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

(11) **EP 3 789 976 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
27.12.2023 Patentblatt 2023/52

(21) Anmeldenummer: **20182825.8**

(22) Anmeldetag: **21.07.2009**

(51) Internationale Patentklassifikation (IPC):
G07D 7/202 *(2016.01)* ***G07D 7/20*** *(2016.01)*
G07D 7/1205 *(2016.01)* ***G07D 7/12*** *(2016.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G07D 7/12; G07D 7/1205; G07D 7/20; G07D 7/205; G07D 7/2075

(54) VERFAHREN ZUR PRÜFUNG DER ECHTHEIT EINES DOKUMENTS, COMPUTERPROGRAMMPRODUKT, PRÜFGERÄT UND DATENVERARBEITUNGSSYSTEM

DOCUMENT AUTHENTICITY TESTING METHOD, COMPUTER PROGRAM PRODUCT, TEST DEVICE AND DATA PROCESSING SYSTEM

PROCÉDÉ DE VÉRIFICATION DE L'AUTHENTICITÉ D'UN DOCUMENT, PRODUIT PROGRAMME INFORMATIQUE, APPAREIL DE VÉRIFICATION ET SYSTÈME DE TRAITEMENT DES DONNÉES

(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: **08.08.2008 DE 102008041113**

(43) Veröffentlichungstag der Anmeldung:
10.03.2021 Patentblatt 2021/10

(62) Dokumentnummer(n) der früheren Anmeldung(en) nach Art. 76 EPÜ:
09780856.2 / 2 313 872

(73) Patentinhaber: **Bundesdruckerei GmbH**
10958 Berlin (DE)

(72) Erfinder:
- **Alheit, Reimund**
  16775 Stechlin-Menz (DE)
- **Kessler, Horst**
  14193 Berlin (DE)
- **Sprenger, Martin**
  10967 Berlin (DE)
- **Kramer, Christian**
  13359 Berlin (DE)
- **Dietrich, Jürgen**
  12557 Berlin (DE)

(74) Vertreter: **Richardt Patentanwälte PartG mbB**
Wilhelmstraße 7
65185 Wiesbaden (DE)

(56) Entgegenhaltungen:
EP-A1- 1 883 053
DE-A1- 19 906 388
JP-A- 2002 170 142
US-A1- 2004 222 283
US-A1- 2006 078 186

EP 3 789 976 B1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Prüfung der Echtheit eines Dokuments sowie ein entsprechendes Computerprogrammprodukt und ein entsprechendes Datenverarbeitungssystem.

[0002] Aus dem Stand der Technik ist es bekannt, Ausweisdokumente optisch zu erfassen, um eine Prüfung der Echtheit der Ausweisdokumente durchzuführen.

[0003] Insbesondere ist die Erfassung der von der International Civil Aviation Organization (ICAO) spezifizierten Maschine Readable Zone (MRZ) auf maschinenlesbaren Reisedokumenten im Infrarot (IR)-Bereich bekannt sowie auch die Überprüfung von fluoreszierenden Sicherheitsmerkmalen durch UV-Bestrahlung. Hierzu wird verwiesen auf US 7,046,346 B2 und US 2007/0260886 A1.

[0004] Die US 2006/078186 A1 beschreibt ein magnetisches Erfassungssystem zur Authentifizierung einer Banknote, welches einen ersten magnetischen Abtastkopf umfasst, der dafür angepasst ist, ein erstes Magnetfeld zur Sättigung der Magnetisierung eines Bereichs der Banknoten zu erzeugen. Das magnetische Erfassungssystem umfasst ferner einen zweiten magnetischen Abtastkopf mit einem Elektromagneten. Der Elektromagnet ist dazu ausgelegt ein zweites Magnetfeld mit einstellbarer Intensität zu erzeugen. Das zweite Magnetfeld weist die entgegengesetzte Polarität des ersten Magnetfeldes auf. Die Intensität des zweiten Magnetfeldes wird durch Änderung der dem Elektromagneten zugeführten Strommenge eingestellt. Die Menge des dem Elektromagneten zugeführten Stroms basiert auf einem Merkmal der zu authentifizierenden Banknote.

[0005] Die US 2004/222283 A1 beschreibt ein System, ein Verfahren und ein Programmprodukt zum Bereitstellen einer Authentifizierung und Erfassung einer Papierwährung, d.h. einer Banknote, an einer Verkaufsstelle in Echtzeit. Es wird ein Terminal einer Verkaufsstelle zur Echtzeitauthentifizierung und -erfassung von Papierwährung bereitgestellt, ein Währungsüberwachungssystem zum Nachverfolgen des Gebrauchs der Papierwährung und zum Durchführen einer Papierwährungsauthentifizierung unter Bezugnahme auf eine Datenbank einer währungsausgebenden Entität und ein Abgleichungssystem zum Abgleichen eines Terminals einer Verkaufsstelle.

[0006] Die JP 2002 170142 A beschreibt eine Zahlmaschine mit einem Tresor für kleine Banknotenbündel unabhängig von Tresoren, welche Nennwerten zugeordnet sind. Banknoten, die von den jeweiligen Tresoren nach Nennwerten geliefert werden, werden versiegelt, wobei die zugehörigen Nennwertinformationen bereitgestellt werden. Kleine Banknotenbündel werden basierend auf den Nennwertinformationen verwaltet und aufbewahrt. Ein kleines Banknotenbündel eines beschriebenen Nennwerts wird ausgewählt und gemäß einem Zahlungsbefehl ausgezahlt.

[0007] Die DE 199 06 388 A1 beschreibt ein Verfahren und eine Vorrichtung zur Personalisierung und Verifizierung von Identitäts- und Sicherheitsdokumenten sowie ein damit verwendbares Sicherheitsdokument. Das Identitäts- oder Sicherheitsdokument weist personenbezogene Daten auf, die in alphanumerischer und/oder graphischer Form auf dem Dokument angebracht und/oder in dieses eingebracht sind. Erfindungsgemäß sind die personenbezogenen Daten und/oder mit diesen korrelierte Daten in einer zweiten, maschinenlesbaren Form auf/in dem Dokument vorhanden und können zusammen mit den personenbezogenen Daten mittels eines entsprechenden Prüfgerätes vom Dokument ausgelesen und auf Übereinstimmung überprüft werden.

[0008] Die EP 1 883 053 A1 beschreibt Techniken zum Erzeugen von Fingerabdrücken von Artikel und zum Verwenden der Fingerabdrücke für verschiedene Anwendungen. Scanbezogene Parameterwerte, einschließlich des Bereichs eines gescannten Artikels, können von Scan zu Scan spezifiziert und variiert werden, um Datenpunkte zu sammeln, die zum Erzeugen von Fingerabdrücken der Artikel verwendet werden. Ferner ein Aktenvernichter beschrieben, der so konfiguriert ist, dass er vor dem Zerkleinern eines Papierblatts das Papierblatt scannt und einen Fingerabdruck des Papierblatts erzeugt. Fingerabdrücke können auch für Medienschlüssel generiert werden, die für den Zugriff auf Mediendaten verwendet werden. Der für einen Medienschlüssel erzeugte Fingerabdruck kann zur Authentifizierung des Medienschlüssels verwendet werden. Der Zugriff auf Mediendaten, die dem Medienschlüssel entsprechen, kann von einer erfolgreichen Authentifizierung des Medienschlüssels abhängig gemacht werden.

[0009] Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein verbessertes Verfahren zur Prüfung der Echtheit eines Dokuments zu schaffen sowie ein Computerprogrammprodukt, ein elektronisches Gerät zur Prüfung der Echtheit eines Dokuments und ein Datenverarbeitungssystem.

[0010] Nach Ausführungsformen der Erfindung wird ein Verfahren zur Prüfung der Echtheit eines Dokuments geschaffen, wobei ein erstes Bild des Dokuments mit ersten Bildaufnahmeparametern aufgenommen wird. Bei den ersten Bildaufnahmeparametern kann es sich um standardisierte Bildaufnahmeparameter handeln, welche unabhängig von dem Typ des Dokuments zur Anwendung kommen.

[0011] In dem ersten Bild wird dann automatisch eine Information durch ein Verfahren der optischen Zeichenerkennung (Optical Character Recognition - OCR) erkannt. Bei der Information handelt es sich um eine unmittelbare oder mittelbare Angabe des Dokumententyps des Dokuments, von dem das erste Bild erfasst worden ist. Beispielsweise beinhaltet die Information eine Angabe des Staates, welcher das Dokument ausgestellt hat, sowie des Ausstellungsdatums. Wenn es sich bei den zu prüfenden Dokumenten um Reisepässe handelt, ergibt sich aus dieser Information der Dokumententyp, da für jeden Staat die Eigenschaften der von ihm heraus-

gegebenen Reisepassdokumente spezifiziert sind. Die Information kann im Klartext in dem von dem ersten Bild erfassten Teilbereich angegeben sein oder in einer codierten Form.

