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

(11) **EP 3 185 221 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
07.06.2023 Patentblatt 2023/23

(21) Anmeldenummer: **15202557.3**

(22) Anmeldetag: **23.12.2015**

(51) Internationale Patentklassifikation (IPC):
G07D 7/005 *(2016.01)* ***G07D 7/207*** *(2016.01)*
G07D 7/20 *(2016.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G07D 7/20; G07D 7/0054; G07D 7/207; G07D 7/2075

(54) **AUTHENTIFIKATIONSVORRICHTUNG UND VERFAHREN ZUR OPTISCHEN ODER AKUSTISCHEN ZEICHENERKENNUNG**

AUTHENTICATION APPARATUS AND METHOD FOR OPTICAL OR ACOUSTIC CHARACTER RECOGNITION

DISPOSITIF D'AUTHENTIFICATION ET PROCEDE DE RECONNAISSANCE OPTIQUE OU ACOUSTIQUE

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

(43) Veröffentlichungstag der Anmeldung:
28.06.2017 Patentblatt 2017/26

(73) Patentinhaber: **Kisters, Friedrich**
8280 Kreuzlingen (CH)

(72) Erfinder: **Kisters, Friedrich**
8280 Kreuzlingen (CH)

(74) Vertreter: **Patentanwälte Dr. Keller, Schwertfeger Partnerschaft mbB**
Westring 17
76829 Landau (DE)

(56) Entgegenhaltungen:
EP-A1- 2 824 641
DE-A1-102014 004 349
DE-B3-102009 036 706
US-A1- 2002 153 661

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

EP 3 185 221 B1

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Authentifikationsvorrichtung und ein Verfahren zur Authentifikation oder Bestimmung der Identität einer Person, eines Gerätes, einer Sache, eines Dienstes, einer Anwendung und/oder eines Computerprogrammes, bei dem eine Authentifikation über ein Sicherheitselement mit wenigstens einem Sicherheitsmerkmal und einer Authentifikationseinrichtung erfolgt, bei der eine optische Zeichenerkennung und anschließende Umwandlung der erkennbaren Zeichen in lesbare Zeichen erfolgt. Schließlich erfolgt ein Abgleich mit hinterlegten Referenzzeichen oder computerlesbaren Referenzmerkmalen.

[0002] Sicherheitselemente mit unterschiedlich ausgeprägten Sicherheitsmerkmalen sind bekannt. So beschreibt beispielsweise die DE 10 2004 055 761 A1 ein blattförmiges Wertdokument, bei dem als Sicherheitsmerkmal ein im nicht sichtbaren Spektralbereich erfassbarer Code sowie weitere Sicherheitsmerkmale in Form von sichtbaren Merkmalen vorgesehen sind. Daneben ist auch bekannt, dass beispielsweise komplexe Oberflächenstrukturen wie Risse und Sprünge als Sicherheitsmerkmal, ähnlich einem Fingerabdruck, für eine Authentifizierung herangezogen werden können. Ein solches Sicherheitselement ist beispielsweise in der US 7,793,837 B1 beschrieben, wobei einzelne Risse derart ausgestaltet sind, dass sie eine Zeichenfolge überlagern. Eine dynamische Veränderung der Rissstruktur und eine dadurch bedingte Veränderung der Auslesbarkeit der abgebildeten Zeichen sind jedoch nicht offenbart.

[0003] Daneben gibt es auch dynamische Sicherheitsmerkmale, beispielsweise in Form von Krakelee-Strukturen, die sich in einer Art und Weise zufällig weiterentwickeln, so dass mögliche Fälschungen nicht vorhersehbar sind. Ein solches Krakelee-Muster in Form von Rissen oder Sprüngen, Ausbrüchen, Abnutzung oder Schrumpfungen ist vom Anmelder beschrieben in der DE 10 2009 003 221 A1. Durch die zufällige Entwicklung des Krakelees wird ein Sicherheitsmerkmal geschaffen, das durch einen Nachahmer nahezu unmöglich zu fälschen ist. Durch die dynamische Weiterentwicklung des Krakelees wird die Fälschungssicherheit noch weiter erhöht.

[0004] Daneben gibt es auch optische Sicherheitsmerkmale, die über ein elektronisch gesteuertes Anzeigeelement dargestellt werden und dadurch optisch variabel sind. Ein solches optisch variables Element ist in der DE 10 2004 045 211 A1 beschrieben. Dabei überdeckt sich ein elektrisch gesteuertes Anzeigeelement und eine defraktive Struktur zumindest bereichsweise, so dass das optische Erscheinungsbild des durch die defraktive Struktur erzeugten optischen Effekts durch das elektrisch gesteuerte Anzeigeelement zumindest teilweise beeinflusst ist. Daneben gibt es auch Verfahren um Zeichen, beispielsweise die Darstellung von Echtheitsdaten oder sonstigen Messwerten zu verschleiern, indem sogenannte Tarndaten visuell dargestellt werden, die über einen mathematischen Algorithmus generiert werden. Eine solche Vorrichtung und ein solches Verfahren sind in der DE 10 2004 049 998 A1 gezeigt.

[0005] Die DE 10 2009 036 706 A1 des Anmelders beschreibt ein digitales Display zur Darstellung von sicherheitsrelevanten Informationen oder Mustern, die sich aufgrund eines Algorithmus und/oder externer Einflüsse verändern. Dabei kann es sich beispielsweise um Zeichen oder ein Muster handeln, die sich zwischen zwei Abfragezeitpunkten dynamisch verändern. Eine Umwandlung der erfassten Zeichen in andere Zeichen ist bei diesem Verfahren jedoch nicht vorgesehen.

[0006] Daneben gibt es Verfahren, um beispielsweise Banknoten zurückzuverfolgen. Diese basieren in der Regel darauf, angezeigte Seriennummern zu analysieren und zuzuordnen. Ein solches Verfahren ist in der DE 10 2009 044 881 A1 beschrieben. Allerdings funktioniert das Verfahren nur, wenn die angezeigte Seriennummer lesbar ist. Sollte eine mechanische Beschädigung des Sicherheitselements vorliegen, beispielsweise indem eine Seriennummer durch einen Riss nicht mehr gelesen werden kann, kann keine Zuordnung mehr erfolgen. Die vorgeschlagene Ausführungsvariante schlägt deshalb vor, dass in einem zweiten Vergleichsschritt ein Vergleich der Seriennummer der physisch vorliegenden Banknote mit in einem Datenspeicher hinterlegten Seriennummernabbildern durchgeführt wird. Neben den reinen Seriennummern werden bei diesem Vergleich auch andere Merkmale, beispielsweise das kennzeichnende Bildmerkmal des Risses, für den Vergleich herangezogen.

[0007] Daneben gibt es Sicherheitsmerkmale, die zur Erhöhung der Fälschungssicherheit sichtbare und nicht sichtbare Sicherheitsmerkmale aufweisen, beispielsweise beschrieben in der DE 10 2007 044 992 B3, bei dem ein erster defraktiver Bereich einen verborgenen, mit dem unbewaffneten Auge nicht sichtbaren Code aufweist, der in die defraktiven Oberflächenstrukturen des Sicherheitselements integriert ist. Jeder Versuch, das optische Erscheinungsbild der offenen Information oder den verborgenen Code zu ändern, nimmt Einfluss auf den verborgenen Code bzw. die offene Information, so dass solche Manipulationsversuche leicht erkannt werden können.

[0008] Daneben gibt es Bestrebungen, Merkmale durch Anwendung von Komplementärfarben verschwinden zu lassen oder sichtbar zu machen. Solche Ansätze sind beispielsweise in der DE 601 26 698 T2, der US 3,632,993 A oder der DE 10 2206 057 507 A1 bekannt.

[0009] Schließlich sind Verfahren bekannt, um Zeichen über eine optische Zeichenerkennung (Optical Character Recognition - OCR) mittels Bilderfassungsmethode in computerlesbare Zeichen, beispielsweise einen Text oder Code, umzuwandeln. Ein solches Verfahren ist beispielsweise in der DE 20 2013 011 992 U1, der DE 10 2008 077 331 B4, der DE 10 2006 037 260 B3 oder der WO02/099735 A1 beschrieben. Schließlich gibt es auch Verfahren zur Identifikation oder Authentifikation, die über dynamische akustischer Sicherheitsinformationen erfolgen, beispielsweise beschrieben vom Anmelder

in der WO 2015/124696 A1.

[0010] Die vom Erfinder eingereichte Patentschrift DE 10 2009 036 706 B3 offenbart ein Sicherheitselement mit einer elektronischen Anzeigevorrichtung, wobei sich die angezeigten Informationen oder Muster aufgrund eines Algorithmus und/oder externer Einflüsse zeitlich verändern.

[0011] Die vom Erfinder eingereichten Offenbarungsschriften EP 2 824 641 A1 und DE 10 2014 004 349 A1 beschreiben gattungsgemäße Authentifikationsvorrichtungen.

[0012] Zwar sind im aufgeführten Stand der Technik statische und dynamische Sicherheitsmerkmale zur Erhöhung der Sicherheit bei einer Authentifikation oder Identifikation von Personen, Diensten oder Sachen bekannt, jedoch gibt es nach wie vor die Möglichkeit, dass Fälscher mit vertretbarem Aufwand gängige Sicherheitsmerkmale kopieren oder Sicherheitsmechanismen umgehen können.

[0013] Vor diesem Hintergrund ist es Aufgabe der vorliegenden Erfindung, eine verbesserte Authentifikationsvorrichtung und Verfahren bereitzustellen, um die Fälschungssicherheit von Sicherheitselementen zu erhöhen.

[0014] Diese Aufgabe wird gelöst durch eine Authentifikationsvorrichtung mit den Merkmalen des Anspruchs 1 und einem Verfahren mit den Merkmalen des Anspruchs 9.

[0015] Die erfindungsgemäße Authentifikationsvorrichtung basiert auf der Durchführung einer Zeichenerkennung eines Sicherheitselements mit wenigstens einem aus Zeichen bestehenden Sicherheitsmerkmal und der anschließenden Umwandlung der Zeichen in interpretierbare Zeichen oder Merkmale, basierend auf dem Erscheinungsbild des Sicherheitselements. Dabei werden die Bedingungen zum Erfassen des Erscheinungsbildes der Zeichen und/oder die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitselements für eine Authentifikationsanfrage durch wenigstens eine Regeleinrichtung festgelegt.

[0016] Die erfindungsgemäße Authentifikationseinrichtung umfasst in ihrer Grundform folgende Komponenten:

- ein Sicherheitselement mit wenigstens einem aus Zeichen bestehenden Sicherheitsmerkmal, die über eine Zeichenerkennung erfassbar sind,
- wenigstens eine Erfassungseinrichtung zum Erfassen des Erscheinungsbilds der Zeichen des Sicherheitsmerkmals,
- wenigstens eine Zeichenerkennungseinrichtung zur Durchführung einer Zeichenerkennung und/oder einer Zeichenanalyse, bei der die erkennbaren Zeichen des Erscheinungsbildes des Sicherheitsmerkmals in maschinenlesbare Zeichen, eine Information und/oder akustische Töne umgewandelt werden,
- wenigstens eine Abgleicheinrichtung zum Abgleich des von der Erfassungseinrichtung erfassten Sicherheitsmerkmals und/oder der von der Zeichenerkennungseinrichtung umgewandelten Zeichen, Informationen oder Tonfolgen mit einem in einem Speicher hinterlegten Referenzmerkmal und/oder einem oder mehreren Referenzzeichen und/oder einem oder mehreren Referenztönen.

[0017] Die erfindungsgemäße Authentifikationsvorrichtung ist dadurch gekennzeichnet, dass sie wenigstens eine Regeleinrichtung umfasst, bei der die Erfassungsbedingungen zum Erfassen des Erscheinungsbilds der Zeichen und/oder die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals für eine Authentifikationsanfrage festgelegt sind und dass das Sicherheitselement wenigstens ein Strukturmerkmal aufweist, welches das Erscheinungsbild des Sicherheitsmerkmals und somit die Erfassbarkeit eines oder mehrerer Zeichen des Sicherheitsmerkmals bei einer Zeichenerkennung und/oder Zeicheninterpretation, vorzugsweise dynamisch, beeinflusst.

[0018] Die Strukturmerkmale sind vorzugsweise so ausgeprägt, dass sie das Erscheinungsbild der Zeichen des Sicherheitsmerkmals beeinflussen, beispielsweise über eine über oder unter das Sicherheitsmerkmal gelagerte Materialschicht. Auch die Zeichen selbst können Strukturmerkmal sein, beispielsweise durch Druck mit einer Tinte, welche ihre physikalische, chemische oder biologische Eigenschaft in einem Zeitraum verändert. Dies kann z.B. die Farbe der Zeichen sein, deren Fluoreszenz oder auch der Grad des Magnetismus, bei Verwendung von Tinten, die Magnetpartikel enthalten.

[0019] In einer alternativen Variante umfasst die erfindungsgemäße Authentifikationsvorrichtung je nach Anwendungsfall mehrere Regeleinrichtungen, welche jeweils die Erfassungsbedingungen zur Erfassung des Erscheinungsbildes zeigen, die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals für eine Authentifikationsanfrage festlegen. Die erfindungsgemäße Regeleinrichtung kann somit Bestandteil der Erfassungseinrichtung und/oder der Zeichenerkennungseinrichtung und/oder der Abgleicheinrichtung sein.

[0020] Erfindungsgemäß besteht das Sicherheitselement aus optisch erfassbaren Zeichen, die über eine optische Zeichenerkennung (OCR-Erkennung) lesbar, in maschinenlesbare Zeichen umwandelt und digital auswertbar sind. Für die Erfassung ist eine Erfassungseinrichtung zum Erfassen des Erscheinungsbildes der Zeichen des Sicherheitsmerkmales vorgesehen, vorzugsweise eine Kamera.

[0021] Das Wort "Zeichen" soll im Kontext der vorliegenden Erfindung im Sinne einer optisch erfassbaren In-

formation ausgelegt werden.

[0022] Demnach kann es sich beispielsweise bei den Zeichen um maschinenlesbare Muster, Zeichen wie Buchstaben, Zahlen oder Symbole handeln. Nachdem die Zeichen erfasst sind, wird eine Zeichenanalyse durchgeführt, bei der die erkennbaren Zeichen des Erscheinungsbildes des Sicherheitsmerkmales in lesbare Zeichen oder eine Information umgewandelt werden.

[0023] Im Falle einer optischen Zeichenerkennung (OCR-Erkennung) werden die von der Erfassungseinrichtung optisch erfassten Bilder der Zeichen in computerlesbare, digitale Zeichen umgewandelt. Diese Zeichen bestehen in der Regel aus Schriftzeichen, Schriftbildern,

[0024] Buchstaben, Zahlen, einer Textfolge, Symbolen oder auch Sonderzeichen.

[0025] Erfindungsgemäß handelt es sich bei der Zeichenerkennungseinrichtung um eine OCR-Einrichtung und bei der Zeichenanalyse um eine OCR-Analyse, welche vorgibt in welches computerlesbare Zeichen ein optisch erfasstes Zeichen umgewandelt werden soll. Die Zeichenerkennungseinrichtung erfasst die optisch erfassbaren Zeichen des Sicherheitselements und wandelt diese in entsprechende maschinenlesbare Zeichen (z. B. Buchstaben, Zahlen, Symbole, Sonderzeichen etc.) um.

[0026] Nach der Umwandlung der Zeichen in computerlesbare Zeichen oder Informationen erfolgt ein Abgleich der von der Zeichenerkennungseinrichtung umgewandelten Zeichen oder Informationen mit einem in einem Speicher hinterlegten Referenzmerkmal und/oder Referenzzeichen. Zusätzlich oder alternativ kann die Abgleicheinrichtung auch einen direkten Abgleich des von der Erfassungseinrichtung erfassten Sicherheitsmerkmals mit einem in einem Speicher hinterlegten Referenzmerkmal und/oder einem oder mehreren Referenzzeichen durchführen. Die Abgleichvorrichtung ist vorzugsweise Bestandteil eines Authentifikationsservers, der die Zeichenerkennung und Zeichenhinterlegung verwaltet.

