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

(11) **EP 4 389 445 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
26.06.2024 Patentblatt 2024/26

(21) Anmeldenummer: **23218840.9**

(22) Anmeldetag: **20.12.2023**

(51) Internationale Patentklassifikation (IPC):
B42D 25/328 *(2014.01)* ***B42D 25/41*** *(2014.01)*

(52) Gemeinsame Patentklassifikation (CPC):
B42D 25/328; B42D 25/41

(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 ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA
Benannte Validierungsstaaten:
KH MA MD TN

(30) Priorität: **20.12.2022 DE 102022214091**

(71) Anmelder: **Bundesdruckerei GmbH**
10969 Berlin (DE)

(72) Erfinder:
- **Tries, Alexander**
  10553 Berlin (DE)
- **Kunath, Christian**
  12203 Berlin (DE)
- **Gahlbeck, Jeffry**
  15517 Fürstenwalde (DE)
- **Sprenger, Martin**
  10317 Berlin (DE)
- **Klünder, Kathrin**
  10179 Berlin (DE)

(74) Vertreter: **Patentanwälte Bressel und Partner mbB**
Potsdamer Platz 10
10785 Berlin (DE)

(54) **SICHERHEITSELEMENT MIT ABSICHERNDEM HOLOGRAFISCHEN SICHERHEITSMERKMAL**

(57) Die Erfindung betrifft ein Sicherheitselement (1) umfassend einen Datenträger (5) mit einem erfassbaren ersten Sicherheitsmerkmal (310), in welchem eine erste Information gespeichert ist, und der Datenträger (5) eine Speicherschicht (511) umfasst, in der mindestens ein zweites erfassbares Sicherheitsmerkmal (320) holografisch gespeichert ist, wobei das zweite Sicherheitsmerkmal (320) eine zweite Information speichert, die aus der ersten Information ableitbar ist, wobei die zweite Information ein maschinenlesbares Muster (250) ist. Die Erfindung betrifft ferner ein Verfahren zur Herstellung eines solchen Sicherheitselements (1), ein Verifikationsverfahren und eine Verifikationsvorrichtung (1300).

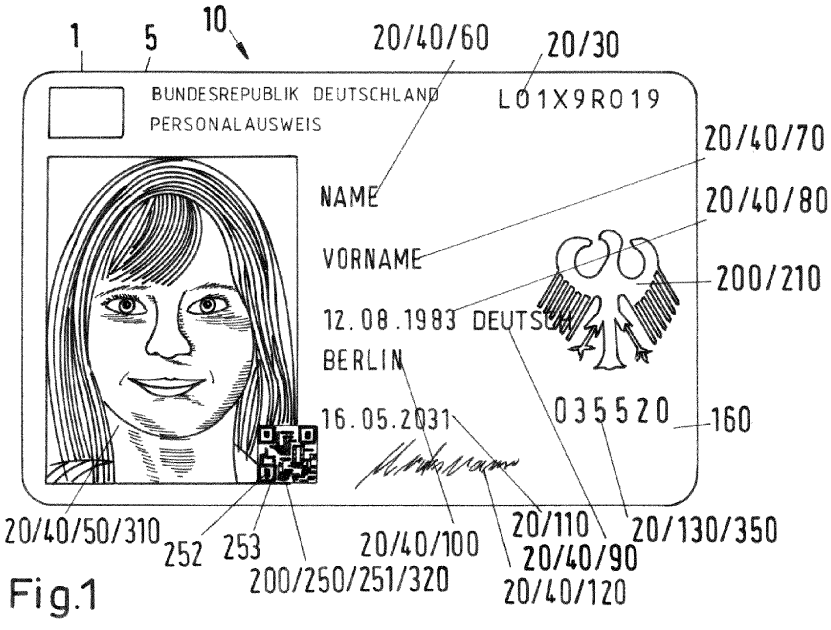

Fig.1

EP 4 389 445 A1

Beschreibung

[0001] Die Erfindung betrifft ein Sicherheitselement mit einem Hologramm, welches in dem Sicherheitselement gespeicherte Informationen gegenüber einer Fälschung absichert.

[0002] Darüber hinaus betrifft die Erfindung ein Verifikationsverfahren sowie eine Verifikationsvorrichtung sowie ein Herstellungsverfahren.

[0003] Sicherheitselemente sind körperliche Gegenstände, die mindestens ein Sicherheitsmerkmal aufweisen, welches das Sicherheitselement gegen Nachahmungen, Verfälschungen, Manipulationen und Ähnliches sichern soll. Sicherheitselemente können beispielsweise Führerscheine, Reisepässe, Visa, Identitätskarten, Banknoten, Bankkarten, Kreditkarten oder Ähnliches sein. Darüber hinaus sind Sicherheitselemente auch solche körperlichen Bestandteile, die beispielsweise in die erstgenannten Sicherheitselemente eingefügt werden. Ein Sicherheitselement kann somit ein Sicherheitsfaden, ein Patch, ein Laminationskörper, eine Hologrammfolie oder Ähnliches sein.

[0004] Bei Sicherheitselementen wie beispielsweise Ausweisen besteht ein großes Interesse daran, dass darin gespeicherte Informationen gegenüber Manipulationen und Fälschungen abgesichert werden. Dies gilt insbesondere für Informationen, die als individualisierende oder personalisierende Informationen bezeichnet werden. Individualisierend sind Informationen, die das entsprechende Sicherheitselement gegenüber anderen gleichartigen Sicherheitselementen individualisieren. Als personalisierend gelten solche individualisierenden Informationen, wenn sie einer Person zuordenbar sind, der das Sicherheitselement selbst zugeordnet ist. Bei einem Personalausweis oder Reisepass sind dies beispielsweise die Angaben, die zu der Person gehören, für die der Reisepass oder der Personalausweis ausgestellt sind.

[0005] Aus dem Stand der Technik ist es bekannt, dass Hologramme als Sicherheitsmerkmale einen erhöhten Fälschungs- oder Manipulationsaufwand erforderlich machen. Daher werden Hologramme bereits seit längerer Zeit als Sicherheitsmerkmale in Sicherheitselementen eingesetzt. Als Hologramm wird hier die Speicherung von Informationen in Strukturen bezeichnet, deren charakteristische Größe und/oder Abstände im Bereich der Wellenlänge von Licht liegen. Hierbei wird als Licht nicht nur das sichtbare Licht, sondern auch elektromagnetische Strahlung der angrenzenden Wellenlängenbereiche wie dem infraroten Wellenlängenbereich und dem UV-Wellenlängenbereich aufgefasst.

[0006] Hologramme lassen sich grundsätzlich nach unterschiedlichen Kriterien klassifizieren. Eine wesentliche Unterscheidung ist die in dicke und dünne Hologramme. Während bei dünnen Hologrammen die Schicht, in der die holografischen Informationen gespeichert sind, in der Größenordnung der Wellenlänge liegt, mit der das Hologramm rekonstruiert werden kann, ist bei dicken Hologrammen der Volumenbereich, in dem die holografischen Informationen gespeichert sind, deutlich größer als die Wellenlänge, mit der das Hologramm rekonstruiert werden kann. Dicke Hologramme werden daher auch als Volumenhologramme bezeichnet.

[0007] Volumenhologramme zeichnen sich beispielsweise dadurch aus, dass sie eine hohe Winkelselektivität und Wellenlängenselektivität bezüglich der Rekonstruktion zeigen. Dies bedeutet, dass die Richtung, aus der das Rekonstruktionslicht für die Rekonstruktion eingestrahlt werden muss, und dessen Wellenlänge stark eingegrenzt bzw. genau festgelegt sind. Bei dünnen Hologrammen gilt dies nicht. Dünne Hologramme sind beispielsweise als Oberflächenprägehologramme bekannt, die häufig verspiegelt sind und beispielsweise in derzeit gängig verwendeten Kreditkarten als Sicherheitsmerkmal enthalten sind.

[0008] Um den Vorteil des verbesserten Schutzes gegen Fälschungen eines Hologramms auszunutzen und hierüber auch Informationen, die mit anderen Verfahren und/oder auf andere Weise in einem Sicherheitselement gespeichert sind, schützen und absichern zu können, ist es bekannt, diese andere Information in dem Hologramm wieder aufzunehmen. Beispielsweise ist in deutschen Personaldokumenten wie beispielsweise Personalausweisen und Reisepässen ein gedrucktes, häufig sogar farbig gedrucktes Portraitbild enthalten und zusätzlich überlagert eine holografische Speicherschicht, in der eine in Graustufen codierte Kopie des Portraitbildes gespeichert ist. Diese Kopie ist beispielsweise bei einem Lichteinfall von Licht einer geeigneten Wellenlänge, im Fall deutscher Personaldokumente im grünen Wellenlängenbereich, das unter 45° auf das Sicherheitsdokument auftrifft, unter 90° zur Oberfläche erfassbar. Die Winkel der Einstrahlung des Rekonstruktionslichts und der Erfassungs- oder Beobachtungsrichtung werden als Rekonstruktionsgeometrie bezeichnet. Zusammen mit den Angaben über die verwendete oder verwendeten Lichtwellenlängen werden diese als Rekonstruktionsbedingungen oder Rekonstruktionsbedingung bezeichnet. Zusätzlich sind in dem Hologramm deutscher Personaldokumente weitere Informationen in alphanumerischen Zeichen codiert, die ebenfalls mittels Druck und/oder Lasergravur, d.h. einer dauerhaften Materialveränderung aufgrund von Laserstrahlung, in dem Personaldokument ein zweites Mal, d.h. redundant, gespeichert sind.

[0009] Für die Herstellung eines in der Serienfertigung individuellen Volumenreflexionshologramms wird bei einigen Ausführungsformen im Stand der Technik ein Master verwendet, wie er beispielsweise in der EP 0 896 260 A2 beschrieben ist. Dort ist eine Vorrichtung zur Herstellung von Volumenhologrammen aus einem Masterhologramm einer Mattscheibe beschrieben, die mit einer oder mehreren Wellenlängen und einem oder mehreren Referenzwinkeln aufgenommen ist. Mit dem Masterhologramm der Mattscheibe können stereoskopische und farbige individuelle Hologramme im Kontaktkopierverfahren hergestellt werden. Die beschriebene Vorrichtung

besitzt eine Strahlungsquelle für Laserstrahlung, zum Bestrahlen eines Masterhologramms und eines Films. Damit Hologramme die verschiedenen Informationen beinhalten, auf einfache Weise hergestellt werden können, ist eine Modulationseinrichtung ein sogenannter räumlicher Lichtmodulator (englisch SLM - Spatial Light Modulator), insbesondere ein Flüssigkristalldisplay (LCD) oder ein LCoS (Liquid Crystal on Silicon) vorhanden, um die kohärente Laserstrahlung zu modulieren.

[0010] Sicherheitselemente in Form von Ausweisdokumenten wie Reisepässen und Personalausweisen werden genutzt, um die Identität von Personen feststellen und überprüfen zu können. Neuerdings wird die Überprüfung häufig über elektronische Medien ausgeführt. Dieses wird beispielsweise als Videoidentverfahren bezeichnet. In einem Videoanruf, wo neben Tondaten auch Videodaten übertragen werden, wird die Identität einer Person überprüft. Hierbei werden Bilddaten des Reisepasses oder Personalausweises zu einer Institution oder Person übertragen, die die Identität einer Person bestätigen sollen. Eine Reihe von Sicherheitsmerkmalen, beispielsweise taktile Sicherheitsmerkmale, aber auch betrachtungsrichtungs- oder erfassungsrichtungsabhängige Sicherheitsmerkmale können bei solchen Verfahren gar nicht oder nur schwer überprüft werden. Für Hologramme ergibt sich die Schwierigkeit, dass diese, sofern sie flächig ausgebildet sind, häufig bei der Bilddatenerfassung nicht vollflächig zeitgleich erfasst und so übertragen werden können, dass diese, insbesondere bei einem flächig ausgebildeten Portraitbild, mit dem daneben oder teilüberlagerten Portraitbild verglichen werden können.