[0012] Mit Hilfe der aus dem ersten Bild erkannten Information wird eine Datenbankabfrage durchgeführt, um zweite Bildaufnahmeparameter zur Aufnahme eines zweiten Bildes des Dokumentes abzufragen. Hierzu sind in einer Datenbank typspezifische zweite Bildaufnahmeparameter gespeichert. Die einem bestimmten Dokumententyp zugeordneten zweiten Bildaufnahmeparameter können also aus der Datenbank abgerufen werden. Hierzu wird die aus dem ersten Bild erkannte Information als Zugriffsschlüssel verwendet.

[0013] Mit den zweiten Bildaufnahmeparametern wird dann ein zweites Bild des Dokuments aufgenommen. Hierbei handelt es sich vorzugsweise um ein Vollbild des Dokuments, welches die gesamte Vorder- und/oder Rückseite des Dokuments beinhalten kann.

[0014] Nach einer Ausführungsform der Erfindung erfolgt die Aufnahme des ersten Bildes mit vordefinierten Einstellungen für die Parameter der Bildaufnahme und der Bildverarbeitung. Hierbei kann es sich um werkseitig in einem nichtflüchtigen Speicher des für die Prüfung der Echtheit des Dokuments verwendeten Geräts gespeicherte Parameter handeln. Für die Dokumententyperkennung des Dokuments kann das erste Bild die sog. MRZ (machine readable zone, z.B. wie von der ICAO spezifiziert) beinhalten. In der MRZ ist zum Beispiel das Dokumentenformat bzw. der Typ und/oder Herstellungsland in maschinenlesbarer Form angegeben.

[0015] Die Auswertung dieser aus der MRZ durch OCR erfassten Information erfolgt über eine entsprechende Abfrage in einer Datenbank, die dokumentenspezifische Parameter für die weiteren Bildaufnahmen, insbesondere die Aufnahme des zweiten Bildes, zur Verfügung stellt, und die die möglichen Prüfungsmerkmale des Dokuments und sonstige individualisierte Informationen beistellt. Die weitere Prüfungsroutine des Geräts läuft dann mit den spezifischen aus der Datenbank ausgelesenen Parametern ab, die abweichend von den Werkseinstellungen sind.

[0016] Nach einer Ausführungsform der Erfindung ist zumindest eines der zu überprüfenden Sicherheitsmerkmale des Dokuments fluoreszierend. Bei dieser Ausführungsform ist besonders vorteilhaft, dass das erste Bild aufgenommen werden kann, ohne die Fluoreszenz des Sicherheitsmerkmals nennenswert anzuregen. Für die Aufnahme des zweiten Bildes kommen dann zweite Bildaufnahmeparameter zur Anwendung, sodass die Fluoreszenz des Sicherheitsmerkmals so angeregt wird, dass eine Überprüfung des Sicherheitsmerkmals in dem zweiten Bild leicht bzw. optimal möglich ist.

[0017] Aufgrund der typspezifischen zweiten Bildaufnahmeparameter kann insbesondere vermieden werden, dass die Fluoreszenz zu wenig angeregt wird, was ein geringes Signal-Rauschleistungsverhältnis bedeuten würde, oder dass die Fluoreszenz zu stark angeregt wird, so dass der optische Sensor in die Sättigung ginge.

[0018] Nach einer Ausführungsform der Erfindung beinhalten die zweiten Bildaufnahmeparameter ein oder mehrere Parameter bezüglich der Beleuchtung des Dokuments, insbesondere hinsichtlich der Intensität der Beleuchtung und/oder bezüglich der Belichtung eines optischen Sensors, mit Hilfe dessen das zweite Bild aufgenommen wird, insbesondere die Belichtungszeit und/oder einen Verstärkungsfaktor. Alternativ oder zusätzlich kann die Strahlungsfrequenz der Beleuchtung in den zweiten Bildaufnahmeparameter spezifiziert sein.

[0019] Erfindungsgemäß beinhaltet die Datenbank neben den typspezifischen zweiten Bildaufnahmeparametern auch typspezifische Angaben zu den Sicherheitsmerkmalen, wobei die typspezifischen Angaben zu den Sicherheitsmerkmalen bei der Datenbankabfrage mit abgefragt werden, um sie für die Überprüfung anhand des zweiten Bildes zu verwenden. Die Angaben zu den Sicherheitsmerkmalen beinhalten Angaben zur Lage und Form der Sicherheitsmerkmale. Diese Soll-Merkmale werden dann mit den in dem zweiten Bild vorhandenen Ist-Merkmalen verglichen, wobei bei hinreichender Übereinstimmung der Ist-Merkmale mit den Soll-Merkmalen von der Echtheit des Dokuments ausgegangen wird.

[0020] Nach einer Ausführungsform der Erfindung handelt es sich bei dem Dokument um ein Wert- oder Sicherheitsdokument, wie zum Beispiel ein ID-Dokument, d. h. ein Ausweisdokument, wie zum Beispiel einen Personalausweis, Reisepass, Führerschein oder Firmenausweis, oder ein Zahlungsmittel, wie zum Beispiel eine Banknote, eine Kreditkarte, oder einen sonstigen Berechtigungsnachweis, wie zum Beispiel eine Eintrittskarte, einen Frachtbrief, ein Visum oder dergleichen.

[0021] In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt mit von einem Prüfgerät ausführbaren Programminstruktionen zur Durchführung eines erfindungsgemäßen Verfahrens.

[0022] Ein elektronisches Gerät zur Prüfung der Echtheit eines Dokuments beinhaltet beispielsweise Mittel zur Aufnahme eines ersten Bildes zumindest eines Teilbereichs des Dokuments mit ersten Bildaufnahmeparametern und zur Aufnahme eines zweiten Bildes des Dokuments mit zweiten Bildaufnahmeparametern, Mittel zur Erkennung einer Information in dem ersten Bild, und Mittel zur Durchführung einer Datenbankabfrage mit Hilfe der Information zur Abfrage der zweiten Bildaufnahmeparameter.

[0023] Die ersten Bildaufnahmeparameter sind für alle unterstützten Dokumententypen dieselben. Die ersten Bildaufnahmeparameter können daher in einem Speicher des elektronischen Geräts gespeichert sein. Die ersten Bildaufnahmeparameter können auch Teil der Firmware des elektronischen Geräts sein.

[0024] Beispielsweise hat das elektronische Gerät ein oder mehrere optische Sensoren zur Sensierung verschiedener optischer Spektralbereiche, sowie ein oder mehrere Strahlungsquellen zur Beleuchtung des Dokuments in unterschiedlichen Spektralbereichen.

[0025] Beispielsweise hat das elektronische Gerät ferner eine Funk-Schnittstelle, insbesondere eine so genannte RFID-Schnittstelle, zur drahtlosen Kommunikation über elektromagnetische Wellen mit einer in dem Dokument integrierten elektronischen Schaltung, insbesondere einem so genannten RFID-Chip. In dem RFID-Chip können digitalisierte Daten eines auf dem Dokument aufgedruckten oder angezeigten Gesichtsbildes abgelegt sein und/oder weitere Daten, wie zum Beispiel biometrische Daten, Angaben zu der Person des Trägers des Dokuments und/oder zu der ausstellenden Behörde des Dokuments.

[0026] Zumindest einige der in dem Chip gespeicherten Daten können kryptografisch gegen unerlaubten Zugriff geschützt sein, sodass nur hierzu autorisierte Prüfgeräte über deren Funk-Schnittstelle die in dem Chip gespeicherten Daten abrufen können. Beispielsweise können Daten, die aus dem zweiten Bild erfasst werden, mit Daten, die aus dem Chip ausgelesen werden, seitens des Prüfgeräts verglichen werden. Sofern die aus dem zweiten Bild erfassten Daten hinreichend mit den aus dem Chip ausgelesenen Daten übereinstimmen, wird von der Echtheit des Dokuments ausgegangen.

[0027] In einem weiteren Aspekt betrifft die Erfindung ein Datenverarbeitungssystem zur Prüfung der Echtheit von Dokumenten.

[0028] Nach Ausführungsformen der Erfindung beinhaltet das Datenverarbeitungssystem mehrere offenbarte Prüfgeräte, die über Kommunikationsverbindungen, wie zum Beispiel über ein Netzwerk, mit der Datenbank kommunizieren können, um von dort die zweiten Bildaufnahmeparameter abzufragen.

[0029] Ausführungsformen der Erfindung sind besonders vorteilhaft, da sich mit Hilfe desselben Verfahrens bzw. desselben Prüfgeräts unterschiedliche Typen von Dokumenten sicher und effizient prüfen lassen. Beispielsweise können sich die Dokumententypen stark hinsichtlich deren Reflexionsverhalten unterscheiden. Dies trifft insbesondere für papierbasierte Dokumente im Vergleich zu Dokumenten mit einer Kunststoffoberfläche zu sowie laminierte Dokumente. Das unterschiedliche Reflexionsverhalten kann bei gleicher Beleuchtung zu unterschiedlichem Kontrast und Ansprechverhalten eines fluoreszierenden Sicherheitsmerkmals führen. Hier schafft die Erfindung Abhilfe, da die Beleuchtung in Abhängigkeit von dem Dokumententyp gewählt wird.