[0027] Eine bloße Erfassung eines Sicherheitsmerkmals, beispielsweise eines aus Zeichen bestehenden Codes, würde im Vergleich zu bestehenden Sicherheitsverfahren alleine noch keine sicherheitserhöhende Maßnahme darstellen. Wird jedoch eine Zeichenfolge durch externe Einflüsse oder ein Strukturmerkmal, wie zum Beispiel ein sich unvorhersehbar bildendes Krakelee in einem darüber liegenden Lack, überlagert und dadurch die darunterliegende Zeichenfolge und damit auch eine OCR-Analyse beeinflusst, wird aus dem statischen Code ein nicht vorhersehbarer dynamischer Code gebildet. In einer Variante ist auch die Zeichenfolge selbst ein Strukturmerkmal beispielsweise indem sie sich dynamisch aufgrund innerer oder äußerer Einflüsse verändert. Ein Beispiels das Bedrucken eines Sicherheitsmerkmals mit einer Tinte oder einem Farbstoff, der seine Farbe oder eine andere chemische, physikalische oder biologische Eigenschaft verändert.

[0028] Erfindungsgemäß ist vorgesehen, dass die Authentifikationseinrichtung eine oder mehrere Regeleinrichtungen umfasst. Die Authentifikationsvorrichtung ist in einer bevorzugten Variante als Authentifikationssystem mit mehreren separaten, zum Teil räumlich getrennten, Komponenten ausgebildet, bestehend aus einer separaten Erfassungseinrichtung (zum Beispiel einer Kamera), einer Zeichenerkennungseinrichtung (zum Beispiel einer OCR-Erkennungseinrichtung) sowie einer Abgleicheinrichtung (zum Beispiel einem Authentifikationsserver). Demzufolge ist es nicht Voraussetzung, dass die einzelnen Komponenten der Authentifikationsvorrichtung eine physische Einheit bilden. Vielmehr ist es bevorzugt, dass die einzelnen Komponenten der Authentifikationsvorrichtung an unterschiedlichen Orten lokalisiert und ggf. über ein Netzwerk miteinander verbunden sind.

[0029] Erfindungsgemäß ist vorgesehen, dass die wenigstens eine Regeleinrichtung der Erfassungseinrichtung, der Zeichenerkennungseinrichtung und/oder der Abgleicheinrichtung zugeordnet ist. Die Regeleinrichtung gibt die Regeln und/oder Parameter für die Erfassung und/oder das Einlesen und/oder die Analyse für die Zeichen des Sicherheitsmerkmals vor. Die Regeleinrichtung mit ihren vorgebenden Regeln und Parametern stellt somit ein weiteres dynamisches Sicherheitsmerkmal neben etwaigen Strukturmerkmalen dar, die als externe Strukturmerkmale (zum Beispiel ein Krakelee) einzelne Zeichen der Zeichenfolge des Sicherheitsmerkmals des Sicherheitselementes überlagern. Der eigentlich statische Code wird sowohl durch die physischen Veränderungen der darüber liegenden Schicht, als auch durch die Veränderung der OCR-Einlese- und Analysebedingungen im Resultat dynamisiert und nicht vorhersehbar verändert.

[0030] Erfindgungsgemäß legt die Regeleinrichtung die Erfassungsbedingungen zum Erfassen des Erscheinungsbildes der Zeichen fest. Da die Erfassung der Zeichen über eine optische Erfassungseinrichtung erfolgt, werden die Parameter für die optische Erfassung, beispielsweise durch eine Kamera oder ein Linsensystem, festgelegt. Dies können beispielsweise kameraspezifische Parameter sein wie Tiefenschärfe, Fokus, Ausschnittsvergrößerungen, Abschnittsverkleinerungen, Schärfefilter oder Belichtungsparameter, einschließlich manipulativer Belichtungen wie beispielsweise einer Über- oder Unterbelichtung, Blitzbelichtungen, Anwendungen von Filtern oder Belichtungen mit Licht bestimmter Farbe, Stärke oder Wellenlänge, oder einer Beschränkung der verwendeten Bildauflösung, sowie anderer ausleserelevanter Parameter.

[0031] Zusätzlich oder alternativ zur Festlegung der Erfassungsbedingungen zum Erfassen des Erscheinungsbildes der Zeichen können auch die Einlesebedingungen für die Zeichenerkennung durch die Regeleinrichtung vorgegeben sein. Hierzu gehören beispielsweise Vorgaben, dass nur bestimmte Zeichen des Sicherheitsmerkmals erfasst werden. Hierzu gehören beispielsweise Zeichen einer vordefinierten Größe, einer

bestimmten Art oder Aufmachung, einer bestimmten Farbe oder einer bestimmten Position.

[0032] Neben den Erfassungsbedingungen und/oder Einlesebedingungen können zusätzlich oder alternativ die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals für eine Authentifikationsanfrage festgelegt werden. Hierzu gehören beispielsweise der Algorithmus oder eine Zuordnungsregel, mit der ein über die Erfassungseinrichtung erfasstes Zeichen nach dem Einlesen interpretiert oder umgewandelt wird. So kann beispielsweise vorgesehen sein, dass bestimmte Zeichen des Sicherheitsmerkmals in andere Schriftzeichen umgewandelt werden. Diese Erfassungs- und Zuordnungsregeln können zwischen der Authentifikationseinrichtung und dem zu authentifizierenden Gerät dynamisch, zufällig, sporadisch oder fortlaufend verändert werden, wobei jeweils die letzte ausgetauschte Einstellung Gültigkeit besitzt.

[0033] Allein durch eine nicht vorhersehbare Selektion bestimmter Zeichen innerhalb der Zeichenfolge des Sicherheitsmerkmals lässt sich die Fälschungssicherheit erhöhen und eine unzulässige Authentifikation vermeiden. Auch lassen sich auf diese Weise mit einem einzigen aus einer Vielzahl von Zeichen bestehenden Sicherheitsmerkmal eine Vielzahl von Authentifikationsmöglichkeiten mit völlig unterschiedlichen Sicherheitsmerkmalen generieren, wodurch kein Rückschluss auf das ganze Sicherheitsmerkmal möglich ist. In einer weiteren Variante können bestimmte Zeichen des Sicherheitsmerkmals auch in andere Zeichen übersetzt oder umgewandelt werden, insbesondere, wenn sie durch dynamische Faktoren, wie z.B. den Batteriestand eines Anzeigegerätes oder der Authentifikationsvorrichtung, verändert, beeinflusst, oder beim Auslesen eines nicht-digitalen Sicherheitselementes durch Krakelee-Risse in der Farbe oder einer darüber liegenden Schicht, physisch verändert werden. Die Zeichenanalyse umfasst daher generell die Umwandlung der von der Zeichenerkennungseinrichtung eingelesenen Zeichen in einer Regel oder einem Algorithmus folgende, umgewandelte maschinenlesbare Zeichen, wobei diese Regel durch weitere, nicht vorhersehbare Faktoren zusätzlich beeinflusst werden kann. Erfindungsgemäß wird aus einem optisch erhaltenen Bild, welches OCR-lesbare Zeichen enthält, eine OCR-Erkennung und anschließende Umwandlung in computerlesbare Zeichen durchgeführt, wobei einzelne oder mehrere Zeichen des Sicherheitselements derart manipuliert sind, dass eine OCR-Erkennung oder OCR-Analyse bei bestimmten Zeichen nicht mehr möglich ist oder die schwer oder nicht lesbaren Zeichen anders interpretiert werden oder gemäß einer Regel anders zugeordnet werden müssen.

[0034] Erfindungsgemäß kommt sicherheitserhöhend hinzu, dass das Sicherheitselement wenigstens ein Strukturmerkmal aufweist, welches das Erscheinungsbild des Sicherheitsmerkmals und somit die Erfassbarkeit eines oder mehrerer Zeichen des Sicherheitsmerkmals einer Zeichenerkennung beeinflusst. Es handelt sich hierbei um ein optisch erfassbares, aus Zeichen bestehendes Sicherheitsmerkmal, bei dem wenigstens einige Zeichen über eine Zeichenerkennungseinrichtung erkannt und in computerlesbare Zeichen umgewandelt werden können. In einer Variante ist vorgesehen, dass das Strukturmerkmal ein oder mehrere Zeichen des Sicherheitsmerkmals überlagert, verändert, modifiziert, auslöscht oder verstärkt, so dass die Zeichenerkennungseinrichtung das modifizierte Zeichen für eine Zeichenanalyse und Zeichenumwandlung nicht mehr heranziehen kann. In einem solchen Fall würde durch die strukturbedingte Veränderung eines oder mehrerer Zeichen innerhalb des Sicherheitsmerkmals aus einem vormals lesbaren Zeichen ein nicht oder verändert lesbares Zeichen werden. Vorzugsweise handelt es sich bei dem Strukturmerkmal um eine Oberflächenveränderung, beispielsweise ein Krakelee-Muster in Form von Rissen, Abplatzungen, Sprüngen oder Ausnehmungen. Durch diese Oberflächenveränderungen werden ein oder mehrere Zeichen des Sicherheitsmerkmals auf eine Weise verändert, dass sie für die Zeichenerkennungseinrichtung nicht mehr lesbar oder interpretierbar sind. In Varianten dieser Ausführungsform können Strukturmerkmale auch 3D-Oberflächenveränderungen wie Oberflächenerhebungen oder Oberflächenvertiefungen sein. Dadurch verändert sich die relative Lage und/oder Position und/oder Anordnung der Zeichen im Vergleich zum Ursprungszustand. Auch Relativverlagerungen von Zeichen auf dem Sicherheitselement oder Farbveränderungen der Zeichen sind möglich, um die Erfassbarkeit und/oder das Einlesen und/oder die spätere Analyse bei der Zeichenerkennung und/oder Zeicheninterpretation zu beeinflussen.

[0035] Nach einer bevorzugten Ausführungsform ist die Oberfläche des erfindungsgemäßen Sicherheitselementes mit einem Material überzogen, welches das Erscheinungsbild des Sicherheitsmerkmals oder einzelner Zeichen davon beeinflusst. Bei einer bevorzugten Variante handelt es sich bei dem Material um einen Lack, welcher das Sicherheitselement überzieht. Nach einer weiteren Variante können die einzelnen Zeichen des Sicherheitsmerkmals auch mit einer bei Tageslicht unsichtbaren Tinte oder Farbe gedruckt oder bedruckt sein.

[0036] Anstelle einer Schicht kann das Strukturmerkmal auch das gesamte dreidimensionale Sicherheitselement aufbauen, beispielsweise mittels 2D-Druck, 3D-Druck, Aufsprühen, Formen, Gießen, Pressen, Zusammensetzen einzelner Bestandteile oder durch Wachstum. In einer bevorzugten Variante kann sich ein so hergestelltes dreidimensionales Sicherheitselement aufgrund biologischer, chemischer, physikalischer oder mechanischer Einflüsse zusätzlich verändern. In einer beispielhaften Variante umfasst ein solches dreidimensionales Sicherheitselement in/oder auf seiner Oberfläche zusätzlich einen Zahlencode, welcher sich aufgrund der Materialeigenschaften dynamisch verändert und auslesbar ist.

[0037] Daneben kann auch der Hintergrund des Si-

cherheitselements bei der Erfassung und/oder Erkennung des Sicherheitsmerkmals eine Rolle spielen, beispielsweise indem durch die Farbgebung oder durch eine physikalische Eigenschaft des Hintergrundes bestimmte Zeichen des Sicherheitsmerkmals nicht mehr lesbar sind oder vormals nicht lesbare Zeichen durch die Behandlung sichtbar werden. Dies kann beispielsweise dadurch erfolgen, dass die Zeichen überschattet werden oder durch eine Trübung nicht mehr lesbar sind. Somit kann ein Strukturmerkmal nicht nur bestimmte Zeichen innerhalb des Sicherheitsmerkmals auslöschen oder verändern, so dass es für eine spätere Zeichenanalyse nicht mehr erkennbar sind, sondern es gilt auch der umgekehrte Fall, dass ein vormals nicht lesbares Zeichen durch eine Strukturmodifikation in ein durch die Zeichenerkennungseinrichtung lesbares Zeichen umwandelbar ist.

[0038] In einer bevorzugten Variante ist vorgesehen, dass sich ein Strukturmerkmal des Sicherheitselements selbst dynamisch in zufälliger Weise verändert und somit zu einem veränderten Erscheinungsbild des Sicherheitselements zwischen zwei Abfragezeitpunkten führt. Dabei ist die dynamische Veränderung des Strukturmerkmals des Sicherheitselements bedingt durch eine Materialeigenschaft des Strukturmerkmals, eine inhärente Eigenschaft des Sicherheitselements und/oder durch eine Beeinflussung über einen externen physikalischen und/oder chemischen und/oder biologischen Faktor. Durch die dynamische Veränderung des Strukturmerkmals werden zwischen zwei Abfragezeitpunkten vormals erkennbare Zeichen in nicht erkennbare Zeichen umgewandelt oder umgekehrt.

[0039] Ein weiteres sicherheitserhöhendes Merkmal ist, dass die Einlesebedingungen für die Erfassung des Erscheinungsbildes des Sicherheitsmerkmals und/oder die Zeichenerkennung und/oder die Zeichenanalyse durch die Regeleinrichtung verändert werden können, und zwar auf eine Weise, dass ein möglicher Fälscher diese Veränderung nicht vorhersehen kann. So können bestimmte Sollwerte oder Parameter vorgegeben werden, welche Einfluss auf die Erfassungseinrichtung haben. Auch können bestimmte Zeichen innerhalb des Sicherheitsmerkmals derart verändert werden, dass sie für eine spätere Zeichenerkennung nicht mehr lesbar sind. So kann beispielsweise bei der Sicherheitsabfrage eine Belichtung mit Komplementärfarben erfolgen, so dass bestimmte Zeichen (alle oder einzelne Zeichen) innerhalb des Sicherheitsmerkmals für eine spätere Zeichenerkennung verstärkt oder abgeschwächt werden. Dies führt dazu, dass vormals schlecht sichtbare oder unsichtbare (nicht erkennbare) Zeichen für die Zeichenerkennung sichtbar (erkennbar) werden und vormals sichtbare (erkennbare) Zeichen nach Anwendung der entsprechenden Komplementärfarbe für die spätere Zeichenerkennung nicht mehr lesbar, interpretierbar oder erkennbar sind. Dies setzt voraus, dass die entsprechenden Zeichen mit Komplementärfarben dargestellt sind und/oder die Belichtung mit einer zu der Zeichenfarbe komplementären Farbe erfolgt. Auch eine Kombination mit einer Regel wäre denkbar. Beispielsweise könnte die Regel lauten, dass violette Zeichen nicht ausgelesen werden. Wird das Sicherheitsmerkmal nun mit einem blauen Licht bestrahlt, werden alle roten Zeichen zu violetten und die vormals violette Zeichen zu annähernd blauen, je nachdem wie intensiv die Bestrahlung und wie groß der Toleranzbereich gewählt wurden.

[0040] Die wenigstens eine Regeleinrichtung der erfindungsgemäßen Authentifikationsvorrichtung umfasst Komponenten, welche software- oder hardwarebasiert Einfluss nehmen auf die Erfassungseinrichtung, die Zeichenerkennungseinrichtung und/oder die Zeichenanalyse. Dies kann durch Übermittlung der spezifischen für das Einlesen/die Erkennung erforderlichen Parameter an die jeweilige Einrichtung erfolgen. Die Auswahl der Paramater kann durch die Authentifikationsvorrichtung vorgegebenen werden oder zufällig erfolgen. Ein Fälscher müsste die falsche Identität somit nicht nur durch Vorweisen eines gestohlenen und gefälschten originalen Sicherheitselementes vortäuschen, sondern auch die entsprechend vorgegebenen Regeln beim Auslesen oder der Zeichenerkennung berücksichtigen, beispielsweise beim Auslesen mit einem Smartphone (Handy) und einer anschließenden Zeichenauswertung.

[0041] Je nach Art und Weise der Veränderung des Zeichens kann bei der späteren Zeichenanalyse eine Erkennungsschwelle festgelegt werden, um ein erkennbares und/oder schwer erkennbares und/oder nicht erkennbares Zeichen zu definieren bzw. zu interpretieren. Ferner kann vorgesehen sein, dass nur bestimmte Farben eines Zeichens des Sicherheitsmerkmals für die spätere Zeichenanalyse herangezogen werden, was beispielsweise durch eine Farbbestimmung der Zeichen erfolgen kann. Auch kann festgelegt werden, dass nur Zeichen einer bestimmten Größe, Position oder Anordnung für eine Zeichenanalyse und somit für eine Authentifikation herangezogen werden. Dies kann beispielsweise über eine Positionsbestimmung der Zeichen, bevorzugt mittels Optik, erfolgen. Ferner kann ein Schärfe- oder Unschärfebereich bei der Erfassung des Sicherheitsmerkmals definiert werden, so dass bestimmte Zeichen nicht mehr lesbar sind. Gleiches gilt auch für einen Tiefenschärfebereich eines dreidimensional aufgebauten Sicherheitselements. Eine Oberfläche kann aus mehreren Ebenen oder Schichten aufgebaut sein, wobei der scharfe Bereich auf eine bestimmte Ebene fokussiert wird. Nur Zeichen dieser Ebene können für eine spätere Zeichenerkennung und somit Zeichenanalyse herangezogen werden. Ferner können spezielle Filter zum Einsatz kommen, die bewirken, dass bestimmte Zeichen des Sicherheitsmerkmals lesbar und/oder nicht lesbar werden. Durch Anwendung des Filters wird, wie auch bei den anderen Verfahrensmaßnahmen, nicht nur das Erscheinungsbild des Sicherheitsmerkmals verändert, sondern auch die daraus resultierende sicherheitsrelevante Information. Bei einer optischen Zeichenerkennung kann dies mit allen optisch möglichen Mitteln erfolgen, beispiels-

weise auch durch Bestrahlung mit einer bestimmten Wellenlänge oder durch Über- oder Unterbelichtung.