[0011] Der Erfindung liegt somit die Aufgabe zugrunde, ein Sicherheitselement zu schaffen, welches eine gute oder verbesserte Absicherung von einfach im Sicherheitsdokument zu erfassenden Informationen ermöglicht und zugleich einfach zu verifizieren ist.

[0012] Die Erfindung wird durch ein Sicherheitselement mit den Merkmalen des Patentanspruchs 1, ein Verfahren zum Herstellen des Sicherheitselements nach Anspruch 10, eine Verifikationsvorrichtung für ein Sicherheitselement nach Anspruch 15, ein Verfahren zum Verifizieren des Sicherheitselements nach Anspruch 16 sowie Computerprogramme nach Ansprüchen 17 gelöst. Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen.

[0013] Der Erfindung liegt die Idee zugrunde, die absichernde Information in der Weise zu codieren und in dem Sicherheitshologramm zu speichern, dass diese einfach und zuverlässig maschinell auswertbar ist. Hierbei wird mindestens eine Information, die auf andere Weise in dem Sicherheitselement gespeichert ist, in codierter Form als Hologramm in dem Sicherheitselement gespeichert. Bei der Verifikation wird die erste Information und die codierte zweite Information zunächst extrahiert und für ein Vergleichen in der Weise aufbereitet, dass entweder die erste Information so codiert wird, wie es bei der Herstellung für die zweite Information der Fall war und die codierte erste Information mit der extrahierten zweiten Information verglichen wird oder alternativ die zweite Information decodiert wird und die decodierte zweite Information mit der ersten Information verglichen wird. Wird eine Gleichheit bei einem der beiden alternativen Verfahren festgestellt, so wird das entsprechende Sicherheitselement als echt gekennzeichnet. Ist hingegen eine Ungleichheit festgestellt, so wird das Sicherheitselement als unecht gekennzeichnet. Das Verifikationsergebnis kann dann verwendet werden, um beispielsweise weitere technische Vorgänge, wie beispielsweise eine Zugangssteuerung automatisch auszulösen.

Definitionen

[0014] Als Codieren oder Codierung wird hier das Übersetzen einer Information in eine andere Darstellung verstanden. Darüber hinaus kann ein Codieren auch ein Verschlüsseln der Information umfassen. Als Verschlüsseln wird eine Transformation bezeichnet, bei der eine Information in eine zweite Information unter Ausnutzung einer weiteren Information, welche als Schlüssel bezeichnet wird, überführt wird und die Transformation und Rücktransformation nur mit Kenntnis einer weiteren Information, d.h. des Schlüssels, möglich ist.

Bevorzugte Ausführungsformen

[0015] Insbesondere wird durch die Erfindung ein Sicherheitselement geschaffen, umfassend einen Datenträger mit einem erfassbaren ersten Sicherheitsmerkmal, in welchem eine erste Information gespeichert ist, und wobei der Datenträger eine Speicherschicht umfasst, in der mindestens ein zweites erfassbares Sicherheitsmerkmal holografisch gespeichert ist, wobei das zweite Sicherheitsmerkmal eine zweite Information speichert, die aus der ersten Information ableitbar ist, wobei die zweite Information ein maschinenlesbares Muster ist.

[0016] Ferner schafft die Erfindung ein Verfahren zum Herstellen eines Sicherheitselements, welches die Schritte umfasst:

Empfangen einer ersten Information;
Codieren der ersten Information, um als Ergebnis der Codierung eine zweite Information zu erhalten;
Bereitstellen oder Herstellen eines Datenträgers, der zumindest eine holografische Speicherschicht umfasst,
holografisches Speichern der zweiten Information in der Speicherschicht mittels eines zweiten Sicherheitsmerkmals als maschinenlesbares Muster und Speichern der ersten Information in dem Datenträger mittels eines ersten Sicherheitsmerkmals.

[0017] Ebenso wird ein Verfahren zur Verifikation geschaffen, welches die Verfahrensschritte umfasst:

Empfangen digitaler Bilddaten des Sicherheitsele-

ments;

Extrahieren einer ersten Information aus einem ersten Teil der digitalen Bilddaten, die das erste Sicherheitsmerkmal abbilden, und Extrahieren der zweiten Information aus einem zweiten Teil der Bilddaten, die das zweite Sicherheitsmerkmal abbilden, Ausführen eines Codierschrittes zum Erzeugen eines Codierergebnisses, wobei entweder die erste Information codiert wird, so dass das Ergebnisergebnis die Codierung der ersten Information ist oder die zweite Information decodiert wird, so dass das Codierergebnis die Decodierung der zweiten Information ist,

Ermitteln eines Vergleichsergebnisses, wobei das Codierergebnis mit der zweiten Information vergleichen wird und deren Gleichheit oder Ungleichheit angibt, wenn das Codierergebnis die Codierung der ersten Information ist, oder das Codierergebnis mit der ersten Information vergleichen wird und deren Gleichheit oder Ungleichheit angibt, wenn das Codierergebnis die Decodierung der zweiten Information ist, und Ausgeben eines Verifikationsergebnisses, wobei das Verifikationsergebnis das Sicherheitselement als echt kennzeichnet, wenn das Vergleichsergebnis eine Gleichheit angibt und als nicht echt kennzeichnet, wenn das Vergleichsergebnis eine Ungleichheit angibt.

[0018] Darüber hinaus wird eine Verifikationsvorrichtung geschaffen, die umfasst:

eine Extraktionseinheit, welche ausgebildet ist, Bilddaten des Sicherheitselements zu empfangen und die erste Information aus dem ersten Sicherheitsmerkmal und eine zweite Information aus dem zweiten Sicherheitsmerkmal zu extrahieren;

eine Codiereinheit zum Erzeugen eines Codierergebnisses, wobei das Codierergebnis entweder die Codierung der ersten Information ist oder die Decodierung der zweiten Information ist;

eine Vergleichereinheit zum Erzeugen eines Vergleichsergebnisses, wobei die Vergleichereinheit ausgebildet ist, das Codierergebnis mit der zweiten Information zu vergleichen, wenn das Codierergebnis die Codierung der ersten Information ist, oder das Codierergebnis mit der ersten Information zu vergleichen, wenn das Codierergebnis die Decodierung der zweiten Information ist; und eine Verifikationseinheit zum Ausgebgen eines Verifikationsergebnisses, wobei das Verifikationsergebnis das Sicherheitselement als echt kennzeichnet, wenn das Vergleichsergebnis eine Gleichheit angibt, und als nicht echt kennzeichnet, wenn das Vergleichsergebnis eine Ungleichheit angibt.

[0019] Ferner wird ein Computerprogramm mit Programmcode zur Durchführung aller Verfahrensschritte des Verifikationsverfahrens geschaffen, wenn das Computerprogramm in einem Computer ausgeführt wird.

[0020] Ferner wird ein Computerprogramm mit Programmcode, der auf einem maschinenlesbaren Datenträger gespeichert ist, zur Durchführung des Verifikationsverfahrens geschaffen, wenn der Programmcode in einem Computer ausgeführt wird.

[0021] Die verschiedenen Ausgestaltungen der Erfindung bieten alle den Vorteil, dass über die Codierung der ersten Information mit einer zweiten Information verknüpft ist, welche ein maschinenlesbarer Code ist, was die Erfassung mittels Bilddaten deutlich verbessert.

[0022] Als maschinenlesbarer Code wird eine Codierung angesehen, die speziell für die Erfassung durch eine maschinelle Einrichtung ausgebildet ist. Hierunter sind Codes zu verstehen, die so ausgebildet sind, dass sie Abbildungsfehler wie Verzerrungen und/oder Abbildungsfehler in Form von Teilbeschädigungen oder Ähnlichem erkennbar und korrigierbar machen. Insbesondere fallen hierunter als eindimensionale Codes bezeichnete Strichcodes, obwohl diese eine zweidimensionale Ausdehnung haben, sowie zweidimensionale Codes, wie beispielsweise QR-Codes oder Ähnliches. Diese bieten den Vorteil, dass sie aufgrund von zum jeweiligen Code gehörenden Vorgaben, wie Normungsvorschriften, Bildverzerrungen einfach erkennbar machen und über entsprechende Mustererkennungssoftware solche "Abbildungsfehler" detektiert und korrigiert werden können, bevor der in dem Muster codierte Inhalt decodiert wird. Darüber hinaus verfügen maschinenlesbare Codes vorzugsweise über mindestens ein Fehlerkorrekturverfahren, wie beispielsweise eine Prüfsumme, oder andere Verfahren, die eine Korrektur einzelner oder mehrerer Fehler aufgrund einer unvollständigen oder leicht fehlerhaften Erfassung ermöglichen. Während Prüfziffern nur die korrekte Erfassung überprüfbar machen, ermöglichen Fehlerkorrekturverfahren, auch die Information trotz einzelner Fehler in Teilbereichen des Musters vollständig korrekt zu erfassen.

[0023] Deutlich verbessert wird die Erfindung, wenn die Codierung eine Verschlüsselung umfasst. Hierdurch kann verhindert werden, dass das maschinenlesbare Merkmal durch Fälscher in einfacher Weise erzeugt werden kann. Wird beispielsweise der Schlüssel, der für die Verschlüsselung benötigt wird, geheim gehalten, so kann das maschinenlesbare Muster aus der ersten Information nicht durch Fälscher codiert werden. Fälschungen werden hierdurch deutlich erschwert. Wird ein Verschlüsselungsverfahren mit einer geheimen Information, d.h. mit einem Schlüssel, verwendet, so ist auch eine Verifikation nur durch jene Personen oder Instanzen möglich, die den Schlüssel kennen.

[0024] Eine weitere Verbesserung, insbesondere hinsichtlich der Nutzeranwendungen des neuartigen Sicherheitselements, kann erreicht werden, wenn das Verschlüsselungsverfahren, welches bei der Codierung ausgeführt wird, ein sogenanntes asymmetrisches Verschlüsselungsverfahren ist. Hierunter werden Verschlüsselungsverfahren verstanden, die zwei miteinan-

der in Beziehung stehende Schlüssel aufweisen. Hierbei wird der eine Schlüssel zum Codieren und der andere Schlüssel zum Decodieren der Information verwendet. Bei einer solchen Ausführungsform ist es möglich, beispielsweise die zweite Information mit einem ersten geheim gehaltenen Schlüssel bei der Herstellung des Sicherheitselements zu codieren. Der zweite für die Decodierung notwendige Schlüssel kann öffentlich gemacht werden und ermöglicht die Verifikation in der Weise, dass überprüft werden kann, ob die in dem Muster gespeicherte Information nach der Entschlüsselung mit der ersten Information, die in dem Sicherheitselement im ersten Sicherheitsmerkmal gespeichert ist, übereinstimmt.

[0025] Eine bevorzugte Ausführungsform der Erfindung sieht somit vor, dass die zweite Information eine Verschlüsselung der ersten Information umfasst, insbesondere die zweite Information asymmetrisch verschlüsselt ist.