[0030] Dies ist insbesondere vorteilhaft für die Überprüfung von fluoreszierenden Sicherheitsmerkmalen. Das Ansprechverhalten eines solchen fluoreszierenden Sicherheitsmerkmals kann von Dokumententyp zu Dokumententyp sehr stark in Abhängigkeit von der eingesetzten Farbe oder Tinte variieren. Bei gleichen Bildaufnahmeparametern können bei einem Dokumententyp fluoreszierende Sicherheitsmerkmale stark übersteuert aufgenommen werden, wohingegen bei einem anderen Dokumententyp kaum eine Anregung der Fluoreszenz vorliegt, sodass das Sicherheitsmerkmal kaum sichtbar wird. Auch hier schafft die Erfindung Abhilfe, da dokumententypspezifisch die zweiten Bildaufnahmeparameter gewählt werden. Hierdurch lässt sich für sämtliche unterstütze Dokumententypen eine optimale Bildqualität erreichen.

[0031] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Figur 1 ein Blockdiagramm einer ersten Ausführungsform eines Prüfgeräts,

Figur 2 ein Flussdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

Figur 3 ein Blockdiagramm einer Ausführungsform eines erfindungsgemäßen Datenverarbeitungssystems.

[0032] Elemente der nachfolgenden Figuren, die einander entsprechen, werden mit denselben Bezugszeichen gekennzeichnet.

[0033] Die Figur 1 zeigt schematisch ein Dokument 100, bei dem es sich um ein Ausweisdokument, wie zum Beispiel einen Reisepass handeln kann. Das Dokument 100 trägt ein Gesichtsbild 102. Das Gesichtsbild 102 kann auf dem Dokument 100 aufgedruckt sein. Alternativ oder zusätzlich hat das Dokument 100 eine integrierte Anzeigevorrichtung, auf der das Gesichtsbild 102 wiedergegeben wird.

[0034] Neben dem Gesichtsbild 102 kann das Dokument 100 weitere Sicherheitsmerkmale, insbesondere optische Sicherheitsmerkmale, beinhalten.

[0035] Zu den optischen Sicherheitsmerkmalen zählen beispielsweise:

- Guillochen: Guillochen werden mit Hilfe von so genanntem Liniendruck auf das Dokument aufgedruckt. Sie bestehen im Allgemeinen aus in verschiedenen Farben übereinander gedruckten Wellen- und Schleifenmustern;
- Mikro-Schrift: Hierbei handelt es sich um aufgedruckte Schriftzüge in kleinster Schrift. Mit bloßem Auge lässt sich die Mikro-Schrift kaum erkennen. Beispielsweise ist Mikro-Schrift auf den Euro-Banknoten als Bildelemente in die Motive eingearbeitet. Mit Hilfe einer Lupe kann die Mikro-Schrift gelesen werden;
- Metamere Systeme: Aufgrund metamerer Farbgleichheit können unterschiedliche spektrale Zusammensetzungen des Lichts bei Menschen den gleichen Farbeindruck hervorrufen;
- Aufdrucke mit Fluoreszenz, Phosphoreszenz und/oder Up-Conversion-Farben;
- Aufdrucke mit Infrarot-Farbe: Die Farbe wird nur unter Infrarot-Strahlung für Lesegeräte mit entsprechenden Sensoren sichtbar. Beispielsweise sind Eu-

ro-Banknoten mit diesem optischen Sicherheitsmerkmal ausgestattet;

- Barcodes, insbesondere ein- oder zweidimensionale Barcodes;

- Optisch variable Farben (OVI - Optical Variable Ink): Bei einer optisch variablen Farbe ändert sich der Farbeindruck je nach Betrachtungswinkel, da das Licht an den Pigmenten gebrochen, gestreut oder reflektiert wird;

- Hologramme und Kinegramme (transparent oder reflektierend);

- Wasserzeichen, insbesondere digitale Wasserzeichen, die eine maschinell auslesbare Information tragen;

- Passerdruck: Verschiedene Muster oder Symbole werden so über- oder aneinander gedruckt, dass sie zusammen ein bestimmtes Bild ergeben. Kleinste Abweichungen im Stand, d.h. so genannte Passerungenauigkeiten, können leicht mit bloßem Auge erkannt werden. Wenn sich die Teilbilder auf verschiedenen Seiten des Dokuments, wie zum Beispiel einer Banknote, befinden, bezeichnet man dieses optische Sicherheitsmerkmal als Durchsichtspasser;

- Durchsichtsfenster: Ein Fenster aus einer transparenten Kunststofffolie ist in dem Dokument eingearbeitet;

- Melierfasern: Dem Papier des Dokuments werden Fasern beigemischt, die unter UV-Licht in verschiedenen Farben leuchten;

- Sicherheitsfaden;

- Mikroperforation.

[0036] Beispielsweise beinhaltet das Dokument einen Sicherheitsfaden 104 sowie einen Aufdruck 106 mit einer fluoreszierenden Farbe, welche nur unter ultravioletter (UV) Beleuchtung sichtbar wird. Das Dokument 100 kann weitere, in der Figur 1 nicht gezeigte optische Sicherheitsmerkmale aufweisen.

[0037] Das Dokument 100 hat ferner einen Teilbereich 108, der maschinenlesbaren Informationen trägt. Bei dem Teilbereich 108 kann es sich beispielsweise um die so genannte Machine Readable Zone (MRZ) handeln, wie von der ICAO spezifiziert. Insbesondere können die Lage und die Größe des Teilbereichs 108 sowie andere Parameter des Teilbereichs 108, wie zum Beispiel die verwendete Schriftgröße und der Schrifttyp, für sämtliche unterstützte Dokumententypen global einheitlich festgelegt sein.

[0038] Das Dokument 100 kann ferner einen in den Dokumentenkörper integrierten elektronischen Chip 110 aufweist. Vorzugsweise ist der Chip 110 zum Aufbau einer drahtlosen Kommunikationsverbindung mit einem Prüfgerät 112 ausgebildet. Bei dem Chip 110 kann es sich zum Beispiel um einen so genannten RFID-Chip handeln.

[0039] Der Chip 110 hat einen elektronischen Speicher 114. In dem elektronischen Speicher 114 kann das Gesichtsbild 102 in digitalisierter Form abgespeichert sein und/oder weitere Daten bezüglich des Inhabers des Dokuments 100 und/oder der das Dokument ausstellenden Stelle. Die in dem elektronischen Speicher 114 gespeicherten Daten können zumindest teilweise kryptografisch geschützt sein, um einen unautorisierten Zugriff auf die Daten zu verhindern. Der kryptografische Schutz der in dem elektronischen Speicher 114 gespeicherten Daten kann beispielsweise durch eine so genannte Basic Access Control und/oder eine Extended Access Control erfolgen, so wie ebenfalls von der ICAO spezifiziert.

[0040] Das Prüfgerät 112 hat zumindest einen optischen Sensor 116 zur optischen Erfassung des Dokuments 100. Ferner hat das Prüfgerät 112 eine Strahlungsquelle 118 für eine Beleuchtung des Dokuments 100 mit Strahlung im infraroten (IR) Bereich sowie eine Strahlungsquelle 120 zur Beleuchtung des Dokuments 100 im ultravioletten (UV) Bereich. Es kann auch eine einzige Strahlungsquelle verwendet werden, die einen breiten Spektralbereich abdeckt. Hieraus können - je nach dem zur Anwendung kommenden Bildaufnahmeparameter - Teilbereiche ausgefiltert werden, die für die jeweilige Aufnahme verwendet werden sollen.

[0041] Vor dem optischen Sensor 116 ist ein Verschluss 122, d. h. ein so genannter Shutter, angeordnet, der während der Belichtungszeit eine Öffnung freigibt, durch welche von dem Dokument 100 reflektierte Strahlung und/oder durch das Dokument transmittierte Strahlung auf den optischen Sensor 116 einfallen kann.

[0042] Bei dem optischen Sensor 116 kann es sich zum Beispiel um eine Kamera handeln, wie zum Beispiel einen CCD-Sensor. Der optische Sensor 116, die Strahlungsquellen 118 und 120 sowie der Verschluss 122 werden von einem Prozessor 124 des Prüfgeräts 112 angesteuert.

[0043] Der Prozessor 124 dient zur Ausführung der Programminstruktionen eines Programms 126. Das Programm 126 beinhaltet Programminstruktionen 128 zur Aufnahme eines ersten Bildes des Teilbereichs 108 anhand erster Bildaufnahmeparameter. Die ersten Bildaufnahmeparameter können in den Programminstruktionen 128 beinhaltet sein.

[0044] Ferner beinhaltet das Programm 126 Programminstruktionen 130 für eine optische Zeichenerkennung (OCR) in dem ersten Bild, d. h. in der MRZ. Das Programm 126 beinhaltet ferner Programminstruktionen 132 zur Durchführung einer Datenbankabfrage anhand einer mittels OCR aus der MRZ gewonnenen Information, welche unmittelbar oder mittelbar den Typ des Dokuments

100 angibt.