[0042] Somit können die durch die Regeleinrichtung vorgegebenen Einlesebedingungen sowohl auf physikalischer Ebene beim Einlesen selbst als auch bei der späteren Zeichenerkennung und/oder Zeichenanalyse vorgegeben werden. Die Zeitpunkte zur Durchführung solcher dynamischer Veränderungen können vorgegeben oder willkürlich sein. So kann der Nutzer, der sich einer Authentifikation unterziehen möchte, sein Sicherheitselement beispielsweise über eine Smartphone-Kamera einlesen und an den Authentifikationsserver übermitteln. Zu diesem Zweck können vorzugsweise Makrolinsen als Vorsatz zu Handylinsen zur besseren Erkennung eingesetzt werden. Der Authentifikationsserver hinterlegt ein Abbild des Sicherheitselements, insbesondere der darauf angebrachten Sicherheitsmerkmale und wertet die in den Sicherheitsmerkmalen enthaltenen Zeichen über eine Zeichenerkennungsmethode (beispielsweise eine OCR-Zeichenerkennung) aus. Die so hinterlegten Informationen sind für einen möglichen Fälscher nicht zu kopieren, ohne dass er in Besitz des Sicherheitselements kommt.

[0043] Doch selbst dann, wenn der Fälscher in den Besitz des Sicherheitselements kommen würde, kann die erfindungsgemäße Regeleinrichtung vorsehen, dass eine Abfrage für eine Authentifikation oder Identifikation nur unter bestimmten Bedingungen zu erfolgen hat, welche nur der Nutzer kennt. Beispielsweise kann vorgesehen sein, dass ein bestimmter Ausschnitt oder Winkel des Sicherheitselements bei der optischen Erfassung durch die Erfassungseinrichtung für eine erfolgreiche Authentifikation erforderlich ist. Ferner könnte eine Regel vorsehen, dass das Sicherheitselement vor Erfassung durch die Erfassungseinrichtung mechanisch bearbeitet wird, beispielsweise durch Umknicken oder Falten, so dass sich die Oberflächenstruktur des Sicherheitselements derart verändert, dass Zeichen des Sicherheitsmerkmals für eine spätere Zeicheninterpretation nicht mehr erkennbar sind und sich das Sicherheitsmerkmal zwingend weiterentwickelt, um eventuelle Fälschungen aufdecken zu können. Eine bevorzugte Variante sieht vor, dass das Sicherheitselement aus einer Schicht besteht oder mit einer Schicht überzogen ist, welche entweder von alleine ein Krakeleemuster ausbildet, oder, wenn auf die Oberfläche des Sicherheitselements mechanisch eingewirkt wird, beispielsweise durch Falten oder Knicken. Eine solche Schicht, welche als Strukturmerkmal das Erscheinungsbild der Zeichen des Sicherheitsmerkmals verändert, kann beispielsweise aus einem Lack, einem Farbstoff, einem Kunststoff, einem künstlichen Polymer oder einem Biopolymer bestehen.

[0044] Physikalische Veränderungen der Oberfläche bzw. der darin oder darauf angebrachten Strukturmerkmale können vor einer Authentifikation oder zur Aktualisierung einer sicherheitsrelevanten Information auch vom Nutzer selbst vorgenommen werden. So kann beispielsweise das Sicherheitselement mit einem Material überzogen sein, das zufällige Risse oder Ausbrüche bildet und damit Zeichen eines Sicherheitsmerkmals derart verändert, dass sie für eine spätere optische Zeichenerkennung nicht mehr oder anders lesbar oder interpretierbar sind. Vorzugsweise ist dabei vorgesehen, dass die über die Erfassungseinrichtung nicht lesbaren oder die über die Zeichenerkennungseinrichtung nicht interpretierbaren Zeichen in Leerstellen oder ein beliebiges anderes Zeichen übersetzt werden. Außerdem kann es vorkommen, dass veränderte Zeichen noch lesbar sind, allerdings gegenüber vorher als andere Zeichen erkannt werden. Dadurch wird eine sicherheitsrelevante Zeicheninformation erzeugt, die für einen möglichen Angreifer nicht vorhersehbar ist.

[0045] Zusammengefasst können bei der optischen Zeichenerkennung drei Zustände vorliegen, wenn ein externer Einfluss oder ein Strukturmerkmal Zeichen eines Sicherheitsmerkmals teilweise verändert. Zum einen können die Zeichen unverändert bleiben, d. h. wenn keine Beeinflussung durch das Strukturmerkmal (zum Beispiel ein Krakelee) stattgefunden hat. Des Weiteren können die Zeichen auch verändert sein, so dass diese Zeichen zu einem anderen Umwandlungsergebnis bei der Zeichenanalyse erkannt werden und somit einen veränderten Code generieren, der nicht vorhersehbar war. Schließlich können die Zeichen auch so beeinflusst sein, dass sie nicht mehr lesbar sind.

[0046] Basierend auf der erfindungsgemäßen Idee kann somit ein Sicherheitselement, welches wenigstens ein Sicherheitsmerkmal umfasst, durch ein Strukturmerkmal (zum Beispiel ein über ein Lack bedingtes Krakelee) optisch derart verändert werden, dass es schon bei einem optischen Vergleich nur sehr schwer wäre, ein solches individuelles Sicherheitsmuster nachzuahmen. Erfindungsgemäß kommt jedoch hinzu, dass eine Zeichenerkennung, vorzugsweise eine optische OCR-Erkennung, durchgeführt wird, bei der einzelne Zeichen des Sicherheitsmerkmals, beispielsweise innerhalb eines komplexen Codes, nicht mehr lesbar sind. Solche Zeichen werden bei einer OCR-Analyse entweder nicht erkannt und somit nicht in computerlesbare Zeichen umgewandelt oder sie werden als falsches Zeichen erkannt und dementsprechend ignoriert, oder in ein anderes computerlesbares Zeichen umgewandelt. Eine Kopie kann das Resultat einer optischen OCR-Analyse nur überlisten, wenn sie in allen oder den entsprechend einer Regel vorgegebenen Aspekten dem Original gleicht, was nur mit unverhältnismäßig großem Aufwand, wenn überhaupt, möglich ist.

[0047] Ferner kann vorgesehen sein, dass bestimmte erkennbare Zeichen auch in andere Informationen übersetzt werden, beispielsweise in beliebig andere Zeichen oder auch Tonfolgen. Die Generierung von spezifischen akustischen Tonfolgen führt dazu, dass ein Nutzer sich über eine charakteristische Tonfolge bei einer Authentifikationsvorrichtung authentifizieren kann. Aufgrund der dynamischen Veränderung und/oder einer wechselnden gültigen Regel der generierten Toninformation, ist es ei-

nem Nachahmer nicht möglich, diese zu fälschen.

[0048] Eine mögliche Authentifikationsvariante läuft so ab, dass ein mit wenigstens einem Sicherheitsmerkmal ausgerüstetes Sicherheitselement zunächst von einer Erfassungseinrichtung des Nutzers eingelesen und anschließend die Zeichen des Sicherheitsmerkmals nach deren Übermittlung in computerlesbare Zeichen, lesbare Informationen, beispielsweise einen Code umgewandelt werden.

Vorzugsweise erfolgt die Übermittlung an eine zentrale Datenbank. Wenn sich beispielsweise der Nutzer bei einem Dienstanbieter authentifizieren muss, kann dieser über seine Erfassungseinrichtung dasselbe Sicherheitselement wie der Nutzer erfassen und an die zentrale Datenbank übermitteln. Die erfindungsgemäße Abgleichvorrichtung kann darauf basierend den Vergleich entsprechend einer vorgegebenen Regel vornehmen. In einer alternativen Variante kann die zentrale Datenbank auf der zweiten Erfassungseinrichtung mitteilen, welche Regeln für den Auslesevorgang gültig sind und der Erfassungseinrichtung lediglich die gültige, entsprechend der Regel erhaltene, Zeichenfolge oder das entsprechende Erscheinungsbild des Sicherheitsmerkmals übermitteln. Die daraus generierte Information kann alternativ auch von der Authentifikationsvorrichtung an den Nutzer zurückgesendet werden. Diese muss die erhaltene Information wiederum einer Authentifikationseinrichtung übermitteln. Nur wenn die übermittelte sicherheitsrelevante Information (z. B. eine Tonfolge oder ein Code) übereinstimmt, ist sichergestellt, dass es sich bei der zu authentifizierenden Person um die korrekte Person handelt. Eine Authentifikation ist dann positiv, wenn die übertragene sicherheitsrelevante Information identisch ist mit der von dem Nutzer übertragenen oder eingegebenen Information.

[0049] In einer weiteren Ausführungsform ist vorgesehen, dass die Authentifikationsvorrichtung ferner eine Anzeigeeinrichtung umfasst, auf der das aktuelle oder modifizierte Erscheinungsbild des Sicherheitselements nach der Übermittlung durch die Authentifikationseinrichtung für eine Authentifikation darstellbar ist. Dabei kann es sich beispielsweise um ein Smartphone (Handy) handeln, auf dessen Display das lokal generierte oder von der Authentifikationsvorrichtung übertragene Sicherheitselement oder daraus isolierte Sicherheitsmerkmale dargestellt werden.

[0050] In einer ersten Variante kann vorgesehen sein, dass beispielsweise über die Kamera eines Smartphones ein für die Authentifikation erforderliches Sicherheitselement mit Sicherheitsmerkmalen eingelesen wird (beispielsweise ein Ticket). Das über die Erfassungseinrichtung erfasste Bild des Sicherheitselementes ist über das Display des Smartphones (= Anzeigevorrichtung) darstellbar. Das erfasste Abbild des Sicherheitselementes wird dann an eine Authentifikationsvorrichtung übertragen. Für eine spätere Authentifikation ist es nicht mehr unbedingt notwendig, dass zwischen der Authentifikationsvorrichtung und dem sich authentifizierenden (ersten) Smartphone eine bestehende Netzwerkverbindung (z.B. Online-Verbindung) besteht. Vielmehr ist eine weitere Authentifikation auch ohne Netzwerkverbindung ("Offline") möglich. Diese erfolgt dadurch, dass eine Erfassungseinrichtung (zum Beispiel ein Lesegerät an einer Supermarktkasse oder die Kamera eines zweiten Smartphones) das auf dem Display des ersten Smartphones angezeigte Sicherheitselement bzw. die darauf abgebildeten Sicherheitsmerkmale optisch erfasst und das so erfasste Erscheinungsbild mit dem in der Authentifikationsvorrichtung hinterlegten Erscheinungsbild des Sicherheitsmerkmals (= Referenzmerkmal) vergleicht. Erfindungsgemäß ist nun vorgesehen, dass wenigstens eine Regeleinrichtung die entsprechenden Regeln für das Erfassen, das Einlesen und/oder eine Analyse der Zeichen vorgibt (z.B. durch eine softwarebasierte Programmanweisung). So kann eine Regeleinrichtung dem Lesegerät vorgeben, dass beispielsweise nur die in einer bestimmten Farbe dargestellten Zeichen innerhalb eines Codes eingelesen werden sollen. Die Abgleicheinrichtung der Authentifikationsvorrichtung übernimmt dann einen Abgleich des von dem Lesegerät erfassten Sicherheitsmerkmals mit dem hinterlegten Referenzmerkmal. Auch das Anzeigegerät selbst kann eine Regeleinrichtung umfassen, die beispielsweise vorgibt, welche Teile des Sicherheitsmerkmals dem Lesegerät gegenüber angezeigt werden sollen. Dabei kann für eine Authentifikation auch vorgegeben sein, dass die Regeln der Regeleinrichtung des Anzeigegerätes mit den Regeln der Regeleinrichtung des Lesegerätes übereinstimmen. Auf diese Weise kann über die wenigstens eine Regeleinrichtung vorgegeben werden, was bildlich von der Anzeigevorrichtung angezeigt und letztendlich für eine Zeichenanalyse und Zeichenumwandlung herangezogen werden soll.

[0051] Auch kann die Abgleicheinrichtung die letzten, für die jeweilige Regeleinrichtung und deren Nutzer, gültigen Zeichenfolgen mitteilen, so dass eine Authentifikation sogar möglich ist, wenn beide Systeme "offline" sind, also weder der Nutzer, noch das Lesegerät eine Verbindung zum jeweiligen Sicherheitsserver hat. Voraussetzung dazu ist, dass sich das Sicherheitsmerkmal seit der letzten Mitteilung der nutzerseitigen Veränderung hinsichtlich der relevanten Zeichen nicht bereits erneut weiterverändert hat, oder eine entsprechende Fehlertoleranz akzeptiert wird.

[0052] Die erfindungsgemäße Vorrichtung und das Verfahren können insbesondere zur Authentifikation oder Bestimmung der Identität einer Person, eines Gerätes, einer Sache, eines Dienstes, einer Anwendung und/oder eines Computerprogramms herangezogen werden. Ferner ist auch der Einsatz damit verbundener Informationen für eine Dokumentation in einem Speichersystem, Quittierungssystem oder Archivierungssystem möglich.

[0053] Die Erfindung wird in den nachfolgenden Ausführungsbeispielen näher erläutert.

[0054] In der in Fig. 1 dargestellten Ausführungsform

ist ein Sicherheitselement 1 mit einer Oberfläche 3 gezeigt. Auf oder in der Oberfläche 3 befindet sich wenigstens ein aus Zeichen bestehendes Sicherheitsmerkmal 2. In der dargestellten Variante handelt es sich bei den Zeichen beispielsweise um einen aus Buchstaben und Zahlen bestehenden Code. Ferner sind Strukturmerkmale 4 vorgesehen, in der gezeigten Variante als Krakeleemuster mit Rissen zu erkennen. Die Strukturmerkmale 4 (d.h. die Risse) führen dazu, dass einzelne Zeichen des Sicherheitsmerkmals 2 (in der dargestellten Variante die Ziffern 2 und 5) durch die Erfassungseinrichtung nicht mehr eindeutig lesbar oder durch die Zeichenerkennungseinrichtung 6 nicht mehr oder anders interpretierbar sind. Dadurch entsteht ein über die Strukturmerkmale 4 verändertes Sicherheitselement, dessen Sicherheitsmerkmale 2 derart verändert sind, dass sie zu einem veränderten Ergebnis bei einer späteren Zeichenerkennung der Zeichen führen. Über eine Kamera als optische Erfassungseinrichtung 5 wird das Erscheinungsbild des Sicherheitselements 1 und/oder der Zeichen des Sicherheitsmerkmals 2 erfasst und von einer Zeichenerkennungseinrichtung 6 ausgewertet. Die Zeichenerkennungseinrichtung 6 führt eine optische Zeichenerkennung (Optical Character Recognition; OCR-Erkennung) durch. Anschließend erfolgt eine Zeichenanalyse, bei der die erkennbaren Zeichen des Erscheinungsbildes des Sicherheitsmerkmals 2 in lesbare Zeichen umgewandelt oder interpretiert werden. In der dargestellten Variante sind die Zeichen A, N, X, 3, 4 lesbar. Die Ziffern 2 und 5 sind aufgrund der überlagerten Risse des Strukturmerkmals 4 nicht mehr eindeutig lesbar und werden - je nach Erkennungseinstellungen - somit nicht durch die Zeichenerkennungseinrichtung 6 nicht umgewandelt oder richtig interpretiert. Dadurch wird eine Information aus erkennbaren und nicht eindeutig erkennbaren Zeichen geschaffen. Gegebenenfalls können die nicht oder schwer erkennbaren Zeichen in alternative Zeichen oder Informationen umgewandelt werden, was die Sicherheit zusätzlich erhöht. Hier lassen sich entsprechende Umwandlungsregeln schaffen. Zum Beispiel wäre es auch möglich, Ziffern oder Buchstaben vollständig durch andere Zeichen bei der OCR-Analyse ersetzen zu lassen.