[0026] Eine entsprechende Weiterbildung des Verfahrens sieht somit vor, dass das Codieren ein Verschlüsseln umfasst, sodass die zweite Information eine Verschlüsselung der ersten Information umfasst, insbesondere die erste Information asymmetrisch verschlüsselt wird.

[0027] Das Verfahren zum Verifizieren wird somit dadurch weitergebildet, dass der Codierschritt einen Kryptografieschritt umfasst und das Codieren ein Verschlüsseln und das Decodieren ein Entschlüsseln umfassen.

[0028] Eine Ausführungsform der Verifikationsvorrichtung sieht vor, dass die Codiereinheit eine Kryptografieeinheit ist und das Codieren ein Verschlüsseln und das Decodieren ein Entschlüsseln umfasst, insbesondere mittels eines asymmetrischen Verschlüsselungsverfahrens.

[0029] Insbesondere ein asymmetrisches Verfahren bietet den Vorteil, dass zwar eine Verifikation, d.h. ein Überprüfen der Echtheit, dadurch möglich wird, dass die zweite Information entschlüsselt werden kann und mit der ersten Information verglichen werden kann, jedoch keine korrekten zweiten Muster aus einer bekannten ersten Information erzeugt werden können. Dieses bleibt der Institution vorbehalten, die die Kenntnis über den geheimen Schlüssel hat, welches in der Regel der Aussteller und/oder Hersteller der Sicherheitselemente ist. Möglich ist aber auch, dass auch der "öffentliche Schlüssel" nicht öffentlich gemacht wird, sondern nur Institutionen, die für die Überprüfung und Verifikation zuständig sind, gegebenenfalls in anderer Weise verschlüsselt zur Verfügung gestellt wird, sodass beispielsweise das Verifikationsverfahren mittels eines Computerprogramms ausführbar ist, jedoch Fälscher, die keinen Zugriff auf dieses geschützte Computerprogramm oder eine Verifizierungsvorrichtung haben, nicht einmal in der Lage sind, die in dem maschinenlesbaren Muster gespeicherte zweite Information zu decodieren und hierbei zu entschlüsseln.

[0030] Will der Aussteller und Erzeuger der Sicherheitselemente bei Verwendung eines asymmetrischen Verschlüsselungsverfahrens dennoch einer breiten Öffentlichkeit das Decodieren und Entschlüsseln möglich machen und gegebenenfalls auch verschiedene Schlüsselpaare aus öffentlichem und geheimem Schlüssel nutzen, so ist es vorteilhaft, wenn ein öffentlicher Schlüssel, mit dem die zweite Information entschlüsselbar ist, in dem Sicherheitselement gespeichert ist.

[0031] Insbesondere wenn verschiedene Schlüsselpaare für ansonsten gleichartige Sicherheitselemente verwendet werden, so ist es sehr vorteilhaft, den öffentlichen Schlüssel in dem jeweiligen Sicherheitsdokument zu speichern. Um hierüber den öffentlichen Schlüssel für die Entschlüsselung des maschinenlesbaren Musters nicht allgemein öffentlich zu machen, kann dieser mit Hilfe eines anderen Verfahrens, d.h. mit anderen Schlüsseln oder Schlüsselpaaren, ebenfalls verschlüsselt sein.

[0032] Besonders bevorzugt wird als erste Information eine Information verwendet, die individualisierend für das Sicherheitselement, besonders bevorzugt personalisierend, ist. Hierbei eignen sich insbesondere biometrische Informationen. Biometrische Informationen können beliebige biometrische Informationen sein. Besonders eignen sich insbesondere ein Augenabstand, eine Nasenlänge, Verhältnisse von bestimmten Abmessungen im Portraitbild oder aber Fingerabdruckmuster oder Ähnliches. Die erste Information kann somit beispielsweise unmittelbar in dem Portraitbild in dessen Darstellung gespeichert sein. Den Augenabstand oder eine Nasenlänge können entsprechende Mustererkennungsprogramme, wie sie im Stand der Technik bekannt sind, aus Bilddaten extrahieren. Da die nicht holografischen Informationen des Sicherheitsdokuments in der Regel vollflächig erfasst werden können, können diese Programme Abbildungsfehler wie Verzerrungen und Ähnliches in der Regel ohne Schwierigkeiten herausrechnen. Es wird somit möglich, ein eine Person eindeutig identifizierendes Merkmal, das Portraitbild, auf einfache Weise abzusichern, d.h. Informationen, die in dem Portraitbild gespeichert sind, unmittelbar abzusichern durch das holografisch gespeicherte maschinenlesbare Muster.

[0033] Eine bevorzugte Ausführungsform des Sicherheitselements sieht somit vor, dass die erste Information eine personalisierende Information, insbesondere eine biometrische Information, ist.

[0034] Einen besonders hohen Schutz des holografischen Merkmals erreicht man, wenn die zweite Information als Volumenhologramm gespeichert ist bzw. gespeichert wird. D.h. das zweite Sicherheitsmerkmal ist vorzugsweise als Volumenhologramm ausgebildet. Während Oberflächenhologramme durch Prägung herstellbar sind, wird für die Herstellung von Volumenhologrammen eine Belichtung mit kohärentem Licht benötigt, um das entsprechende Hologramm auszubilden. Daher ist der Aufwand deutlich erhöht. Darüber hinaus sind Ausprägungen mit Volumenhologrammen möglich, die eine hohe Beugungseffizienz aufweisen und somit in Bilddaten gut erfassbar sind.

[0035] Bei einer bevorzugten Ausführungsform der Er-

findung ist vorgesehen, dass die zweite Information als zweidimensionales Muster mit mindestens zwei Typen von Musterelementen ausgebildet ist, wobei die Musterelemente eines Typs bei der holografischen Rekonstruktion einen einheitlichen optischen Eindruck in bei der Rekonstruktion erfassten Bilddaten hervorrufen und unterschiedliche Typen von Musterelementen bei der Rekonstruktion unterschiedliche optische Eindrücke in den bei der Rekonstruktion erfassten Bilddaten hervorrufen. Hierunter fallen binäre Muster, wie beispielsweise QR-Codes. Ein Typ von Musterelement kann somit bei einer Ausführungsform die Beugungseffizienz 0 zugeordnet sein. Einem solchen Musterelement entspricht ein Ortsbereich in dem rekonstruierten Muster, welches keinen Lichteffekt in den Bilddaten zeigt. Dem anderen Typ von Musterelement sind Ortsbereiche zugeordnet, die einen hellen Lichteffekt in den Bilddaten zeigen.

[0036] Bei anderen Ausführungsformen kann ein binäres zweidimensionales Muster Musterelemente umfassen, die alle eine von Null verschiedene Beugungseffizienz aufweisen, Die einen Musterelemente weisen hierbei vorzugsweise eine Beugungseffizienz von mindestens 10%, jedoch höchsten 30% auf und die anderen Musterelemente eine Beugungseffizienz von mindestens 60%, vorzugsweise von mehr als 70%. Vorzugsweise sind die hellen Musterelemente mindestens "doppelt so hell", vorzugsweise mindestens "dreimal so hell", wie die dunkeln Musterelemente. Ein solches zweidimensionale maschinenlesbares Muster ist somit in den Bilddaten eine helle, jedoch Helligkeitsschwankungen bzw. Helligkeitsvariationen aufweisende Fläche. Ein solches Sicherheitsmerkmal ist schwerer zu fälschen und nachzubilden.

[0037] Es sind jedoch auch Ausführungsformen möglich, bei denen nicht nur zwei Typen von Musterelementen, sondern mehr Typen von Musterelementen verwendet werden, die sich beispielsweise hinsichtlich der Beugungseffizienz, d.h. der Helligkeit der Musterelemente, im rekonstruierten Bild des holografisch gespeicherten Musters unterscheiden. Dieses ist vergleichbar mit Graustufenwerten bei einer Speicherung von fotografischen Daten mittels eines Druckverfahrens.

[0038] Darüber hinaus sind weiterhin noch besser abgesicherte und schwerer nachzuahmende Muster dadurch herstellbar, dass unterschiedliche Typen von Musterelementen mit Hilfe unterschiedlicher Wellenlängen in das Volumenhologramm gespeichert sind oder werden. So können einzelne Musterelemente beispielsweise einen grünen Farbeindruck hervorrufen, wohingegen andere Musterelemente einen roten Farbeindruck hervorrufen. Zusätzlich können mehrere "rote" Typen von Musterelementen und mehrere "grüne" Typen von Musterelementen existieren, die sich untereinander entsprechend jeweils durch die Beugungseffizienz unterscheiden, was sich in der Helligkeit der erzeugten Musterelemente in den Bilddaten zeigt. Ein Fälschungsaufwand wird deutlich erhöht. Auch die Möglichkeit der zu codierenden Information in einem Muster wird hierdurch deutlich gesteigert. Dies bedeutet, dass auf derselben Fläche oder mit derselben Anzahl von Musterelementen im gespeicherten holografischen Muster eine größere Informationsvielfalt gespeichert werden kann. Während bei zwei Typen von Musterelementen in einem Musterelement zwei unterschiedliche Informationen speicherbar sind, sind in einem Musterelement bei Verwendung von drei Typen drei verschiedene Informationen speicherbar. Über die Anzahl der Musterelemente wird der Informationsgehalt entsprechend potenziert.

[0039] Nach einer Ausführungsform der Erfindung sind somit vorzugsweise die Musterelemente intensitätsmodulierte Flächenbereiche, die jeweils einen Flächenbereich eines flächigen Streuers oder eines Spiegels holografisch speichern.

[0040] Eine besonders hohe Absicherung erhält man, wenn auch die erste Information ebenfalls holografisch in der Speicherschicht gespeichert ist oder gespeichert wird. Das Sicherheitselement kann in diesem Fall ein holografischer Film sein, in dem beispielsweise sowohl das Portraitbild als Farbstufenbild, beispielsweise mit grünen Pixeln, die unterschiedliche Beugungseffizienz aufweisen, gespeichert ist und zugleich das maschinenlesbare Muster in derselben Hologrammfolie räumlich versetzt oder sogar teilweise oder vollständig überlagert gespeichert ist. Vollständig oder teilweise überlagert bedeutet in diesem Falle, dass in dem Bereich, in dem das zweidimensionale Muster, welches die zweite Information speichert, ausgebildet ist, keine Informationen des die erste Information speichernden Sicherheitsmerkmals ausgebildet sind. Als teilüberlagert oder vollständig überlagert wird eine Information daher angenommen, weil sie in den ansonsten beispielsweise rechteckigen oder quadratischen Bereich, in dem das erste Sicherheitsmerkmal, z.B. das Portraitbild, ausgebildet ist, teilweise oder vollständig angeordnet ist.

[0041] Bei anderen Ausführungsformen, bei denen die erste Information mittels des ersten Sicherheitsmerkmals in einer anderen Schicht als der Speicherschicht des Hologramms ausgebildet ist, beispielsweise auf die Hologrammschicht gedruckt ist, kann eine echte teilweise oder vollständige Überlagerung vorliegen, bei der Teile des Sicherheitsmerkmals, welches die erste Information speichert., im selben Flächenbereich des Sicherheitselements wie das maschinenlesbare Muster ausgebildet sind. Dieses steigert die Absicherung des abzusichernden ersten Sicherheitsmerkmals.