[0045] Das Programm 126 beinhaltet ferner Programminstruktionen 134 zur Aufnahme des zweiten Bildes des Dokuments 100 anhand der von der Datenbank 136 empfangenen typspezifischen zweiten Bildaufnahmeparameter. Bei dem zweiten Bild kann es sich um ein Gesamtbild, d. h. ein vollständiges Bild des Dokuments, handeln, was auch als Full-Page-Reading bezeichnet wird.

[0046] Das Programm 126 beinhaltet ferner Programminstruktionen 138 zur Auswertung des zweiten Bildes, um ein oder mehrere Sicherheitsmerkmale des Dokuments zu überprüfen. Wenn die zum Beispiel in der Datenbank 136 dem Dokumententyp des Dokuments 100 zugeordneter Sicherheitsmerkmale in dem zweiten Bild vorhanden sind, so gilt das Dokument 100 als echt.

[0047] Das Programm 126 kann ferner Programminstruktionen 140 beinhalten, um eine Nutzer-Schnittstelle zur Verfügung zu stellen. Die Nutzer-Schnittstelle 140 kann durch eine optische und/oder akustische Signalausgabe gebildet werden. Beispielsweise wird ein erstes Signal ausgegeben, wenn das Dokument als echt erkannt worden ist und ein zweites Signal, wenn das Dokument die Echtheitsprüfung nicht bestanden hat.

[0048] Die Nutzer-Schnittstelle kann auch als grafische Nutzer-Schnittstelle ausgebildet sein. In diesem Fall ist ein Bildschirm 142 mit dem Prüfgerät 112 verbunden; beispielsweise kann der Bildschirm 142 dazu dienen, das zweite Bild des Dokuments wiederzugeben, um das zweite Bild einer Sichtprüfung zu unterziehen.

[0049] Beispielsweise soll das Prüfgerät 112 zur Prüfung von Reisepässen unterschiedlicher Länder verwendbar sein. Bei den unterstützten Dokumententypen handelt es sich also um die Reisepässe der verschiedenen Länder, die jeweils unterschiedlich spezifiziert sind.

[0050] Beispielsweise handelt es sich bei einem ersten Dokumententyp um den Reisepass eines Landes A. Für diesen Dokumententyp ist die Aufnahme des zweiten Bildes mit bestimmten zweiten Bildaufnahmeparametern optimal. Für die Beleuchtung ist dieses der Parameter I(A), welcher beispielsweise die Stromstärke oder Spannung zur Ansteuerung der Strahlungsquelle 120 angibt sowie der Parameter T(A), der die Belichtungszeit, d. h. die Öffnungszeit für den Verschluss 122 angibt. Alternativ oder zusätzlich kann als Belichtungsparameter auch die Leuchtdauer der Strahlungsquelle 120 angegeben sein.

[0051] Ferner können in der Datenbank 136 dem ersten Dokumententyp, d. h. dem Reisepass des Landes A, ein oder mehrere Sicherheitsmerkmale zugeordnet sein, die beispielsweise über ihre Lage in dem Dokument und deren Form spezifiziert sein können. Entsprechend verhält es sich für einen weiteren Dokumententyp, d. h. dem Reisepass des Landes B, für welches andere, zweite Bildaufnahmeparameter in der Datenbank 136 angegeben sind, nämlich der Parameter I(B) für die Beleuchtung und der Parameter T(B) für die Belichtungszeit sowie eine Spezifizierung der Sicherheitsmerkmale des Reisepass des Landes B, beispielsweise hinsichtlich deren Lage und Form.

[0052] Beispielsweise betrifft also jeder Eintrag in der Datenbank 136 einen bestimmten Dokumententyp, d. h. hier den Reisepass eines bestimmten Landes.

[0053] Optional kann das Prüfgerät 112 eine Schnittstelle 144 zur Kommunikation mit dem Chip 110 aufweisen. Beispielsweise kann es sich bei der Schnittstelle 144 um eine so genannte RFID-Schnittstelle handeln. Auch die Schnittstelle 144 kann von dem Prozessor 124 angesteuert werden.

[0054] Die Programminstruktionen 128, 130, 132, 134, 138 und 140 können ganz oder teilweise als so genannte Firmware realisiert sein. Eine Aktualisierung der Programminstruktionen kann dann über ein so genanntes Firmware-Update erfolgen. Insbesondere können auf diese Art und Weise die ersten Bildaufnahmeparameter zur Aufnahme des ersten Bildes aktualisiert werden, wenn diese Teil der Programminstruktionen, insbesondere Teil der Programminstruktionen 128, sind.

[0055] Zur Prüfung des Dokuments 100 wird also wie folgt vorgegangen:
Die Ausführung der Programminstruktionen 128 wird gestartet, sodass die Strahlungsquelle 118 aktiviert wird, um das Dokument 100 mit IR-Strahlung zu bestrahlen. Ferner wird der Verschluss 122 angesteuert, sodass er sich während einer durch die ersten Bildaufnahmeparameter gegebenen Öffnungszeit öffnet. Die Stromstärke oder die Spannung für die Ansteuerung der Strahlungsquelle 118 ist ebenfalls durch die ersten Bildaufnahmeparameter gegeben.

[0056] Durch den optischen Sensor 116 wird also das erste Bild des Teilbereichs 108 mit den ersten Bildaufnahmeparametern aufgenommen.

[0057] Nach Aufnahme des ersten Bildes wird die Ausführung der Programminstruktionen 130 gestartet, um die OCR durchzuführen. Als Ergebnis der OCR wird eine Information in dem Bild erkannt, wie zum Beispiel eine Angabe des Landes, welches das Dokument 100 ausgestellt hat. Im Weiteren wird ohne Beschränkung der Allgemeinheit davon ausgegangen, dass es sich hierbei um das Land A handelt.

[0058] Nach Erkennung der Information wird die Ausführung der Programminstruktionen 132 gestartet. Durch Ausführung der Programminstruktionen 132 wird eine Datenbankabfrage generiert, welche die Information, d. h. die Angabe "Land A", als Zugriffsschlüssel beinhaltet. Die Datenbank 136 antwortet daraufhin auf die Datenbankabfrage durch Ausgabe der dem Dokumententyp für das Land A zugeordneten Datenbankeinträge, d. h. der zweiten Bildaufnahmeparameter I(A) und T(A) sowie der Beschreibung der Sicherheitsmerkmale, die diesem Dokumententyp in der Datenbank 136 zugeordnet sind.

[0059] Nach Empfang der Antwort von der Datenbank 136 wird die Ausführung der Programminstruktionen 134 gestartet, um das zweite Bild, d. h. ein Gesamtbild, von dem Dokument 100 mit Hilfe der zweiten Bildaufnahmeparameter aufzunehmen. Hierzu wird die Strahlungs-

quelle 120 entsprechend dem Parameter I(A) angesteuert, um die optimale Beleuchtung gemäß der Spezifikation der zweiten Bildaufnahmeparameter zu gewährleisten. Ferner wird der Verschluss 122 angesteuert, um den optischen Sensor 116 während der Belichtungszeit T(A) zu belichten.

[0060] Nach dem so das Gesamtbild von dem Dokument 100 durch den optischen Sensor 116 aufgenommen worden ist, wird die Ausführung der Programminstruktionen 138 zur Auswertung des zweiten Bildes gestartet. Durch Ausführung der Programminstruktionen 138 wird beispielsweise geprüft, ob in dem zweiten Bild die in der Antwort der Datenbank 136 spezifizierten Sicherheitsmerkmale vorhanden sind.

[0061] Wenn eine hinreichende Übereinstimmung zwischen dem in dem zweiten Bild aufgefundenen Sicherheitsmerkmalen zu den in der Antwort der Datenbank spezifizierten Sicherheitsmerkmale durch Ausführung der Programminstruktionen 138 festgestellt wird, so wird durch Ausführung der Programminstruktionen 140 ein entsprechendes Signal über die Nutzer-Schnittstelle ausgegeben, um einen Benutzer von dem Ergebnis der Überprüfung des Dokuments 100 zu informieren.

[0062] Alternativ oder zusätzlich kann ein solches, das Ergebnis der Überprüfung des Dokuments anzeigendes Signal an ein weiteres Gerät ausgegeben werden, welches dieses Signal weiterverarbeitet. Bei diesem weiteren Gerät kann es sich zum Beispiel um ein Drehkreuz oder dergleichen handeln, welches bei Empfang eines Signals, welches die Echtheit des Dokuments 100 angibt, freigegeben wird.