[0055] Über eine Abgleicheinrichtung 7 erfolgt ein Abgleich des von der Erfassungseinrichtung 5 erfassten Sicherheitsmerkmals 2 durch einen Vergleich der von der Zeichenerkennungseinrichtung 6 umgewandelten Zeichen des Sicherheitsmerkmals 2 mit einem in einem Speicher hinterlegten Referenzmerkmal.

[0056] Erfindungsgemäß ist nun vorgesehen, dass nicht nur eine einfache optische Zeichenerkennung und Umwandlung von erkennbaren Zeichen erfolgt. Die Authentifikationsvorrichtung umfasst ferner wenigstens eine Regeleinrichtung 8, bei der die Erfassungsbedingungen zum Erfassen des Erscheinungsbildes der Zeichen und/oder die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals 2 für eine Authentifikationsanfrage festgelegt sind. So kann die Regeleinrichtung 8 beispielsweise festlegen, dass nur die verstärkt hervorgehobenen Zeichen A und X in der Zeichenfolge des Sicherheitsmerkmals 2 für die spätere Zeichenerkennung durch die Zeichenerkennungseinrichtung 6 herangezogen werden. Dies kann beispielsweise durch eine bestimmte Farbgebung unter Anwendung eines Filters erfolgen. Alternativ kann eine Bestrahlung des Sicherheitselements 1 mit Komplementärfarben erfolgen, so dass beispielsweise die Buchstaben A und X verstärkt werden, während die anderen Zeichen des Sicherheitsmerkmals 2 durch Anwendung der Komplementärfarbe ausgelöscht oder zumindest abgeschwächt werden. Die Regeleinrichtung 8 kann auch vorgeben, dass nur bestimmte Zeichen der Zeichenfolge des Sicherheitsmerkmals 2 für eine Authentifikation herangezogen werden, beispielsweise nur bestimmte Zeichenpositionen oder Ausschnitte des Sicherheitselements 1.

[0057] Die Regeleinrichtung 8 kann aber nicht nur die Einlesebedingungen für die Erfassungseinrichtung 5 vorgeben, sondern auch die Analyseparameter für eine spätere Zeichenanalyse. Diese können beispielsweise vorsehen, dass nur bestimmte Zeichen der Zeichenfolge des Sicherheitselements 2 für eine Umwandlung herangezogen und somit für eine spätere Authentifikation relevant werden.

[0058] Zeichen, welche beispielsweise aus mehreren Farben zusammengesetzt sind, können je nach Ausgestaltung, der Anwendung von Komplementärlicht oder Art der Ausleseregel unterschiedliche Ergebnisse liefern: Besteht beispielsweise die Ziffer "8" zur einen Hälfte aus blauer und zur anderen Hälfte aus roter Farbe, so würde diese Ziffer bei Anwendung der Ausleseregel, dass nur die Farbe "blau" gilt, als Ziffer "3" interpretiert. Dies ist auch der Fall, wenn das Zeichen unter blauem Licht auf einem Bildschirm ausgelesen würde, da sich in diesem Fall der rote Teil zu weiß verändert. Beim Auslesen eines gedruckten Bildes unter blauem Licht würde sich dieser rote Teil zu schwarz verändern, während der blaue Teil blau bliebe. Eine Ausleseregel, dass nur blau ausgelesen werden soll, würde also in jedem Fall die Ziffer "3" als Resultat liefern.

[0059] In Fig. 2 ist ein nicht erfindungsgemäßes Beispiel des Verfahrens bzw. der Authentifikationsvorrichtung gezeigt. Dabei ist vorgesehen, dass zunächst eine Zeichenerkennung der Zeichen des Sicherheitsmerkmals 2 des Sicherheitselements 1 erfolgt, wobei alle oder ein Teil der Zeichen durch die Zeichenerkennungseinrichtung 6 nach Erfassung durch die Erfassungseinrichtung 5 in eine akustische Tonfolge umgewandelt werden. Dadurch entsteht eine charakteristische, von den auf dem Sicherheitselement 1 aufgeprägten Zeichen abhängige akustische Signatur, die für eine Authentifikation über die Abgleicheinrichtung 7 herangezogen werden können. So kann bei dieser Variante vorgesehen sein, dass die generierte Tonfolge dem Nutzer für die Authentifikation übermittelt wird, so dass dieser die übermittelte Tonfolge für eine Authentifikation abspielen muss, damit die Tonfolge über eine separate weitere Erfassungsein-

richtung 5, in diesem Fall ein Mikrofon, wiederum eingelesen und mit der hinterlegten Referenztonfolge über die Abgleicheinrichtung 7 verglichen wird (akustische Signatur). Stimmen beide Tonfolgen entsprechend den Vorgaben überein, so verläuft die Authentifikation positiv.

[0060] Es ist auch der umgekehrte Fall möglich, nämlich dass die Authentifikationseinrichtung das Sicherheitselement des Nutzers liest und aus Teilen der erfassten Zeichen einen individuellen Klang generiert, welcher über das Mikrophon des Nutzers aufgenommen und digital an einen zentralen Authentifikationsserver weitergeleitet wird, der wiederum von der Authentifikationseinrichtung diesen Klang ebenfalls erhalten und hinterlegt hat und dessen akustische Übereinstimmung prüft.

[0061] Sicherheitserhöhend kann bei dieser Variante nun vorgesehen werden, dass nach der Übermittlung der korrekten Tonfolge in einem weiteren Verlauf die akustische Information vor der Erfassung durch die Erfassungseinrichtung 5 verändert wird, beispielsweise durch Einspielen weiterer Signale, wie Umgebungsgeräusche, welche die Tonfolge oder das Tongemisch verändern. Dadurch wird eine neue akustische Signatur generiert, die wiederum als neue Sicherheitsinformation in der Authentifikationsvorrichtung hinterlegt werden kann. Diese neue akustische Signatur dient dann als Ausgangsbasis für eine spätere Identifikation des Nutzers.

[0062] In Fig. 3 ist ein beispielhaftes Sicherheitselement 1 gezeigt, bei dem eine Vielzahl von Sicherheitsmerkmalen 2 in Form von Codes zu erkennen ist. Die Sicherheitsmerkmale 2 sind unterschiedlich aufgemacht, indem die Zeichen aus unterschiedlichen Farben, unterschiedlichen Größen, Schriften oder Zeichenabständen bestehen. Die Oberfläche 3 des Sicherheitselementes 1 ist mit einem Lack überzogen, in dem sich ein Krakelee bzw. Risse als Strukturmerkmal 4 ausbilden. Die Risse durchziehen das Sicherheitselement 1 und überlagern dadurch einzelne Zeichen der Sicherheitsmerkmale 2.

[0063] Dieses Sicherheitselement 1 wird im Zuge einer Authentifikationsabfrage von einer Erfassungseinrichtung (nicht gezeigt) erfasst und einer optischen Zeichenerkennung (OCR-Analyse) unterzogen. Die erkennbaren Zeichen werden in entsprechende computerlesbare Zeichen umgewandelt. Zeichen, die nicht eindeutig erkennbar sind oder von einem Strukturmerkmal 4 überlagert sind, erhalten eine andere Zuordnung, beispielweise eine Leerstelle oder ein beliebiges anders Zeichen, wodurch ein individueller Code generiert wird, der nicht vorhersehbar ist und sich vom eingelesenen Code unterscheidet. Über eine oder mehrere Regeleinrichtungen (nicht gezeigt) kann nun bestimmt werden, wie das Einlesen oder die OCR-Analyse erfolgen soll. So kann beim Erfassen des Sicherheitselementes 1 festgelegt werden, dass nur kursiv geschriebene Zeichen des Sicherheitsmerkmals 2 eingelesen werden sollen. Eine weitere Regel kann vorsehen, dass nur Zeichen mit einer bestimmten Farbgebung erfasst werden. Ferner können auch Regeln für die OCR-Umwandlung vorgegeben werden, beispielswiese Schwellenwerte für eine eindeutige/unscharfe Erkennung von Zeichen.

[0064] Ein solches Sicherheitselement 1 ist für einen Fälscher mit überschaubarem Aufwand unmöglich zu kopieren. Auch kennt dieser die einzelnen Regeln für die Erfassung oder die OCR-Umwandlung nicht, so dass er unmöglich die beim Authentifikationsserver als Referenzmerkmal hinterlegte Sicherheitsinformation vorhersehen kann. Zur Authentifikation werden dieselben Regeln verwendet, die zuvor schon beim erstmaligen Einlesen des Sicherheitselementes 1 herangezogen wurden. Handelt es sich hierbei um das Original, so verläuft die Authentifikation positiv. Sollte der Vergleich zu viele Unterschiede bei der Zeichenerkennung oder Zeicheninterpretation zu Tage fördern, so würde die Authentifikation fehlschlagen und ein Alarm ausgelöst werden.

[0065] In Fig. 4 ist eine weitere Variante der erfindungsgemäßen Authentifikationsvorrichtung gezeigt. Die Authentifikationsvorrichtung kann dabei aus mehreren, räumlich getrennten Komponenten bestehen, die beispielsweise über ein Netzwerk (zum Beispiel dem Internet) miteinander verbunden sind. Ausgangspunkt ist ein physisches Sicherheitselement 1 (z.B. Ticket), auf dessen Oberfläche 3 Sicherheitsmerkmale 2 in Form eines Codes ausgebildet sind. Einzelne Zeichen des Sicherheitsmerkmals 2 werden von Rissen als Strukturmerkmal 4 überlagert und sind dadurch für eine spätere OCR-Analyse nicht mehr einwandfrei auswertbar. Über ein Handy 1 erfolgt eine optische Erfassung des Sicherheitselementes 1 mittels eingebauter HandyKamera, die als Erfassungseinrichtung 5 dient. Nach der erfolgten Erfassung des Sicherheitselementes 1 wird auf dem Anzeigegerät des Handy 1 das Sicherheitselement 1 dargestellt und an einen Server als Bild oder bereits ausgelesenes Sicherheitsmerkmal in Codeform gesendet, der zum einen das Abbild des Sicherheitselementes 1 hinterlegen kann, zugleich jedoch auch eine Zeichenerkennung bzw. einen Abgleich mit einem Referenzmerkmal durchführen kann. Aus diesem Grund umfasst der Server eine Zeichenerkennungseinrichtung 6 sowie eine Abgleicheinrichtung 7. Das Handy 1 und/oder 2 kann die Funktionen des Servers übernehmen, insbesondere wenn es sich um eine lokale Anmeldung auf dem Handy handelt. In diesem Fall würde der Server lediglich aktualisiert werden.

[0066] Die Authentifikation erfolgt in der dargestellten Ausführungsvariante über ein weiteres Auslesegerät (Handy 2). Mit diesem Auslesegerät als weitere Erfassungseinrichtung 5 erfolgt das Einlesen des im Anzeigegerät des Handy 1 dargestellten Sicherheitselementes 1. Eine Regeleinrichtung 8 gibt vor, dass das Auslesen beispielsweise mit Rotlicht erfolgen soll, so dass in dem Sicherheitselement 1 nur die Ziffern 5 und 3 des Sicherheitsmerkmals 2 erkennbar sind.

[0067] Die Ausleseregel kann, je nach Variante, entweder vom Server selbst oder dem Handy 2 vorgegeben werden, sofern dieses eine eigene Regeleinrichtung 8 umfasst, welche die Ausleseregel zum Einlesen des

Sicherheitselementes 1 vorgibt. Dabei können das Handy 1, der Server und/oder das Handy 2 eine eigene Regeleinrichtung 8 umfassen, was vom jeweiligen Anwendungsfall abhängt. So lassen sich individuell die Regeln und Parameter für das Einlesen und die anschließende Auswertung des Sicherheitsmerkmals für die einzelnen Komponenten der Authentifikationsvorrichtung festlegen.

[0068] Schon ohne Umwandlung der von der Erfassungseinrichtung 5 erfassten Zeichen des Anzeigegerätes des Handy 1 ist ausreichend, um ein hohes Maß an Sicherheit zu garantieren. Sicherheitserhöhend kann nun hinzukommen, dass die mit dem Auslesegerät des Handy 2 erfassten Zeichen des Sicherheitsmerkmals 2 zusätzlich einer OCR-Erkennung unterzogen wird, um lesbare Zeichen in computerlesbare Zeichen umzuwandeln. Dabei sind einzelne Zeichen aufgrund der überlagerten Strukturmerkmale 4 nicht mehr einwandfrei interpretierbar.

[0069] Ein besonderes Merkmal der hier gezeigten Ausführungsvariante der erfindungsgemäßen Authentifikationsvorrichtung liegt darin, dass das Anzeigegerät des Handy 1 mit dem Server bei einer Authentifikationsabfrage nicht verbunden sein muss, d. h. die Authentifikation kann auch dann durchgeführt werden, wenn das Handy 1 "offline" ist. Über die Abgleicheinrichtung 7 des Servers erfolgt ein Vergleich des von dem Auslesegerät des Handys 2 erfassten Sicherheitsmerkmals 2 mit dem hinterlegten Referenzzeichen. Eine doppelte Authentifikation kann durchgeführt werden, wenn das Handy 1 eine intakte Netzwerkverbindung hat, d.h. "online" ist, denn dann kann das Handy 2 das erfasste Sicherheitsmerkmal 2 durch eine Rückabfrage mit dem Handy 1 gegenprüfen.

[0070] In einer weiteren bevorzugten (nicht gezeigten) Variante ist vorgesehen, dass eine mobile Kommunikationseinrichtung (z.B. das Handy 1 oder Handy 2) die Zeichenerkennungseinrichtung 6 und/oder die Abgleicheinrichtung 7 und/oder Regeleinrichtung 8 umfasst. Dann bräuchte man keinen separaten Server. Das Handy würde dessen Funktionen übernehmen.

[0071] Fig. 5 zeigt eine alternative Variante der erfindungsgemäßen Authentifikationsvorrichtung (= Authentifikationseinrichtung), bei der alle Komponenten der Authentifikationsvorrichtung eine Verbindung innerhalb eines Netzwerkes haben (= alle Einrichtungen online). Auch hier wird über ein Handy 1 zunächst ein physisches Sicherheitselement 1 mittels Handykamera erfasst und an den Authentifikationsserver übertragen, der bedarfsweise eine Zeichenerkennung über eine Zeichenerkennungseinrichtung 6 und gegebenenfalls einen Zeichenabgleich mit einem hinterlegten Referenzzeichen über eine Abgleicheinrichtung 7 vornehmen kann.

[0072] Zusätzlich ist eine lokale Datenbank vorgesehen, die einen Speicher mit eingelesenen Codes für einen "offline"-Betrieb umfasst. Dabei erfolgt eine regelmäßige Aktualisierung entsprechend einer vorgegebenen Regel (z.B. eine Definition) zwischen dem Authentifikationsserver und der lokalen Datenbank. Diese Datenbank kann sich auch direkt auf dem Handy 2 befinden. Das Auslesen soll gemäß Ausleseregel mit Rotlicht erfolgen. Zeichen, welche in Komplementärfarben zu dem roten Licht dargestellt sind, sind bei der OCR-Analyse nicht darstellbar und werden neutralisiert.

[0073] Für eine Authentifikation wird zunächst das Sicherheitselement 1 auf dem Display (Anzeigegerät) des Handy angezeigt. Sofern das Handy 1 mit einer Regeleinrichtung 8 versehen ist, kann das Anzeigen des Sicherheitselementes 1 auch entsprechend vorgegebener Bedingungen oder Regeln erfolgen. In jedem Fall wird das angezeigte Sicherheitsmerkmal des Handy 1 von dem Auslesegerät des Handy 2 erfasst. Auch das Auslesen kann entsprechend vorgegebener Regeln mittels einer Regeleinrichtung 8 erfolgen, so dass in der dargestellten Variante als Resultat die Ziffern "5" und "3" der Zeichenfolge des Sicherheitsmerkmals 2 sichtbar sind. Anschließend erfolgt eine Überprüfung ("check") mit dem Authentifikationsserver dahingehend, ob das vom Auslesegerät des Handy 2 erfasst Sicherheitsmerkmal 2 mit dem hinterlegten Sicherheitsmerkmal übereinstimmt. Die hinterlegten Referenzdaten können entweder beim Authentifikationsserver selbst oder einer internen oder externen lokalen Datenbank hinterlegt sein. Die Regeleinrichtung 8 kann entweder beim Server, dem Handy 1 oder Handy 2 zugeordnet sein oder mehreren dieser Einrichtungen.