[0042] Bei noch einer stärker abgesicherten Form des Sicherheitselements ist vorgesehen, dass ein drittes Sicherheitsmerkmal in dem Datenträger gespeichert ist, dass entweder die erste Information oder die zweite Information ein weiteres mal in dem Datenträger redundant speichert, wobei sich die Speichermethoden, mit der das dritte Sicherheitsmerkmal ausgebildet ist bzw. gespeichert wird, von der Methode unterscheidet, mit der die redundant gespeicherte erste Information mittels des ersten Sicherheitsmerkmals ausgebildet ist bzw. gespeichert wird oder die redundant gespeicherte zweite Infor-

mation mittels des zweiten Sicherheitsmerkmals ausgebildet ist bzw. gespeichert wird. Hierdurch werden Ausführungsformen möglich, bei denen beispielsweise ein Portraitbild einmal in das Sicherheitselement gedruckt wird, beispielsweise mittels eines farbigen Tintenstrahldrucks, einmal als monofarbiges oder sogar vollfarbiges Portraitbild des Volumenhologramms und zusätzlich als monochromatisches oder polychromatisches maschinenlesbares Muster gespeichert wird oder ist.

[0043] Es versteht sich, dass das Verifikationsverfahren bei solchen Ausführungsformen dahingehend erweitert werden kann, dass eine Übereinstimmung der ersten Information und der dritten Information bzw. der Sicherheitsmerkmale, mit denen die erste Information und die dritte Information in dem Sicherheitselement gespeichert werden, zusätzlich vorgenommen werden kann, zu der Prüfung, ob die in dem maschinenlesbaren Muster codierte zweite Information mit der ersten Information, welche in dem ersten und dem dritten Sicherheitsmerkmal gespeichert ist, entsprechend übereinstimmt. Der Aufwand, um eine Manipulation eines Sicherheitselements auszuführen, wird hierdurch enorm gesteigert und Fälschungen werden leichter erkennbar.

[0044] Eine weitere Steigerung der Fälschungssicherheit und somit höhere Absicherung erhält man bei einer Ausführungsform, bei der das zweidimensionale Muster eine Vielzahl von verschiedenen Typen von Musterelementen umfasst, wobei die Vielzahl von Typen von Musterelementen Musterelemente umfasst, die bei unterschiedlichen Wellenlängen rekonstruieren und für mindestens eine dieser unterschiedlichen Wellenlängen Typen von Musterelementen umfassen, die unterschiedliche Beugungseffizienzen aufweisen.

[0045] Bevorzugt umfasst die Vielzahl von Musterelementen für jede der verschiedenen Wellenlängen unterschiedliche Typen von Musterelementen, die sich hinsichtlich der Beugungseffizienz unterscheiden.

[0046] Vorzugsweise existieren für mindestens eine der unterschiedlichen Wellenlängen, bei denen Typen von Musterelementen der Vielzahl von Musterelementen rekonstruieren, vorzugsweise für alle unterschiedlichen Wellenlängen, jeweils mindestens zwei Typen von Musterelementen, deren Beugungseffizienz sich mindestens um 10% unterscheiden. Andere Ausführungsformen können einen größeren Unterschied von mindestens 25% oder sogar 50% vorsehen.

[0047] Hierdurch wird zusätzlich eine Steigerung der Informationsdichte erreicht, d.h. der mit einer vorgegebenen Anzahl von physisch ausgebildeten Musterelementen speicherbaren Informationsmenge.

[0048] Vorzugsweise liegen mindestens zwei der verschiedenen Wellenlängen, vorzugsweise alle verschiedenen Wellenlängen, im optisch sichtbaren Wellenlängenbereich. Hierdurch wird eine Rekonstruktion mit weißem Licht, das ein kontinuierliches Spektrum aufweist, wie beispielsweise das Sonnenlicht, möglich. Volumenreflexionshologramme weisen eine ausreichende Wellenselektivität auf, dass die unterschiedlichen mit den unterschiedlichen Rekonstruktionswellenlängen korrespondierenden Farben für einen menschlichen Betrachter oder ein Farbkamerasystem erkenn- oder erfassbar sind.

[0049] Bei einer anderen Ausführungsform liegen die Rekonstruktionswellenlängen aller verschiedenen Typen von Musterelementen des Musters im nicht sichtbaren Wellenlängenbereich. Hierdurch wird ein verdecktes Sicherheitsmerkmal geschaffen.

[0050] Bei einer Weiterbildung ist das Muster des zweiten Sicherheitsmerkmals aus verschiedenen Typen von Musterelementen gebildet, die nicht mit Wellenlängen des sichtbaren Lichts rekonstruieren und räumlich dem ersten Sicherheitsmerkmal in der Weise überlagert sind, dass zumindest ein Teil der erfassbaren ersten Information bezogen auf eine flächige Ausdehnung des Sicherheitselements an derselben Position gespeichert ist, wie Musterelemente des Musters des zweiten Sicherheitsmerkmals.

[0051] Vorzugsweise werden das erste und das zweite Sicherheitselement optisch erfasst.

[0052] Nachfolgend wird die Erfindung unter Bezugnahme auf eine Zeichnung näher erläutert. Hierbei zeigen:

- Fig. 1 eine schematische Darstellung eines als Ausweisdokument ausgebildeten Sicherheitselements;
- Fig. 2 eine schematische Darstellung einer Vorrichtung zur Herstellung eines Sicherheitselements;
- Fig. 3 eine weitere schematische Darstellung einer anderen Ausführungsform zur Herstellung eines Sicherheitsdokuments;
- Fig. 4 eine schematische Darstellung eines Systems zur Verifikation eines Sicherheitselements;
- Fig. 5 eine schematische Darstellung eines Ablaufdiagramms eines Verifikationsverfahrens; und
- Fig. 6 eine schematische Darstellung eines weiteren Sicherheitselements.

[0053] Fig. 1 zeigt schematisch ein Sicherheitselement 1. Das Sicherheitselement ist als Datenträger 5 in Form eines als Ausweis ausgebildeten Sicherheitsdokuments 10 ausgebildet. In dem Sicherheitselement 1 sind individualisierende Daten 20 gespeichert. Diese umfassen beispielsweise eine Ausweisnummer 30, ein Gültigkeitsdatum 110 sowie eine Kennung 130, die beispielsweise einen öffentlichen Schlüssel 350 eines Schlüsselpaares für eine asymmetrische Verschlüsselung sein kann. Als weitere individualisierende Daten 20 sind personalisierende Daten 40 in dem Sicherheitselement 1 gespeichert. Diese umfassen ein vorzugsweise farbig aufgedrucktes Portraitbild 50, einen Namen 60, einen Vorna-

men 70, ein Geburtsdatum 80, eine Nationalität 90, einen Geburtsort 100 und eine Abbildung der Unterschrift 120. Die verschiedenen personalisierenden Daten 40 können, wie für das Portraitbild erwähnt, gedruckt sein oder auf beliebige andere Weise in das Sicherheitselement gespeichert sein. Beispielsweise können diese mittels Lasermarkierung durch permanente Umwandlung von Substratmaterial, beispielsweise von transparentem Kunststoff in geschwärzten Kunststoff gespeichert sein. Darüber hinaus können einzelne oder alle der mittels Lasermarkierung ausgebildeten Daten zusätzlich auch taktil erfassbar sein.

[0054] Zusätzlich zu den individualisierenden Daten 20 sind in dem Sicherheitselement 1 auch allgemeine Sicherheitsmerkmale 150 enthalten. Von diesen seien hier nur exemplarisch ein Sicherheitsdruck 160 sowie als eines der holografischen Merkmale 200 ein Hoheitssymbol 210, hier in Form eines Adlers, erwähnt. Das beispielsweise mittels rotem Licht rekonstruierende Hoheitssymbol 210 ist vorzugsweise als dreidimensionales Volumenhologramm ausgebildet, welches Parallaxeneffekte zeigt, d.h. seine Erscheinung bei Änderung der Betrachtungsrichtung ändert. Dies bedeutet, dass die dreidimensionale Gestalt des Adlers in dem Hologramm gespeichert ist. Zusätzlich als weiteres holografisches Merkmal 200 enthält das Sicherheitselement 1 ein zweidimensionales maschinenlesbares Muster 250. In der dargestellten Ausführungsform ist dieses als QR-Code ausgeführt. Das maschinenlesbare Muster 250 ist ein zweidimensionales Muster 251. Das zweidimensionales Muster 251 besteht aus Musterbereichen oder Musterelementen 252, 253, die entweder hell rekonstruieren (252) oder nicht rekonstruieren (253) und somit dunkel erscheinen. In der dargestellten Ausführungsform ist das Muster somit anhand von binären Musterelementen 252, 253 gebildet. Andere Ausführungsformen können vorsehen, dass die einzelnen beugenden Musterelemente unterschiedliche Beugungseffizienzen und somit unterschiedliche Helligkeitswerte aufweisen. Beispielsweise rekonstruiert das maschinenlesbare Muster mit Licht im grünen Wellenlängenbereich. Das maschinenlesbare Muster speichert bei einer bevorzugten Ausführungsform eine zweite Information, die aus einer in einem ersten Sicherheitsmerkmal 310 in dem Sicherheitselement gespeicherten erste Information abgeleitet ist. Beispielsweise stellt das vorzugsweise farbig gedruckte Portraitbild das erste Sicherheitsmerkmal 310 dar, in dem über eine Darstellung von Augen 51 ein Augenabstand 52 in dem Sicherheitselement 1 gespeichert ist. Das holografisch gespeicherte maschinenlesbare Muster 250 als zweites Sicherheitsmerkmal 320 umfasst diese erste Information, nämlich den Augenabstand als codierte zweite Information. Besonders bevorzugt wird hierbei eine asymmetrische Verschlüsselung ausgeführt, sodass die Gestalt des maschinenlesbaren Musters auch bei Kenntnis des Augenabstands 52 durch einen Fälscher nicht erzeugbar ist.

[0055] Bei anderen Ausführungsformen kann die erste Information beispielsweise in dem Portraitbild mit Hilfe einer Farbzusammensetzung gedruckt sein, die bei einer Beleuchtung mit Licht im sichtbaren Wellenlängenbereich nicht wahrnehmbar sind, jedoch eine Lumineszenz, insbesondere im sichtbaren Wellenlängenbereich, bei einer Anregung mit Licht im nichtsichtbaren Wellenlängenbereich, insbesondere im UV-Bereich oder im IR-Bereich, zeigt. Ebenfalls ist es möglich, diese erste Information so mit einer Druckzubereitung zu verdrucken, dass diese sowohl bei einer Anregung im UV-Wellenlängenbereich als auch im IR-Wellenlängenbereich dieselbe Information preisgeben. Hierzu wird in der Druckzubereitung sowohl ein bei UV-Anregung lumineszierender Farbstoff oder ein bei UV-Anregung lumineszierendes Pigment als auch ein eine Up-Konversion zeigender IR-anregbarer Farbstoff oder ein IR-anregbares Pigment verwendet. Diese Information kann beispielsweise ein Fingerabdruckmuster sein oder auch andere biometrische Daten oder nichtbiometrische personalisierende Daten umfassen.

