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

(11) **EP 2 039 527 A2**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
25.03.2009 Patentblatt 2009/13

(51) Int Cl.:
B42D 15/10 *(2006.01)*

(21) Anmeldenummer: **08015554.2**

(22) Anmeldetag: **03.09.2008**

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

(30) Priorität: **19.09.2007 DE 102007044992**

(71) Anmelder: **OVD Kinegram AG**
6301 Zug (CH)

(72) Erfinder:
- **Peters, John, Anthony, Dr.**
  8804 Au (CH)
- **Tompkin, Wayne, Robert, Dr.**
  5400 Baden (CH)
- **Schilling, Andreas, Dr.**
  6332 Hagendorn (ZG) (CH)

(74) Vertreter: **LOUIS, PÖHLAU, LOHRENTZ**
Postfach 30 55
90014 Nürnberg (DE)

(54) Diffraktives Sicherheitselement mit individualisiertem Code

(57) Es wird ein Sicherheitselement zur Erhöhung der Fälschungssicherheit eines Sicherheitsdokuments, insbesondere eines Ausweises, eines Passes oder einer Identifikationskarte, beschrieben. Das Sicherheitselement (1) weist einen ersten diffraktiven Bereich (15) auf, der einen offenen, mit einem unbewaffneten Auge sichtbaren Code aufweist. Der erste diffraktive Bereich weist weiter einen verborgenen, mit dem unbewaffneten Auge nicht sichtbaren Code auf, der aus der Anordnung in dem ersten Bereich (1) angeordneter diffraktiver Mikrobereiche und/oder aus der Struktur des ersten diffraktiven Bereichs (1) rekonstruierbar ist. Weiter wird ein Verfahren zur Erhöhung der Fälschungssicherheit eines Sicherheitsdokuments beschrieben.

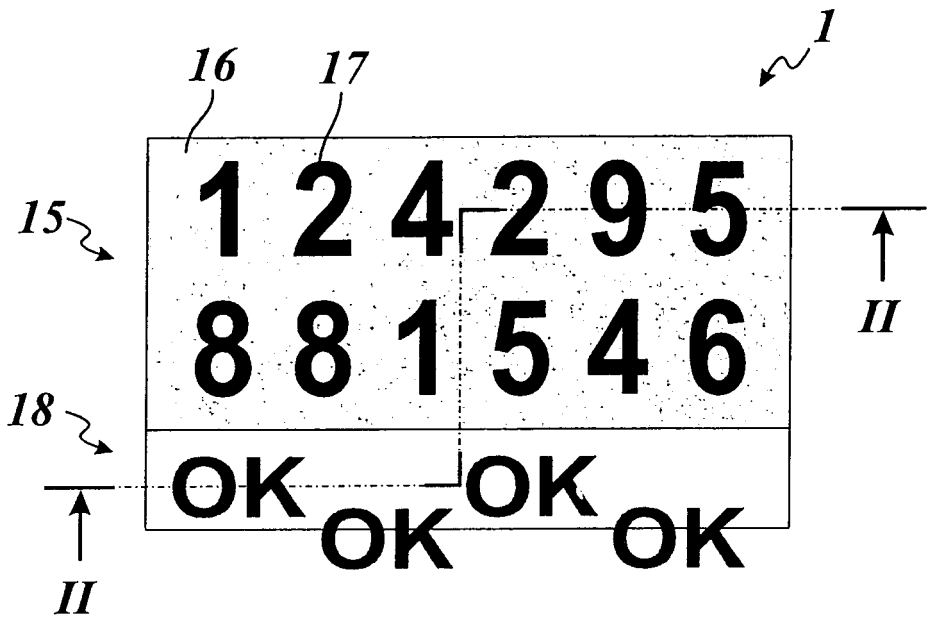

Fig. 1

EP 2 039 527 A2

Beschreibung

[0001] Die Erfindung betrifft ein Sicherheitselement und ein Verfahren zur Verifikation eines Sicherheitselements.

[0002] Diffraktive Sicherheitselemente werden eingesetzt, um die Fälschungssicherheit eines Sicherheitsdokuments, insbesondere eines Ausweises, eines Passes oder einer Identifikationskarte, oder eines Produkts zu erhöhen. Die Sicherheitselemente weisen unterschiedliche Sicherheitsmerkmale auf, die je nach Ausbildung die Sicherheit gegen Kopieren oder Verfälschen, die Überprüfung ohne oder mit Hilfsmitteln ermöglichen sowie Informationen bereitstellen, die zur Verifikation des Sicherheitselements oder zur automatischen Identifizierung einer Person verwendet werden können.

[0003] Aufgabe der vorliegenden Erfindung ist es, ein verbessertes Sicherheitselement, das kostengünstig herstellbar und fälschungssicher ist, und ein Verfahren zur Verifikation eines Sicherheitselements anzugeben.

[0004] Erfindungsgemäß wird diese Aufgabe mit einem Sicherheitselement zur Erhöhung der Fälschungssicherheit eines Sicherheitsdokuments, insbesondere eines Ausweises, eines Passes oder einer Identifikationskarte, oder eines Produkts, gelöst, wobei vorgesehen ist, dass das Sicherheitselement einen ersten Bereich aufweist, in dem zumindest bereichsweise in einer Schicht des Sicherheitselements ein zumindest bereichsweise mit einer Reflexionsschicht versehenes diffraktives Oberflächenrelief abgeformt ist, welches eine offene, mit einem unbewaffneten Auge sichtbare Information zeigt, und dass der erste Bereich weiter einen verborgenen, mit dem unbewaffneten Auge nicht sichtbaren, optisch auslesbaren maschinenlesbaren Code aufweist, der aus einer Anordnung von in dem ersten Bereich angeordneten und sich von dem umgebenden Bereich optisch unterscheidenden Mikrobereichen gebildet ist, in denen ein sich von dem umgebenden Bereich unterscheidendes Oberflächenrelief abgeformt ist und/oder die Reflexionsschicht entfernt ist, und/oder der maschinenlesbare Code von dem in die Schicht abgeformten Oberflächenrelief generiert ist. Weiter wird die Aufgabe durch ein Verfahren zur Erhöhung der Fälschungssicherheit eines Sicherheitsdokuments, insbesondere eines Ausweises, eines Passes oder einer Identifikationskarte gelöst, wobei vorgesehen ist, dass ein Sicherheitselement bereitgestellt wird, das einen ersten Bereich aufweist, in dem zumindest bereichsweise in eine Schicht des Sicherheitselements ein zumindest bereichsweise mit einer Reflexionsschicht versehenes diffraktives Oberflächenrelief abgeformt ist, welches eine offene, mit einem unbewaffneten Auge sichtbare Information zeigt, wobei der erste Bereich weiter einen verborgenen, mit dem unbewaffneten Auge nicht sichtbaren, optisch auslesbaren maschinenlesbaren Code aufweist, der aus einer Anordnung von in dem ersten Bereich angeordneten und von dem umgebenden Bereich sich optisch unterscheidenden Mikrobereichen gebildet ist, in denen ein sich von dem umgebenden Bereich unterscheidendes Oberflächenrelief abgeformt ist und/oder die Reflexionsschicht entfernt ist, und/oder der maschinenlesbare Code von dem in die Schicht abgeformten Oberflächenrelief generiert ist, und dass der verborgene maschinenlesbare Code mit einem Lesegerät zur Verifikation des Sicherheitselements ausgelesen wird.

[0005] Der Betrachter nimmt so im ersten Bereich die offene Information wahr, der in dem selben Bereich codierte maschinenlesbare Code bleibt ihm jedoch verborgen.

[0006] Das erfindungsgemäße Sicherheitselement zeichnet sich dadurch aus, dass der verborgene Code in die diffraktive Oberflächenstruktur des Sicherheitselements integriert ist. Der verborgene Code ist nur kopierbar, wenn die Oberflächenstruktur des Sicherheitselements abgeformt wird. Das ist jedoch bereits durch eine die diffraktive Oberfläche bedeckende Schutzschicht zu verhindern, die den mechanischen Zugang zu der diffraktiven Oberfläche verschließt. Weiter hat jeder Versuch, das optische Erscheinungsbild der offenen Information oder den verborgenen Code zu ändern, Einfluss auf den verborgenen Code bzw. die offene Information, so dass solche Manipulationsversuche leicht erkannt werden können.

[0007] Weiter ist der eingebrachte Code auch im Dauergebrauch beständig, weil er nicht durch eine durch Beanspruchung ablösbare Substanz, wie eine Druckfarbe oder dergleichen, dargestellt ist. Weitere Vorteile ergeben sich im Fertigungsprozess, der keine zusätzlichen Arbeitsschritte erfordert.

[0008] Weiter ist von Vorteil, dass der verborgene Code in den ersten Bereichs derart integriert ist, dass er auch bei Verwendung vergrößernder optischer Hilfsmittel, wie Lupe oder Mikroskop, nicht zu Tage tritt.

[0009] Das erfindungsgemäße Verfahren sieht einen verborgenen maschinenlesbaren Code vor, der mittels eines Lesegeräts ausgelesen wird. Damit sind die Voraussetzungen geschaffen, um die Verifikation des Sicherheitselements automatisch und mit hoher Zuverlässigkeit vorzunehmen.

[0010] Weitere vorteilhafte Ausbildungen sind in den Unteransprüchen bezeichnet.

[0011] Es kann vorgehen sein, dass die offene, mit einem unbewaffneten Auge sichtbare Information ein offener, optisch maschinenauslesbarer Code ist.

[0012] Weiter kann vorgesehene sein, dass der offene Code und/oder der verborgene Code aus alphanumerischen Zeichen und/oder aus einem Barcode gebildet sind bzw. ist.

Der Barcode kann vorteilhafterweise zur Vereinfachung der maschinellen Überprüfung des offenen Codes vorgesehen sein. Der durch alphanumerische Zeichen dargestellte Code kann beispielsweise vorgesehen sein, um ihn zur Überprüfung manuell in eine Datenbank einzugeben oder um unverschlüsselte Klardaten, wie ein Verfallsdatum, abzulesen.

[0013] In einer vorteilhaften Ausbildung ist vorgese-

hen, dass der offene und/oder verborgene Code ein individualisierter Code sind bzw. ist. Der individualisierte Code kann beispielsweise produktspezifische Daten enthalten, wobei es möglich ist, für jedes Produktexemplar einen spezifischen Code zu vergeben.

[0014] Der offene individualisierte Code, der mit einem Laser eingebracht sein kann, ist vorzugsweise als ein alphanumerischer Code, als ein Barcode oder als eine Kombination aus alphanumerischem Code und Barcode realisiert. Der alphanumerische Code weist vorzugsweise weniger als 20 Zeichen auf, während ein Barcode (insbesondere ein 2D-Barcode) wesentlich mehr Information enthalten kann. Dabei kann der alphanumerische Code ein Teil der durch den Barcode repräsentierten Informationsmenge enthalten. Beispielsweise kann der alphanumerische Code eine Serien- oder eine Dokument-Nummer sein. Der Barcode kann, wenn dieser die Seriennummer eines Produktes enthält, weiter beispielsweise den Produktnamen, Angaben zum Hersteller, Verfallsdatum, Herkunftsland oder Vertriebsland als zusätzliche Informationen enthalten. Der Barcode kann, wenn dieser eine Dokument-Nummer enthält, weiter beispielsweise Landesnamen, Ausstellungsdatum, Ablaufdatum, Name des Besitzers oder Geburtsdatum als zusätzliche Informationen enthalten.