[0074] In einer alternativen Variante kann das Auslesegerät des Handy 2 auch das physische Sicherheitselement 1 selbst auslesen.

[0075] In Fig. 6 ist eine Verfahrensvariante gezeigt, bei der einzelne oder alle Einrichtungen der erfindungsgemäßen Authentifikationsvorrichtung keine Netzwerkverbindungen haben (= alle Einrichtungen offline). In diesem Fall kommuniziert das Auslesegerät des Handy 2 direkt mit der lokalen Datenbank und führt eine Überprüfung des vom Anzeigegerät des Handy 1 erhaltenen Sicherheitsmerkmals 2 direkt mit der lokalen Datenbank durch. Bei dieser Variante würde somit keine Zeichenerkennung oder Abgleich mit dem Authentifikationsserver erfolgen.

[0076] In Fig. 7 ist die Situation dargestellt, dass lediglich das Handy 1 offline ist, während das Handy 2 online ist. In diesem Fall würde eine Überprüfung des Sicherheitsmerkmals 2 über den Authentifikationsserver erfolgen. Die lokale Datenbank wäre bei dieser Verfahrensvariante für eine Überprüfung des eingelesenen Sicherheitsmerkmals 2 nicht erforderlich.

[0077] In Fig. 8 ist die Situation dargestellt, bei der das Handy 1 online ist, während das Handy 2 offline ist. In diesem Fall würde eine Kommunikationsverbindung zwischen dem Authentifikationsserver und dem Handy 1 bestehen. Das Auslesegerät des Handy 2 kann nach wie vor das physische Sicherheitselement 1 direkt auslesen oder über das Anzeigegerät des Handy 1 dargestellte Sicherheitsmerkmal 2, wenn das Handy 1 online ist. Ansonsten erfolgt wiederum eine Überprüfung des ausgelesenen Sicherheitsmerkmals 2 über eine lokale Daten-

bank.

Patentansprüche

1. Authentifikationsvorrichtung, umfassend

- ein Sicherheitselement (1) mit wenigstens einem aus Zeichen bestehenden Sicherheitsmerkmal (2), die über eine Zeichenerkennung erfassbar sind, wobei das Sicherheitselement (1) wenigstens ein Strukturmerkmal (4) aufweist, welches das Erscheinungsbild des Sicherheitsmerkmals (2) und somit die Erfassbarkeit eines oder mehrerer Zeichen des Sicherheitsmerkmals (2) bei einer Zeichenerkennung und/oder Zeicheninterpretation beeinflusst,
- wenigstens eine Erfassungseinrichtung (5) zum Erfassen des Erscheinungsbilds der Zeichen des Sicherheitsmerkmals (2),
- wenigstens eine optische Zeichenerkennungseinrichtung (6) zur Durchführung einer optischen Zeichenerkennung (OCR), bei der die erkennbaren Zeichen des Erscheinungsbildes des Sicherheitsmerkmals (2) in maschinenlesbare Zeichen umgewandelt werden, wobei einzelne oder mehrere Zeichen des Sicherheitselements derart manipuliert sind, dass bei einer OCR-Erkennung oder OCR-Analyse schwer oder nicht lesbare Zeichen anders interpretiert werden oder gemäß einer Regel neu zugeordnet werden,
- wenigstens eine Abgleicheinrichtung (7) zum Abgleich des von der Erfassungseinrichtung (5) erfassten Sicherheitsmerkmals (2) und/oder der von der Zeichenerkennungseinrichtung (6) umgewandelten Zeichen mit einem in einem Speicher hinterlegten Referenzmerkmal, **dadurch gekennzeichnet, dass** die Authentifikationsvorrichtung wenigstens eine Regeleinrichtung (8) umfasst, welche die Regeln und/oder Parameter für die Erfassung und/oder das Einlesen und/oder die Analyse für die Zeichen des Sicherheitsmerkmals in einer Weise vorgibt, dass die Erfassungsbedingungen zum Erfassen des Erscheinungsbilds der Zeichen und/oder die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals (2) für eine Authentifikationsanfrage der Regeleinrichtung (8) in einer nicht vorhersehbaren Weise verändert werden, indem die Auswahl der Parameter durch die Authentifikationsvorrichtung vorgegeben wird oder zufällig erfolgt.

2. Authentifikationsvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** das Strukturmerkmal (4) eine Materialschicht und/oder eine Eigenschaft des Sicherheitselementes (1) und/oder des Sicherheitsmerkmals (2) oder Teilen davon ist, welches das das Erscheinungsbild des Sicherheitsmerkmals (2) und somit die Erfassbarkeit eines oder mehrerer Zeichen des Sicherheitsmerkmals (2) bei einer Zeichenerkennung und/oder Zeicheninterpretation beeinflusst.

3. Authentifikationsvorrichtung nach Anspruch 2, **dadurch gekennzeichnet, dass** das Strukturmerkmal (4) des Sicherheitselements (1) ausgewählt ist aus der Gruppe bestehend aus einem Krakeleemuster in Form von Rissen, Abplatzungen, Sprüngen oder Ausnehmungen; 3D-Oberflächenveränderungen wie Oberflächenerhebungen oder Oberflächenvertiefungen, Relativverlagerungen von Zeichen auf dem Sicherheitselement (1), farbliche oder mechanische Veränderungen der Zeichen und/oder des Hintergrundes des Sicherheitselements (2) wie Überschattungen oder Trübungen, wobei das Strukturmerkmal (4) zumindest teilweise das Sicherheitsmerkmal (2) überlagert, entfernt oder auf sonstige Weise verändert.

4. Authentifikationsvorrichtung nach einem der Ansprüche 2 bis 3, **dadurch gekennzeichnet, dass** sich ein Strukturmerkmal (4) des Sicherheitselements (1) selbst dynamisch in zufälliger Weise verändert und somit zu einem veränderten Erscheinungsbild des Sicherheitselements (1) zwischen zwei Abfragezeitpunkten führt, wobei die dynamische Veränderung des Strukturmerkmals (4) des Sicherheitselements (1) bedingt ist durch eine Materialeigenschaft des Strukturmerkmals (4), eine inhärente Eigenschaft des Sicherheitselements (1) und/oder durch eine Beeinflussung über einen externen physikalischen und/oder chemischen und/oder biologischen Faktor.

5. Authentifikationsvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** die Einlesebedingungen für die Erfassung des Erscheinungsbildes des Sicherheitsmerkmals (2) und/oder die Zeichenerkennung und/oder die Zeichenanalyse eine Erkennungsschwelle für ein erkennbares und/oder nicht erkennbares Zeichen, eine Intensitätsmessung der Helligkeit- und/oder der Farbwerte der Zeichen, eine Farbbestimmung der Zeichen, eine Größenbestimmung der Zeichen, eine Positionsbestimmung der Zeichen, ein Schärfen- oder Unschärfebereich, die Anwendung eines Filters oder einer Maske, eine Über- oder Unterbelichtung, eine Belichtung mit Komplementärfarben oder eine sonstige Eigenschaft der Zeichen umfassen.

6. Authentifikationsvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** das Sicherheitselement (1) ein Biopolymer umfasst, welches entweder

schichtartig aufgebaut ist, oder das Sicherheitselement (1) oder Teile davon bildet, oder bei dem Zeichen des Sicherheitsmerkmals (2) aus einem Biopolymer gebildet sind, wobei sich das Biopolymer aufgrund biologischer, chemischer, physikalischer oder mechanischer Einflüsse zusätzlich verändert.

7. Authentifikationsvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** ferner eine Anzeigeeinrichtung vorgesehen ist, auf der das aktuelle oder modifizierte Erscheinungsbild des Sicherheitselements (1) nach Übermittlung durch oder an die Abgleicheinrichtung (7) für eine Authentifikation darstellbar ist.

8. Authentifikationsvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** die Regeleinrichtung (8) Bestandteil der Erfassungseinrichtung (5) und/oder der Zeichenerkennungseinrichtung (6) und/oder der Abgleicheinrichtung (7) ist.

9. Verfahren zur Authentifikation oder Bestimmung der Identität einer Person, eines Gerätes, einer Sache, eines Dienstes, einer Anwendung und/oder eines Computerprogramms, bei dem eine Authentifikation über ein Sicherheitselement (1) mit wenigstens einem Sicherheitsmerkmal (2) und einer Authentifikationseinrichtung erfolgt, umfassend die Schritte:

- Bereitstellen eines Sicherheitselements (1) mit wenigstens einem aus Zeichen bestehenden Sicherheitsmerkmal (2), die über eine Zeichenerkennung erfassbar sind, wobei das Sicherheitselement (1) wenigstens ein Strukturmerkmal (4) aufweist, welches das Erscheinungsbild des Sicherheitsmerkmals (2) und somit die Erfassbarkeit eines oder mehrerer Zeichen des Sicherheitsmerkmals (2) bei einer Zeichenerkennung und/oder Zeicheninterpretation beeinflusst,
- Erfassen des Erscheinungsbilds der Zeichen des Sicherheitsmerkmal (2) über eine Erfassungseinrichtung,
- Durchführen einer optischen Zeichenerkennung (OCR), bei der die erkennbaren Zeichen des Erscheinungsbildes des Sicherheitsmerkmals (2) in maschinenlesbare Zeichen umgewandelt werden, wobei die erkennbaren Zeichen des Erscheinungsbildes des Sicherheitsmerkmals (2) in maschinenlesbare Zeichen umgewandelt werden, wobei einzelne oder mehrere Zeichen des Sicherheitselements derart manipuliert sind, dass bei einer OCR-Erkennung oder OCR-Analyse schwer oder nicht lesbare Zeichen anders interpretiert werden oder gemäß einer Regel neu zugeordnet werden,
- Abgleichen des von der Erfassungseinrichtung (5) erfassten Sicherheitsmerkmals (2) und/oder der von der Zeichenerkennungseinrichtung (6) umgewandelten Zeichen mit einem in einem Speicher hinterlegten Referenzmerkmal,

dadurch gekennzeichnet, dass die Regeln und/oder Parameter für die Erfassung und/oder das Einlesen und/oder die Analyse für die Zeichen des Sicherheitsmerkmals in einer Weise vorgegeben werden, dass die Erfassungsbedingungen zum Erfassen des Erscheinungsbilds der Zeichen und/oder die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals (2) für eine Authentifikationsanfrage in einer nicht vorhersehbaren Weise verändert werden, indem die Auswahl der Parameter durch die Authentifikationsvorrichtung vorgegeben wird oder zufällig erfolgt.

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** zumindest eine Einlesebedingung zwischen zwei Abfragezeitpunkten einer Sicherheitsabfrage verändert wird, wodurch ein zuvor beim ersten Abfragezeitpunkt erkennbares Zeichen in ein nicht erkennbares Zeichen, oder ein zuvor nicht erkennbares Zeichen in ein erkennbares Zeichen, oder ein erkennbares Zeichen in ein anderes erkennbares Zeichen umgewandelt wird.

11. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** für die Authentifikation nur bestimmte Zeichen innerhalb des Sicherheitsmerkmals (2) herangezogen werden, wobei die Auswahl über eine Regeleinrichtung (8) erfolgt, welche die Erfassungsbedingungen zum Erfassen des Erscheinungsbilds der Zeichen und/oder die Einlesebedingungen für die Zeichenerkennung und/oder die Analyseparameter für die Zeichenanalyse der Zeichen des Sicherheitsmerkmals (2) vorgibt.

12. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** zumindest eine Einlesebedingung vorsieht, dass die Erfassung des Erscheinungsbilds der Zeichen des Sicherheitsmerkmal (2) zumindest abschnittsweise so beeinflusst wird, dass bestimmte Zeichen für die spätere Zeichenerkennung und/oder Zeichenanalyse nicht lesbar sind, oder nicht lesbare Zeichen für eine spätere Zeichenerkennung und/oder Zeichenanalyse lesbar werden, und/oder lesbare Zeichen in einer späteren Zeichenerkennung anders interpretiert werden.

13. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** das Sicherheitselement (1) auf einer Anzeigevorrichtung dargestellt wird, wobei eine Einlesebedingung vorsieht, dass die Wiedergabe des Erscheinungsbilds der Zeichen des Sicherheitsmerkmal in der Anzeigevorrichtung zumindest abschnittsweise so beeinflusst ist, dass bestimmte Zeichen für die spätere Zeichenerkennung und/oder

Zeichenanalyse nicht lesbar sind, oder nicht lesbare Zeichen für eine spätere Zeichenerkennung und/oder Zeichenanalyse lesbar werden, und/oder lesbare Zeichen in einer späteren Zeichenerkennung anders interpretiert werden.

14. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** das Einlesen des Sicherheitselements (1) oder Teile davon unter einer Beleuchtung mit Komplementärfarben erfolgt, so dass bestimmte Zeichen für die spätere Zeichenerkennung und/oder Zeichenanalyse nicht lesbar sind, oder nicht lesbare Zeichen für eine spätere Zeichenerkennung und/oder Zeichenanalyse lesbar werden, und/oder lesbare Zeichen in einer späteren Zeichenerkennung anders interpretiert werden.

Claims

1. Authentication device comprising

- a security element (1) with at least one security feature (2) consisting of characters which can be detected via character recognition, wherein the security element (1) has at least one structural feature (4) which influences the appearance of the security feature (2) and thus the detectability of one or more characters of the security feature (2) during character recognition and/or character interpretation,
- at least one detection device (5) for detecting the appearance of the characters of the security feature (2),
- at least one optical character recognition device (6) for carrying out optical character recognition (OCR) in which the recognizable characters of the appearance of the security feature (2) are converted into machine-readable characters, wherein one or more characters of the security element are manipulated in such a way that, in an OCR recognition or OCR analysis, characters that are difficult or impossible to read are interpreted differently or are reassigned according to a rule,
- at least one comparison device (7) for comparing the security feature (2) detected by the detection device (5) and/or the characters, converted by the character recognition device (6) with a reference feature stored in a memory, **characterized in that** the authentication device comprises at least one control device (8), which prescribes the rules and/or parameters for the detection and/or reading and/or analysis for the characters of the security feature in such a way that the detection conditions for detecting the appearance of the characters and/or the reading conditions for the character recognition and/or the analysis parameters for the character analysis of the characters of the security feature (2) are specified for an authentication request of the control device (8) are changed in an unpredictable way by the selection of the parameters being predetermined by the authentication device or being random.

2. Authentication device according to Claim 1, **characterized in that** the structural feature (4) is a material layer and/or a property of the security element (1) and/or the security feature (2) or parts thereof, which the appearance of the security feature (2) and thus influences the detectability of one or more characters of the security feature (2) during character recognition and/or character interpretation.

3. Authentication device according to Claim 2, **characterized in that** the structural feature (4) of the security element (1) is selected from the group consisting of a crackle pattern in the form of cracks, flaking, fissures or recesses; 3D surface changes such as surface elevations or surface depressions, relative displacements of characters on the security element (1), colour or mechanical changes in the characters and/or the background of the security element (2) such as overshadowing or clouding, wherein the structural feature (4) at least partially overlays , removes or otherwise alteres the security feature (2).

4. Authentication device according to one of Claims 2 to 3, **characterized in that** a structural feature (4) of the security element (1) itself changes dynamically in a random manner and thus leads to a changed appearance of the security element (1) between two query times, wherein the dynamic change of the structural feature (4) of the security element (1) is caused by a material property of the structural feature (4), an inherent property of the security element (1) and/or by being influenced by an external physical and/or chemical and/or biological factor.

5. Authentication device according to Claim 1, **characterized in that** the reading conditions for the detection of the appearance of the security feature (2) and / or the character recognition and / or the character analysis comprise a recognition threshold for a recognizable and / or unrecognizable character, an intensity measurement of the brightness and/or the colour values of the characters, a character colour determination, a character size determination, a character position determination, a focus or blur area, the application of a filter or mask, an over- or under-exposure, an exposure with complementary colours or other property of characters.

6. Authentication device according to Claim 1, **characterized in that** the security element (1) comprises a

biopolymer which is either built up in layers or forms the security element (1) or parts thereof, or in which characters of the security feature (2) are formed from a biopolymer, wherein the biopolymer additionally changes due to biological, chemical, physical or mechanical influences.

7. Authentication device according to Claim 1, **characterized in that** a display device is also provided on which the current or modified appearance of the security element (1) can be displayed after transmission by or to the comparison device (7) for authentication.

8. Authentication device according to Claim 1, **characterized in that** the control device (8) is part of the detection device (5) and/or the character recognition device (6) and/or the comparison device (7).

