



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
20.09.2023 Patentblatt 2023/38

(51) Internationale Patentklassifikation (IPC):
G06K 19/00 (2006.01)

(21) Anmeldenummer: **23183050.6**

(52) Gemeinsame Patentklassifikation (CPC):
B42D 25/305; B42D 25/485

(22) Anmeldetag: **06.08.2021**

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

• **KNEBEL, Michael**
13086 Berlin (DE)
• **KRÜGER, Per**
14542 Werder (Havel) (DE)

(30) Priorität: **07.08.2020 DE 102020120842**

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

(62) Dokumentnummer(n) der früheren Anmeldung(en) nach Art. 76 EPÜ:
21755950.9 / 4 192 692

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

(72) Erfinder:
• **GRIESER, Ralf**
10589 Berlin (DE)

Bemerkungen:

- Diese Anmeldung ist am 03.07.2023 als Teilanmeldung zu der unter INID-Code 62 erwähnten Anmeldung eingereicht worden.
- Die Patentansprüche wurden nach dem Anmeldetag / dem Tag des Eingangs der Teilanmeldung eingereicht (R. 68(4) EPÜ).

(54) **ERZEUGUNG VON DOKUMENTENVORLAGEN MIT SICHERHEITSMERKMALEN**

(57) Offenbart ist eine Verwendung einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument zur Herstellung des Wert- oder Sicherheitsdokuments, wobei die elektronische Dokumentenvorlage für das Wert- oder Sicherheitsdokument erzeugt ist mit einem Verfahren aufweisend die folgenden Schritte: Zurverfügungstellung (301) einer Datenbank (DB), in der verschiedenen Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet sind, wobei das optische Lesegerät zur Trennung der Kanäle ausgebildet ist, Auswahl (302) einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank und Instanziierung der ausgewählten Typen jeweils durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht des Wert- oder Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs, Prüfung (303) des Layoutentwurfs, wobei für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft wird, ob diese einen gemeinsamen der Kanäle belegen, und wenn dies der Fall ist, die Ausgabe eines Signals, und Eingabe einer Korrektur (304) des Layoutentwurfs als Antwort auf das Signal, sowie die Speicherung (305) des resultierenden korrigierten Layoutentwurfs als die elektronische Dokumentenvorlage.

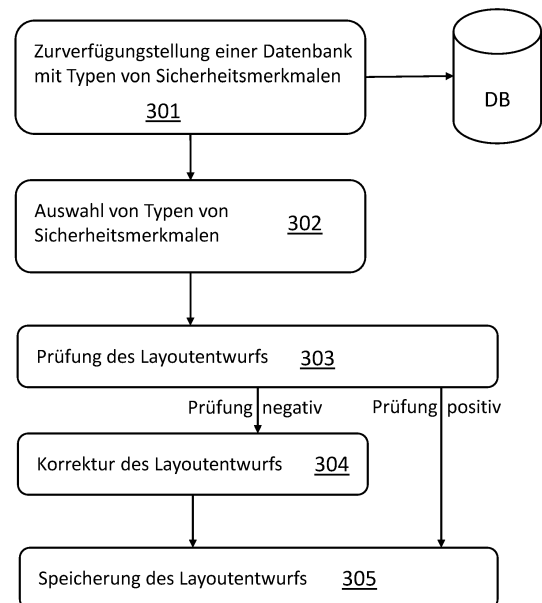


Fig. 3

Beschreibung

Gebiet

[0001] Die Erfindung betrifft eine Verwendung einer Dokumentenvorlagen mit Sicherheitsmerkmalen zur Herstellung eines Wert- oder Sicherheitsdokument, insbesondere eines sogenannten Wert- oder Sicherheitsdokuments wie z.B. eines Personalausweises, eines Reisepasses oder einer Kreditkarte. Ferner betrifft die Erfindung eine Kombination aus einer Dokumentenvorlage für ein Wert- oder Sicherheitsdokument und dem Wert- oder Sicherheitsdokument, welches hergestellt ist unter Verwendung der Dokumentenvorlage.

Stand der Technik

[0002] Dokumente, z.B. Wert- und Sicherheitsdokumente wie etwa Personalausweise, Reisepässe oder Kreditkarten, kommen bei vielen sicherheitskritischen Anwendungsszenarien zum Einsatz. Entsprechend hoch ist die Gefahr, dass ein berechtigter Besitzer eines solchen Dokuments oder ein unberechtigter Dritter das Dokument physisch nach dessen Herausgabe manipuliert, um sich z.B. unberechtigter Weise Zutritt zu einem geschützten Gebäudekomplex, Zugriff auf geschützte Daten, oder Zugriff auf die Leistungen von Diensten zu verschaffen. Beispielsweise könnte ein unberechtigter Dritter versuchen, das Gesichtsbild des Besitzers, welches auf einem bereits hergestellten und herausgegebenen Ausweisdokument oder auf einem personalisierten Werdokument aufgedruckt ist, durch sein eigenes Gesichtsbild oder durch ein gemorphtes Bild zu ersetzen (Identitätsdiebstahl). Auch andere Manipulationen sind möglich, beispielsweise eine Manipulation von Orts- und Altersangaben auf dem Dokument oder die Anfertigung einer physischen Kopie eines echten Dokuments.