[0015] Die Eingabe des individualisierten Codes kann, wie weiter unten beschrieben, während oder nach der Herstellung des Sicherheitselements erfolgen, d. h. sie kann auch durch den Hersteller des Produkts oder auch bei der Verteilung des Produkts vorgenommen werden. Gleichermaßen können Sicherheitsdokumente mit individualisierten Codes versehen werden, beispielsweise Pässe, Führerscheine oder Identifikationskarten. Auf diese Weise kann zum Beispiel bei Produkten der Weg vom Hersteller bis zum Verbraucher nachvollzogen werden.

[0016] In ähnlicher Weise kann der maschinenlesbare Code im ersten Bereich (Hintergrundbereich) eine Information enthalten, bei der es sich jedoch nicht um eine in Bezug auf das jeweilige Sicherheitselement individualisierte Information handelt. Diese Information ist für alle produzierten oder für eine Gruppe von produzierten Sicherheitselementen gleich. Es kann sich um ein einfaches Logo handeln, es kann sich aber auch um ein einfaches Bild handeln, dass wichtige Informationen über die Kategorie oder das Produkt gibt. Beispielsweise kann es sich um ein Firmenlogo handeln, das mit dem Buchstaben "F" kombiniert ist, wenn das Produkt in Frankreich verkauft wird, und das beispielsweise mit dem Buchstaben "B" kombiniert ist, wenn das Produkt in Brasilien verkauft wird. Die vorstehend genannte im ersten Bereich verborgene Information kann aber auch dazu dienen, Dokumentklassen voneinander zu unterscheiden, beispielsweise indem das Hoheitszeichen eines Landes mit dem Buchstaben "P" für einen Pass oder mit dem Buchstaben "V" für ein Visum kombiniert wird.

[0017] Vorzugsweise sind die Mikrobereiche derart über den ersten Bereich verstreut angeordnet, dass die mittlere Flächenbelegung durch den Mikrobereich im ersten Bereich bezogen auf einen unterhalb des Auflösungsvermögens des menschlichen Auges liegenden Flächenbereich konstant ist, insbesondere bezogen auf einen Flächenbereich von 300 μm x 300 μm konstant ist. Die Mikrobereiche beeinflussen so in keiner Weise das optische Erscheinungsbild der offenen Information und gehen im Rauschen unter.

[0018] Weiter ist bevorzugt, dass die Mikrobereiche eine Flächenausdehnung im Bereich von 10 μm x 10 μm bis 30 μm x 30 μm aufweisen. Die Größenangabe schränkt nicht ein, dass es sich bei den Mikrobereichen um quadratische Mikrobereiche handelt. Vielmehr können die Mikrobereiche einen beliebige Gestalt haben, beispielsweise auch kreisförmig, elliptisch, rhombisch oder rechteckförmig. Der quadratische Mikrobereich kann bevorzugt sein, weil er den Größenbereich vollständig ausfüllt.

[0019] Weiter kann auch ein Mikrobereich, der nur in einer Ausdehnung eine Abmessung kleiner als 300 μm aufweist, in der anderen Ausdehnung aber eine Abmessung größer als 300 μm, zum Beispiel von einigen Millimetern aufweist, vom unbewaffneten Auge nicht getrennt wahrgenommen werden. Es ist somit auch möglich, die Mikrobereiche in einem Raster anzuordnen, dessen Rastweite in einer ersten Richtung kleiner oder gleich 300 μm und in einer zweiten Richtung mehr als 1 mm beträgt. Bei diesem Raster kann es sich auch um ein geometrisch transformiertes Raster handeln. Mehrere, durch ein solches Raster definierte Bereiche sind als Mikrobereiche ausgebildet und bilden so die Anordnung der Mikrobereiche.

[0020] Es kann vorteilhafterweise vorgesehen sein, dass die Mikrobereiche mit einer Reflexionsschicht belegt sind. Auf diese Weise kann ein besonders hoher Kontrast zu dem umgebenden Bereich ausgebildet sein. Die Mikrobereiche können in diesem Fall prinzipiell Oberflächenreliefs aufweisen, wie sie für den ersten Bereich vorgesehen sind, sofern sie sich in mindestens einem Parameter von dem Oberflächenrelief des ersten Bereichs unterscheiden. Es ist möglich, dass die Mikrobereiche eine Gitterstruktur aufweisen, die einfallendes Licht in eine Vorzugsrichtung beugt, lediglich einen bestimmten Spektralbereich in eine Vorzugsrichtung beugt, das einfallende Licht linear polarisiert bzw. in seiner Polarisation ändert, oder dass sie eine Struktur aufweisen, die als Retroreflektor wirkt und das reflektierte Licht in Richtung des einfallendes Lichtes lenkt.

Weiter ist es auch möglich, dass mittels eines Lasers die Reflexionsschicht in den Mikrobereichen partiell entfernt wird und so ein optischer Unterschied zu dem umgebenden Bereich erzielt wird.

[0021] Der verborgene Code wird hierbei von der Anordnung der Mikrobereiche in dem ersten Bereich bestimmt. Nach Erfassung der Anordnung wird eine vordefinierte Transformationsfunktion verwendet, um die Anordnung auf den zugeordneten Codewert abzubilden.

[0022] Es kann weiter vorgesehen sein, dass nicht

mehr als 100 bis 1000 Mikrobereiche/mm^2 in dem ersten Bereich vorgesehen sind. In Abhängigkeit von der Größe der Mikrobereiche kann beispielsweise bei einer Größe von 30 μm x 30 μm die Flächendichte 250 Mikrobereiche/mm^2 betragen, bei einer Größe von 10 μm x 10 μm kann die Flächendicht 1000 Mikrobereiche/mm^2 betragen. Bei zu hoher Flächendichte der Mikrobereiche könnte das optische Erscheinungsbild der offenen Information verfälscht sein, obwohl die einzelnen Mikrobereiche mit dem unbewaffneten menschlichen Auge nicht sichtbar sind und der verborgene Code verborgen bleibt.

[0023] In einer weiteren vorteilhaften Ausbildung ist vorgesehen, dass in dem ersten Bereich ein Hologramm als Oberflächenrelief in die Schicht abgeformt ist, welches

[0024] lediglich bei Bestrahlung mit monochromen kohärenten Licht einer vordefinierten Wellenlänge den verborgenen maschinenlesbaren Code zeigt.

Wenngleich der Aufwand für die Erstellung (computergenerierter) Hologramme und für die Umwandlung des Hologramms in ein Oberflächenrelief vergleichsweise hoch ist, so bietet das Hologramm doch den Vorteil, dass Fehlstellen die abgespeicherte Information nicht zerstören, sondern nur zu einer geringeren Auflösung der Informationsdarstellung führen. Das Holgramm kann entweder ein klassiches Fourier-Hologramm oder ein computergeneriertes Holgramm (Kinoform) sein. Weiter von Vorteil ist, dass das Auslesen der Information nur durch einen kohärenten monochromatischen Lichtstrahl, wie er von Lasern bereitgestellt wird, möglich ist. Der Laserstrahl muss weiter eine vordefinierte Lichtwellenlänge besitzen, um eine effiziente Bilderzeugung zu ermöglichen.

[0025] Weitere vorteilhafte Ausbildungen sind auf die Ausbildung des Oberflächenreliefs des ersten Bereichs gerichtet.

[0026] Es kann vorgesehen sein, dass in dem ersten Bereich eine einheitliche diffraktive Struktur als Oberflächenrelief in die Schicht abgeformt ist.

[0027] Es kann weiter vorgesehen sein, dass in dem ersten Bereich zwei oder mehr diffraktive Strukturen als Oberflächenrelief in die Schicht abgeformt sind, die in Form eines ein- oder zweidimensionalen Musters angeordnet sind. Die diffraktiven Strukturen können sich beispielsweise hinsichtlich ihrer Polarisationseigenschaften und/oder Gitterperiode und/oder Gitterorientierung und/oder Gitterform und/oder Gittertiefe und/oder Gitterprofilform unterscheiden. Entsprechend unterscheidet sich der optisch variable Eindruck, den sie bei der Beleuchtung mit polychromatischem Licht zeigen.

[0028] Weiter ist es möglich, dass in den ersten Bereich eine diffraktive Struktur als Oberflächenrelief in die Schicht abgeformt ist, die mindestens einem kontinuierlich variierenden Parameter aufweist. Beispielsweise kann der Grauwert, der sich bei der Beleuchtung mit polychromatischem Licht einstellt, kontinuierlich zunehmen oder abnehmen. Dabei ist es möglich, dass die kontinuierliche Änderung durch ein eindimensionales Muster von hinreichend viel unterschiedlichen diffraktiven Strukturen erzeugt wird, wobei die Auflösung so hoch sein kann, dass ein unbewaffnetes menschliches Auge keinen stufenweisen Verlauf, sondern einen kontinuierlichen Verlauf wahrnimmt.

[0029] Die offene, mit einem unbewaffneten Auge sichtbare Information kann ein offener, optisch maschinenauslesbarer Code sein.

[0030] Vorteilhafterweise kann vorgesehen sein, dass die Reflexionsschicht als eine metallische Schicht ausgebildet ist. Die metallische Schicht zeigt ein gutes Reflexionsverhalten. Es kann jedoch auch vorgesehen sein, hochbrechende Schichten (HRI-Schichten) zu verwenden. An den Grenzflächen kann die hochbrechende Schicht an Luft oder an eine niedrigbrechende Schicht grenzen. Vorzugsweise ist das Oberflächenrelief mit einer Kleberschicht überzogen mittels der das Sicherheitselement auf ein Substrat appliziert ist.

[0031] Es kann vorgesehen sein, dass die Dicke der Reflexionsschicht im Bereich von 10 nm bis 100 nm ist. In Abhängigkeit von der Schichtdicke und dem Material der Reflexionsschicht kann die Schicht halbtransparent oder transparent ausgebildet sein. Das diffraktive Oberflächenrelief ist vorzugsweise in eine Replizierschicht abgeformt, bei der es sich um eine thermoplastische Kunststofffolie oder um eine UV-härtende Lackschicht handeln kann.

[0032] Es kann vorgesehen sein, dass der offene Code durch eine Lasergravur in den ersten Bereich eingebracht ist, indem die Reflexionsschicht im Bereich des Codes entfernt ist. Vorteilhafterweise wird zum partiellen Entfernen der Reflexionsschicht Lasergravur eingesetzt. Der Kontrast des Codes kann erhöht werden, wenn unter der Replizierschicht eine Farbschicht angeordnet ist, beispielsweise eine schwarze Farbpigmente enthaltende Schicht.

[0033] Es kann vorgesehen sein, der offene Code und/oder der verborgene Code ein individualisierter Code sind bzw. ist.

[0034] Es ist möglich, dass der verborgene Code eine Information zur Verifizierung des Sicherheitselements bereitstellt. Dabei kann vorgesehen sein, dass diese Information verschlüsselt ist, wobei als Verschlüsselungsverfahren ein asymmetrisches Verschlüsselungsverfahren bevorzugt ist, bei dem ein Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel verwendet wird. So ist es möglich, dass der verborgene Code mittels des privaten Schlüssels bei der Individualisierung des Sicherheitselements generiert wird und im Folgenden der öffentliche Schlüssel zur Verifizierung bzw. Auslesung der Information eingesetzt wird. Weiter ist es noch möglich, dass zur Verifizierung bzw. Auslesung der Information der verborgene Code und der offene Code miteinander verknüpft werden, beispielsweise der offene Code/verborgene Code einen öffentlichen Schlüssel zur Entschlüsselung zur Entschlüsselung des verborgenen bzw. offenen Codes darstellt.

[0035] Weiter kann vorgesehen sein, dass das Sicher-

heitselement einen zweiten Bereich aufweist, in dem das Sicherheitselement als optisch variables Element (OVD) ausgebildet ist.