[0056] In Fig. 2 ist exemplarisch eine Vorrichtung zum Herstellen eines Sicherheitselements gezeigt. Die Vorrichtung 500 umfasst einen Hologrammbelichter 600. Dieser weist eine kohärente Lichtquelle 610 und gegebenenfalls weitere kohärente Lichtquellen 615 auf. Zwischen der kohärenten Lichtquelle 610 und einem Hologrammmaster 630 ist in der Strahlführung ein räumlicher Lichtmodulator 620 angeordnet. Dieser ist mit einer Steuereinrichtung 700 verknüpft. Die Steuereinrichtung 700 ist beispielsweise als Computer 710 mit einem Eingang 720 zum Empfangen von Daten 720 zur Individualisierung und Personalisierung ausgebildet. Über diesen Computer 710 wird der Hologrammbelichter 600 gesteuert. Zur Herstellung des Sicherheitselements wird eine fotoempfindliche Schicht 510 bereitgestellt und in Kontakt mit dem Hologrammmaster 630 gebracht, der in der dargestellten Ausführungsform beispielsweise als Hologrammmaster eines Reflexionsvolumenhologramms ausgebildet ist. Dieser umfasst ein Hologramm eines flächig homogen leuchtend reflektierenden Bereichs, der ein Abbild einer Streuscheibe oder eines Spiegels ist. Der räumliche Lichtmodulator 620 wird so gesteuert, dass beispielsweise einzelne Bereiche des die homogen leuchtende Fläche darstellenden Hologrammmasters belichtet und somit in die fotoempfindliche Schicht 510 kopiert werden und andere Bereiche nicht beleuchtet und somit nicht rekonstruiert und kopiert werden. Es ergibt sich das binäre maschinenlesbare Muster, wie es beispielsweise in Fig. 1 als zweites Sicherheitselements 320 in Form des holografisch gespeicherten maschinenlesbaren Muster 250 des ausgebildet ist. Alternativ kann auch die für die Belichtung der einzelnen Musterelemente 252, 253 gewählte Intensität über den räumlichen Lichtmodulator verändert werden, sodass Musterelemente 252, 253 mit unterschiedlicher Helligkeit in dem maschinenlesbaren Muster auftreten. Neben der einen kohärenten Lichtquelle kann eine weitere kohärente Lichtquelle 615, welche eine andere Lichtwellenlänge

aufweist, genutzt werden, um entweder andere holografische Elemente, wie beispielsweise das in Fig. 1 gezeichnete Hoheitssymbol 210, mit Hilfe des Hologrammmasters 630, in dem das Hoheitssymbol als Hologramm für die andere Wellenlänge gespeichert ist, zu kopieren. Hierfür wird das Licht der weiteren kohärenten Lichtquelle in der Regel nicht über den räumlichen Lichtmodulator 620 geführt. Bei anderen Ausführungsformen kann jedoch vorgesehen sein, dass das maschinenlesbare holografische Muster Musterelemente umfasst, die bei unterschiedlichen Wellenlängen rekonstruieren und auch das Licht der weiteren kohärenten Lichtquelle 615 zumindest teilweise über den räumlichen Lichtmodulator geführt wird. Ebenso ist es möglich, einen zweiten räumlichen Lichtmodulator (nicht dargestellt für das Licht der weiteren kohärenten Lichtquelle 615 zu nutzen. Andere Ausführungsformen können noch weitere kohärente Lichtquellen für noch weitere Wellenlängen und gegebenenfalls Licht räumlicher Lichtmodulatoren vorsehen.

[0057] Nachdem das maschinenlesbare Muster in die Speicherschicht 511 in Form der fotoempfindlichen Schicht 510 gespeichert ist, wird bei der dargestellten Ausführungsform die erste Information beispielsweise mittels einer Druckeinrichtung 800 auf die fertig entwickelte und fixierte fotoempfindliche Schicht 510 aufgedruckt. Die erste Information wird hierbei mittels eines ersten Sicherheitsmerkmals 310 gespeichert, welches ein alphanumerischer Druck, ein mittels lumineszierenden Farbmitteln ausgeführter Druck und/oder auch ein Farbdruck beispielsweise in Form eines Portraitbild sein kann. Die erste Information kann in dem ersten Sicherheitsmerkmal auch mittels anderer Verfahren, beispielsweise über eine klassische Lasermarkierung, d.h. über eine teilweise Karbonisierung von Substratschichten, oder Ähnliches ausgebildet und gespeichert werden.

[0058] In Fig. 3 ist eine weitere Ausführungsform einer Vorrichtung zum Herstellen eines Sicherheitselements 1 gezeigt. Gleiche technische Merkmale sind in allen Figuren mit denselben Bezugszeichen versehen und werden nicht erneut gesondert beschrieben. Bei der Ausführungsform nach Fig. 3 wird zusätzlich zu der fotoempfindlichen Schicht 510 eine weitere Substratschicht 520, beispielsweise eine Kunststoffschicht, bereitgestellt und zeitgleich oder zeitversetzt mit dem holografischen Belichten der fotoempfindlichen Schicht 510 mit dem ersten Sicherheitsmerkmal bedruckt, welches die erste Information speichert. Anschließend werden die Substratschicht 520 und gegebenenfalls weitere Substratschichten mit der fotoempfindlichen Schicht 510 zusammengeführt und in einem Laminationsverfahren mittels einer Laminationseinrichtung 900 miteinander verbunden. Hierbei können Haftvermittler eingesetzt werden. Andere Ausführungsformen sehen vor, dass die fotoempfindliche Schicht 510, welches ebenfalls ein Schichtenverbund sein kann, ohne Einsatz eines Haftvermittlers mit der mindestens einen Substratschicht 520 zu einem Laminationskörper zusammengefügt wird. Ein solcher Laminationskörper wird auch als Datenträger 5 bezeichnet, da in ihm Daten gespeichert sind. Auch die bedruckte fotoempfindliche Schicht 510, die gemäß der Ausführungsform nach Fig. 2 erzeugt wird, stellt einen Datenträger 5 dar.

[0059] Während die Ausführungsform nach Fig. 2 ein Sicherheitselement 1 herstellt, welches in der Regel ein Vorprodukt für die Herstellung eines Personaldokuments oder anderen Sicherheits- oder Wertdokuments ist, wird mit der Vorrichtung nach Fig. 3 vorzugsweise ein Sicherheitselement 1 als ein fertiges Sicherheitsdokument 10 in Form eines Laminationskörpers hergestellt. Es versteht sich für den Fachmann, dass die Vorrichtung 500 weitere Einrichtungen enthalten kann, die weitere Sicherheitsmerkmale und Sicherheitselemente einfügt, und dass auch nach dem Herstellen des Laminationskörpers weitere Verfahrensschritte ausgeführt werden können, wie beispielsweise eine Lasergravur und/oder eine elektronische Personalisierung, indem Informationen in einem in das Sicherheitsdokument mit einlaminierten elektronischen Datenspeicher gespeichert werden. Auch die erste Information kann beispielsweise in einem solchen elektronischen Chip in einen als Sicherheitsdokument ausgebildetes Sicherheitselement gespeichert sein.

[0060] In Fig. 4 ist schematisch ein Verifikationssystem 1000 zum Verifizieren eines Sicherheitselements 1 gezeigt. Das Verifikationssystem umfasst in der dargestellten Ausführungsform eine Bilddatenerfassungseinrichtung 1100, eine Verifikationsvorrichtung 1300 sowie eine Zugangssperre 1400. Die Bilddatenerfassungseinrichtung 1100 umfasst eine Kamera 1150. Diese ist ausgebildet, bei Einstrahlung von Rekonstruktionslicht 1110 geeigneter Wellenlänge unter einem vorgegebenen Rekonstruktionswinkel auf ein Sicherheitselement 1 gebeugtes Licht 1120 zum Erfassen des zweiten Sicherheitselements 320 sowie zusätzlich im sichtbaren Licht sichtbare Sicherheitselemente wie das erste Sicherheitselement 310 zu erfassen. Das Rekonstruktionslicht kann von einer Lichtquelle 1130 bereitgestellt werden, die beispielsweise weißes Licht erzeugt, wenn das zweite holografisch gespeicherte zweite Sicherheitsmerkmal 320 als Volumenhologramm gespeichert ist. Die Lichtquelle 1130 kann jedoch auch als Laser ausgebildet sein. Die Bilderfassungseinrichtung 1100 kann auch eine Anregungsquelle 1140 in Form einer UV-Lampe oder Ähnliches umfassen, um lumineszierende Bestandteile des ersten Sicherheitselements 310 erfassbar zu machen. Die Bilddatenerfassungseinrichtung stellt Bilddaten 1200 zur Verfügung. Die Verifikationsvorrichtung 1300, die beispielsweise als Computer 1305 mit einer Recheneinrichtung 1310, einer Speichereinrichtung 1320 ausgebildet ist und einen in der Speichereinrichtung abgelegten Programmcode 1330 aufweist, weist einen Eingang 1340 zum Empfangen der Bilddaten 1200 auf. Mittels des Programmcodes, der auf der Recheneinrichtung 1310 ausgeführt wird, werden eine Extraktionseinheit 1350, eine Codiereinheit 1360, welche gegebenenfalls eine Kryptografieeinheit 1365 umfasst, eine Vergleiche-

reinheit 1370 sowie eine Verifikationseinheit 1380 realisiert.

[0061] Die Extraktionseinheit ist ausgebildet, aus den Bilddaten eine erste Information, beispielsweise einen Augenabstand aus dem Portraitbild, welches ein erstes Sicherheitsmerkmal darstellt, und als eine zweite Information das maschinenlesbare Muster extrahiert. Die Codiereinheit 1360 decodiert bei einer Ausführungsform das maschinenlesbare Muster. Hierbei wird ein Codierergebnis erhalten, welches bei einem echten Sicherheitselement der ersten Information gleichen soll, die von der Extraktionseinheit 1350 aus dem ersten Sicherheitsmerkmal extrahiert ist. Dies ist beispielsweise der Augenabstand. Die Vergleichereinheit 1370 vergleicht dann beispielsweise die erste Information mit der decodierten zweiten Information und stellt fest, ob Gleichheit oder Ungleichheit vorliegt. Anhand des Vergleichsergebnisses fällt die Verifikationseinheit 1380 ein Verifikationsergebnis, welches über eine Ausgabeeinheit 1385 beispielsweise einem Ausgang 1388 zugeführt wird. Die Ausgabeeinheit kann auch eine bildliche Darstellung des Ergebnisses ausgeben. Mit dem Ausgang 1388 ist in der dargestellten Ausführungsform des Verifikationssystems 1000 eine Zugangssperre 1400 verknüpft, die abhängig von dem Verifikationsergebnis beispielsweise den Zugang zu einem geschützten Bereich freigibt oder sperrt. Das Verifikationsergebnis kann auch beispielsweise als Signal ausgegeben werden, welches weiter verarbeitet werden kann.

[0062] Alternativ zu der Decodierung des extrahierten maschinenlesbaren Musters kann auch die erste Information in gleicher Weise codiert werden, wie diese bei der Herstellung des maschinenlesbaren Musters ausgeführt wurde, und somit mit der zweiten Information der Vergleichereinheit auf Gleichheit oder Ungleichheit verglichen werden.

[0063] Besonders bevorzugt ist die erste Information, beispielsweise der Augenabstand, in dem maschinenlesbaren Muster als zweite Information in verschlüsselter Form enthalten. Besonders bevorzugt hat die Verschlüsselung mittels eines asymmetrischen Verschlüsselungsverfahrens stattgefunden. Beispielsweise ist der Augenabstand mit einem geheimen Schlüssel verschlüsselt und in das maschinenlesbare Muster codiert worden. Bei der Verifikation kann nun bei der Decodierung des Musters ein Kryptografieschritt ausgeführt werden, der mit einem öffentlich bekannten Schlüssel ausgeführt wird. Hierdurch erhält man erneut einen Wert für den Augenabstand, der mit dem aus dem ersten Sicherheitsmerkmal extrahierten Augenabstand verglichen werden kann.