[0063] Nach Ausführungsformen der Erfindung kann in die Überprüfung des Dokuments 100 auch der Chip 110 einbezogen werden. Hierzu werden die in dem elektronischen Speicher 114 des Chips 110 gespeicherten Daten von der Schnittstelle 144 des Prüfgeräts 112 ausgelesen. Diese Daten können dann mit aus dem ersten und/oder zweiten Bild erkannten Daten verglichen werden. Die Übereinstimmung der aus dem elektronischen Speicher 114 gelesenen Daten und der aus dem ersten und/oder zweiten Bild erkannten Daten kann eine notwendige Voraussetzung für das Bestehen der Echtheitsprüfung des Dokuments 100 sein.

[0064] Beispielsweise werden die aus dem elektronischen Speicher 114 gelesenen digitalisierten Daten des Gesichtsbildes 102 neben dem zweiten Bild auf dem Bildschirm 142 wiedergegeben, sodass die beiden Bilder auf Stimmigkeit überprüft werden können.

[0065] Ferner ist es auch möglich, dass zum Beispiel der fluoreszierende Aufdruck 106 Daten beinhaltet, die in dem zweiten Bild zum Vorschein kommen, da es ja mit Hilfe der UV-Strahlungsquelle 120 aufgenommen worden ist. Auch diese Daten können mit aus dem elektronischen Speicher abgerufenen Daten abgeglichen werden, indem diese Daten zum Beispiel auf dem Bildschirm 142 ausgegeben oder maschinell miteinander verglichen werden.

[0066] Die Figur 2 zeigt ein entsprechendes Flussdiagramm. In dem Bild 200 wird zur Prüfung eines Dokuments ein erstes Bild mit ersten Bildaufnahmeparametern aufgenommen, wobei die ersten Bildaufnahmeparameter standardisiert sind. Die ersten Bildaufnahmeparameter kommen also unabhängig vom Dokumententyp in jedem Fall zur Anwendung. Vorzugsweise wird für die Aufnahme des ersten Bildes einer Beleuchtung im IR-Bereich verwendet, da im IR-Bereich das Reflexionsverhalten weitgehend unabhängig vom Dokumententyp ist und ferner fluoreszierende Sicherheitsmerkmale durch Bestrahlung im IR-Bereich nicht angesprochen werden. Das erste Bild zur Aufnahme der MRZ kann also für alle Dokumententypen auf der Basis der standardisierten ersten Bildaufnahmeparameter mit einer hohen Qualität aufgenommen werden, und zwar gleichermaßen für Dokumententypen mit einer Papieroberfläche und für Dokumententypen mit einer im sichtbaren Bereich stärker reflektierenden Kunststoffoberfläche.

[0067] In dem Schritt 202 wird dann eine Information, beispielsweise mit OCR, in dem ersten Bild erkannt. Hierbei handelt es sich um eine Information, die unmittelbar oder mittelbar den Dokumententyp angibt, wie zum Beispiel das Land, welches das Dokument ausgestellt hat.

[0068] In dem Schritt 204 wird mit Hilfe der in dem Schritt 202 erkannten Information eine Datenbankabfrage durchgeführt. Die Datenbank antwortet auf die Datenbankabfrage mit zweiten Bildaufnahmeparametern, welche spezifisch für den Dokumententyp des zu prüfenden Dokuments sind.

[0069] In dem Schritt 206 wird daraufhin ein zweites Bild, vorzugsweise ein Gesamtbild, des Dokuments mit Hilfe der typspezifischen Bildaufnahmeparameter aufgenommen, welche die Datenbank in dem Schritt 204 ausgegeben hat. In dem Schritt 208 erfolgt daraufhin eine Überprüfung der optischen Sicherheitsmerkmale des Dokuments anhand des so erfassten zweiten Bildes.

[0070] Die Figur 3 zeigt eine Ausführungsform eines erfindungsgemäßen Datenverarbeitungssystems 146. Das Datenverarbeitungssystem 146 beinhaltet mehrere Prüfgeräte 112, die jeweils im Prinzip so aufgebaut sind wie das Prüfgerät 112 in der Ausführungsform der Figur 1. Im Unterschied zu der Ausführungsform der Figur 1 beinhalten aber die Prüfgeräte 112 in der Ausführungsform der Figur 3 nicht die Datenbank 136. Stattdessen beinhalten die Prüfgeräte 112 jeweils eine Kommunikations-Schnittstelle 148 zur Kommunikation über ein Netzwerk 150.

[0071] Bei dem Netzwerk 150 kann es sich um ein Ethernet, ein Virtual Private Network (VPN) oder ein anderes Kommunikations-Netzwerk handeln. Insbesondere kann ein Internet-Protokoll (IP) für die Kommunikation über das Netzwerk 150 zur Anwendung kommen.

[0072] In der hier betrachteten Ausführungsform sind eine Datenbank 152 und eine Datenbank 154 über das Netzwerk 150 von den Prüfgeräten 112 abfragbar. Die Datenbank 152 beinhaltet die den Dokumententypen zugeordneten zweiten Bildaufnahmeparameter. In der hier betrachteten Ausführungsform beinhalten die zweiten

Bildaufnahmeparameter neben Angaben zur Beleuchtung I und zur Belichtung T auch eine Angabe zu der Frequenz F, welche für die Beleuchtung zur Aufnahme des zweiten Bildes verwendet werden soll.

[0073] Dagegen beinhaltet die Datenbank 152 in der Ausführungsform der Figur 3 nicht Angaben zu den Sicherheitsmerkmalen, wie dies bei der Datenbank 136 in der Ausführungsform der Figur 1 der Fall ist. Diese Angaben sind gemäß der Ausführungsform der Figur 3 dagegen in der separaten Datenbank 154 typspezifisch gespeichert. Bei dieser Ausführungsform werden also durch Ausführung der Programminstruktionen 132 zwei Datenbankabfragen generiert, nämlich zur Abfrage der Datenbanken 152 und 154.

Bezugszeichenliste

[0074]

100	Dokument
102	Gesichtsbild
104	Sicherheitsfarben
106	Aufdruck
108	Teilbereich
110	Chip
112	Prüfgerät
114	elektronischer Speicher
116	optischer Sensor
118	Strahlungsquelle
120	Strahlungsquelle
122	Verschluss
124	Prozessor
126	Programm
128	Programminstruktionen
130	Programminstruktionen
132	Programminstruktionen
134	Programminstruktionen
136	Datenbank
138	Programminstruktionen
140	Programminstruktionen
142	Bildschirm
144	Schnittstelle
146	Datenverarbeitungssystem
148	Kommunikations-Schnittstelle
150	Netzwerk
152	Datenbank
154	Datenbank

Patentansprüche

1. Verfahren zur Prüfung der Echtheit eines Dokuments (100) mit folgenden Schritten:

- Aufnahme eines ersten Bildes des Dokuments mit ersten Bildaufnahmeparametern,
- Erkennung einer Information in dem ersten Bild, wobei die Erkennung der Information in dem ersten Bild mittels optischer Zeichenerkennung erfolgt, wobei die Information die Angabe eines Dokumententyps beinhaltet oder wobei aus der Information ein Dokumententyp des Dokuments ableitbar ist,
- Durchführung einer Datenbankabfrage einer Datenbank (136; 152, 154) mit Hilfe der Information zur Abfrage von zweiten Bildaufnahmeparametern, wobei die Datenbank (136; 152) für jeden vordefinierten Dokumententyp typspezifische zweite Bildaufnahmeparameter beinhaltet, wobei die typspezifischen zweiten Bildaufnahmeparameter mit Hilfe der Information als Datenbankschlüssel abrufbar sind,
- Aufnahme eines zweiten Bildes des Dokuments mit den zweiten Bildaufnahmeparametern, wobei die zweiten Bildaufnahmeparameter typspezifische Parameter bezüglich der Beleuchtung des Dokuments und/oder bezüglich der Belichtung eines optischen Sensors, mit Hilfe dessen das zweite Bild aufgenommen wird, beinhalten.
- Überprüfung von ein oder mehreren Sicherheitsmerkmalen des Dokuments anhand des zweiten Bildes,

wobei die Datenbank (136; 154) typspezifische Angaben zu den Sicherheitsmerkmalen beinhaltet, wobei die typspezifischen Angaben zu den Sicherheitsmerkmalen bei der Durchführung der Datenbankabfrage mit abgefragt werden und für die Überprüfung verwendet werden, wobei die Angaben zu den Sicherheitsmerkmalen Angaben zu Lage und Form der Sicherheitsmerkmale beinhalten, wobei diese Angaben als Soll-Merkmale mit in dem zweiten Bild vorhandenen Ist-Merkmalen verglichen werden, wobei bei hinreichender Übereinstimmung der Ist-Merkmale mit den Soll-Merkmalen von der Echtheit des Dokuments ausgegangen wird.

2. Verfahren nach Anspruch 1, wobei die Aufnahme des ersten Bildes in einem ersten Frequenzbereich und die Aufnahme des zweiten Bildes in einem zweiten Frequenzbereich erfolgen, wobei die ersten und zweiten Frequenzbereiche voneinander verschieden sind.

3. Verfahren nach Anspruch 2, wobei es sich bei dem ersten Frequenzbereich um einen IR-Frequenzbereich und bei dem zweiten Frequenzbereich um einen UV-Frequenzbereich handelt.