[0036] Weiter kann vorgesehen sein, dass der zweite Bereich anstelle oder zusätzlich zum ersten Bereich einen offenen, mit dem unbewaffneten Auge sichtbaren maschinenlesbaren Code aufweist. Ein OVD kann die Fälschungssicherheit weiter erhöhen und leicht überprüfbare und einprägsame Sicherheitsmerkmale bereitstellen. Beispielsweise kann das OVD beim Kippen zwei oder mehr unterschiedliche Bilder, beispielsweise den Schriftzug "OK" in unterschiedlicher Lage und/oder Farbe und/oder Größe zeigen.

[0037] In einer weiteren vorteilhaften Ausbildung ist vorgesehen, dass in dem zweiten Bereich eine metallische Reflexionsschicht vorgesehen ist, die in Form einer RFID-Antenne ausgeformt ist und die Reflexionsschicht des OVD bildet.

Radiofrequenz-Identifikation kann auch ohne einen RFID-Chip durchgeführt werden,

[0038] indem die RFID-Antenne zu einem Resonanzkreis verschaltet ist und die Resonanzfrequenz der RFID-Antenne überprüft wird. Dazu wird die RFID-Antenne in ein auf die Resonanzfrequenz abgestimmtes elektromagnetisches Feld gebracht, das von einem Lesegerät bereitgestellt werden kann. Die RFID-Antenne kann optisch so maskiert werden, dass sie bei flüchtiger Betrachtung nicht wahrnehmbar ist.

[0039] Weiter ist es möglich, dass das Sicherheitselement einen RFID-Chip aufweist, der Funktionen für die Bereitstellung eines elektronischen Produkt-Codes (EPC) bereitstellt. Der RFID-Chip kann beispielsweise in den Schichtaufbau des zweiten Bereichs integriert sein und vorteilhafterweise als organischer Schaltkreis ausgebildet sein, so dass er in einfacher Weise durch Drucktechniken als Massenprodukt herstellbar ist.

[0040] Es kann vorgesehen sein, dass mit dem weiter oben beschriebenen Verfahren sowohl die offene Information als auch der verborgene Code ausgelesen werden.

[0041] Weiter kann vorgesehen sein, dass die offene Information und/oder der verborgene Code mit einem in einer Datenbank abgelegten Datensatz verglichen werden.

[0042] Moderne Mobiltelefone verfügen über eingebaute digitale Kameras mit einer Auflösung von einigen Millionen Bildpunkten. Eine derartig hohe Auflösung ermöglicht die Verifikation der verborgenen Information durch Nutzung des Mobiltelefons als leicht zugängliches Lesegerät, beispielsweise zur Überprüfung der Echtheit eines Produktes, das mit dem Sicherheitselement versehen ist. Dazu wird ein mit der Kamera des Mobiltelefons aufgenommenes Foto des Sicherheitselements mittels MMS (Multimedia Messaging Service) an einen Datenbankserver übermittelt. Der Datenbankserver wandelt das Foto in einen elektronischen Datensatz und fragt mit diesem Datensatz eine Produktdatenbank ab. Das Ergebnis kann per MMS oder SMS (Short Message Service) an das Mobiltelefon übermittelt werden, so dass innerhalb kurzer Zeit ein Prüfergebnis über die Echtheit des Produkts und/oder spezifische Produktinformationen, die zur Beobachtung des Graumarktes oder für

[0043] Produktverfolgung und Produktüberwachung relevant sind, vorliegt bzw. vorliegen. Im Allgemeinen bestehen unterschiedliche Informations- und Sicherheitsebenen. Ein Sicherheitselement kann beispielsweise neben einem TRUSTSEAL® einen mittels Laserablation eingeschriebenen alphanumerischen Code und einen zweidimensionaler Barcode aufweisen. Zum Ersten wird das TRUSTSEAL®, das in dem oberen Abschnitt des OVD angeordnet ist und beispielsweise den Produktnamen oder den Hersteller angibt, durch den Verbraucher visuell verifiziert. Zum Zweiten kann der alphanumerische Code, der die Seriennummer angibt, zum Beispiel durch Eingabe des Codes in ein Mobiltelefon und Versenden des Codes als SMS-Nachricht an einen Server und durch Rückantwort des Servers in Form einer SMS-Nachricht verifiziert werden. Alternativ kann die Übermittlung an den Server durch ein spezielles Lesegerät oder mittels MMS-Nachricht, die ein digitales Photo des alphanumerischen Codes wie oben beschrieben enthält, vorgesehen sein. Zum Dritten kann der zweidimensionale Barcode, der Informationen wie Seriennummer, Herstellungsdatum, Zielmarkt, Versionsnummer oder Produktspezifikation bereitstellt, vor Ort durch den Markeninhaber ausgelesen werden, um Produktspezifikationen zu erhalten, die mehr Daten als die alphanumerischen Daten umfassen. Zum Vierten kann das Sicherheitselement verborgene Informationen mit hoher Sicherheitsrelevanz enthalten, die ein spezielles Lesegerät oder eine hochauflösende Kamera, die das Bild wie oben beschrieben als MMS-Nachricht an einen Server zur Decodierung sendet, erfordern. Diese geheimen Informationen würden typischerweise den Produktnamen, den Herkunftsort und den Zielmarkt enthalten.

[0044] Es kann weiter vorgesehen sein, dass die offene, mit einem unbewaffneten Auge sichtbare Information ein offener, optisch maschinenauslesbarer individualisierter Code ist und dass der individualisierte Code in der Datenbank gespeichert wird und zur Verifikation des Sicherheitselements die Datenbank abgefragt wird. Wenn es sich bei dem individualisierten Code um einen Barcode handelt, kann die Digitalisierung des Codes entfallen. Wenn es sich um einen alphanumerischen Code handelt, kann ein Texterkennungsverfahren vorgesehen sein, um den individualisierten Code maschinenlesbar zu machen. Vorteilhafterweise können beide vorgenannte Codeausführungen vorgesehen sein.

[0045] Es kann ein Lesegerät zum Auslesen der offenen und verborgenen Informationen aus dem Sicherheitselement vorgesehen sein, das mindestens folgende Komponenten aufweist:

- eine transparente Trägerplatte, auf der das Sicherheitselement auf seiner Frontseite ablegbar ist,
- eine Kamera, die so angeordnet oder ausgerichtet

ist, dass sie die auf der transparenten Trägerplatte aufliegende Frontseite des Sicherheitselements abbildet,

- eine polychromatische nichtkollimierte Lichtquelle, die unterhalb der Trägerplatte angeordnet ist, und
- eine monochromatische kohärente oder semi-kohärente Punktlichtquelle, zum Beispiel eine Laserdiode oder eine LED, wobei die Punktlichtquelle unterhalb der Trägerplatte angeordnet ist und so ausgerichtet ist, dass die optische Achse der Punktlichtquelle in einem Winkel von 45 bis 135°, vorzugsweise in einem Winkel von 85° bis 95° auf den Bereich der Trägerplatte auftrifft, in dem das Sicherheitselement ablegbar ist.

[0046] Als Kamera kann vorteilhafterweise eine elektronische Kamera mit einem Sensorchip vorgesehen sein, wobei die Kamera weiter einen Datenausgang zum Anschluss an einen Computer aufweisen kann.

[0047] Es kann vorgesehen sein, dass die Punktlichtquelle eine Laserdiode oder eine LED ist. Es ist aber auch möglich, dass die Punktlichtquelle aus einer polychromatischen nicht punktförmigen Lichtquelle und einem davor angeordneten Schlitz, d. h. einem sehr schmalen Spalt ausgebildet ist, wobei das aus dem Spalt austretende Licht durch einen Wellenlängenfilter geleitet wird. Da eine solche Lichtquelle sehr lichtschwach sein kann, kann in diesem Falle ein hochempfindlicher Sensorchip vorgesehen sein, um die verborgene Information sichtbar zu machen.

Die Erfindung wird nun anhand von Ausführungsbeispielen näher erläutert. Es zeigen

[0048]

Fig. 1 ein erstes Ausführungsbeispiel eines erfindungsgemäßen Sicherheitselements in der Draufsicht;

Fig. 2 eine schematische Schnittdarstellung des Sicherheitselements in Fig. 1 längs der Schnittlinie II-II;

Fig. 3 ein erstes Ausführungsbeispiel eines Lesegeräts für das Sicherheitselement in Fig. 1;

Fig. 4 ein erstes Ausführungsbeispiel eines Sicherheitsdokuments mit dem Sicherheitselement in Fig. 1;

Fig. 5 eine Anordnung zur Verifikation des Sicherheitsdokuments in Fig. 4;

Fig. 6 ein zweites Ausführungsbeispiel eines Sicherheitsdokuments mit dem Sicherheitselement in Fig. 1;

Fig. 7 eine Anordnung zur Verifikation des Sicherheitsdokuments in Fig. 5;

Fig. 8 ein zweites Ausführungsbeispiel eines erfindungsgemäßen Sicherheitselements in der Draufsicht;

Fig. 9 ein Ausführungsbeispiel eines Sicherheitsdokuments mit dem Sicherheitselement in Fig. 7;

Fig. 10 eine Anordnung zur Verifikation des Sicherheitsdokuments in Fig. 8;

Fig. 11 ein drittes Ausführungsbeispiel eines erfindungsgemäßen Sicherheitselements in schematischer Draufsicht;

Fig. 12a bis 12c weitere Ausführungsbeispiele eines erfindungsgemäßen Sicherheitselements;

Fig. 13 ein zweites Ausführungsbeispiel eines Lesegeräts für das Sicherheitselement in Fig. 1.

[0049] Fig. 1 zeigt ein Sicherheitselement 1, das in einem ersten Bereich 15 ein computergeneriertes Hologramm 16 und alphanumerische Zeichen 17 aufweist. Die alphanumerischen Zeichen 17 sind in dem in Fig. 1 dargestellten Ausführungsbeispiel in zwei Zeilen zu je sechs Zeichen angeordneten und bilden eine zwölfstellige Nummer, d. h. eine sichtbare Information. Die sichtbare, in Form eines alphanumerischen Codes dargestellte Information ist mit unbewaffnetem Auge lesbar. Bei Information kann es sich beispielsweise um eine individualisierte Information handeln. Anstatt der alphanumerischen Zeichen kann auch ein Barcode vorgesehen sein, oder es können sowohl die alphanumerischen Zeichen als auch der Barcode vorgesehen sein. Der Barcode kann insbesondere vorgesehen sein, um das maschinelle Auslesen der individualisierten Information zu erleichtern. Der Barcode kann entweder als eindimensionaler oder als zweidimensionaler Barcode ausgebildet sein. Der Barcode kann mehr Informationen enthalten, als in dem alphanumerischen Code enthalten sind oder er kann die gleichen Informationen bereitstellen, die der alphanumerische Code bereitstellt.

[0050] In das computergenerierte Hologramm 16 ist eine verborgene Information eingeschrieben, die bei Beleuchtung mit "weißem" Licht und Betrachtung mit unbewaffnetem Auge nicht wahrnehmbar ist. Bei der verborgenen Information kann es sich zum Beispiel wie bei der vorstehend beschriebenen sichtbaren Information um alphanumerische Zeichen und/oder um einen Barcode und/oder um ein Logo handeln. Typischerweise kann das computergenerierte Hologramm ein sehr einfach ausge-

führtes Logo und/oder eine Anzahl von alphanumerischen Zeichen enthalten, beispielsweise ein Firmenlogo und einen Ländercode. Der Ländercode kann beispielsweise zur Unterscheidung von Zielmärkten mit unterschiedlichem Preisniveau vorgesehen sein. Das Hologramm 16 erscheint einem Betrachter als eine Mattfläche, die einen Hintergrund für die alphanumerischen Zeichen 17 bildet. Der erste Bereich 15 bildet also einen diffraktiven Sicherheitsbereich, der die Fälschungssicherheit des Sicherheitselements 1 gegenüber Sicherheitselementen erhöht, bei denen im Hintergrundbereich der individualisierten Information zwar die Fälschung erschwerende diffraktive Strukturen vorgesehen sind, jedoch keine verborgene Information eingeschrieben ist.