[0064] Anhand von Fig. 5 wird schematisch das Ablaufdiagramm einer Verifikation gemäß einer Ausführungsform eines Verifikationsverfahrens 2000 noch einmal erläutert. Optional findet ein Erfassen der Bilddaten des Sicherheitselements 2100 statt. Hierbei wird das Hologramm des Sicherheitselements 1120 rekonstruiert. Andere Ausführungsformen können vorsehen, dass lediglich die bereits erfassten Bilddaten empfangen werden 2200. Aus den Bilddaten werden aus dem ersten Sicherheitsmerkmal die erste Information und das maschinenlesbare Muster als zweite Information extrahiert 2300. Anschließend wird ein Codierschritt ausgeführt 2400, um eine mit der ersten Information zu vergleichende Information aus der zweiten Information abzuleiten oder die erste Information so zu codieren, dass sie mit der zweiten Information vergleichbar ist.

[0065] Bei einer bevorzugten Ausführungsform wird hierbei ein Kryptografieschritt ausgeführt 2410. Insbesondere wird die zweite Information, die vorzugsweise mit einem asymmetrischen Verschlüsselungsverfahren erzeugte Verschlüsselung der ersten Information ist, mit einem öffentlich bekannten Schlüssel entschlüsselt. Anschließend wird die erste Information mit dem Codier- bzw. Kryptografieergebnis verglichen 2500. Anschließend wird eine Verifikationsentscheidung abhängig davon gefällt, ob eine Gleichheit zwischen dem Codier- bzw. Kryptografieergebnis und den ursprünglich extrahierten Informationen festgestellt ist oder nicht 2600. Abschließend wird die Verifikationsentscheidung ausgegeben 2650. Bei einigen Ausführungsformen findet dann zusätzlich eine automatische Verarbeitung des Verifikationsergebnisses beispielsweise über eine Zugangssteuerung an einer Personenschleuse oder Ähnlichen statt 2700.

[0066] In Fig. 6 ist ein weiteres Ausführungsbeispiel eines Sicherheitselements 1 in Form eines als Ausweis ausgebildeten Sicherheitsdokuments 10 gezeigt. Technisch gleiche Merkmale zu der Ausführungsform nach Fig. 1 sind nicht erneut erläutert. Die Ausführungsform unterscheidet sich von der nach Fig. 1 insbesondere dadurch, dass das Portraitbild 50, welches zum einen gedruckt ist, zusätzlich als holografisches Portraitbild 260 in Hell/Dunkel oder Helligkeitsstufen ausgebildet gespeichert ist. Das holografisch ausgebildete maschinenlesbare Muster 250 ist zusätzlich in derselben Speicherschicht, einer fotoempfindlichen Schicht, jedoch an anderer Stelle ausgebildet. Hierdurch findet eine Mehrfachabsicherung der ersten Information statt, die sowohl in dem ersten Sicherheitsmerkmal 310, welches als holografisches Portraitbild ausgebildet ist, als auch in dem dritten Sicherheitsmerkmal 330, dem gedruckten Portraitbild 50, als auch in codierter, vorzugsweise verschlüsselter Form, in dem holografischen maschinenlesbaren Muster des zweiten Sicherheitsmerkmals 320 gespeichert ist.

[0067] Bei einer Abwandlung ist das maschinenlesbare Muster 250 des zweiten Sicherheitsmerkmals 320 farbig ausgebildet. Die Musterelemente, welche eine erfassbare Beugungseffizienz aufweisen, rekonstruieren bei mindestens zwei verschiedenen Wellenlängen, deren Licht für einen menschlichen Betrachter vorzugsweise verschiedene Farbeindrücke hervorruft, denen also unterschiedliche Farben zugeordnet sind. Vorzugsweise weist das Muster Musterelemente auf, die bei drei oder mehr Wellenlängen, also drei oder mehr Farben rekonstruieren. Hierdurch wird eine Fälschung weiter deutlich

erschwert und die Informationsdichte der speicherbaren Information des Musters gesteigert.

[0068] Bei einer anderen Ausführungsform umfasst das Muster 250 mindestens zwei unterschiedliche Typen von Musterelementen, die bei derselben Wellenlänge rekonstruieren und jeweils eine von null verschiedene Begungseffizienz aufweisen. Vorzugsweise gibt es mindestens drei oder mehr unterschiedliche Typen von Musterelementen, die bei derselben Wellenlänge wahrnehmbar rekonstruieren und jeweils eine von Null verschiedene wahrnehmbare oder erfassbare Beugungseffizienz aufweisen. Das Muster kann zusätzlich Musterelemente aufweisen, die nicht oder nicht wahrnehmbar rekonstruieren.

[0069] Die hier beschriebenen Variationen können in allen Ausführungsformen vorgenommen werden und mit den übrigen Merkmalen kombiniert werden, um die Erfindung umzusetzen.

[0070] Es versteht sich, dass in dem maschinenlesbaren holografisch gespeicherten Muster neben der codierten ersten Information auch weitere Informationen in verschlüsselter oder unverschlüsselter Form gespeichert sein können.

[0071] Das Sicherheitselement wird vorzugsweise in einer fotoempfindlichen Schicht oder in einem Laminationskörper umfassend eine fotoempfindliche Schicht ausgebildet. Die fotoempfindliche Schicht umfasst vorzugsweise Fotopolymere. Es kann jedoch jede Schicht genutzt werden, in die ein Hologramm belichtet werden kann. Die anderen Substratschichten, die in einem Laminationskörper mit der fotoempfindlichen Schicht verbunden werden, können beliebige gebräuchliche Substratschichten sein. Diese umfassen insbesondere Polycarbonat, Polyethylen, PVC, aber auch Verbundstoffe wie ABS, Papier, Baumwolle oder Ähnliches. Als Druckverfahren kommen beliebige Druckverfahren in Betracht. Besonders geeignet sind jedoch digitale Druckverfahren, insbesondere ein Tintenstrahldruckverfahren. Hierbei werden insbesondere Drucktinten eingesetzt, die auf Basis des Kunststoffmaterials hergestellt sind, auf welchem der Druck ausgeführt wird. Insbesondere eignen sich hier als Substratschicht Polycarbonatschichten und als Drucktinten Zubereitungen, die ein Bindemittel mit einem Polycarbonatderivat, vorzugsweise auf Basis eines geminal disubstituierten Dihydroxydiphenylcycloalkans, umfassen, wie diese unter anderem in der DE 10 2008 012 423 A1 beschrieben sind.

[0072] Es versteht sich für den Fachmann, dass die mit den unterschiedlichen Ausführungsformen beschriebenen Merkmale beliebig zur Bildung weiterer Ausführungsformen kombiniert werden können.

Bezugszeichen

[0073]

1	Sicherheitselement
5	Datenträger
10	Sicherheitsdokument
20	Individualisierende Daten
30	Ausweisnummer
40	Personalisierende Daten
50	Portraitbild
51	Augen
52	Augenabstand
60	Name
70	Vorname
80	Geburtsdatum
90	Nationalität
100	Geburtsort
110	Gültigkeitsdatum
120	Unterschrift
130	Kennung
150	allgemeine Sicherheitsmerkmale
160	Sicherheitsdruck (Hintergrund)
200	Holografische Merkmale
210	Hoheitssymbol
250	maschinenlesbares Muster
251	zweidimensionales Muster
252	Musterelement
253	Musterelement
260	holografisches Portraitbild
310	erstes Sicherheitsmerkmal
320	zweites Sicherheitsmerkmal
330	drittes Sicherheitsmerkmal
350	öffentlicher Schlüssel
500	Vorrichtung zum Herstellen eines Sicherheitselements
510	fotoempfindliche Schicht
511	Speicherschicht
520	Substratschicht
600	Holobelichter
610	kohärente Lichtquelle
615	weitere kohärente Lichtquelle
620	räumlicher Lichtmodulator
630	Hologrammmaster
700	Steuereinrichtung
710	Computer
720	Eingang
800	Druckeinrichtung
900	Laminationseinrichtung
1000	Verifikationssystem
1100	Bilddatenerfassungseinrichtung
1110	Rekonstruktionslicht
1120	gebeugtes Licht (rekonstruierte Hologramminformation)
1130	Lichtquelle
1140	Anregungsquelle (z.B. UV-Lampe)
1150	Kamera
1200	Bilddaten
1300	Verifikationsvorrichtung
1305	Computer
1310	Rechnereinrichtung
1320	Speichereinrichtung
1330	Programmcode

1340 Eingang
1350 Extraktionseinheit
1360 Codiereinheit
1365 Kryptografieeinheit
1370 Vergleichereinheit
1380 Verifikationseinheit
1385 Ausgabeeinheit
1388 Ausgang
1400 Zugangssperre
2000 Verifikationsverfahrens
2100 Erfassen von Bilddaten eines Sicherheitselements
2110 Rekonstruieren des Hologramms des Sicherheitselements
2200 Empfangen von Bilddaten des Sicherheitselements
2300 Extrahieren der ersten Information und der zweiten Information
2400 Ausführen eines Codierschrittes
2410 Ausführen eines Kryptografieschrittes
2500 Vergleichen des Codierergebnisses mit den extrahieren Informationen
2600 Fällen einer Verifikationsentscheidung
2650 Ausgeben der Verifikationsentscheidung
2700 Zugangssteuerung basierend auf dem Verifikationsergebnis

Patentansprüche

1. Sicherheitselement (1) umfassend

einen Datenträger (5) mit einem erfassbaren ersten Sicherheitsmerkmal (310), in welchem eine erste Information gespeichert ist, und
der Datenträger (5) eine Speicherschicht (511) umfasst, in der mindestens ein zweites erfassbares Sicherheitsmerkmal (320) holografisch gespeichert ist, wobei das zweite Sicherheitsmerkmal (320) eine zweite Information speichert, die aus der ersten Information ableitbar ist,
dadurch gekennzeichnet, dass
die zweite Information ein maschinenlesbares Muster (250) ist.

2. Sicherheitselement (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** die zweite Information eine Verschlüsselung der ersten Information ist, insbesondere die zweite Information asymmetrisch verschlüsselt ist.

3. Sicherheitselement (1) nach Anspruch 2, **dadurch gekennzeichnet, dass** ein öffentlicher Schlüssel (350), mit dem die zweite Information entschlüsselbar ist, in dem Sicherheitselement (1) gespeichert ist.

4. Sicherheitselement (1) nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die erste Information eine personalisierende Information, insbesondere eine biometrische Information ist.

5. Sicherheitselement (1) nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die zweite Information mittels des zweiten Sicherheitsmerkmals (320) als Volumenhologramm gespeichert ist.

6. Sicherheitselement (1) nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** das zweite Sicherheitsmerkmal (320), das die zweite Information speichert, als zweidimensionales Muster (251) mit mindestens zwei Typen von Musterelementen (252; 253) ausgebildet ist, wobei die Musterelemente (252; 253) eines Typs bei der holografischen Rekonstruktion einen einheitlichen optischen Eindruck in bei der Rekonstruktion erfassten Bilddaten (1200) hervorrufen und unterschiedliche Typen von Musterelementen (252; 253) bei der Rekonstruktion unterschiedliche optische Eindrücke in den bei der Rekonstruktion erfassten Bilddaten (1200) hervorrufen.