9. Method for authentication or determination of the identity of a person, a device, an object, a service, an application and/or a computer program, in which authentication takes place via a security element (1) with at least one security feature (2) and an authentication device, comprising the steps:

- Providing a security element (1) with at least one security feature (2) consisting of characters which can be detected via character recognition, wherein the security element (1) has at least one structural feature (4) which influences the appearance of the security feature (2) and thus the detectability of one or more characters of the security feature (2) during character recognition and/or character interpretation,
- detecting the appearance of the characters of the security feature (2) via a detection device,
- Carrying out optical character recognition (OCR) in which the recognizable characters of the appearance of the security feature (2) are converted into machine-readable characters, wherein the recognisable characters of the appearance of the security feature (2) are converted into machine-readable characters, wherein individual or several characters of the security feature are manipulated in such a way that, during an OCR recognition or OCR analysis, characters that are difficult or impossible to read are interpreted differently or are reassigned according to a rule,
- comparing the security feature (2) detected by the detection device (5) and/or the characters converted by the character recognition device (6) with a reference feature stored in a memory, **characterised in that** the rules and/or parameters for the detection and/or reading and/or analysis for the characters of the security feature are predetermined in such a way that the detection conditions for detecting the appearance of the characters and/or the reading conditions for character recognition and/or the analysis parameters for character analysis of the characters of the security feature (2) for an authentication request are changed in an unpredictable way by the selection of the parameters being predetermined by the authentication device or being random.

10. Method according to Claim 9, **characterized in that** at least one reading condition is changed between two query times of a security query, whereby a character previously recognizable at the first query time is converted into an unrecognizable character, or a previously unrecognizable character is converted into recognizable character, or a recognizable character is converted into another recognizable character.

11. Method according to Claim 9, **characterized in that** only certain characters within the security feature (2) are used for the authentication, wherein the selection being made via a control device (8) which specifies the detection conditions for detecting the appearance of the characters and/or the reading conditions for the character recognition and / or the analysis parameters for the character analysis of the characters of the security feature (2).

12. Method according to Claim 9, **characterized in that** at least one reading condition provides that the detection of the appearance of the characters of the security feature (2) is influenced at least in sections in such a way that certain characters are not readable for later character recognition and/or character analysis, or unreadable characters become readable for later character recognition and/or character analysis, and/or readable characters are interpreted differently in later character recognition.

13. Method according to Claim 9, **characterized in that** the security element (1) is displayed on a display device, wherein a reading condition provides that the reproduction of the appearance of the characters of the security feature in the display device is influenced at least in sections in such a way that certain characters for the later character recognition and/or character analysis are unreadable, or unreadable characters become readable for later character recognition and/or character analysis, and/or readable characters are interpreted differently in later character recognition.

14. Method according to Claim 9, **characterized in that** the reading of the security element (1) or parts thereof takes place under illumination with complementary colours, so that certain characters are not readable for later character recognition and/or character

analysis, or unreadable characters become readable for later character recognition and/or character analysis, and/or readable characters are interpreted differently in later character recognition.

Revendications

1. Dispositif d'authentification, comprenant

- un élément de sécurité (1) muni d'au moins une caractéristique de sécurité (2) constituée de caractères qui peuvent être détectés par une reconnaissance de caractères, l'élément de sécurité (1) présentant au moins une caractéristique de structure (4) qui influe sur l'apparence de la caractéristique de sécurité (2) et donc sur la détectabilité d'un ou de plusieurs caractères de la caractéristique de sécurité (2) lors d'une reconnaissance de caractères et/ou d'une interprétation de caractères,
- au moins un dispositif de détection (5) pour détecter l'apparence des caractères de la caractéristique de sécurité (2),
- au moins un dispositif de reconnaissance de caractères optique (6) pour réaliser une reconnaissance de caractères optique (OCR), via laquelle les caractères reconnaissables de l'apparence de la caractéristique de sécurité (2) sont convertis en caractères lisibles par machine, un ou plusieurs caractères de l'élément de sécurité étant manipulés de telle sorte que lors d'une reconnaissance OCR ou d'une analyse OCR, des caractères difficilement lisibles ou illisibles sont interprétés différemment ou sont réassociés conformément à une règle,
- au moins un dispositif de mis en correspondance (7) pour mettre en correspondance la caractéristique de sécurité (2) détectée par le dispositif de détection (5) et/ou les caractères convertis par le dispositif de reconnaissance de caractères (6) muni d'une caractéristique de référence stockée dans une mémoire, **caractérisé en ce que** le dispositif d'authentification comprend au moins un dispositif de régulation (8) qui prédéfinit les règles et/ou les paramètres pour la détection et/ou la lecture et/ou l'analyse des caractères de la caractéristique de sécurité d'une manière telle que les conditions de détection pour la détection de l'apparence des caractères et/ou les conditions de lecture pour la reconnaissance de caractères et/ou les paramètres d'analyse pour l'analyse de caractères des caractères de la caractéristique de sécurité (2) sont modifiées d'une manière imprévisible pour une demande d'authentification du dispositif de régulation (8), la sélection des paramètres étant prédéfinie par le dispositif d'authentification ou survenant de manière aléatoire.

2. Dispositif d'authentification selon la revendication 1, **caractérisé en ce que** la caractéristique de structure (4) est une couche de matériau et/ou une propriété de l'élément de sécurité (1) et/ou de la caractéristique de sécurité (2) ou de parties de ceux-ci, qui influe sur l'apparence de la caractéristique de sécurité (2) et donc sur la détectabilité d'un ou de plusieurs caractères de la caractéristique de sécurité (2) lors d'une reconnaissance de caractères et/ou d'une interprétation de caractères.

3. Dispositif d'authentification selon la revendication 2, **caractérisé en ce que** la caractéristique de structure (4) de l'élément de sécurité (1) est sélectionnée dans le groupe constitué par un motif craquelé sous forme de fissures, d'éclats, de sauts ou d'évidements ; des modifications de surface 3D telles que des élévations ou des creux de surface, des déplacements relatifs de caractères sur l'élément de sécurité (1), des modifications de couleur ou mécaniques des caractères et/ou de l'arrière-plan de l'élément de sécurité (2) telles que des ombrages ou des opacités, la caractéristique de structure (4) chevauchant, enlevant ou modifiant autrement au moins partiellement la caractéristique de sécurité (2).

4. Dispositif d'authentification selon l'une quelconque des revendications 2 à 3, **caractérisé en ce qu'**une caractéristique de structure (4) de l'élément de sécurité (1) se modifie elle-même de manière dynamique de manière aléatoire et conduit ainsi à une apparence modifiée de l'élément de sécurité (1) entre deux instants d'interrogation, la modification dynamique de la caractéristique de structure (4) de l'élément de sécurité (1) étant conditionnée par une propriété de matériau de la caractéristique de structure (4), une propriété inhérente de l'élément de sécurité (1) et/ou par une influence sur un facteur externe physique et/ou chimique et/ou biologique.

5. Dispositif d'authentification selon la revendication 1, **caractérisé en ce que** les conditions de lecture pour la détection de l'apparence de la caractéristique de sécurité (2) et/ou la reconnaissance de caractères et/ou l'analyse de caractères comprennent un seuil de reconnaissance pour un caractère reconnaissable et/ou non reconnaissable, une mesure d'intensité des valeurs de luminosité et/ou de couleur des caractères, une détermination de couleur des caractères, une détermination de taille des caractères, une détermination de position des caractères, une zone de netteté ou de flou, l'application d'un filtre ou d'un masque, une sur- ou sous-exposition, une exposition avec des couleurs complémentaires ou une autre propriété des caractères.

6. Dispositif d'authentification selon la revendication 1, **caractérisé en ce que** l'élément de sécurité (1) comprend un biopolymère qui est structuré directement sous forme de couche ou forme l'élément de sécurité (1) ou des parties de celui-ci, ou les caractères de la caractéristique de sécurité (2) étant formés à partir d'un biopolymère, le biopolymère se modifiant en outre en raison d'influences biologiques, chimiques, physiques ou mécaniques.

7. Dispositif d'authentification selon la revendication 1, **caractérisé en ce qu'**un dispositif d'affichage est en outre prévu, sur lequel l'apparence actuelle ou modifiée de l'élément de sécurité (1) peut être représentée après transmission par ou au niveau du dispositif de mise en correspondance (7) pour une authentification.

8. Dispositif d'authentification selon la revendication 1, **caractérisé en ce que** le dispositif de régulation (8) fait partie intégrante du dispositif de détection (5) et/ou du dispositif de reconnaissance de caractères (6) et/ou du dispositif de mise en correspondance (7).

9. Procédé d'authentification ou de détermination de l'identité d'une personne, d'un appareil, d'une chose, d'un service, d'une application et/ou d'un programme informatique, l'authentification survenant par l'intermédiaire d'un élément de sécurité (1), muni d'au moins une caractéristique de sécurité (2), et d'un dispositif d'authentification, comprenant les étapes consistant à :

- fournir un élément de sécurité (1) muni d'au moins une caractéristique de sécurité (2) constituée de caractères qui peuvent être détectés par une reconnaissance de caractères, l'élément de sécurité (1) présentant au moins une caractéristique de structure (4) qui influe sur l'apparence de la caractéristique de sécurité (2) et donc sur la détectabilité d'un ou de plusieurs caractères de la caractéristique de sécurité (2) lors d'une reconnaissance de caractères et/ou d'une interprétation de caractères,
- détecter l'apparence des caractères de la caractéristique de sécurité (2) par l'intermédiaire d'un dispositif de détection,
- réaliser une reconnaissance de caractères optique (OCR), les caractères reconnaissables de l'apparence de la caractéristique de sécurité (2) étant convertis en caractères lisibles par machine, les caractères reconnaissables de l'apparence de la caractéristique de sécurité (2) étant convertis en caractères lisibles par machine, un ou plusieurs caractères de l'élément de sécurité étant manipulés de telle sorte que lors d'une reconnaissance OCR ou d'une analyse OCR, des caractères difficilement lisibles ou illisibles sont interprétés différemment ou sont réassociés conformément à une règle,
- mettre en correspondance la caractéristique de sécurité (2) détectée par le dispositif de détection (5) et/ou les caractères convertis par le dispositif de reconnaissance de caractères (6) avec une caractéristique de référence stockée dans une mémoire, **caractérisé en ce que** les règles et/ou les paramètres pour la détection et/ou la lecture et/ou l'analyse pour les caractères de la caractéristique de sécurité sont prédéterminés de telle manière que les conditions de détection pour la détection de l'apparence des caractères et/ou les conditions de lecture pour la reconnaissance de caractères et/ou les paramètres d'analyse pour l'analyse de caractères des caractères de la caractéristique de sécurité (2) sont modifiés d'une manière imprévisible pour une demande d'authentification, la sélection des paramètres étant prédéterminée par le dispositif d'authentification ou survenant de manière aléatoire.

10. Procédé selon la revendication 9, **caractérisé en ce qu'**au moins une condition de lecture est modifiée entre deux instants d'interrogation d'une interrogation de sécurité, grâce à quoi un caractère précédemment reconnaissable au premier instant d'interrogation est converti en un caractère non reconnaissable, ou un caractère précédemment non reconnaissable est converti en un caractère reconnaissable, ou un caractère reconnaissable est converti en un autre caractère reconnaissable.

11. Procédé selon la revendication 9, **caractérisé en ce que** pour l'authentification, seuls des caractères déterminés sont utilisés à l'intérieur de la caractéristique de sécurité (2), la sélection s'effectuant par l'intermédiaire d'un dispositif de régulation (8) qui prédéfinit les conditions de détection pour la détection de l'apparence des caractères et/ou les conditions de lecture pour la reconnaissance de caractères et/ou les paramètres d'analyse pour l'analyse de caractères des caractères de la caractéristique de sécurité (2).

12. Procédé selon la revendication 9, **caractérisé en ce qu'**au moins une condition de lecture prévoit que la détection de l'apparence des caractères de la caractéristique de sécurité (2) est influencée au moins par sections de telle sorte que des caractères déterminés ne sont pas lisibles pour la reconnaissance de caractères et/ou l'analyse de caractères ultérieure(s), ou que des caractères non lisibles deviennent lisibles pour une reconnaissance de caractères et/ou une analyse de caractères ultérieure(s), et/ou que des caractères lisibles soient interprétés différem-

ment dans une reconnaissance de caractères ultérieure.

13. Procédé selon la revendication 9, **caractérisé en ce que** l'élément de sécurité (1) est représenté sur un dispositif d'affichage, une condition de lecture prévoyant que la reproduction de l'apparence des caractères de la caractéristique de sécurité dans le dispositif d'affichage est influencée au moins par sections de telle sorte que certains caractères ne soient pas lisibles pour la reconnaissance de caractères et/ou l'analyse de caractères ultérieure(s), ou que des caractères non lisibles deviennent lisibles pour une reconnaissance de caractères et/ou une analyse de caractères ultérieure(s), et/ou que des caractères lisibles soient interprétés différemment dans une reconnaissance de caractères ultérieure.

14. Procédé selon la revendication 9, **caractérisé en ce que** la lecture de l'élément de sécurité (1) ou de parties de celui-ci survient sous un éclairage avec des couleurs complémentaires, de sorte que des caractères déterminés ne sont pas lisibles pour la reconnaissance de caractères et/ou l'analyse de caractères ultérieure(s), ou des caractères non lisibles deviennent lisibles pour une reconnaissance de caractères et/ou une analyse de caractères ultérieure(s), et/ou que des caractères lisibles soient interprétés différemment dans une reconnaissance de caractères ultérieure.

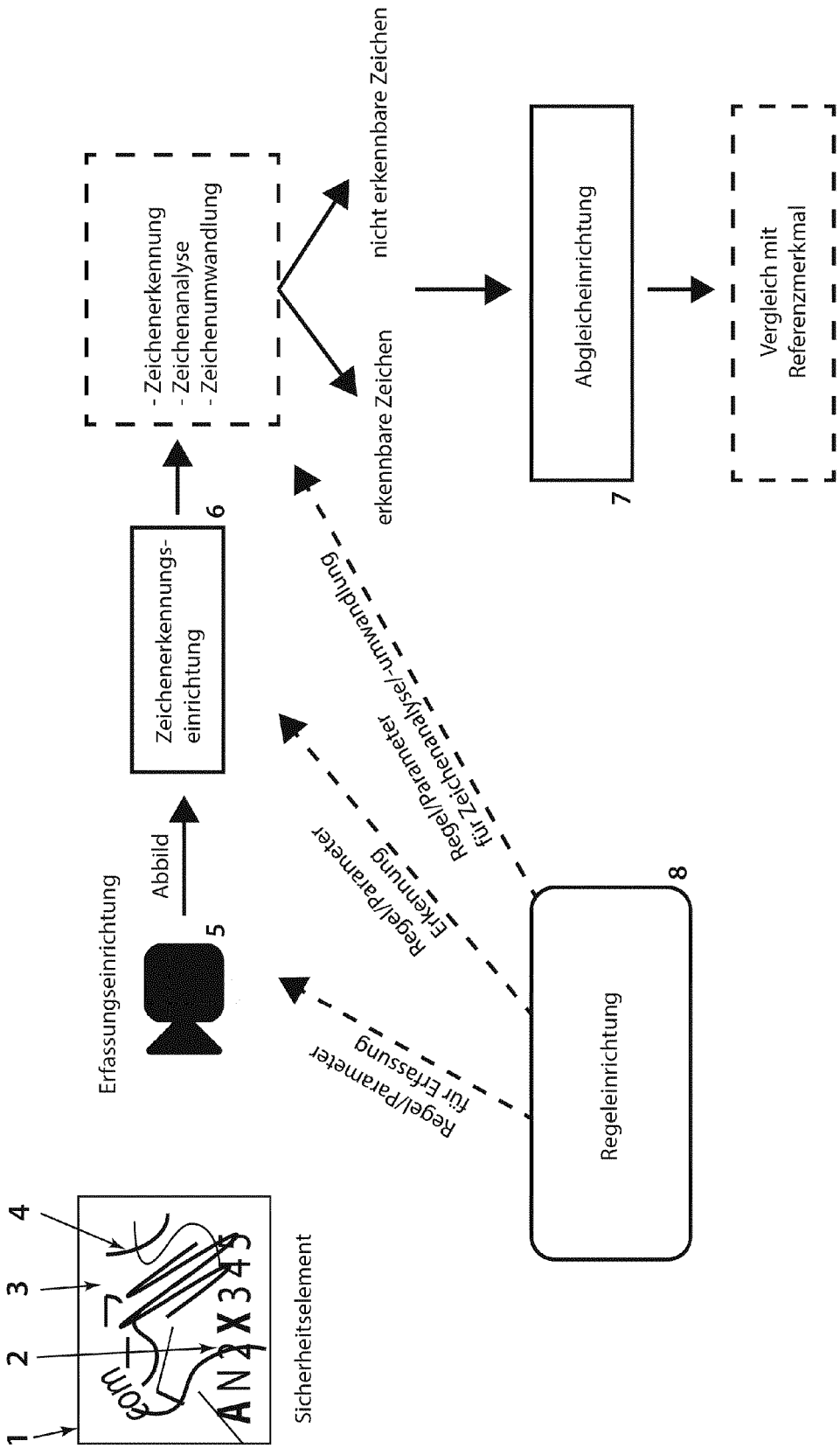

1
2
3
4
Sicherheitselement
Erfassungseinrichtung
5
Abbild
Zeichenerkennungs-
einrichtung
6
- Zeichenerkennung
- Zeichenanalyse
- Zeichenumwandlung
nicht erkennbare Zeichen
erkennbare Zeichen
Abgleicheinrichtung
7
Vergleich mit
Referenzmerkmal
Regeleinrichtung
8
Regel/Parameter
für Erfassung
Regel/Parameter
Erkennung
Regel/Parameter
für Zeichenanalyse/-umwandlung