[0051] In einen zweiten Bereich 18 des Sicherheitselements 1 ist ein Kippbild abgeformt, das bei unterschiedlichem Kippwinkel des Sicherheitselements 1 unterschiedliche Bilder zeigt, beispielsweise die Zeichenfolge "OK" in unterschiedlichen Positionen und/oder Farben und/oder Formen. Ein solches Sicherheitsmerkmal ist leicht erkennbar und auffällig.

[0052] Fig. 2 zeigt nun eine unmaßstäbliche Schnittdarstellung des Sicherheitselements 1 längs der Schnittlinie II-II in Fig. 1.

[0053] Das Sicherheitselement 1 ist als ein Mehrschichtkörper ausgebildet, der als oberste Schicht eine Schutzschicht 21 aufweist, die eine Replizierschicht 22 überbedeckt. Die Replizierschicht 22 kann eine Dicke von 2 bis 20 μm aufweisen und aus einem thermoplastischen Kunststoff oder einem UV-härtbaren Lack gebildet sein. In die von der Schutzschicht 21 abgewandte Oberfläche der Replizierschicht 22 sind Oberflächenprofile abgeformt, die von einer metallischen Schicht 23 bedeckt sind, die als Reflexionsschicht wirkt. Die metallische Schicht 23 kann beispielsweise durch Sputtern oder Bedampfen aufgebracht sein, eine Schichtdicke im Bereich von 15 bis 50 nm aufweisen und aus Aluminium, Gold, Kupfer oder dergleichen gut reflektierendem Metall oder Metalllegierung bestehen. Die metallische Schicht 23 ist in Abschnitten 25 beispielsweise durch Laserabtrag der metallischen Schicht zwecks Gravur der alphanumerischen Zeichen 17 unterbrochen. Laserablation ist das typische Verfahren zum Einschreiben der alphanumerischen Zeichen 17. Die Zeichen können im Herstellerbetrieb oder auch später eingeschrieben werden. Sofern die alphanumerischen Zeichen 17 im Herstellerbetrieb eingeschrieben werden, kann dies bevor das Sicherheitselement komplett erzeugt ist oder danach geschehen. Das Einschreiben kann zu jedem nach der Metallisation folgenden Herstellungsschritt vorgesehen sein. Die metallische Schicht 23 ist an ihrer von der Replizierschicht abgewandten Seite von einer Kleberschicht 24 bedeckt. Wenn das Einschreiben nach dem Aufbringen der Kleberschicht 24 vorgesehen ist, dann ist die Laserleistung so gewählt, dass nur die metallische Schicht 23 abgetragen wird, indem sie von dem Laserstrahl verdampft wird und kleine Konglomerate an den Rändern der freigelegten Bereiche der metallischen Schicht 23 bildet. In der Tat

[0054] können die alphanumerischen Zeichen 17 auch nachdem das Sicherheitselement 1 auf einem Produkt oder auf einem Dokument angebracht ist, durch Laserablation eingeschrieben werden. Beispielsweise kann das Sicherheitselement 1 auf ein Visum platziert werden und sodann kann mit einem Laser die Nummer des Visums in das Sicherheitselement eingeschrieben werden.

[0055] Anstelle der metallischen Schicht 23 kann beispielsweise auch eine Schicht aus einem Material mit hohem Brechungsindex (HRI-Schicht), eine kombinierte HRI-Metall-Schicht, eine dielektrische Dünnschicht oder eine Flüssigkristallschicht vorgesehen sein.

[0056] Bei der Kleberschicht 24 kann es sich beispielsweise um eine Heißkleberschicht handeln, so dass das Sicherheitselement 1 auf ein Sicherheitsdokument, wie eine Identifikationskarte, einen Ausweis oder eine Kreditkarte applizierbar ist. Bei dem in Fig. 1 dargestellten Sicherheitselement handelt es sich um die Transferlage einer Transferfolie, insbesondere einer Heißprägefolie, welche weiter eine Trägerschicht und eine optionale Ablöseschicht zwischen Trägerschicht und Schutzschicht aufweist. Es ist weiter auch möglich, dass das Sicherheitselement 1 eine Laminierfolie ist, die beispielsweise anstelle der Schutzschicht 21 eine Trägerfolie, beispielsweise eine 12 bis 42 μm dicke PET-Folie aufweist.

[0057] Im ersten Bereich 15 ist das Oberflächenprofil der Replizierschicht 22 aus miteinander verschachtelten diffraktiven Gittern ausgebildet, deren Gitterparameter, insbesondere Azimutwinkel, Spatialfrequenz und Profilform sich unterscheiden und die das einfallende Licht in unterschiedliche Richtungen ablenken, so dass jeweils nur eines der Gitter Licht in das Auge des Betrachters ablenkt. Wegen der Wellenlängenabhängigkeit der Diffraktion können durch Wahl der Spatialfrequenz einzelne Lichtfarben ausgeblendet werden, sofern das Sicherheitselement 1 mit polychromatischem Licht, wie zum Beispiel Tageslicht, beleuchtet wird. So können beispielsweise rote und grüne Bilder durch Kippen des Sicherheitselements 1 nacheinander erzeugt werden. Weiter ist auch die Verwendung von Beugungsstrukturen Nullter Ordnung möglich, bei denen die Gitterperiode unterhalb

[0058] der Wellenlänge des sichtbaren Lichtes liegt, so dass durch die Ausgestaltung des Gitters die Polarisation des rückgebeugten Lichtes beeinflusst werden kann.

[0059] Im zweiten Bereich 18 ist das Oberflächenprofil mit einem großen Tiefen-zu-Breiten-Verhältnis der Erhebungen bzw. Vertiefungen ausgebildet. Wegen des großen Tiefen-zu-Breiten-Verhältnisses, das vorteilhafterweise im Bereich von 1 bis 5 gewählt ist, kommt es zu Mehrfachreflexionen des einfallenden Lichtes, das auf diese Weise zerstreut wird und den optischen Eindruck einer dunklen matten Fläche hervorruft.

[0060] Die in dem Hologramm 16 verborgene Information kann durch kohärentes monochromatisches Licht sichtbar gemacht werden, beispielsweise durch Be-

leuchtung des Hologramms mit einem roten Laserstrahl. Weil sich ein Hologramm dadurch auszeichnet, dass Unterbrechungen lediglich die Auflösung der gespeicherten Information verringern, ist das durch den Laserstrahl erzeugte holographische Bild nicht durch die alphanumerischen Zeichen 17 überlagert. Bei der in dem Hologramm 16 gespeicherten verborgenen Information kann es sich vorzugsweise um alphanumerische Zeichen und/oder um einen Barcode handeln. Es ist jedoch auch möglich, dass es sich um ein graphisches Objekt oder dergleichen handelt, wie beispielsweise ein Firmenlogo. Zur verbesserten maschinellen Identifizierung können auch einfache geometrische Objekte, wie Kreise oder Dreiecke, vorgesehen sein.

[0061] Fig. 3 zeigt nun ein Lesegerät 3 zum Auslesen der in dem Sicherheitselement gespeicherten Informationen. Das Sicherheitselement 1 ist auf ein Sicherheitsdokument 4 appliziert, wie weiter oben beschrieben. Das Lesegerät 3 trägt an seiner Oberseite eine dicke Glasplatte 31, auf deren Oberseite ein Projektionsschirm 32 angeordnet ist. Der Projektionsschirm 32 ist auf seiner der Oberseite der Glasplatte 31 zugewandten Unterseite weiß gefärbt. Es kann auch vorgesehen sein, dass der Projektionsschirm 32 durch einen weißen Farbaufdruck oder durch einen in die Oberfläche der Glasplatte 3 eingebrachten Mattglasbereich gebildet ist.

[0062] Weiter ist in dem Lesegerät 3 ein Laser 33 so angeordnet, dass der aus dem Laser 33 austretende kohärente Lichtstrahl schräg auf die Unterseite der Glasplatte 31 trifft, in der Glasplatte 31 zum Einfallslot hin gebrochen wird, an dem in dem ersten Bereich 15 (siehe Fig. 1 und 2) des Sicherheitselements 1 angeordneten Hologramm 16 reflektiert wird, an der Unterseite der Glasplatte 31 reflektiert wird und sodann auf den Projektionsschirm 32 trifft und dort die in dem Hologramm 16 verborgene Information darstellt. Vorteilhafterweise kann vorgesehen sein, dass der Bildstrahl unter Totalreflexion auf den Projektionsschirm 32 trifft, wozu beispielsweise zur Einkopplung des Lichtstrahls in die Glasplatte 31 eine spezielle Einkoppelstruktur vorgesehen sein kann.

[0063] Weiter ist in dem Lesegerät 3 eine polychromatische bzw. Weißlicht-Quelle angeordnet, die das Sicherheitselement 1 beleuchtet, wodurch die in den ersten Bereich eingeschriebenen alphanumerischen Zeichen 17 sichtbar sind.

[0064] Zur Auswertung der auf dem Projektionsschirm 32 und auf dem ersten Bereich 15 des Sicherheitselements 1 dargestellten Information ist eine Kamera 35 vorgesehen. Bei der Kamera 35 kann es sich vorteilhafterweise um eine sogenannte digitale Kamera mit einem digitalen Bildsensor handeln, die einen Signalausgang zum Anschluss an einen Signaleingang eines Computers aufweist. Auf diese Weise kann im einfachsten Fall das von der Kamera 35 empfangene Bild auf einem Computermonitor dargestellt und manuell ausgewertet werden. Es ist vorteilhaft, wenn der zweidimensionale Bildsensor den Projektionsschirm 32 als auch die auf dem Sicherheitselement 1 eingetragenen alphanumerischen Zeichen 17 (s. Fig. 1) simultan abbildet.

[0065] Fig. 4 zeigt nun das Sicherheitsdokument 4 in Fig. 3 in der Draufsicht. Es handelt sich bei dem in Fig. 4 dargestellten Sicherheitsdokument 4 um eine Identifikationskarte, die neben dem Sicherheitselement 1 ein Passbild 41 der Inhaberin, lesbare individualisierte Daten 42 (Name, Vorname, Geburtsdatum) der Inhaberin und eine Unterschrift 43 der Inhaberin aufweist.

[0066] Die in dem Sicherheitselement 4 gespeicherten Informationen können in einer Datenbank hinterlegt sein, die bei der Prüfung des Sicherheitsdokuments 4 abgefragt wird.

[0067] Fig. 5 zeigt beispielhaft eine für die vorgenannte Prüfung geeignete Vorrichtung. Die Kamera 35 des Lesegeräts 3 ist mit einem lokalen Computer 51 verbunden, der mit einer Texterkennungssoftware ausgerüstet ist. Texterkennungssoftware ist auch als OCR-Software bekannt.

[0068] Der Computer 51 ist über ein Netzwerk 52, bei dem es sich in dem in Fig. 5 dargestellten Ausführungsbeispiel um das Internet handelt, mit einem Datenbankserver 53 verbunden. In einer auf dem Datenbankserver 53 eingerichteten Datenbank sind die zur Verifizierung der in dem Sicherheitselement 1 gespeicherten Information benötigten Daten gespeichert. Es ist vorteilhafterweise vorgesehen, dass zwischen dem Computer 51 und dem Datenbankserver 53 eine sichere Verbindung ausgebildet ist, beispielsweise eine verschlüsselte Verbindung. Der Computer 51 ist mit einem Computerarbeitsplatz 54 verbunden, über den die Steuerung des Lesegeräts 3 sowie die Bedienung des Computers 51 möglich ist.