4. Verfahren nach Anspruch 1, 2 oder 3, wobei das erste Bild nur einen Teilbereich (108) des Dokuments beinhaltet, der hinsichtlich seiner Lage in dem Dokument vordefiniert ist, wobei die ersten Bildaufnahmeparameter zur Aufnahme des Teilbereichs unabhängig von einem Typ des Dokuments verwen-

det werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei es sich bei dem zweiten Bild um ein Gesamtbild des Dokuments handelt.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei zumindest eines der Sicherheitsmerkmale fluoreszierend ist.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verfahren ferner umfasst:

- Auslesen von in einem Chip (110) des Dokuments gespeicherten Daten mit einer Schnittstelle (144) zur Kommunikation mit dem Chip,
- Vergleichen von Daten, die aus dem zweiten Bild erfasst werden, mit den aus dem Chip ausgelesenen Daten, wobei eine Übereinstimmung der aus dem zweiten Bild erfassten Daten mit den aus dem Chip ausgelesenen Daten eine notwendige Voraussetzung für das Bestehen der Echtheitsprüfung des Dokuments ist.

8. Computerprogrammprodukt mit von einem Prüfgerät ausführbaren Programminstruktionen zur Ausführung eines Verfahrens nach einem der vorhergehenden Ansprüche.

9. Datenverarbeitungssystem, welches konfiguriert ist zum Ausführen eines Verfahrens zur Prüfung der Echtheit von Dokumenten nach einem der Ansprüche 1 bis 7 mit:

- zumindest einem elektronischen Gerät mit:
  - Mitteln (116, 118, 120, 122, 128, 134) zur Aufnahme eines ersten Bildes zumindest eines Teilbereichs (108) des Dokuments mit ersten Bildaufnahmeparametern und zur Aufnahme eines zweiten Bildes des Dokuments mit zweiten Bildaufnahmeparametern,
  - Mitteln (130) zur Erkennung einer Information in dem ersten Bild, wobei die Erkennung der Information in dem ersten Bild mittels optischer Zeichenerkennung erfolgt,
  - Mitteln (132) zur Durchführung einer Datenbankabfrage einer Datenbank (136; 152, 154) mit Hilfe der Information zur Abfrage der zweiten Bildaufnahmeparameter,
  - Mitteln (138) zur Überprüfung von ein oder mehreren Sicherheitsmerkmalen des Dokuments anhand des zweiten Bildes,
- zumindest einer Datenbank (136; 152), die für jeden Dokumententyp typspezifische zweite Bildaufnahmeparameter beinhaltet, wobei die typspezifischen zweiten Bildaufnahmeparameter mit Hilfe der Information als Datenbankschlüssel abrufbar sind, wobei die Datenbank (136; 154) typspezifische Angaben zu den Sicherheitsmerkmalen beinhaltet, welche die Lage der Sicherheitsmerkmale in dem Dokument und deren Form spezifizieren, wobei die typspezifischen Angaben zu den Sicherheitsmerkmalen bei der Durchführung der Datenbankabfrage mit abgefragt werden und für die Überprüfung verwendet werden, wobei die Angaben zu den Sicherheitsmerkmalen Angaben zu Lage und Form der Sicherheitsmerkmale beinhalten, wobei diese Angaben als Soll-Merkmale mit in dem zweiten Bild vorhandenen Ist-Merkmalen verglichen, wobei bei hinreichender Übereinstimmung der Ist-Merkmale mit den Soll-Merkmalen von der Echtheit des Dokuments ausgegangen wird,

wobei es sich bei der Datenbank um eine interne Datenbank (136) des zumindest einen elektronischen Geräts handelt oder wobei es sich bei der Datenbank um eine externe Datenbank (152, 154) handelt, mit welcher das zumindest ein elektronisches Gerät mit einer Kommunikationsschnittstelle über eine Kommunikationsverbindung verbindbar ist, um die Datenbankabfrage durchzuführen.

10. Datenverarbeitungssystem nach Anspruch 9, wobei das elektronische Gerät ferner umfasst:

- eine Schnittstelle (144) zur Kommunikation mit einem Chip (110) des Dokuments zum Auslesen von in dem Chip des Dokuments gespeicherten Daten,
- Mittel zum Vergleichen von Daten, die aus dem zweiten Bild erfasst werden, mit den aus dem Chip ausgelesenen Daten, wobei eine Übereinstimmung der aus dem zweiten Bild erfassten Daten mit den aus dem Chip ausgelesenen Daten eine notwendige Voraussetzung für das Bestehen der Echtheitsprüfung des Dokuments ist.

Claims

1. A method for testing the authenticity of a document (100) comprising the following steps:

- recording a first image of the document with first image recording parameters,
- recognising a piece of information in the first image, wherein the recognition of the information in the first image is performed by optical character recognition, wherein the information specifies a document type or wherein a document type of the document can be derived from

the information,
- making a database query to a database (136; 152, 154) using the information to query second image recording parameters, wherein the database (136; 152) for each predefined document type contains type-specific second image recording parameters, wherein the type-specific second image recording parameters can be retrieved by using the information as a database key, - recording a second image of the document with the second image recording parameters, wherein the second image recording parameters contain type-specific parameters regarding the illumination of the document and/or regarding the exposure of an optical sensor, by means of which the second image is recorded,
- checking one or more security features of the document against the second image,

wherein the database (136; 154) contains type-specific details on the security features, wherein the type-specific details on the security features are also queried when performing the database query and are used for the verification, wherein the details on the security features contain information on the location and form of the security features, wherein these details are compared as target features with the actual features present in the second image, wherein if the actual features sufficiently match the target features the authenticity of the document is assumed.

2. The method according to claim 1, wherein the first image is recorded in a first frequency range and the second image is recorded in a second frequency range, wherein the first and second frequency ranges differ from one another.

3. The method according to claim 2, wherein the first frequency range is an IR frequency range and the second frequency range is a UV frequency range.

4. The method according to claim 1, 2 or 3, wherein the first image contains only a partial area (108) of the document, which is predefined with regard to its location in the document, wherein the first image recording parameters for recording the partial area are used independently of a type of document.

5. The method according to any one of the preceding claims, wherein the second image is a complete image of the document.

6. The method according to any one of the preceding claims, wherein at least one of the security features is fluorescent.

7. The method according to any one of the preceding claims, wherein the method further comprises:

- reading data stored on a chip (110) of the document with an interface (144) for communicating with the chip,
- comparing data captured from the second image with data read from the chip, wherein a match between the data captured from the second image and the data read from the chip is a necessary prerequisite for passing the authenticity test of the document.

8. A computer program product having program instructions which can be executed by a testing device for performing a method according to any one of the preceding claims.

9. A data processing system, which is configured for performing a method for testing the authenticity of documents according to any one of claims 1 to 7, comprising:

- at least one electronic device, having:

  - means (116, 118, 120, 122, 128, 134) for recording a first image of at least a partial area (108) of the document with first image recording parameters and for recording a second image of the document with second image recording parameters,
  - means (130) for recognising a piece of information in the first image, wherein the recognition of the information in the first image is performed by optical character recognition,
  - means (132) for making a database query to a database (136; 152, 154) using the information to query the second image recording parameters,
  - means (138) for checking one or more security features of the document against the second image,

- at least one database (136; 152), which contains type-specific second image recording parameters for each document type, wherein the type-specific second image recording parameters can be retrieved by using the information as a database key, wherein the database (136; 154) contains type-specific information on the security features which specify the location of the security features in the document and their form, wherein the type-specific information on the security features is also queried when performing the database query and is used for the verification, wherein the details on the security features include details on the location and form of the security features, wherein these details

are compared as target features with actual features present in the second image, wherein if the actual features sufficiently match the target features it is assumed that the document is authentic,

wherein the database is an internal database (136) of the at least one electronic device or wherein the database is an external database (152, 154), to which the at least one electronic device with a communication interface can be connected via a communication connection in order to perform the database query.

10. The data processing system according to claim 9, wherein the electronic device further comprises:

- an interface (144) for communicating with a chip (110) of the document for reading data stored on the chip of the document,
- means for comparing data which are captured from the second image with the data read from the chip, wherein a match between the data captured from the second image and the data read from the chip is a necessary prerequisite for passing the authenticity test of the document.