Fig. 1

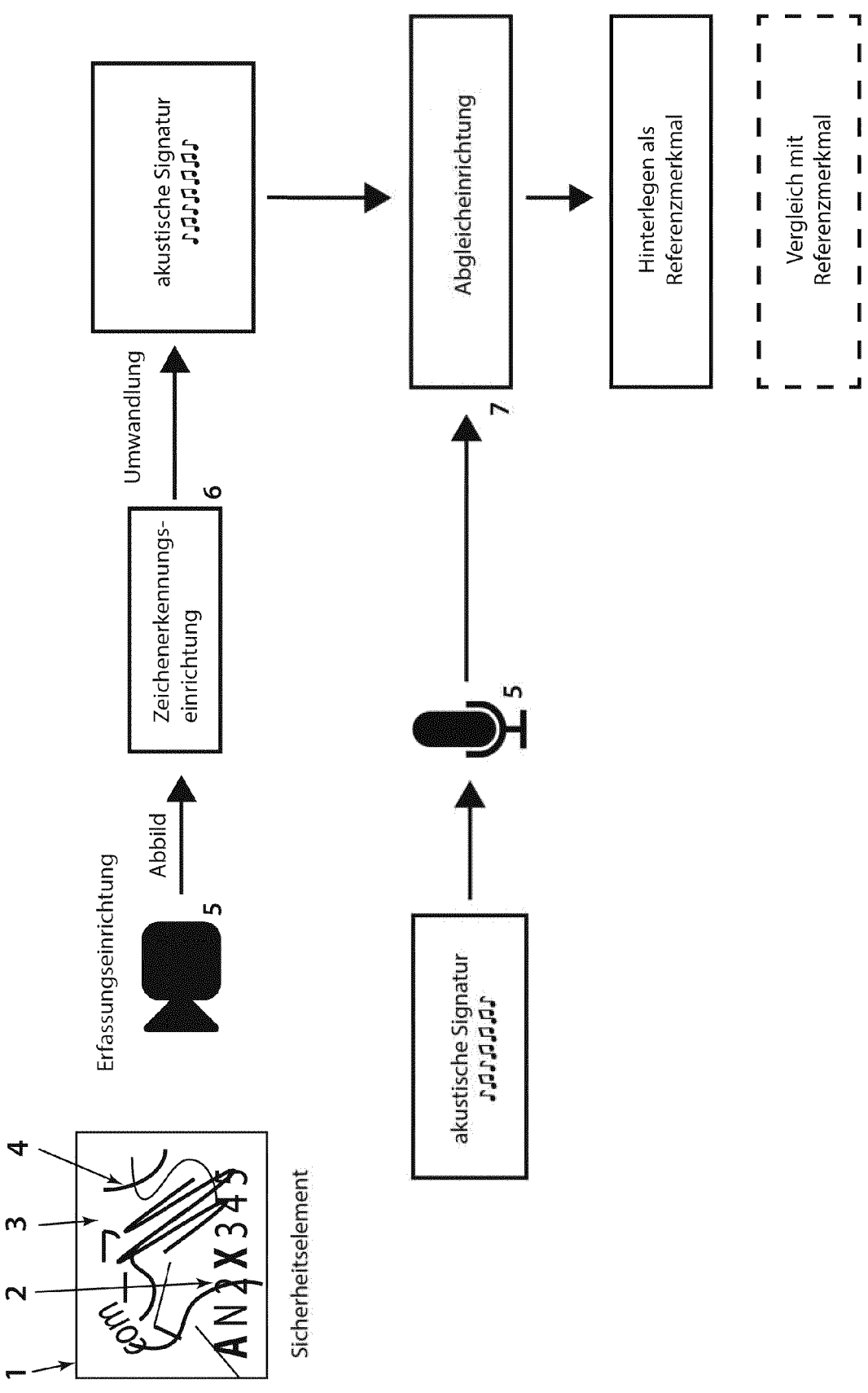

1
2
3
4
Sicherheitselement
Erfassungseinrichtung
Abbild
5
Zeichenerkennungs-einrichtung
6
Umwandlung
akustische Signatur
akustische Signatur
5
7
Abgleicheinrichtung
Hinterlegen als Referenzmerkmal
Vergleich mit Referenzmerkmal

Fig. 2

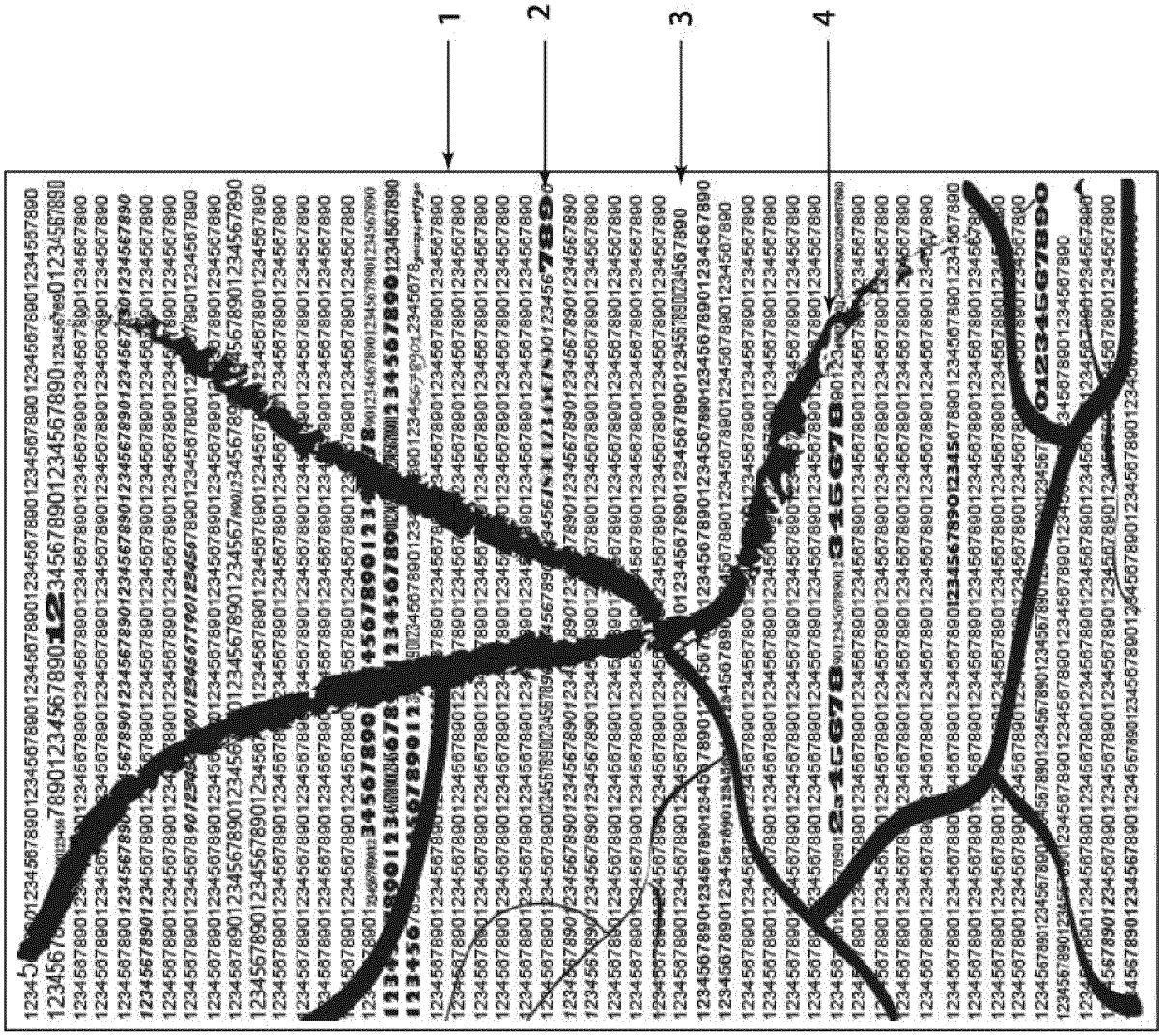


Fig. 3

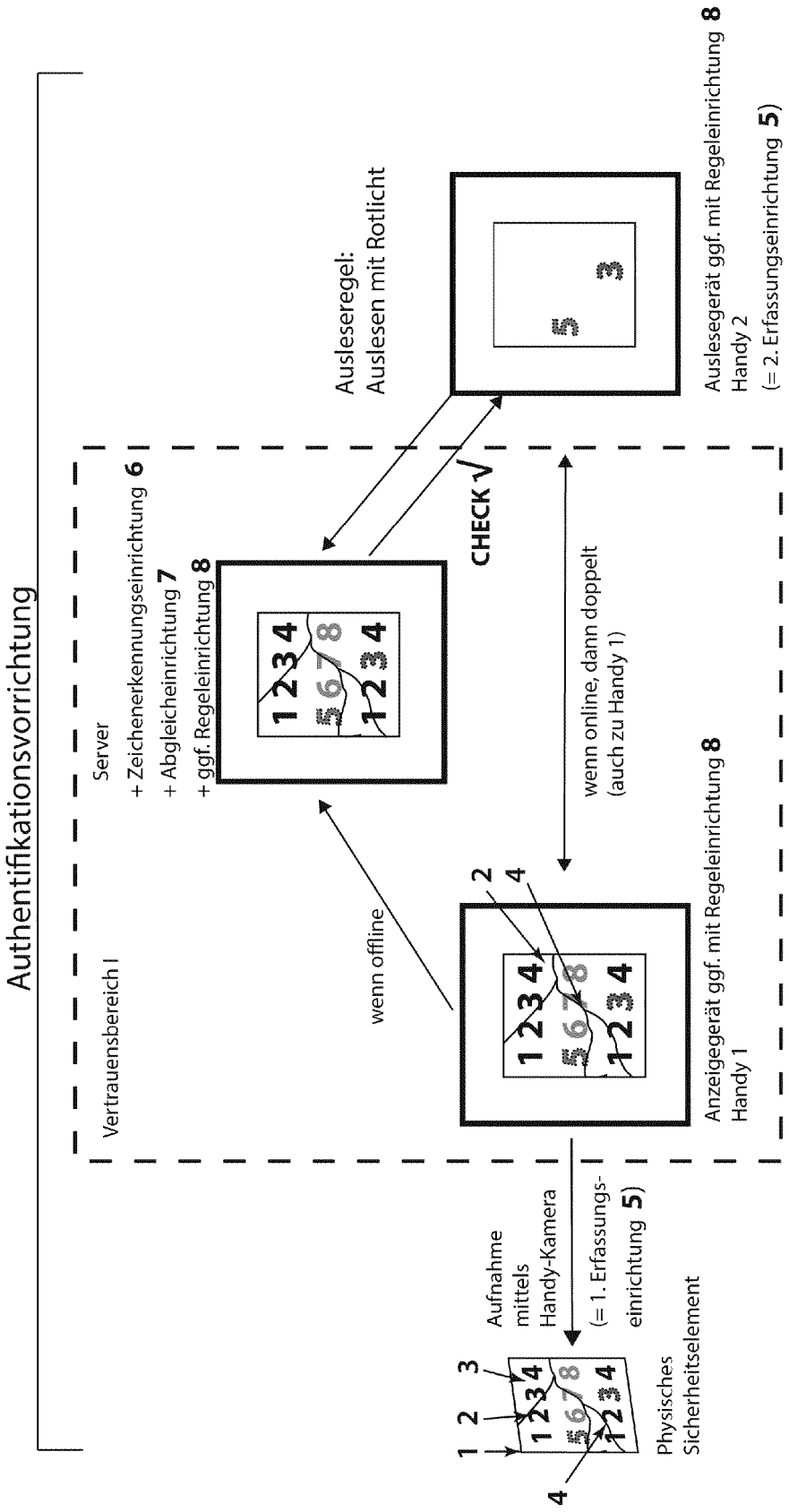

Authentifikationsvorrichtung
Vertrauensbereich I
Server
+ Zeichenerkennungseinrichtung 6
+ Abgleicheinrichtung 7
+ ggf. Regeleinrichtung 8
Auslesegerät ggf. mit Regeleinrichtung 8
Handy 2
(= 2. Erfassungseinrichtung 5)
Auslesregel:
Auslesen mit Rotlicht
CHECK √
wenn online, dann doppelt
(auch zu Handy 1)
wenn offline
Anzeigegerät ggf. mit Regeleinrichtung 8
Handy 1
Aufnahme
mittels
Handy-Kamera
(= 1. Erfassungs-
einrichtung 5)
Physisches
Sicherheitselement

Fig. 4

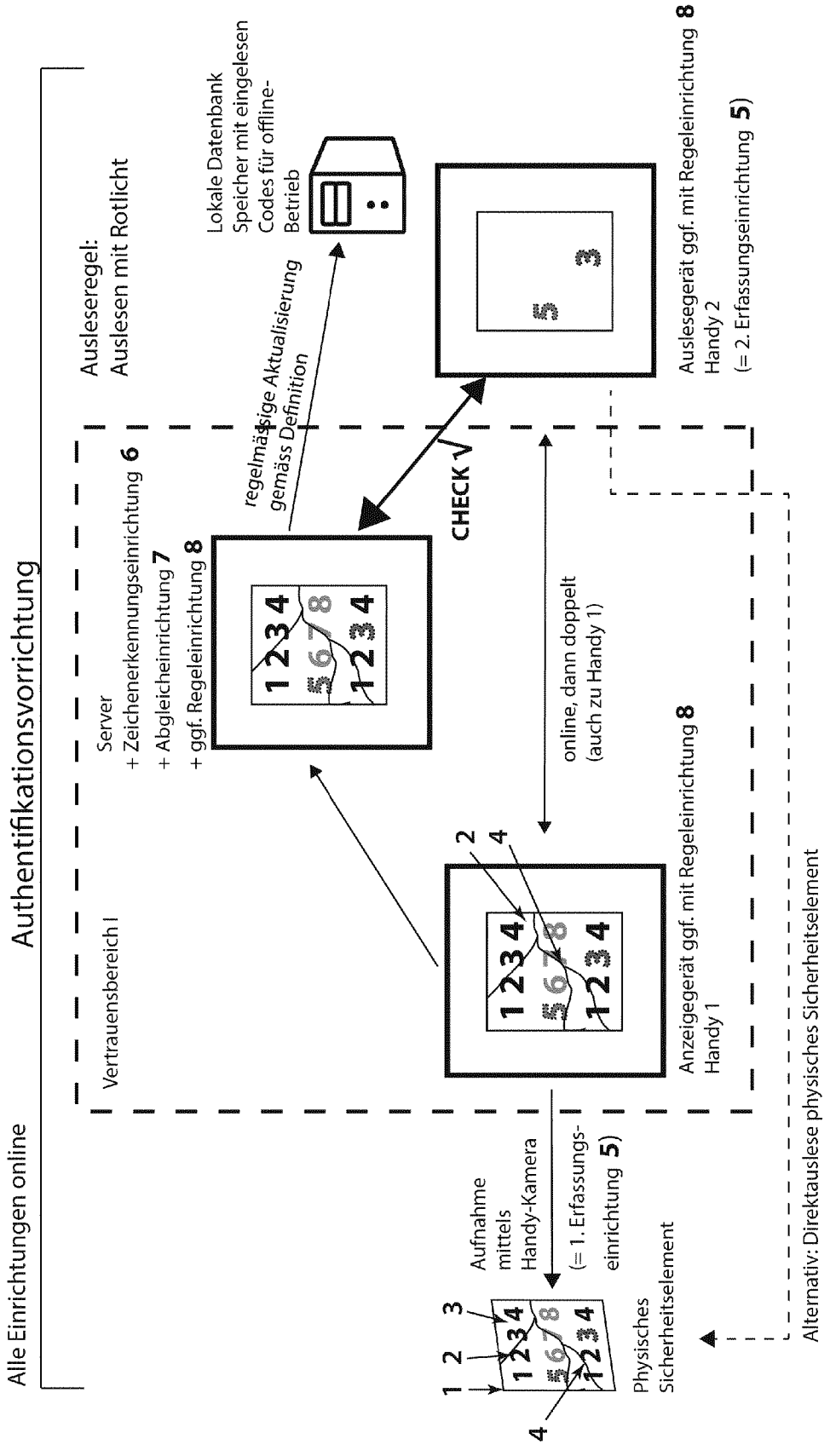

Alle Einrichtungen online
Authentifikationsvorrichtung
Vertrauensbereich I
Server
+ Zeichenerkennungseinrichtung 6
+ Abgleicheinrichtung 7
+ ggf. Regeleinrichtung 8
Auslesen mit Rotlicht
Auslesegerät ggf. mit Regeleinrichtung 8
Handy 2
(= 2. Erfassungseinrichtung 5)
Lokale Datenbank
Speicher mit eingelesen
Codes für offline-
Betrieb
regelmässige Aktualisierung
gemäss Definition
CHECK √
online, dann doppelt
(auch zu Handy 1)
Anzeigegerät ggf. mit Regeleinrichtung 8
Handy 1
Aufnahme
mittels
Handy-Kamera
(= 1. Erfassungs-
einrichtung 5)
Physisches
Sicherheitselement
Alternativ: Direktauslese physisches Sicherheitselement