[0069] Fig. 6 zeigt nun ein Sicherheitsdokument 6, das wie das in Fig. 4 dargestellte Sicherheitsdokument 4 ausgebildet ist, jedoch zusätzlich zu dem Sicherheitselement 1, dem Passbild 41, den lesbaren individualisierten Daten 42 und der Unterschrift 43 einen Speicherchip 61 aufweist, in dem Daten zur Verifikation des Sicherheitsdokuments 6 oder der Inhaberin des Sicherheitsdokuments abgelegt sein können, beispielsweise biometrische Daten der Inhaberin. Anstatt des Speicherchips 61 kann auch ein RFID-Tag (Baugruppe zur Radiofrequenz-Identifikation) vorgesehen sein, der gegenüber dem Speicherchip 61 den Vorteil aufweisen kann, dass er drahtlos abfragbar ist.

[0070] Fig. 7 zeigt nun ein Lesegerät 7, das sich von dem in Fig. 3 und 5 dargestellten Lesegerät 3 dadurch unterscheidet, dass es zusätzlich ein Chip-Lesegerät 71 zum Auslesen der in dem Speicher-Chip 61 des Sicherheitsdokuments 6 gespeicherten

[0071] Information aufweist. Sowohl das Chip-Lesegerät 71 als auch die Kamera 35 sind mit dem Computer 51 verbunden, der wie weiter oben beschrieben, mit dem Computerarbeitsplatz 54 verbunden ist.

[0072] Fig. 8 zeigt nun ein Sicherheitselement 8, das einen ersten Bereich 81, der als diffraktiver Sicherheitsbereich, d. h. als ein Sicherheitsbereich mit einem dif-

fraktiven Oberflächenrelief, ausgebildet ist, und einen zweiten Bereich 82 aufweist, der als ein OVD ausgebildet ist, dessen Kontur als RFID-Antenne für ein RFID-Tag geformt ist.

[0073] Die RFID-Antenne ist durch ein Lesegerät detektierbar, das die Resonanzfrequenz der RFID-Antenne ermittelt, wie weiter unten beschrieben. Ein RFID-Chip ist in diesem Ausführungsbeispiel nicht benötigt.

[0074] Der erste Bereich 81 ist wie der Bereich 15 in Fig. 1 ausgebildet, d. h. er stellt sowohl eine offene Information als auch eine verborgene Information bereit, die durch ein Lesegerät auslesbar ist.

[0075] Fig. 9 zeigt nun ein Sicherheitsdokument 9, das sich von dem in Fig. 4 dargestellten Sicherheitsdokument im Wesentlichen durch die Art des Sicherheitselements unterscheidet. Bei dem Sicherheitsdokument 9 handelt es sich um eine Identifikationskarte, die neben dem Passbild 41 der Inhaberin, den lesbaren individualisierten Daten 42 (Name, Vorname, Geburtsdatum) der Inhaberin und der Unterschrift 43 der Inhaberin das Sicherheitselement 8 in Fig. 8 aufweist.

[0076] Fig. 10 zeigt ein Lesegerät 10, das sich von dem in Fig. 3 und 5 dargestellten Lesegerät 3 dadurch unterscheidet, dass es zusätzlich ein RFID-Lesegerät 101 zur Bestimmung der Resonanzfrequenz der RFID-Antenne des Sicherheitselements 8 aufweist. Sofern die RFID-Antenne des Sicherheitselements 8 nicht die Sollfrequenz aufweist, wird das Sicherheitsdokument 9 nicht akzeptiert.

[0077] Sowohl das RFID-Lesegerät 101 als auch die Kamera 35 sind mit dem Computer 51 verbunden, der wie weiter oben in Fig. 5 beschrieben, über das Netzwerk 52 mit dem Datenbankserver 53 verbunden ist. Weiter ist der Computerarbeitsplatz 54 zur Ein-

[0078] und Ausgabe von Daten vorgesehen, beispielsweise zum Auslösen des Lesevorgangs, zur Datenbankabfrage oder dergleichen. Bei dem Netzwerk 52 kann es sich beispielsweise um das Internet, wie weiter oben beschrieben, oder um ein Firmennetzwerk handeln, wobei unter "Firmennetzwerk" auch das Netzwerk einer Verwaltung oder Behörde verstanden wird.

[0079] Fig. 11 zeigt nun ein drittes Ausführungsbeispiel eines erfindungsgemäßen Sicherheitselements. Ein Sicherheitselement 11 weist einen ersten Bereich 111 auf, der ein diffraktiver Sicherheitsbereich ist und einen als OVD ausgebildeten zweiten Bereich 115. Der zweite Bereich 115 ist in dem in Fig. 11 dargestellten Ausführungsbeispiel vorgesehen, um in einprägsamer und werbewirksamer Form darauf hinzuweisen, dass es sich bei dem mit dem Sicherheitselement 11 markierten Produkt um ein Originalprodukt handelt. Der zweite Bereich 115 kann beispielsweise neben dem Hinweis, dass es sich um ein Originalprodukt handelt, ein Firmenlogo und eine Produktbezeichnung aufweisen. Entsprechend den vielfältigen Gestaltungsmöglichkeiten, die ein OVD bietet, können beispielsweise beim Kippen des Sicherheitselements Farbeffekte, unterschiedliche Bilder oder unterschiedliche Bildgrößen sowie Bewegungseffekte gezeigt werden.

[0080] Der erste Bereich 111 weist einen Hintergrund 113 mit diffraktivem Oberflächenrelief auf, in den alphanumerische Zeichen 112 eingebracht sind, die eine offene Information ausgeben. Es kann sich dabei vorzugsweise um eine individualisierte Information handeln, die nur einmal vergeben ist, beispielsweise um eine Produktverfolgung vom Verbraucher über Einzelhändler und Großhändler bis zum Hersteller zu ermöglichen. Bei dem Hintergrund 113 kann es sich beispielsweise um ein Kreuzgitter, eine Mattstruktur oder dergleichen handeln.

[0081] In dem Hintergrund 113 sind Mikrobereiche 114 mit diffraktivem Oberflächenrelief vorgesehen, die mit einem unbewaffneten Auge nicht wahrnehmbar sind. Es kann sich beispielsweise um spiegelnde Mikrobereiche in den Abmessungen 10 μm x 10 μm handeln.

[0082] In der Darstellung in Fig. 11 sind die Mikrobereiche 114 sehr stark vergrößert wiedergegeben. Es können beispielsweise in einer Grundversion 4096 Pixelstellen in einer Fläche von 50 mm x 50 mm vorgesehen sein, um 2 Zeichen oder 4096 ID-Nummern zu speichern. Eine erweiterte Version kann 10 Zeichen oder ID-Nummern zwischen 1 und 4 Milliarden speichern. In einer weiteren Version sind bis zu 1 Milliarde Codes in einer Fläche von 17 mm x 17 mm speicherbar.

[0083] Zur sicheren Auslesbarkeit der verborgenen Information kann ein guter Kontrast zwischen den Mikrobereichen 114 und dem Hintergrund 113 vorteilhaft sein.

[0084] In einem ersten vorteilhaften Ausführungsbeispiel wurden spiegelnde Mikrobereiche 114 auf einem Hintergrund 113 mit isotroper Mattstruktur angeordnet.

[0085] In einem zweiten vorteilhaften Ausführungsbeispiel wurden spiegelnde Mikrobereiche 114 auf einem Hintergrund angeordnet, der als isotrope Mattstruktur kombiniert mit einem Kreuzgitter mit einer Spatialfrequenz von 1050 Linien/mm ausgebildet ist.

[0086] Es kann weiter vorgesehen sein, dass die verborgene Information verschlüsselt ist, so dass zum Auslesen der Information zusätzlich ein Schlüssel erforderlich ist, der nur dem Hersteller oder dem Besitzer des Produkts bekannt ist.

[0087] Moderne Mobiltelefone verfügen über eingebaute digitale Kameras mit einer Auflösung von einigen Millionen Bildpunkten. Eine derartig hohe Auflösung ermöglicht die Verifikation der verborgenen Information durch ein beispielsweise von einem Verbraucher, Vertreiber oder einem Überwachungsorgan mit der Kamera des Mobiltelefons aufgenommenes Foto, das mittels MMS an einen Datenbankserver übermittelbar ist. Der Datenbankserver kann das Foto in einen elektronischen Datensatz wandeln und mit einer Produktdatenbank vergleichen. Das Ergebnis kann per MMS oder SMS an das Mobiltelefon übermittelt werden, so dass innerhalb kurzer Zeit ein Prüfergebnis über die Echtheit des Produkts und/oder spezifische Produktinformationen, die zur Beobachtung des Graumarktes oder für Produktverfolgung und Produktüberwachung relevant sind, vorliegt bzw. vorliegen.

[0088] Die Kamera des Mobiltelefons erzeugt zugleich ein Bild der alphanumerischen Zeichen 112 sowie der Mikrobereiche 114, wobei die alphanumerischen Zeichen 112 individualisierte Informationen über das Produkt oder Dokument und die Mikrobereiche 114 Informationen über die Produkt- oder Dokumentklasse geben können.

[0089] Die Fig. 12a bis 12c zeigen Sicherheitselemente 12a bis 12c, die sich hinsichtlich der Ausbildung des Hintergrunds unterscheiden. Die Sicherheitselemente 12a bis 12c weisen alphanumerische Zeichen 124 auf, die durch Laserablation in einen Hintergrundbereich 121 eingebracht sind. Im Bereich der alphanumerischen Zeichen 124 ist der Hintergrundbereich 121 abgetragen.

[0090] Der Hintergrundbereich 121 weist einen kontinuierlich veränderbaren optischen Effekt auf, beispielsweise einen Helligkeitsverlauf mit kontinuierlich sinkenden oder ansteigenden Grauwerten. In dem in Fig. 12a dargestellten Ausführungsbeispiel ist der Helligkeitsverlauf in Längsrichtung des Sicherheitselements 12a vorgesehen, also parallel zur Anordnung der alphanumerischen Zeichen 124.

[0091] Das Sicherheitselement 12b in Fig. 12b weist einen Hintergrundbereich auf, der aus zwei nebeneinander angeordneten Hintergrundbereichen 122 und 123 gebildet ist. Die Hintergrundbereiche 122 und 123 bilden ein eindimensionales Muster. Die Hintergrundbereiche 122 und 123 weisen Oberflächenreliefs mit unterschiedlichen diffraktiven Strukturen auf, die sich in mindestens einem Parameter voneinander unterscheiden. Beispielsweise können sich die Hintergrundbereiche 122 und 123 unterscheiden hinsichtlich

- Polarisationseigenschaft
- Gitterperiode
- Gitterorientierung
- Gitterform
- Gittertiefe
- Gitterprofilform
- Ausbildung des diffraktiven Oberflächenreliefs

[0092] Es kann vorgesehen sein, dass der optische Eindruck der beiden Hintergrundbereiche gleich ist, so dass die unterschiedliche Ausbildung der Hintergrundbereiche bei Betrachtung mit unbewaffnetem Auge nicht erkennbar ist. Es kann weiter vorgesehen sein, dass mehr als zwei unterschiedliche Hintergrundbereiche den Hintergrund des Sicherheitselements 12b bilden. Bei genügend feiner Untergliederung kann das Sicherheitselement 12b den optischen Eindruck des Sicherheitselements 12a (Fig. 12a) vermitteln.

[0093] Fig. 12c zeigt nun das Sicherheitselement 12c, das einen Hintergrund mit einem zweidimensionalen Muster aufweist. In dem in Fig. 12c dargestellten Ausführungsbeispiel ist das Sicherheitselement 12c als ein quadratisches Sicherheitselement ausgebildet mit den zwei Hintergrundbereichen 122 und 123. Der Hintergrundbereich 122 bildet ein in der oberen linken Ecke des quadratischen Hintergrunds angeordnetes Quadrat mit halber Kantenlänge des Hintergrunds sowie einen davon beabstandeten senkrecht angeordneten Streifen, der sich von der oberen Kante bis zu der unteren Kante des Hintergrunds erstreckt.