7. Sicherheitselement (1) nach Anspruch 6, **dadurch gekennzeichnet, dass** die Musterelemente intensitätsmodulierte Flächenbereiche sind, die jeweils einen Flächenbereich eines flächigen Streuers oder eines Spiegels holografisch speichern.

8. Sicherheitselement (1) nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die erste Information mittels des ersten Sicherheitselements (310) ebenfalls holografisch in der Speicherschicht (511) gespeichert ist.

9. Sicherheitselement (1) nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** ein drittes Sicherheitsmerkmal (330) in dem Datenträger (5) gespeichert ist, das entweder die die erste Information (310) oder die zweite Information (320) ein weiteres Mal in dem Datenträger (5) redundant speichert, wobei sich die Speichermethoden, mit der das dritte Sicherheitsmerkmal (330) ausgebildet ist, sich von der Methode unterscheidet, mit der die redundant gespeicherte erste Information mittels des ersten Sicherheitsmerkmals (310) ausgebildet ist oder die redundant gespeicherte zweite Information mittels des zweiten Sicherheitsmerkmals (320) ausgebildet ist.

10. Verfahren zum Herstellen eines Sicherheitselement (1) nach einem der Ansprüche 1 bis 9, umfassend die Schritte:

Empfangen einer ersten Information;
Codieren der ersten Information, um als Ergebnis der Codierung eine zweite Information zu erhalten;
Bereitstellen oder Herstellen eines Datenträgers (5), der zumindest eine holografische Speicherschicht (511) umfasst,
holografisches Speichern der zweiten Information in der Speicherschicht (511) mittels eines zweiten Sicherheitsmerkmals (320) als maschinenlesbares Muster (250) und Speichern der ersten Information in dem Datenträger (5) mittels eines ersten Sicherheitsmerkmals (310).

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet, dass** das Codieren ein Verschlüsseln umfasst, sodass die zweite Information eine Verschlüsselung der ersten Information ist, insbesondere die erste Information mittels eines asymmetrischen Verschlüsselungsverfahren in die zweite Information verschlüsselt wird.

12. Verfahren nach Anspruch 10 oder 11, **dadurch gekennzeichnet, dass** die zweite Information mittels eines Kontaktkopierverfahrens mit Hilfe eines Hologrammmasters (630) eines flächigen Streuers oder Spiegels als Volumenhologramm gespeichert wird.

13. Verfahren nach einem der Ansprüche 10 bis 12, **dadurch gekennzeichnet, dass** die erste Information mittels des ersten Sicherheitsmerkmals (310) ebenfalls holografisch in der Speicherschicht gespeichert wird.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet**, die erste Information und die zweite Information mittels unterschiedlicher Wellenlängen gespeichert werden.

15. Verifikationsvorrichtung (1300) für ein Sicherheitselement (1) nach einem der Ansprüche 1 bis 9, umfassend:

eine Extraktionseinheit (1350), welche ausgebildet ist, Bilddaten des Sicherheitselements (1) zu empfangen und die erste Information aus dem ersten Sicherheitsmerkmal (310) und eine zweite Information aus dem zweiten Sicherheitsmerkmal (320) zu extrahieren;
eine Codiereinheit (1360) zum Erzeugen eines Codierergebnisses, wobei das Codierergebnis entweder die Codierung der ersten Information ist oder die Decodierung der zweiten Information ist;
eine Vergleichereinheit zum Erzeugen eines Vergleichsergebnisses, wobei die Vergleichereinheit (1370) ausgebildet ist, das Codierergebnis mit der zweiten Information zu vergleichen, wenn das Codierergebnis die Codierung der ersten Information ist, oder das Codierergebnis mit der ersten Information zu vergleichen, wenn das Codierergebnis die Decodierung der zweiten Information ist; und eine Verifikationseinheit (1380) zum Ausgebgen eines Verifikationsergebnisses, wobei das Verifikationsergebnis das Sicherheitselement (1) als echt kennzeichnet, wenn das Vergleichsergebnis eine Gleichheit angibt und als nicht echt kennzeichnet, wenn das Vergleichsergebnis eine Ungleichheit angibt.

16. Verfahren zum Verifizieren eines Sicherheitselements (1) nach einem der Ansprüche 1 bis 9, umfassend die Verfahrensschritte:

Empfangen digitaler Bilddaten (1200) des Sicherheitselements (1);
Extrahieren einer ersten Information aus einem ersten Teil der digitalen Bilddaten (1200), die das erste Sicherheitsmerkmal (310) abbilden, und Extrahieren der zweiten Information aus einem zweiten Teil der Bilddaten (1200), die das zweite Sicherheitsmerkmal (320) abbilden, Ausführen eines Codierschrittes zum Erzeugen eines Codierergebnisses, wobei entweder die erste Information codiert wird, so dass das Ergebnisergebnis die Codierung der ersten Information ist oder die zweite Information decodiert wird, so dass das Codierergebnis die Entschlüsselung der zweiten Information ist,
Ermitteln eines Vergleichsergebnisses, wobei das Codierergebnis mit der zweiten Information vergleichen wird und deren Gleichheit oder Ungleichheit angibt, wenn das Codierergebnis die Codierung der ersten Information ist, oder das Codierergebnis mit der ersten Information vergleichen wird und deren Gleichheit oder Ungleichheit angibt, wenn das Codierergebnis die Decodierungung der zweiten Information ist, und Ausgeben eines Verifikationsergebnisses, wobei das Verifikationsergebnis das Sicherheitselement (1) als echt kennzeichnet, wenn das Vergleichsergebnis eine Gleichheit angibt und als nicht echt kennzeichnet, wenn das Vergleichsergebnis eine Ungleichheit angibt.

17. Computerprogramm mit Programmcode (1320) zur Durchführung aller Verfahrensschritte nach Anspruch 16, wenn das Computerprogramm in einem Computer (1305) ausgeführt wird.

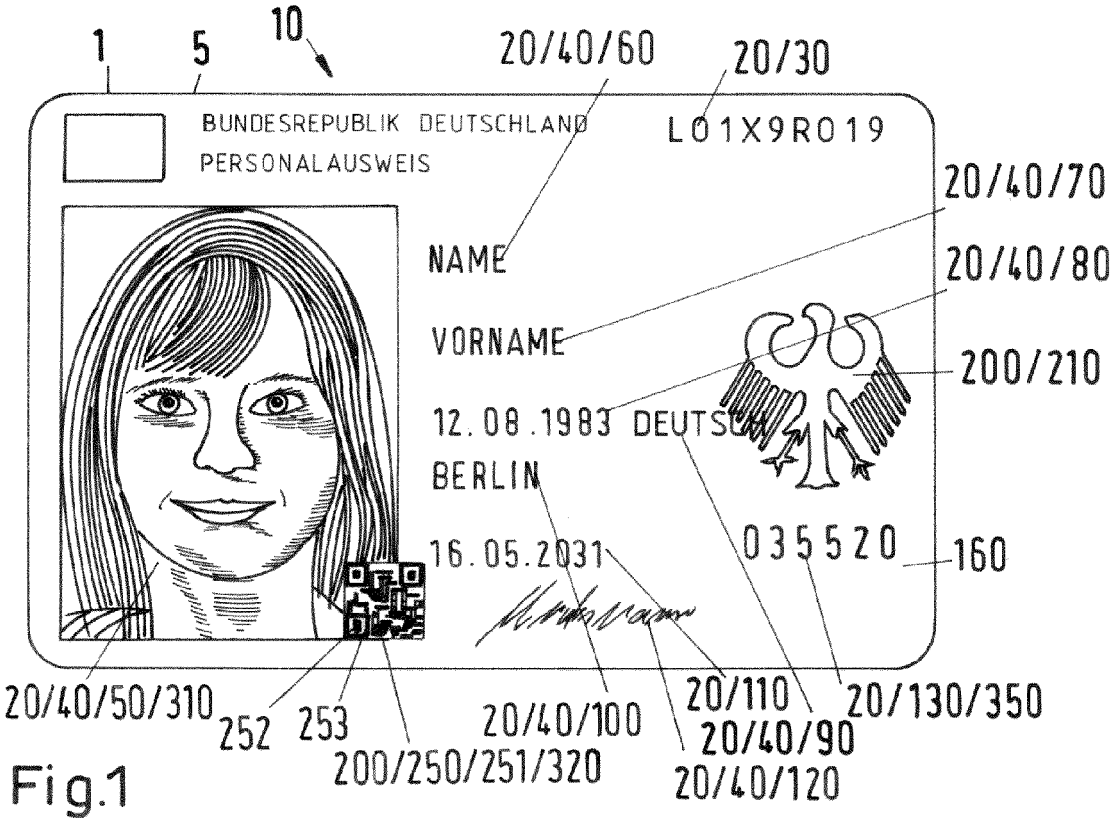
1
5
10
20/40/60
20/30
BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
L01X9R019
20/40/70
NAME
20/40/80
VORNAME
200/210
12.08.1983 DEUTSCH
BERLIN
16.05.2031
035520
160
20/40/50/310
252
253
200/250/251/320
20/40/100
20/110
20/40/90
20/40/120
20/130/350

Fig.1

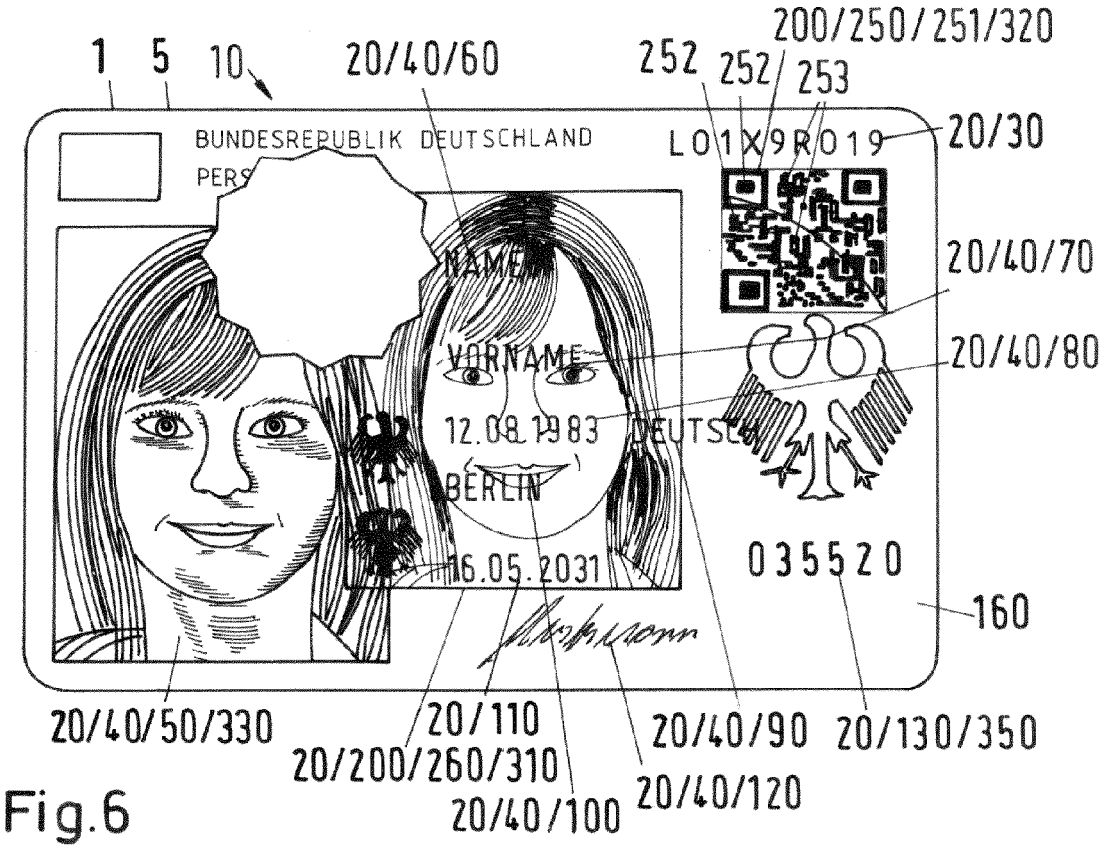
200/250/251/320
1
5
10
20/40/60
252
252
253
BUNDESREPUBLIK DEUTSCHLAND
PERS
L01X9R019
20/30
20/40/70
NAME
VORNAME
20/40/80
12.08.1983 DEUTSCH
BERLIN
16.05.2031
035520
160
20/40/50/330
20/110
20/200/260/310
20/40/100
20/40/120
20/40/90
20/130/350