Fig. 5

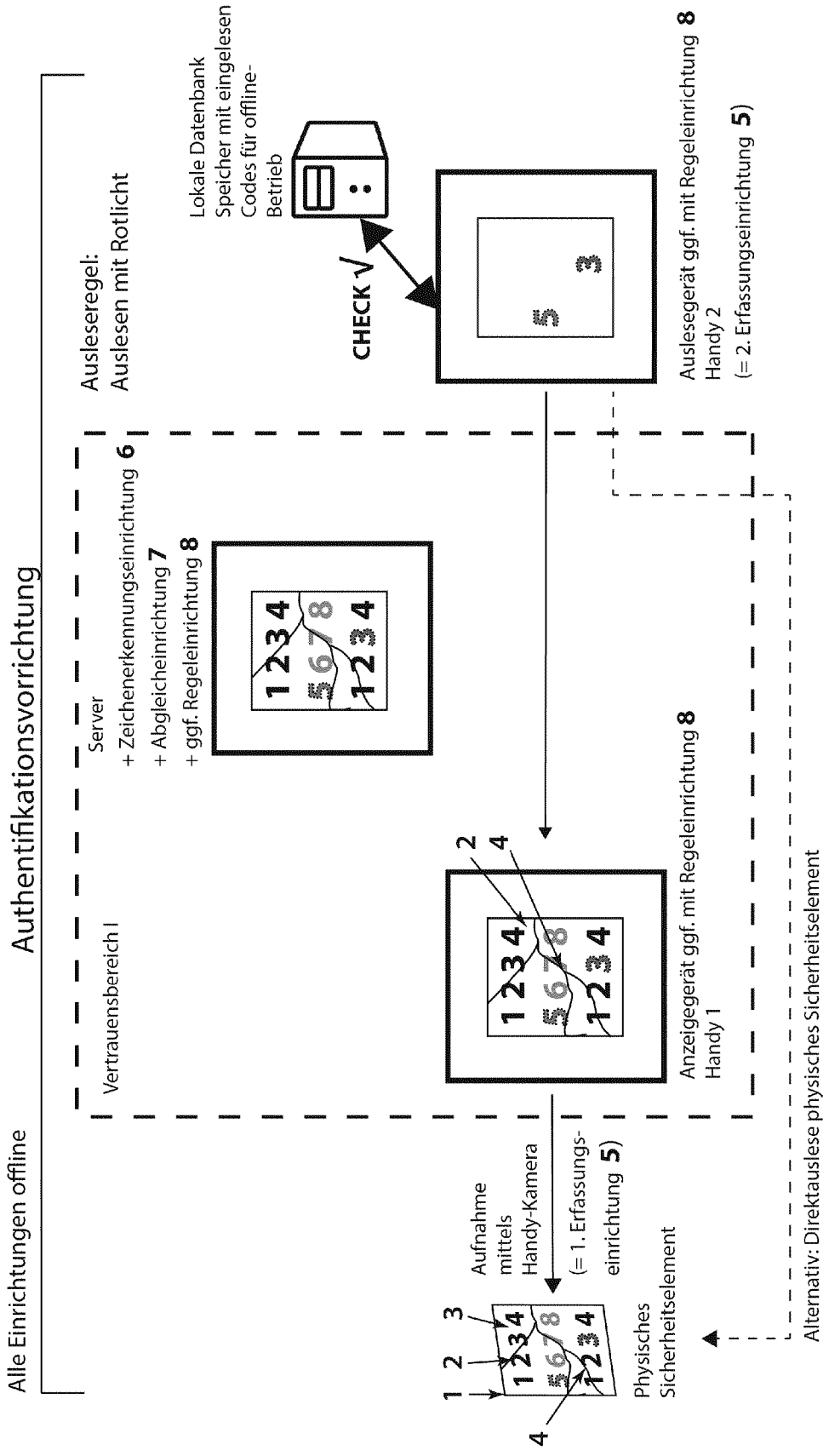

Alle Einrichtungen offline
Authentifikationsvorrichtung
Vertrauensbereich I
Server
+ Zeichenerkennungseinrichtung 6
+ Abgleicheinrichtung 7
+ ggf. Regeleinrichtung 8
Auslesen mit Rotlicht
Auslesegerät ggf. mit Regeleinrichtung 8
Handy 2
(= 2. Erfassungseinrichtung 5)
Lokale Datenbank
Speicher mit eingelesen
Codes für offline-
Betrieb
CHECK √
Anzeigegerät ggf. mit Regeleinrichtung 8
Handy 1
Aufnahme
mittels
Handy-Kamera
(= 1. Erfassungs-
einrichtung 5)
Physisches
Sicherheitselement
Alternativ: Direktauslese physisches Sicherheitselement

Fig. 6

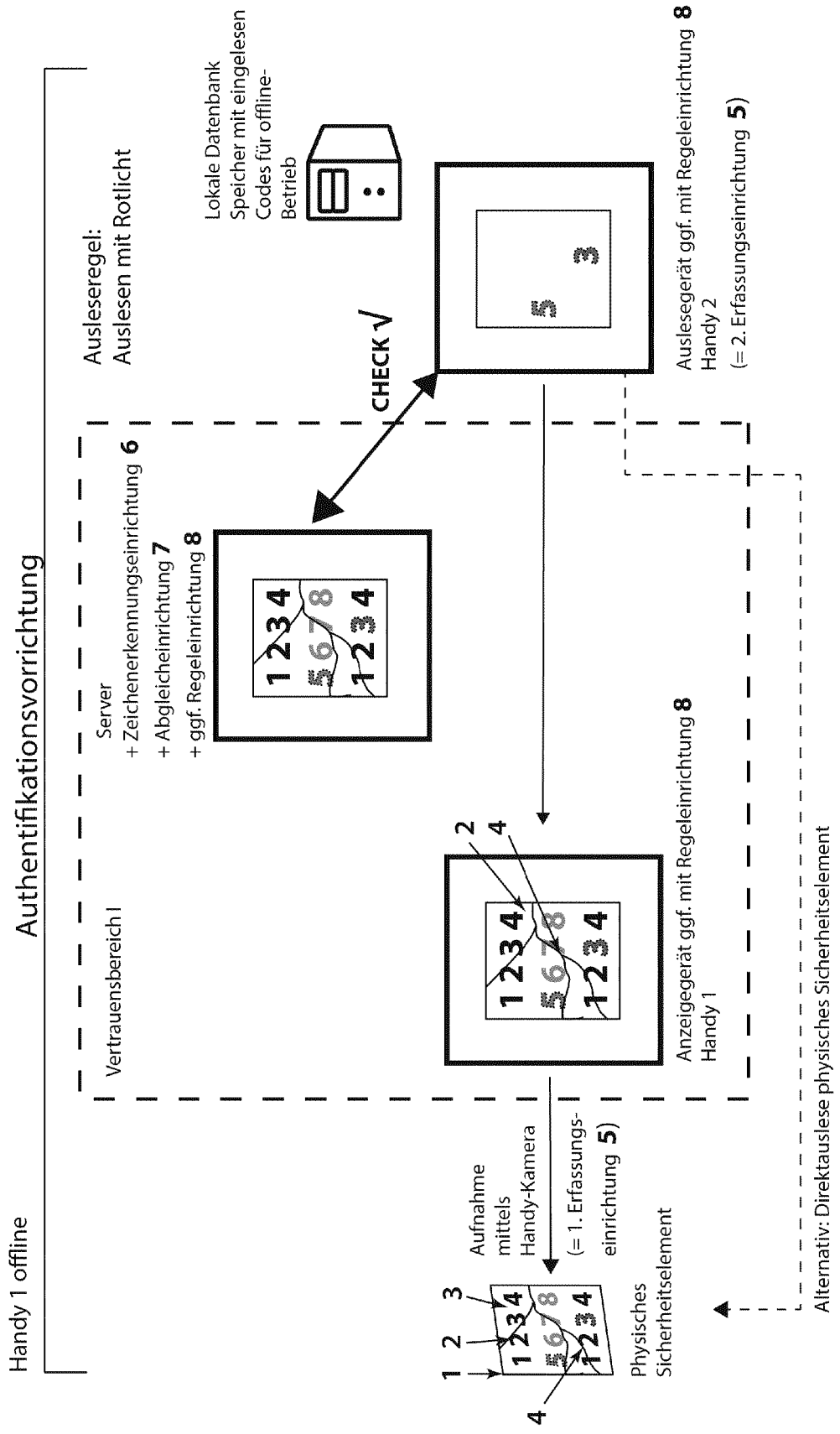

Handy 1 offline
Authentifikationsvorrichtung
Vertrauensbereich I
Server
+ Zeichenerkennungseinrichtung 6
+ Abgleicheinrichtung 7
+ ggf. Regeleinrichtung 8
Auslesen mit Rotlicht
Auslesegerät ggf. mit Regeleinrichtung 8
Handy 2
(= 2. Erfassungseinrichtung 5)
Lokale Datenbank
Speicher mit eingelesen
Codes für offline-
Betrieb
CHECK √
Anzeigegerät ggf. mit Regeleinrichtung 8
Handy 1
Aufnahme
mittels
Handy-Kamera
(= 1. Erfassungs-
einrichtung 5)
Physisches
Sicherheitselement
Alternativ: Direktauslese physisches Sicherheitselement

Fig. 7

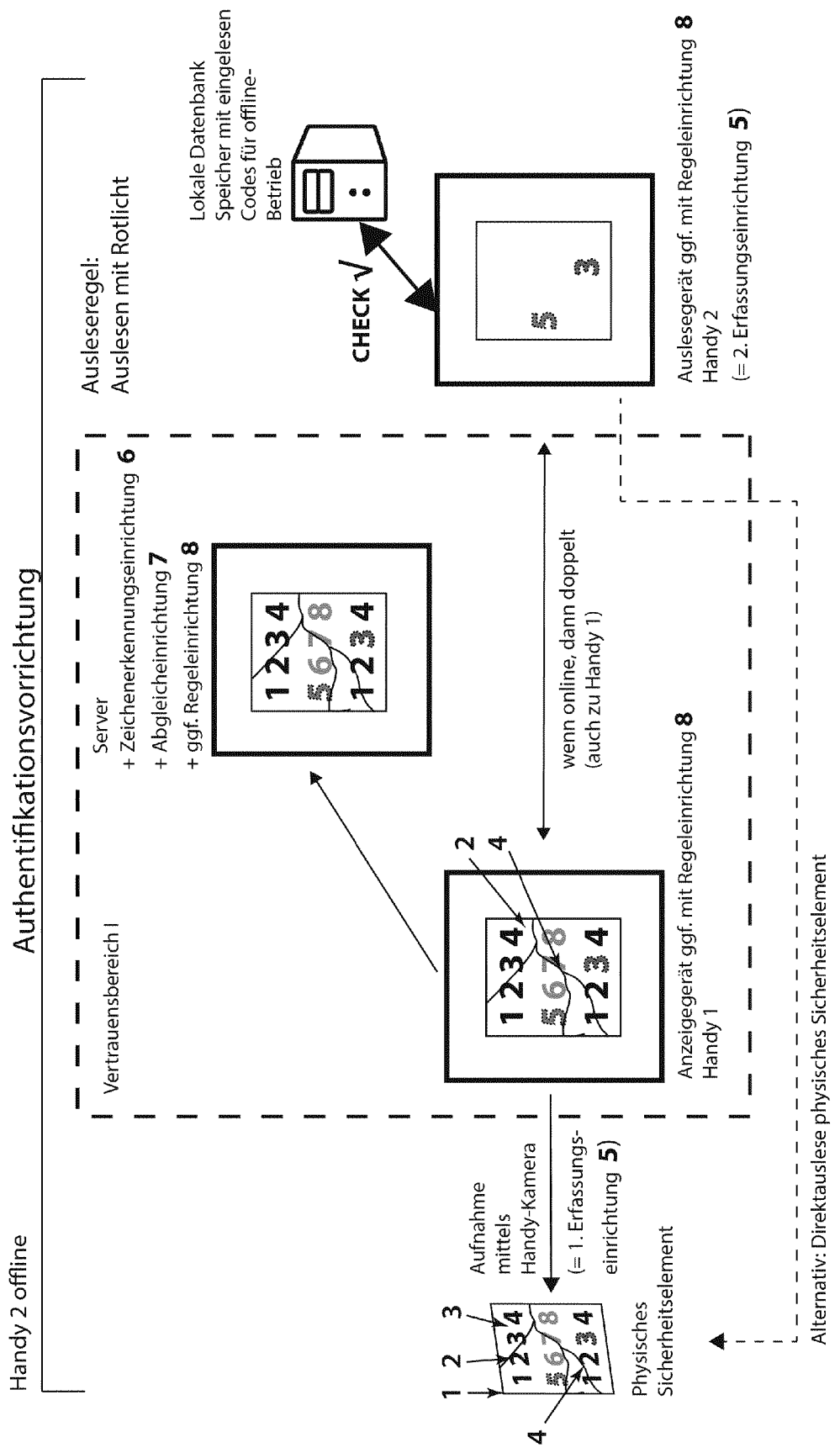

Handy 2 offline
Authentifikationsvorrichtung
Vertrauensbereich I
Server
+ Zeichenerkennungseinrichtung 6
+ Abgleicheinrichtung 7
+ ggf. Regeleinrichtung 8
Auslesegerät ggf. mit Regeleinrichtung 8
Handy 2
(= 2. Erfassungseinrichtung 5)
Auslesegerät ggf. mit Regeleinrichtung 8
Handy 1
Auslesegerät:
Auslesen mit Rotlicht
Lokale Datenbank
Speicher mit eingelesen
Codes für offline-
Betrieb
CHECK √
wenn online, dann doppelt
(auch zu Handy 1)
Aufnahme
mittels
Handy-Kamera
(= 1. Erfassungs-
einrichtung 5)
Physisches
Sicherheitselement
Alternativ: Direktauslese physisches Sicherheitselement

Fig. 8

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- DE 102004055761 A1 **[0002]**
- US 7793837 B1 **[0002]**
- DE 102009003221 A1 **[0003]**
- DE 102004045211 A1 **[0004]**
- DE 102004049998 A1 **[0004]**
- DE 102009036706 A1 **[0005]**
- DE 102009044881 A1 **[0006]**
- DE 102007044992 B3 **[0007]**
- DE 60126698 T2 **[0008]**
- US 3632993 A **[0008]**
- DE 102206057507 A1 **[0008]**
- DE 202013011992 U1 **[0009]**
- DE 102008077331 B4 **[0009]**
- DE 102006037260 B3 **[0009]**
- WO 02099735 A1 **[0009]**
- WO 2015124696 A1 **[0009]**
- DE 102009036706 B3 **[0010]**
- EP 2824641 A1 **[0011]**
- DE 102014004349 A1 **[0011]**