[0094] Die verborgene Information kann in die Sicherheitselemente 12a bis 12c vorteilhafterweise analog zu dem in Fig. 11 dargestellten Ausführungsbeispiel eingeschrieben sein. Es ist aber auch möglich, dass eine oder mehrere der Hintergrundbereiche 121 bis 123 als computergeneriertes Hologramm ausgebildet sind, wie weiter oben in Fig. 1 beschrieben.

[0095] Die Eigenschaften der Lichtquelle des Lesegerätes können für eine Echtheitskontrolle kontrolliert und variiert werden. Zum Beispiel können zwei Lichtquellen vorgesehen sein, wobei

- die Polarisation der Lichtquellen unterschiedlich ist, oder
- die Position und damit der Einfallswinkel der Lichtquellen unterschiedlich ist, oder
- die Wellenlänge der Lichtquellen unterschiedlich ist.

[0096] Durch Anfertigung von zwei Bildern, die jeweils mit einer der beiden Lichtquellen aufgenommen sind, kann man die Echtheit des Sicherheitselementes prüfen.

[0097] Fig. 13 zeigt ein zweites Ausführungsbeispiel eines Lesegeräts zum Auslesen der in dem Sicherheitselement 1 in Fig. 1 gespeicherten Informationen. Das Sicherheitselement 1 ist auf ein Sicherheitsdokument 4 appliziert, wie weiter oben beschrieben.

[0098] Ein Lesegerät 13 ist wie das weiter oben in Fig. 3 beschriebene Lesegerät 3 aufgebaut, mit dem Unterschied, dass es sich bei der Glasplatte 31, auf der das Sicherheitsdokument 4 ablegbar ist, um eine dünne Glasplatte handelt, und dass kein Projektionsschirm auf der Oberseite der Glasplatte 31 angeordnet ist.
Weiter ist in dem Lesegerät 13 kein Laser zur Erzeugung eines kohärenten Lichtstrahls vorgesehen, sondern eine monochromatische kohärente Punktlichtquelle 133, die ein Strahlenbündel 134 zur Beleuchtung des Sicherheitselements 1 aussendet. Die Punktlichtquelle 133 ist parallel zur optischen Achse der Kamera 35 angeordnet, wobei der Abstand der Punktlichtqelle 133 zur optischen Achse der Kamera 35 so gering wie möglich gewählt ist. Idealerweise fällt die Strahlachse der Punktlichtquelle 133 mit der optischen Achse der Kamera 35 zusammen. Die optische Achse der Punktlichtquelle 133 trifft in einem Winkel von 45° bis 135°, vorzugsweise in einem Winkel von 85° bis 95° auf den Bereich der Glasplatte 31 auf, in dem das Sicherheitselement 1 ablegbar ist.

[0099] Als Punktlichtquelle 133 kann beispielsweise eine Laserdiode oder eine LED vorgesehen sein, die monochromatisches kohärentes Licht abstrahlt. Kohärenz bezeichnet in der Physik eine Eigenschaft von Wellen, die zeitlich und räumlich unveränderliche Interferenzerscheinungen ermöglicht. Wird nicht-kohärentes Licht

durch einen sehr schmalen Spalt gesendet, verhält sich das austretende Licht, als sei der Spalt eine Punktlichtquelle, die kohärentes Licht aussendet. Dabei nimmt mit zunehmendem Abstand zur Lichtquelle die räumliche Kohärenz zu. Durch einen Wellenlängenfilter kann die zeitliche Kohärenz erhöht werden. Das auf das Sicherheitselement 1 auftreffende kohärente Strahlenbündel 134 macht nun die in dem Sicherheitselement 1 verborgene Information sichtbar, wobei durch den Ersatz des Lasers 33 durch die Punktlichtquelle 133 einige wesentliche Verbesserungen gegenüber dem in Fig. 3 beschriebenen Lesegerät 3 erreicht sind:

- Kostenreduzierung,
- einfacher und kompakter Aufbau des Lesegeräts;
- hohe Unempfindlichkeit gegenüber Lagetoleranzen der die verborgene Information enthaltenden Bereiche des Sicherheitselements 1.

[0100] Eine vergleichbare Erhöhung der Unempfindlichkeit gegen Lagetoleranzen wäre nur durch die Verwendung von mehr als einem Laser 33 in Fig. 3 erzielbar bzw. durch eine zusätzliche Vorrichtung zur zeilenweisen Ablenkung des Laserstrahls.

[0101] Die Punktlichtquelle 133 weist zwar eine gegenüber dem Laser 33 verringerte Kohärenz auf, aber es hat sich gezeigt, dass eine hohe Kohärenz nicht notwendig ist, wenngleich mit höherer Kohärenz die Sichtbarkeit der verborgenen Information steigt. Die verborgene Information wird bei Beleuchtung mit der Punktlichtquelle 133 typischerweise mit einem Regenbogeneffekt dargestellt.

[0102] Als Punktlichtquelle 133 wurde beispielsweise eine Laserdiode von 1 mW Leistung und einer Wellenlänge von 635 nm ohne Kollimations-Optik verwendet. Das von der Laserdiode ausgesendete Strahlenbündel 134 hatte einen Öffnungswinkel von 34°. Ebenso wurde eine LED als Punktlichtquelle 133 eingesetzt.

[0103] Die in dem Lesegerät 13 angeordnete polychromatische bzw. Weißlicht-Quelle 34 kann wie in Fig. 3 weiter oben beschrieben ausgebildet sein. Sie ist als breitbandige, nicht kollimierte Lichtquelle ausgebildet und kann beispielsweise auch durch eine größere Anzahl weißer oder farbiger LEDs oder eine Elektrolumineszenzplatte gebildet sein.

Patentansprüche

1. Sicherheitselement zur Erhöhung der Fälschungssicherheit eines Sicherheitsdokuments, insbesondere eines Ausweises, eines Passes oder einer Identifikationskarte,
   dadurch gekennzeichnet,
   dass das Sicherheitselement (1, 8, 11) einen ersten Bereich (15, 81, 111) aufweist, in dem zumindest bereichsweise in einer Schicht des Sicherheitselements (1, 8, 11) ein zumindest bereichsweise mit einer Reflexionsschicht versehenes diffraktives Oberflächenrelief abgeformt ist, welches eine offene, mit einem unbewaffneten Auge sichtbare Information zeigt, und dass der erste Bereich weiter einen verborgenen, mit dem unbewaffneten Auge nicht sichtbaren, optisch auslesbaren maschinenlesbaren Code aufweist, der aus einer Anordnung von in dem ersten Bereich (15, 81, 111) angeordneten und sich von dem umgebenden Bereich optisch unterscheidenden Mikrobereichen (114) gebildet ist, in denen ein sich von dem umgebenden Bereich unterscheidendes Oberflächenrelief abgeformt ist und/oder die Reflexionsschicht entfernt ist, und/oder der maschinenlesbare Code von dem in die Schicht abgeformten Oberflächenrelief generiert ist.

2. Sicherheitselement nach Anspruch 1,
   dadurch gekennzeichnet,
   dass der verborgene Code ein mittels eines Lasers individualisierter Code ist.

3. Sicherheitselement nach Anspruch 1 oder 2,
   dadurch gekennzeichnet,
   dass die von den Mikrobereichen (114) belegte Fläche in dem ersten Bereich bezogen auf jeden Flächenbereich von 300 μm x 300 μm konstant ist.

4. Sicherheitselement nach einem der vorangehenden Ansprüche,
   dadurch gekennzeichnet,
   dass die Mikrobereiche (114) eine Flächenausdehnung im Bereich von 10 μm x 10 μm bis 30 μm x 30 μm aufweisen.

5. Sicherheitselement nach einem der vorangehenden Ansprüche,
   dadurch gekennzeichnet,
   dass nicht mehr als 100 bis 1000 Mikrobereiche/mm^2 in dem ersten Bereich vorgesehen sind.

6. Sicherheitselement nach einem der vorangehenden Ansprüche,
   dadurch gekennzeichnet,
   dass der verborgene Code durch die Anordnung der Mikrobereiche (114) bestimmt ist.

7. Sicherheitselement nach einem der vorangehenden Ansprüche,
   dadurch gekennzeichnet,
   dass in dem ersten Bereich (15, 81) ein Hologramm als Oberflächenrelief in die Schicht abgeformt ist, welches lediglich bei Bestrahlung mit monochromen kohärenten Licht einer vordefinierten Wellenlänge den verborgenen maschinenlesbaren Code zeigt.

8. Sicherheitselement nach Anspruch 7,
   dadurch gekennzeichnet,
   dass das Hologramm bei Beleuchtung mit polychro-

matischem Licht als Mattstruktur erscheint.

9. Sicherheitselement nach einem der Ansprüche 1 bis 8,
dadurch gekennzeichnet,
dass in dem ersten Bereich zwei oder mehr unterschiedliche diffraktive Strukturen als Oberflächenrelief in die Schicht abgeformt sind.

10. Sicherheitselement nach einem der Ansprüche 14 bis 17,
dadurch gekennzeichnet,
dass der offene Code durch eine Lasergravur in den ersten Bereich (15, 81, 111) eingebracht ist, indem die Reflexionsschicht im Bereich des Codes entfernt ist.

11. Verfahren zur Erhöhung der Fälschungssicherheit eines Sicherheitsdokuments, insbesondere eines Ausweises, eines Passes oder einer Identifikationskarte,
dadurch gekennzeichnet,
dass ein Sicherheitselement (1, 8, 11) bereitgestellt wird, das einen ersten Bereich (15, 81, 111) aufweist, in dem zumindest bereichsweise in eine Schicht des Sicherheitselements (1, 8, 11) ein zumindest bereichsweise mit einer Reflexionsschicht versehenes diffraktives Oberflächenrelief abgeformt ist, welches eine offene, mit einem unbewaffneten Auge sichtbare Information zeigt, wobei der erste Bereich weiter einen verborgenen, mit dem unbewaffneten Auge nicht sichtbaren, optisch auslesbaren maschinenlesbaren Code aufweist, der aus einer Anordnung von in dem ersten Bereich (15, 81, 111) angeordneten und von dem umgebenden Bereich sich optisch unterscheidenden Mikrobereichen (114) gebildet ist, in denen ein sich von dem umgebenden Bereich unterscheidendes Oberflächenrelief abgeformt ist und/oder die Reflexionsschicht entfernt ist, und/oder der maschinenlesbare Code von dem in die Schicht abgeformten Oberflächenrelief generiert ist, und dass der verborgene maschinenlesbare Code mit einem Lesegerät zur Verifikation des Sicherheitselements ausgelesen wird.

12. Verfahren nach Anspruch 11,
dadurch gekennzeichnet,
dass weiter auch die offene Information mittels des Lesegeräts ausgelesen wird, wobei die offene, mit einem unbewaffneten Auge sichtbare Information ein offener, optisch maschinenauslesbarer individualisierter Code ist.

13. Verfahren nach Anspruch 11 oder 12,
dadurch gekennzeichnet,
dass die offene Information und/oder der verborgene Code mit einem in einer Datenbank abgelegten Datensatz verglichen werden.

14. Verfahren nach Anspruch 13,
dadurch gekennzeichnet,
dass der offene Code und/oder der verborgene Code bei der Individualisierung des Sicherheitselements (1, 8, 11) als individualisierter Code generiert wird, in den ersten Bereich des Sicherheitselements (1, 8, 11) eingeschrieben wird, und dass der individualisierte Code in der Datenbank gespeichert wird und zur Verifikation des Sicherheitselements (1, 8, 11) die Datenbank abgefragt wird.