Fig.6

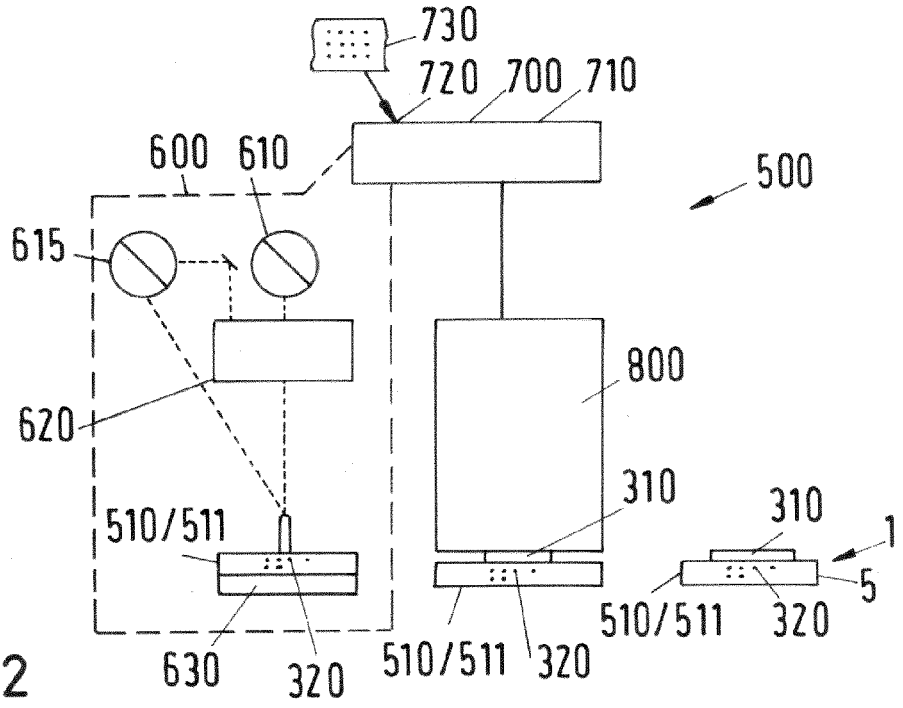
730
720
700
710
600
610
500
615
800
620
310
310
510/511
1
5
510/511
320
630
320
510/511
320

Fig.2

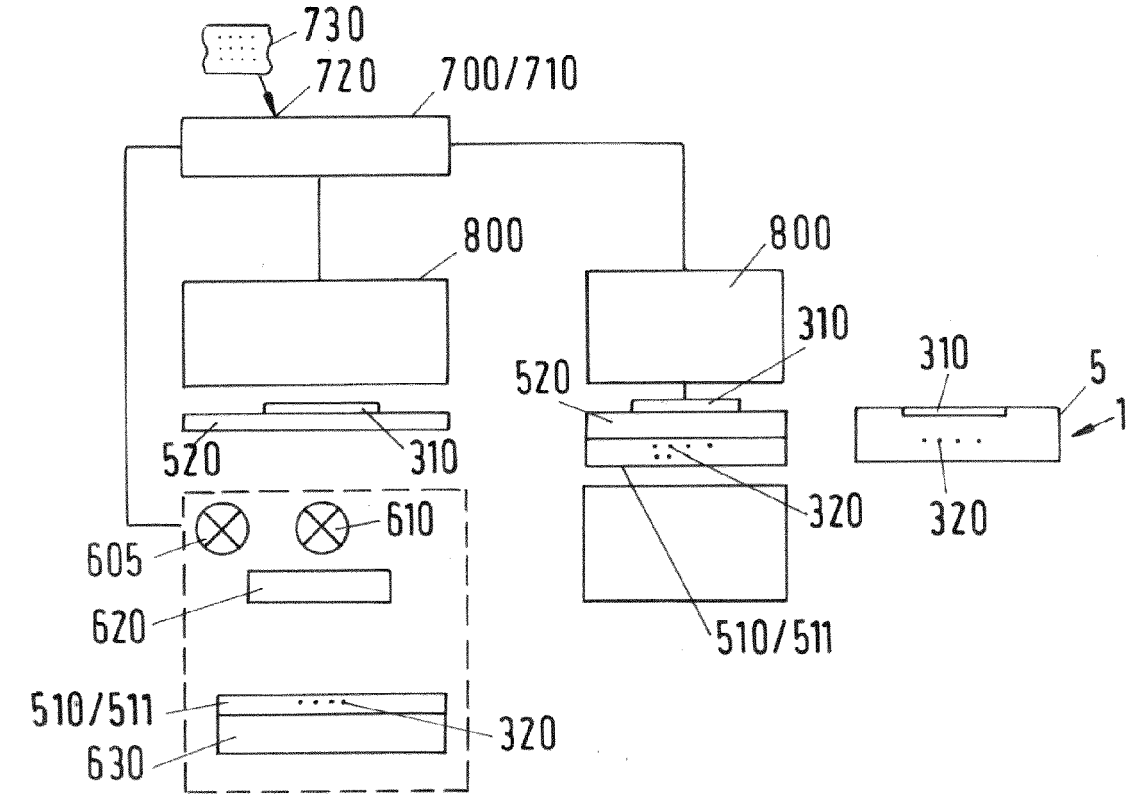
730
720
700/710
800
800
310
520
310
5
1
520
310
320
320
610
605
620
510/511
510/511
320
630

Fig.3

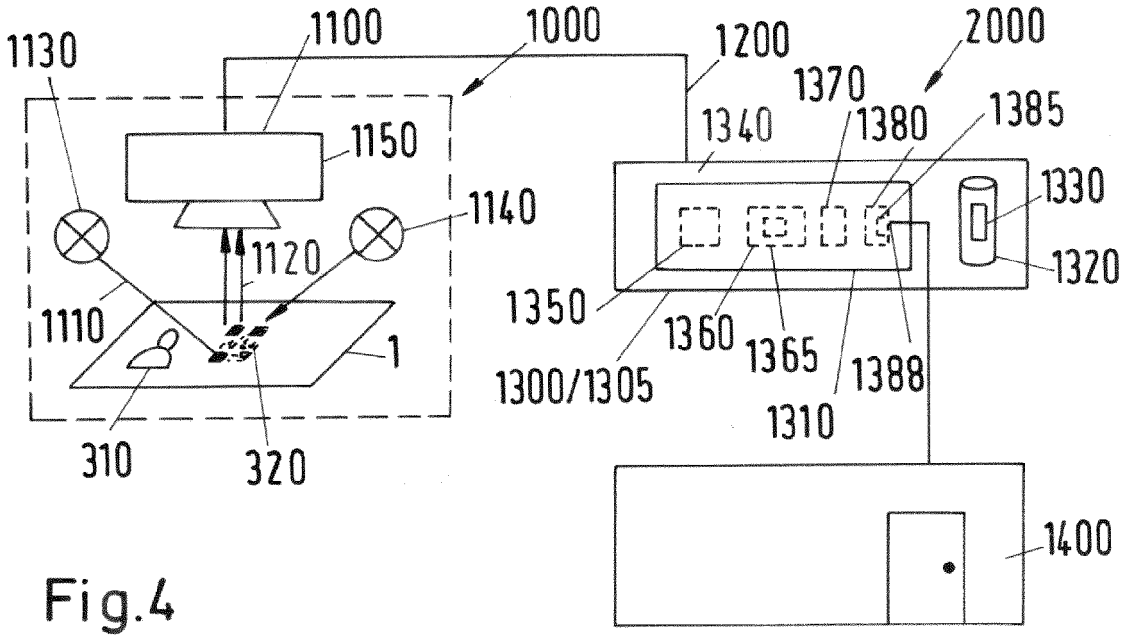
1130
1100
1000
1200
2000
1370
1340
1380
1385
1150
1330
1140
1320
1120
1350
1360
1365
1388
1110
1
1300/1305
1310
310
320
1400

Fig.4

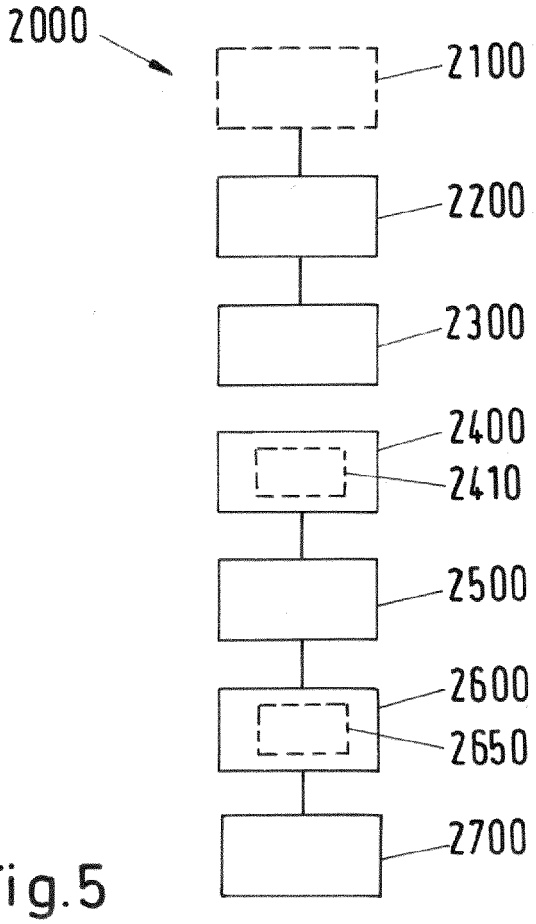
2000
2100
2200
2300
2400
2410
2500
2600
2650
2700

Fig.5

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 23 21 8840

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X Y	DE 10 2016 103694 A1 (OVD KINEGRAM AG [CH]) 7. September 2017 (2017-09-07) * Abbildung 1 * -----	1-13, 15-17 14	INV. B42D25/328 B42D25/41
Y	DE 10 2016 104300 A1 (LEONHARD KURZ STIFTUNG & CO KG [DE]; OVD KINEGRAM AG [CH]) 14. September 2017 (2017-09-14) * Absatz [0146] * -----	14	

RECHERCHIERTE SACHGEBIETE (IPC)

B42D

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	28. März 2024	Langbroek, Arjen

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 23 21 8840

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

28-03-2024

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102016103694 A1	07-09-2017	AR 108685 A1	19-09-2018
		DE 102016103694 A1	07-09-2017
DE 102016104300 A1	14-09-2017	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

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

- EP 0896260 A2 **[0009]**
- DE 102008012423 A1 **[0071]**