer Verarbeitungseinheit (**2**) in Verbindung mit dem Prüfen von Zugangsberechtigung zu vertraulichen Informationen, die auf einem tragbaren Datenträger (**1**) gespeichert sind, wobei das Prüfen auf einem digitalen Bild eines Fingerabdrucks einer Person, deren Zugangsberechtigung zu vertraulichen Informationen zu prüfen ist, basiert, folgende Schritte umfassend:
– Empfangen des digitalen Bildes des Fingerabdrucks von der Person, deren Zugangsberechtigung zu vertraulichen Informationen zu prüfen ist;
– Empfangen von Merkmal-Bezugsdaten eines Fingerabdrucks für eine Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, von dem Datenträger (**1**);
– Vorverarbeiten des digitalen Bildes des Fingerabdrucks, wobei das Vorverarbeiten Extrahieren von Merkmalen aus dem digitalen Bild des Fingerabdrucks und Vergleichen dieser mit den Merkmal-Bezugsdaten umfasst; und
– Übertragen des vorverarbeiteten digitalen Bildes des Fingerabdrucks, das ein digitales Bild des Fingerabdrucks der Person, deren Zugangsberechtigung zu prüfen ist, umfasst, zu dem Datenträger (**1**), wo das vorverarbeitete digitale Bild des Fingerab-

drucks zu vergleichen ist mit Bezugsfingerabdruckdaten, die auf dem Datenträger gespeichert sind und ein digitales Bild wenigstens eines Teilbereichs des Fingerabdrucks der Person, die die Zugangsberechtigung zu den vertraulichen Informationen hat, umfassen, um zu bestimmen, ob die Zugangsberechtigung zu den vertraulichen Informationen besteht.

25. Verfahren nach Anspruch 24, des Weiteren den Schritt des Bestimmens der Drehung sowie der Übertragung des digitalen Bildes des Fingerabdrucks relativ zu den Fingerabdruck-Bezugsdaten umfassend.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