Revendications

1. Procédé de test de l'authenticité d'un document (100) comprenant les étapes suivantes :

- enregistrement d'une première image du document avec des paramètres d'enregistrement de première image,
- reconnaissance d'un élément d'information dans la première image, dans lequel la reconnaissance des informations dans la première image est exécutée par reconnaissance optique de caractères, dans lequel les informations spécifient un type de document ou dans lequel un type de document du document peut être déduit des informations,
- réalisation d'une requête de base de données dans une base de données (136 ; 152, 154) en utilisant les informations pour rechercher des paramètres d'enregistrement de seconde image, dans lequel la base de données (136 ; 152) pour chaque type de document prédéfini contient des paramètres d'enregistrement de seconde image spécifiques d'un type, dans lequel les paramètres d'enregistrement de seconde image spécifiques d'un type peuvent être récupérés par utilisation des informations comme clé de base de données,

- enregistrement d'une seconde image du document avec les paramètres d'enregistrement de seconde image, dans lequel les paramètres d'enregistrement de seconde image contiennent des paramètres spécifiques d'un type concernant l'éclairage du document et/ou concernant l'exposition d'un capteur optique, au moyen de quoi la seconde image est enregistrée,

- contrôle d'une ou de plusieurs caractéristiques de sécurité du document par rapport à la seconde image,

dans lequel la base de données (136 ; 154) contient des détails spécifiques d'un type sur les caractéristiques de sécurité, dans lequel les détails spécifiques d'un type sur les caractéristiques de sécurité sont également recherchés lors de l'exécution de la requête de base de données et sont utilisés pour la vérification, dans lequel les détails sur les caractéristiques de sécurité contiennent des informations sur l'emplacement et la forme des caractéristiques de sécurité, dans lequel ces détails sont comparés en tant que caractéristiques cibles aux caractéristiques réelles présentes dans la seconde image, dans lequel si les caractéristiques réelles correspondent suffisamment aux caractéristiques cibles, l'authenticité du document est supposée.

2. Procédé selon la revendication 1, dans lequel la première image est enregistrée dans une première plage de fréquences et la seconde image est enregistrée dans une seconde plage de fréquences, dans lequel les première et seconde plages de fréquence diffèrent l'une de l'autre.

3. Procédé selon la revendication 2, dans lequel la première plage de fréquences est une plage de fréquences IR et la seconde plage de fréquences est une plage de fréquences UV.

4. Procédé selon la revendication 1, 2 ou 3, dans lequel la première image contient uniquement une zone partielle (108) du document, qui est prédéfinie par rapport à son emplacement dans le document, dans lequel les paramètres d'enregistrement de première image pour l'enregistrement de la zone partielle sont utilisés indépendamment d'un type de document.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel la seconde image est une image complète du document.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel au moins une des caractéristiques de sécurité est fluorescente.

7. Procédé selon l'une quelconque des revendications

précédentes, dans lequel le procédé comprend en outre :

- lecture des données stockées sur une puce (110) du document avec une interface (144) pour communication avec la puce,
- comparaison des données capturées depuis la seconde image avec des données lues depuis la puce, dans lequel une correspondance entre les données capturées depuis la seconde image et les données lues depuis la puce est un prérequis nécessaire pour la réussite du test d'authenticité du document.

8. Produit de programme informatique ayant des instructions de programme qui peuvent être exécutées par un dispositif de test pour l'exécution d'un procédé selon l'une quelconque des revendications précédentes.

9. Système de traitement des données, qui est conçu pour l'exécution d'un procédé pour le test de l'authenticité de documents selon l'une quelconque des revendications 1 à 7, comprenant :

- au moins un dispositif électronique, ayant :

  - des moyens (116, 118, 120, 122, 128, 134) d'enregistrement d'une première image d'au moins une zone partielle (108) du document avec des paramètres d'enregistrement de première image et d'enregistrement d'une seconde image du document avec des paramètres d'enregistrement de seconde image,
  - des moyens (130) pour la reconnaissance d'un élément d'information dans la première image, dans lequel la reconnaissance des informations dans la première image est exécutée par reconnaissance optique de caractères,
  - des moyens (132) de réalisation d'une requête de base de données (136 ; 152, 154) en utilisant les informations pour rechercher les paramètres d'enregistrement de seconde image,
  - des moyens (138) de contrôle d'une ou de plusieurs caractéristiques de sécurité du document par rapport à la seconde image,

- au moins une base de données (136 ; 152), qui contient des paramètres d'enregistrement de seconde image spécifiques d'un type pour chaque type de document, dans lequel les paramètres d'enregistrement de seconde image spécifiques d'un type peuvent être récupérés par utilisation des informations comme clé de base de données, dans lequel la base de données (136 ; 154) contient des informations spécifiques d'un type sur les caractéristiques de sécurité qui spécifient l'emplacement des caractéristiques de sécurité et leur forme, dans lequel les informations spécifiques d'un type sur les caractéristiques de sécurité sont également recherchées lors de l'exécution de la requête de base de données et sont utilisées pour la vérification, dans lequel les détails sur les caractéristiques de sécurité contiennent des détails sur l'emplacement et la forme des caractéristiques de sécurité, dans lequel ces détails sont comparés en tant que caractéristiques cibles aux caractéristiques réelles présentes dans la seconde image, dans lequel si les caractéristiques réelles correspondent suffisamment aux caractéristiques cibles, il est supposé que le document est authentique,

dans lequel la base de données est une base de données interne (136) de l'au moins un dispositif électronique ou dans lequel la base de données est une base de données externe (152, 154), à laquelle l'au moins un dispositif électronique avec une interface de communication peut être connecté via une connexion de communication pour exécuter la requête de base de données.

10. Système de traitement de données selon la revendication 9, dans lequel le dispositif électronique comprend en outre :

- une interface (144) pour communication avec une puce (110) du document pour la lecture de données stockées sur la puce du document,
- des moyens de comparaison des données qui sont capturées depuis la seconde image avec les données lues depuis la puce, dans lequel une correspondance entre les données capturées depuis la seconde image et les données lues depuis la puce est un prérequis nécessaire pour la réussite du test d'authenticité du document.

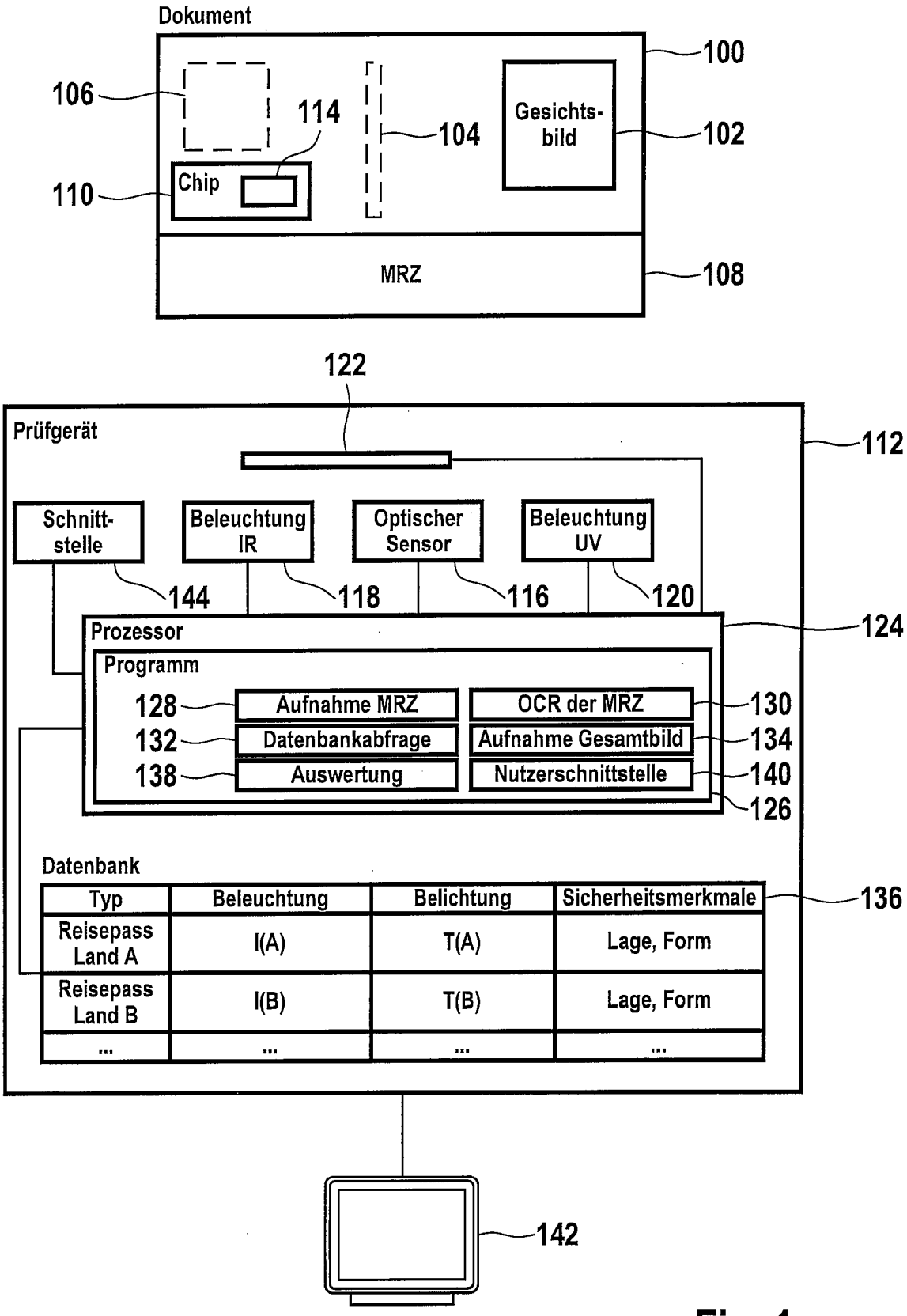
Dokument
100
106
114
104
Gesichts-
bild
102
Chip
110
MRZ
108
122
Prüfgerät
112
Schnitt-
stelle
Beleuchtung
IR
Optischer
Sensor
Beleuchtung
UV
144
118
116
120
Prozessor
124
Programm
128
Aufnahme MRZ
OCR der MRZ
130
132
Datenbankabfrage
Aufnahme Gesamtbild
134
138
Auswertung
Nutzerschnittstelle
140
126
Datenbank
136
Typ
Beleuchtung
Belichtung
Sicherheitsmerkmale
Reisepass
Land A
I(A)
T(A)
Lage, Form
Reisepass
Land B
I(B)
T(B)
Lage, Form
...
...
...
...
142