15. Lesegerät zur Durchführung des Verfahrens nach einem der Ansprüche 11 bis 14,
dadurch gekennzeichnet,
dass das Lesegerät (13) mindestens folgende Komponenten aufweist:

- eine transparente Trägerplatte (31), auf der das Sicherheitselement (1, 8, 11) auf seiner Frontseite ablegbar ist,
- eine Kamera (35), die so angeordnet und ausgerichtet ist, dass sie die auf der transparenten Trägerplatte (31) aufliegende Frontseite des Sicherheitselements (1, 8, 11) abbildet,
- eine polychromatische nichtkollimierte Lichtquelle (34), die unterhalb der Trägerplatte (31) angeordnet ist, und
- eine monochromatische kohärente oder semikohärente Punktlichtquelle (133), wobei die Punktlichtquelle unterhalb der Trägerplatte (31) angeordnet ist und so ausgerichtet ist, dass die optische Achse der Punktlichtquelle in einem Winkel von 45° bis 135°, vorzugsweise in einem Winkel von 85° bis 95° auf den Bereich der Trägerplatte (31) auftrifft, in dem das Sicherheitselement (1, 8, 11) ablegbar ist.

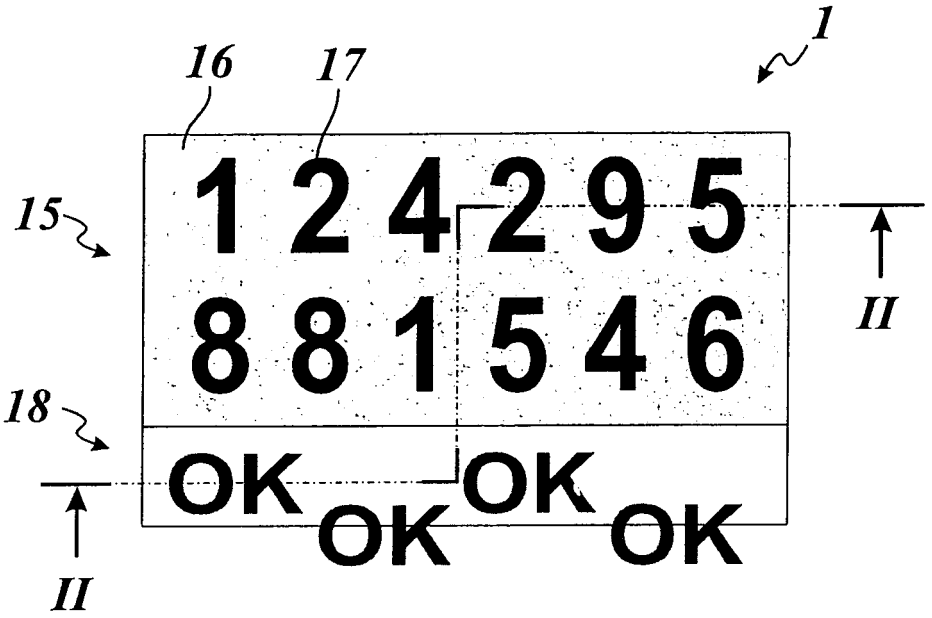

Fig. 1

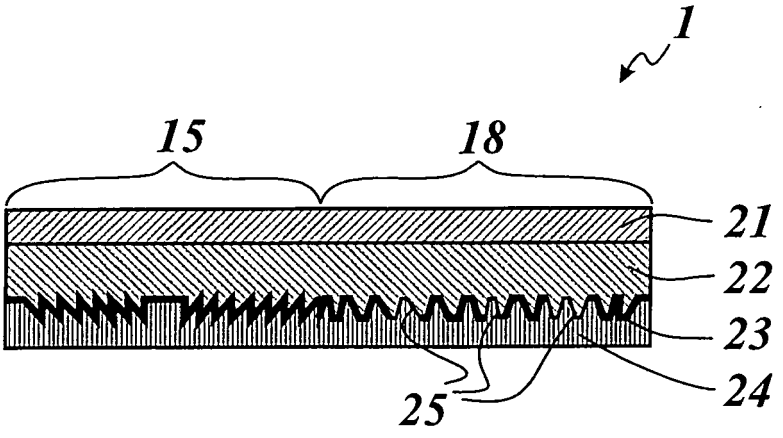

Fig. 2

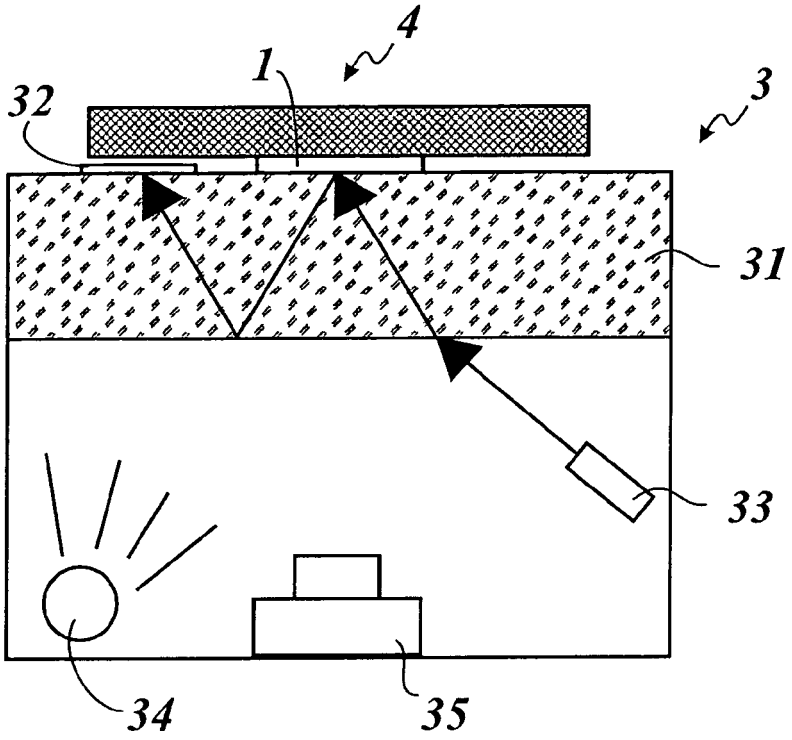
4
1
32
3
31
33
34
35

Fig. 3

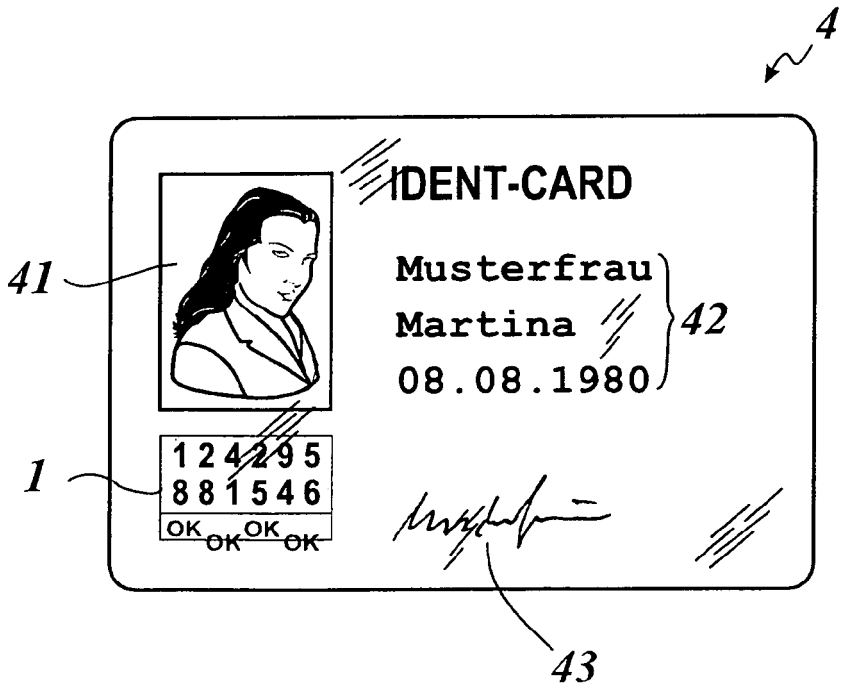
4
IDENT-CARD
41
Musterfrau
Martina
08.08.1980
42
1
124295
881546
OK OK OK
43

Fig. 4

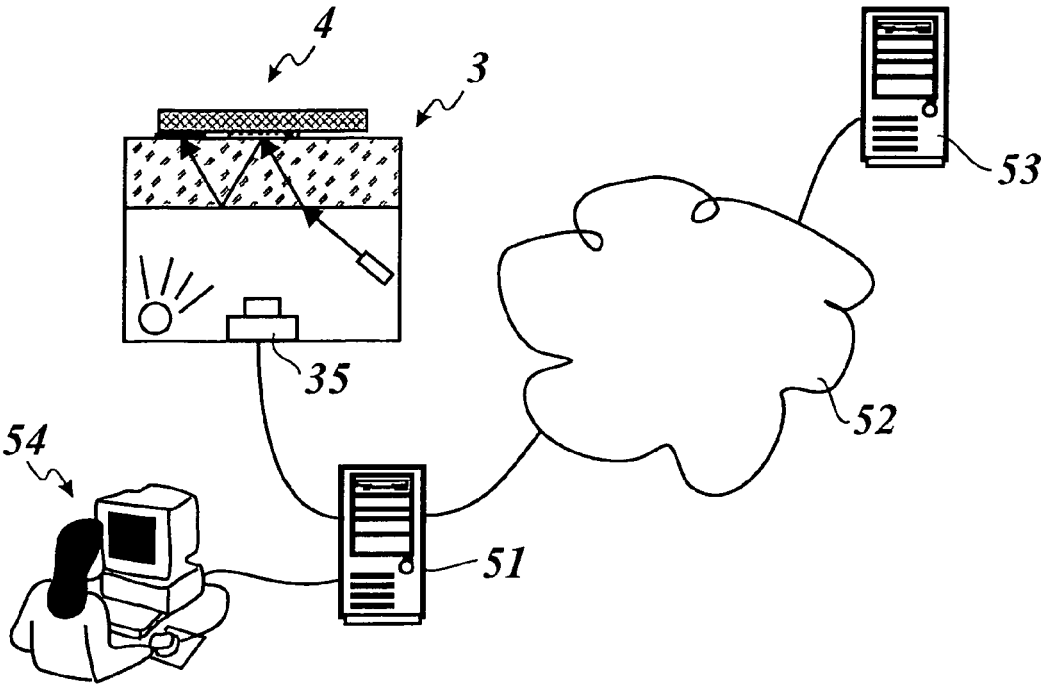
4
3
53
35
52
54
51

Fig. 5

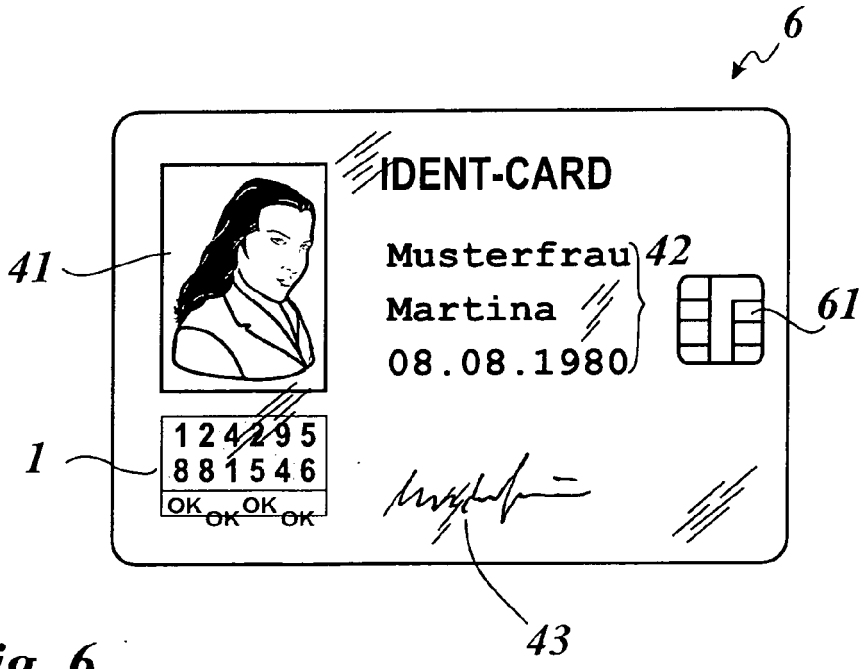
6
IDENT-CARD
41
Musterfrau
Martina
08.08.1980
42
61
1
124295
881546
OK OK OK
43