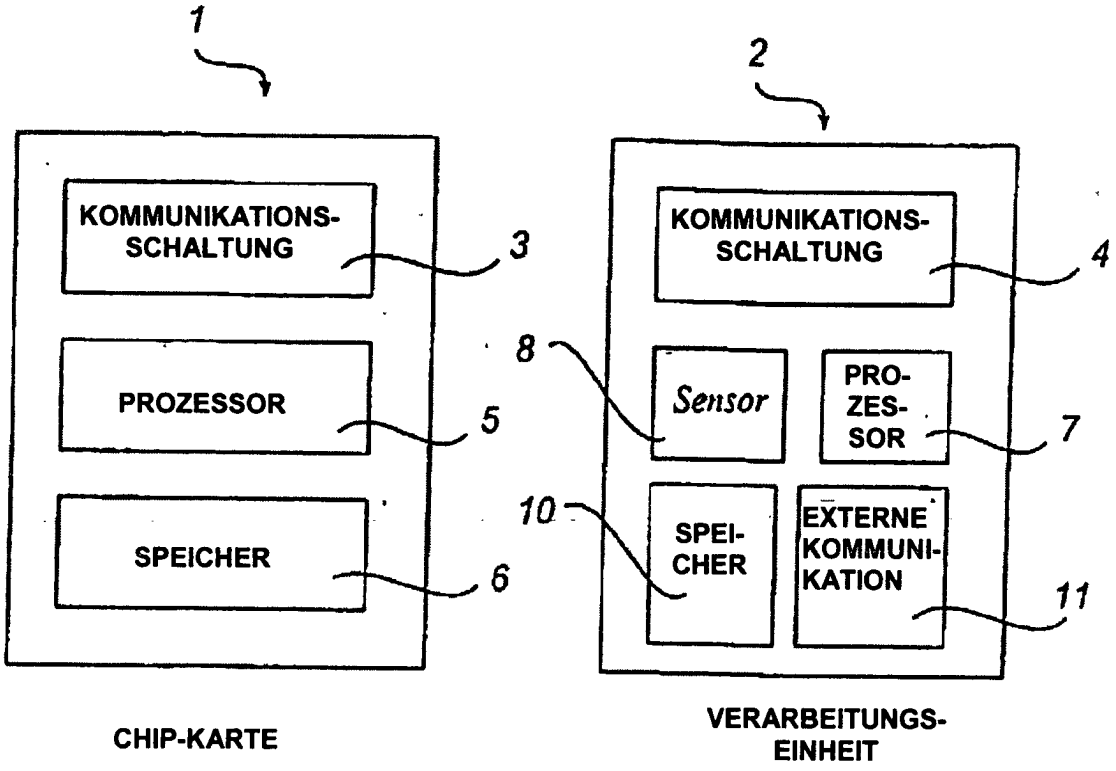

Fig. 1

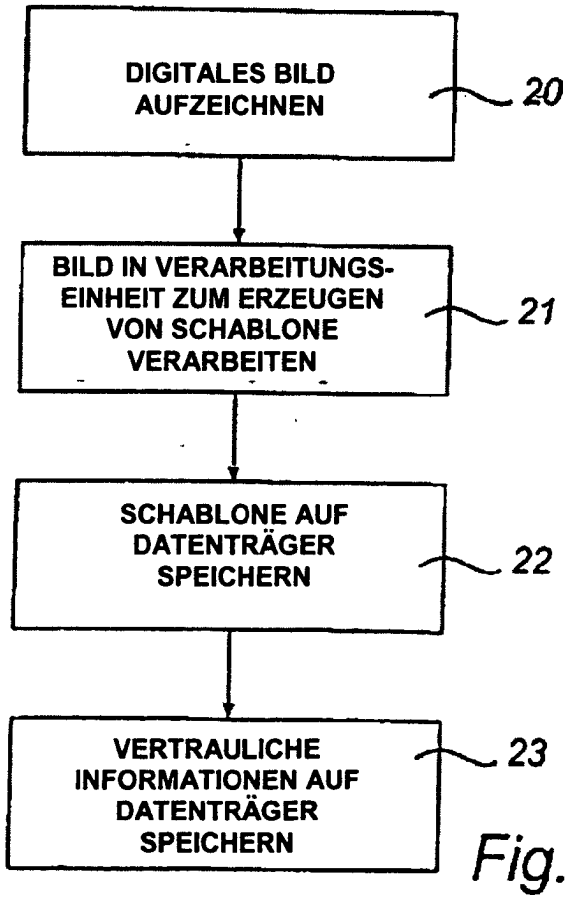

Fig. 2

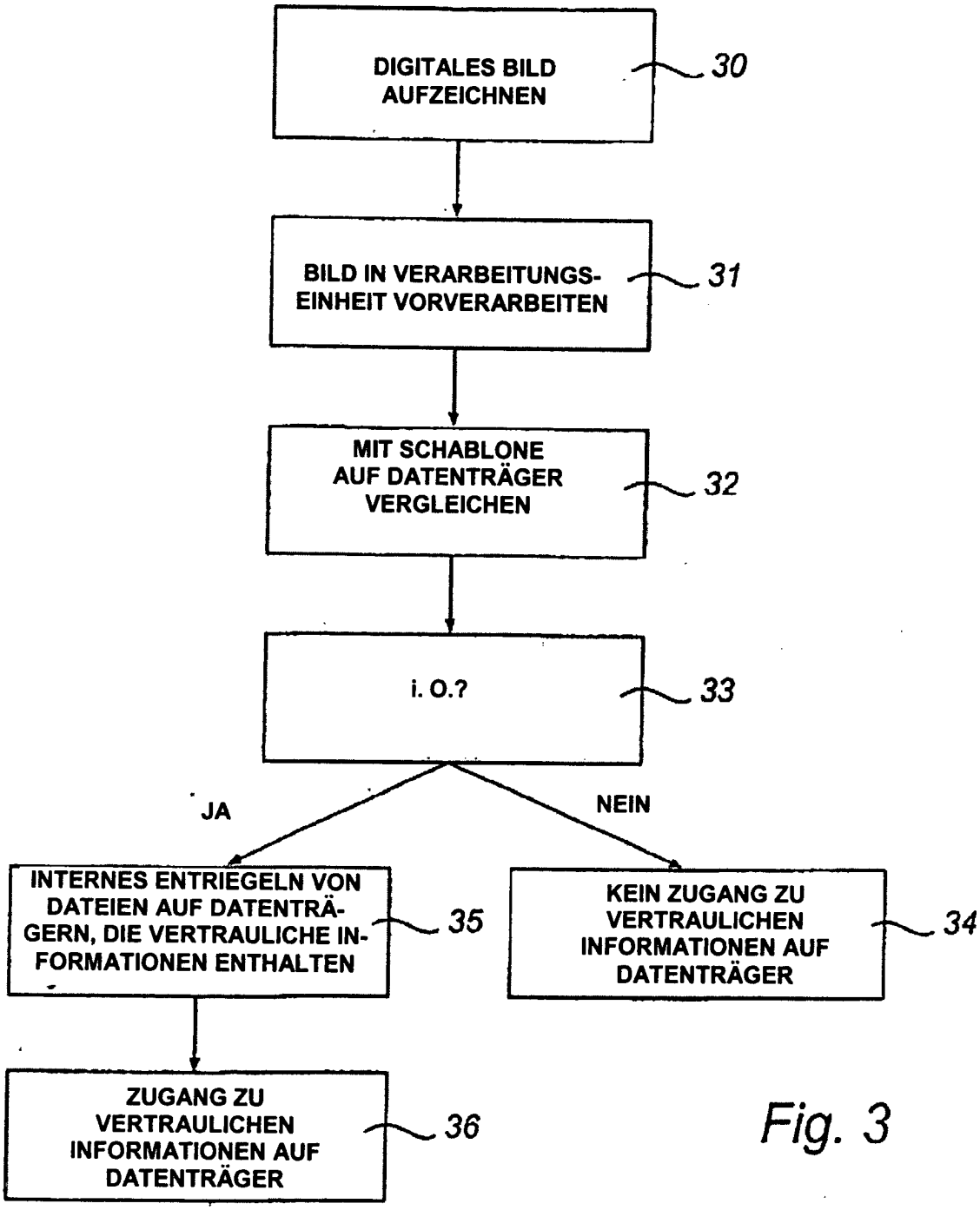
DIGITALES BILD AUFZEICHNEN
30
BILD IN VERARBEITUNGS-EINHEIT VORVERARBEITEN
31
MIT SCHABLONE AUF DATENTRÄGER VERGLEICHEN
32
i. O.?
33
JA
NEIN
INTERNES ENTRIEGELN VON DATEIEN AUF DATENTRÄGERN, DIE VERTRAULICHE INFORMATIONEN ENTHALTEN
35
KEIN ZUGANG ZU VERTRAULICHEN INFORMATIONEN AUF DATENTRÄGER
34
ZUGANG ZU VERTRAULICHEN INFORMATIONEN AUF DATENTRÄGER
36

Fig. 3