Fig. 1

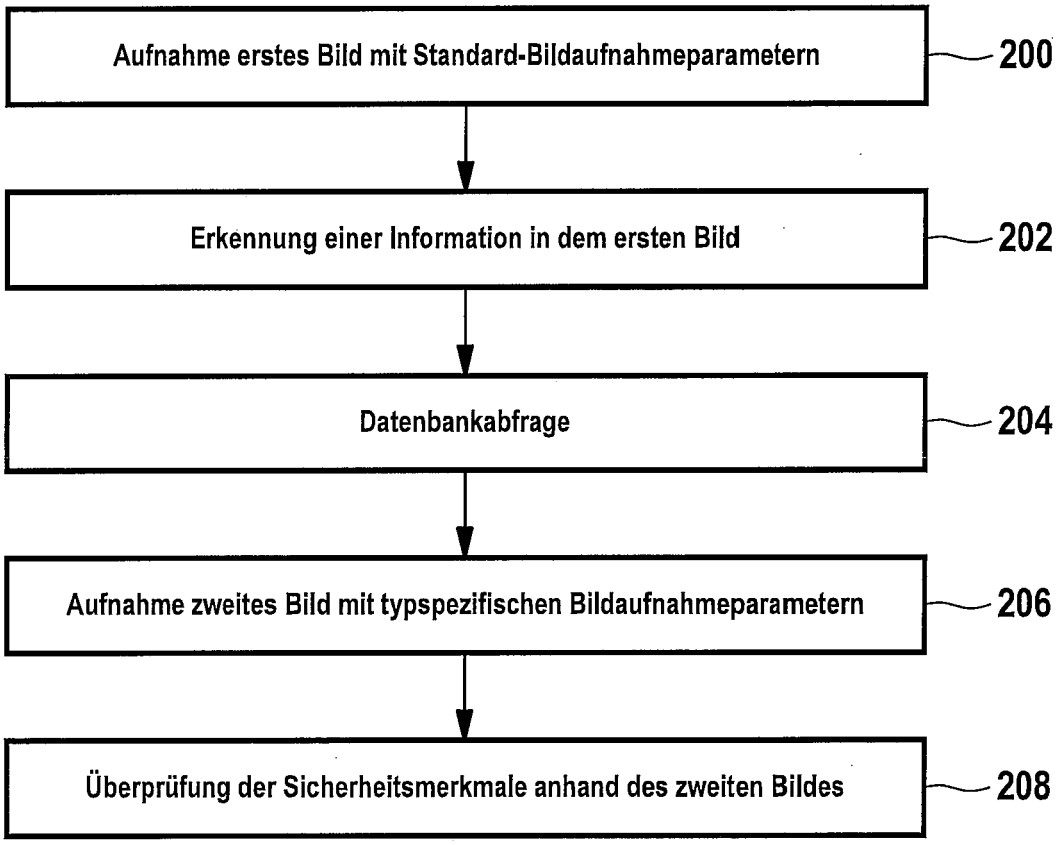
Aufnahme erstes Bild mit Standard-Bildaufnahmeparametern
200
Erkennung einer Information in dem ersten Bild
202
Datenbankabfrage
204
Aufnahme zweites Bild mit typspezifischen Bildaufnahmeparametern
206
Überprüfung der Sicherheitsmerkmale anhand des zweiten Bildes
208

Fig. 2

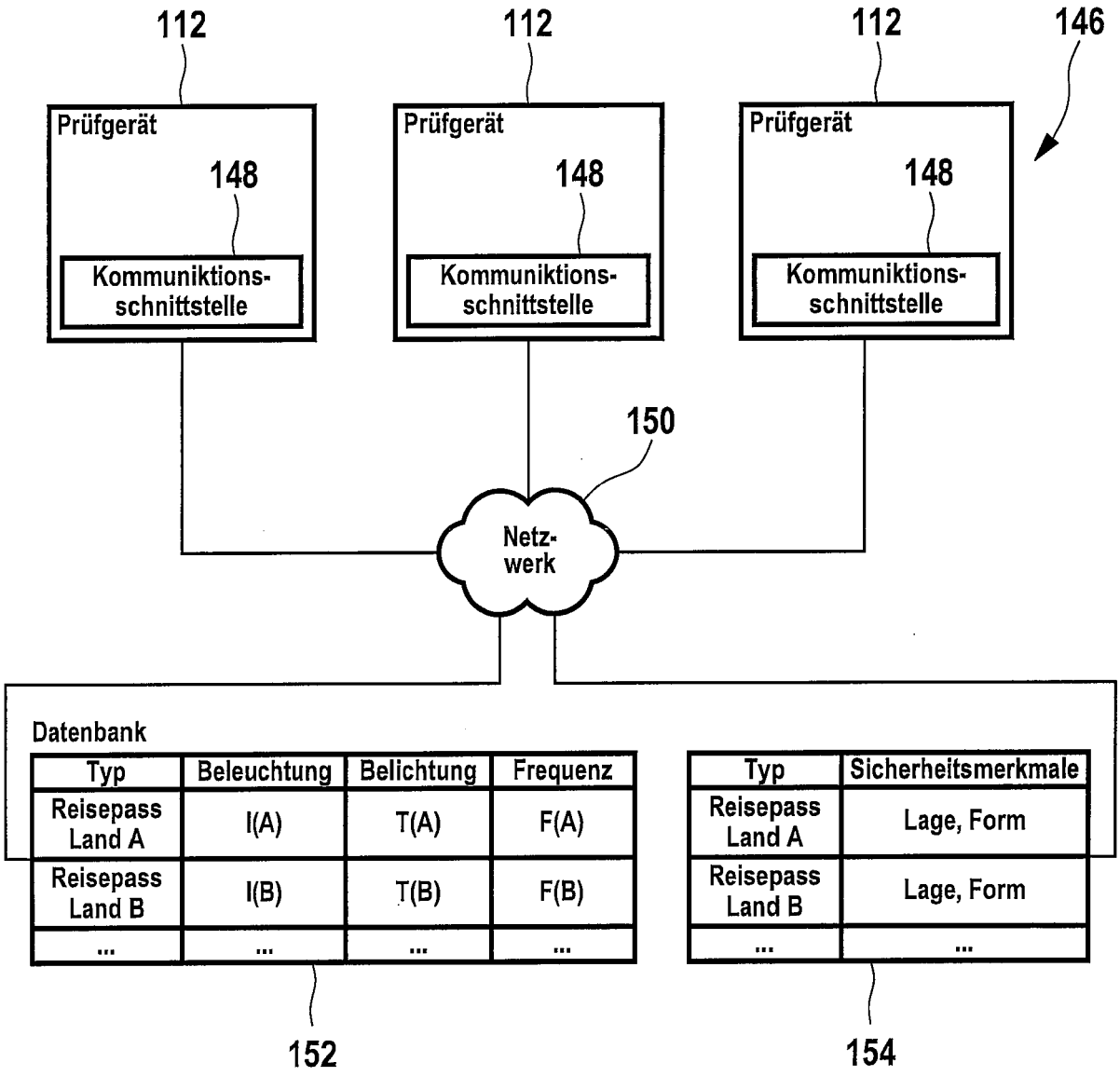
112
112
112
146
Prüfgerät
148
Kommuniktions-schnittstelle
Prüfgerät
148
Kommuniktions-schnittstelle
Prüfgerät
148
Kommuniktions-schnittstelle
150
Netz-werk
Datenbank
Typ
Beleuchtung
Belichtung
Frequenz
Reisepass Land A
I(A)
T(A)
F(A)
Reisepass Land B
I(B)
T(B)
F(B)
...
...
...
...
152
Typ
Sicherheitsmerkmale
Reisepass Land A
Lage, Form
Reisepass Land B
Lage, Form
...
...
154

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 7046346 B2 **[0003]**
- US 20070260886 A1 **[0003]**
- US 2006078186 A1 **[0004]**
- US 2004222283 A1 **[0005]**
- JP 2002170142 A **[0006]**
- DE 19906388 A1 **[0007]**
- EP 1883053 A1 **[0008]**