Fig. 6

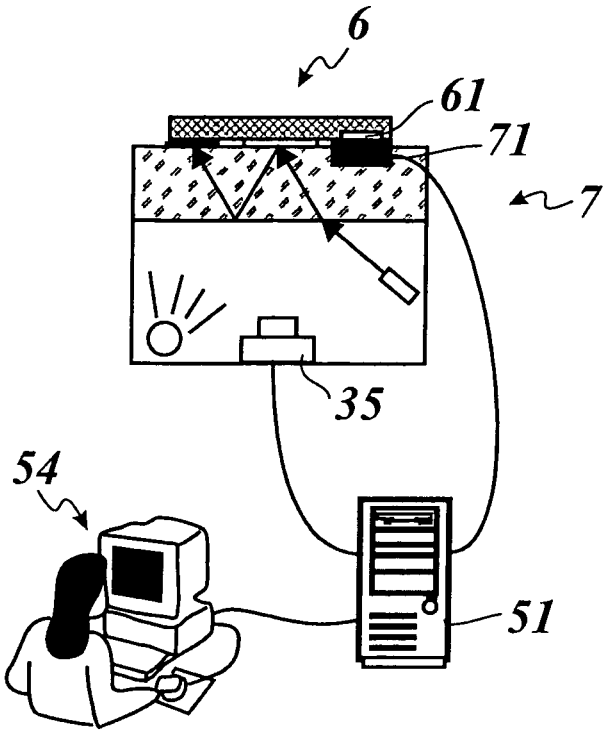

Fig. 7

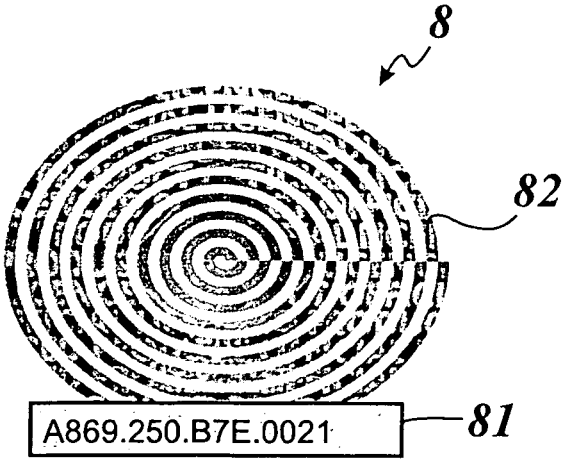

Fig. 8

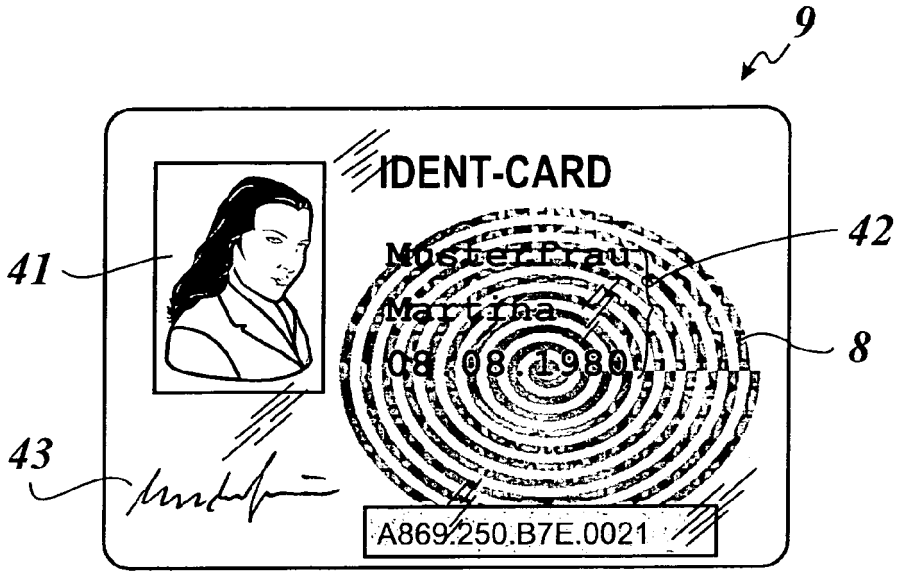
9
IDENT-CARD
Musterfrau
Martina
08 08 1980
A869.250.B7E.0021
41
42
8
43

Fig. 9

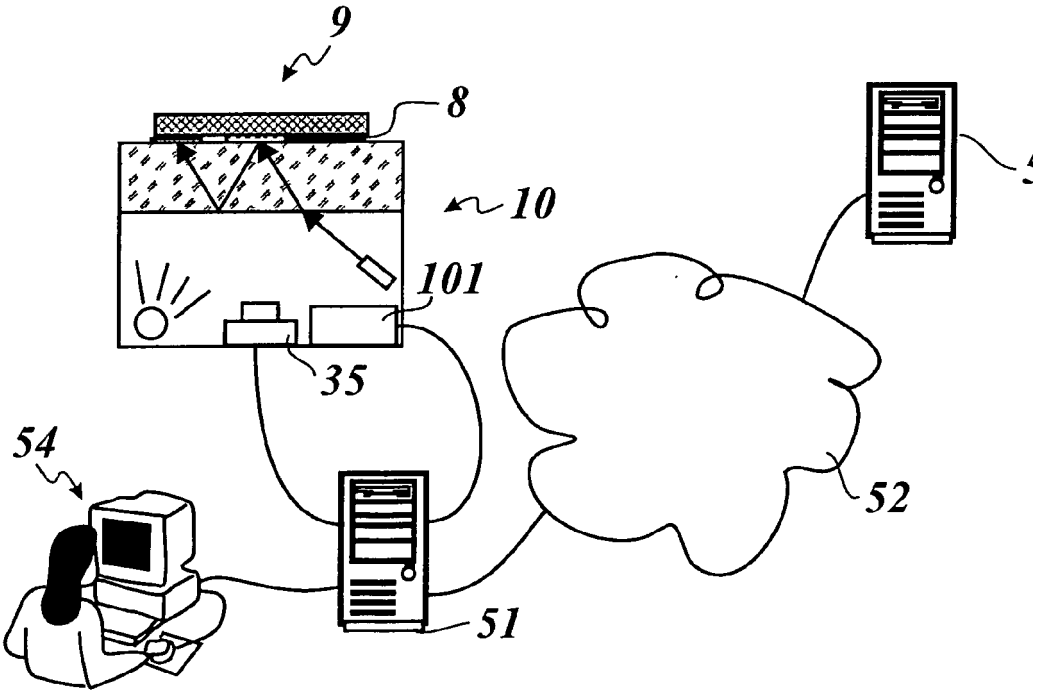
9
8
10
101
35
54
52
51

Fig. 10

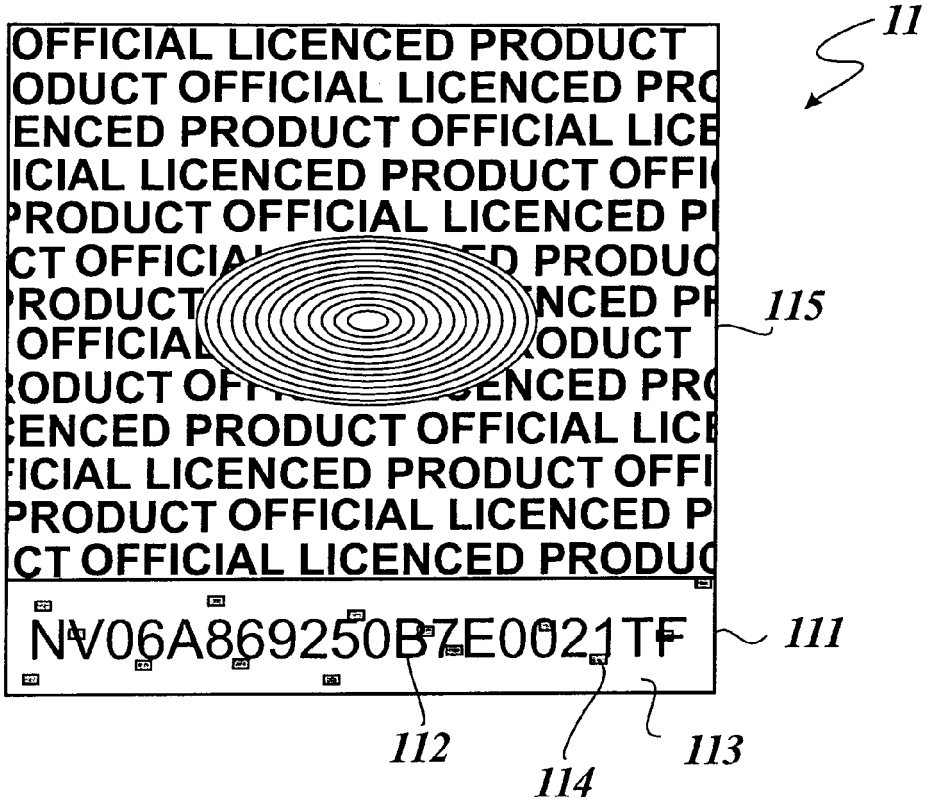

Fig. 11

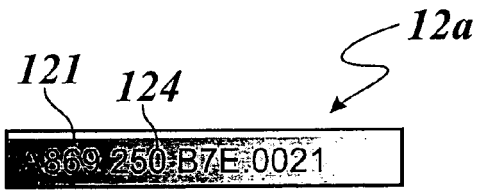

Fig. 12a

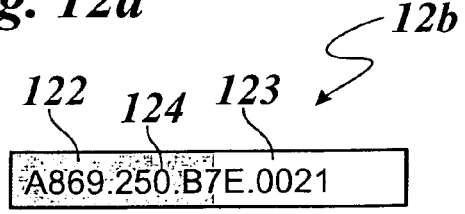

Fig. 12b

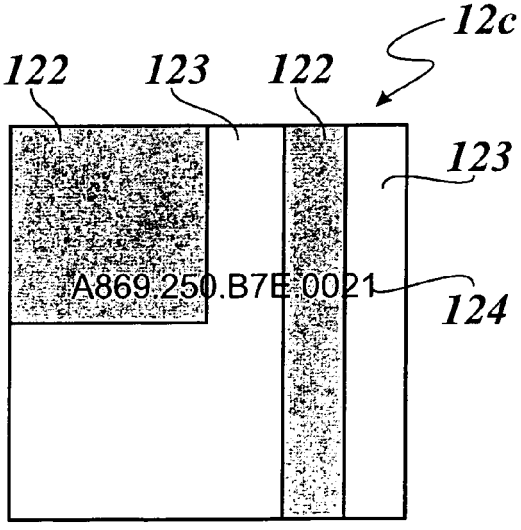

Fig. 12c