[0003] Sofern das Dokument über elektronische Komponenten, wie insbesondere einen Datenspeicher und einen Mikroprozessor verfügt, gibt es im Stand der Technik verschiedene Ansätze, ein Dokument oder zumindest den Inhalt von dessen Datenspeicher mittels individueller Kennungen, kryptographischer Schlüssel, Signaturen und sonstiger dokumentenindividueller oder personenindividueller Daten oder Algorithmen eindeutig und manipulationssicher identifizierbar zu machen.

[0004] Allerdings verfügen nicht alle Wert- und Sicherheitsdokumente auch über entsprechende Datenspeicher und/oder Mikroprozessoren, um mittels algorithmischer und/oder kryptographischer Verfahren die Manipulationssicherheit des Dokuments und/oder dessen Informationsgehalt zu gewährleisten. Selbst für den Fall, dass entsprechende elektronische Komponenten vorhanden sind, ist deren Verwendung im Zuge einer Integritätsprüfung oftmals zeitaufwändig oder komplex. Die besagten elektronischen Mittel zur Integritätssicherung sind oftmals auch ungenügend, nämlich dann, wenn die Integrität des Dokuments zumindest bei manchen Gele-

genheiten auch anhand rein optischer Merkmale, wie etwa eines Hologramms, eines Gesichtsbilds des Inhabers des Dokuments, einer handschriftlichen Unterschrift des Inhabers etc., erfolgen soll. Beispielsweise dient das Gesichtsbild einer Person, das auf einem Reisepass, Personalausweis oder Mitarbeiterausweis dieser Person aufgedruckt ist, regelmäßig des Nachweises gegenüber anderen Personen, dass der Besitzer des Dokuments die Person ist, für welche der Ausweis ausgestellt wurde. Es ist in solchen Szenarien also nicht ausreichend, nur sicherzustellen, dass elektronische Komponenten oder Datenspeicher des Dokuments integer sind, d.h. nicht manipuliert wurden.

[0005] Die GB 2 352 708 A beschreibt einen Ausweis, welcher ein Substrat umfasst, auf dem Zeichen angezeigt werden; und eine zumindest teilweise transparente Auflage, auf der Zeichen und optional eine fotografische Darstellung sowie eine Handschrift gedruckt werden können, die das Substrat zumindest teilweise bedeckt, so dass die Zeichen auf dem Substrat und der Auflage nebeneinander sichtbar sind.

[0006] Die WO 00/38932 A1 beschreibt ein Dokument, welches auf einem Substrat wenigstens eine Dokumentennummer, eine optische Markierung mit einer maschinell lesbaren Kennung und ein Speicherfeld für die Aufnahme einer Kontrollnummer auf. Die Kontrollnummer wird erst im Moment der Abgabe an eine berechnete Person mittels einer kryptographischen Operation aus wenigstens der Dokumentennummer, der Kennung und einem ersten geheimen Schlüssel erzeugt und in das Speicherfeld eingeschrieben. Ein derart erzeugtes Echtheitszertifikat ist mit einem Verifikator unter Verwendung einer kryptographischen Operation und der auf dem Dokument gespeicherten Information mittels eines zweiten Schlüssels auf seine Echtheit überprüfbar.

[0007] Die WO 2018/109035 A2 beschreibt ein Verfahren zur Verifikation eines Sicherheitsdokuments mittels eines Lesegeräts. Erste Transmissions- und/oder Reflexionseigenschaften eines ersten Bereichs des Sicherheitsdokuments werden in einem ersten Spektralbereich von dem Lesegerät erfasst. Hieraus wird ein diese Eigenschaften spezifizierender erster Datensatz erstellt. Der erste Bereich überlappt ein auf dem Sicherheitsdokument angeordnetes oder in das Sicherheitsdokument eingebettetes optisches Sicherheitselement zumindest bereichsweise. Zweite Transmissions- und/oder Reflexionseigenschaften des ersten Bereichs des Sicherheitsdokuments werden in einem zweiten Spektralbereich von dem Lesegerät erfasst. Hieraus wird eine diese Eigenschaften spezifizierender zweiter Datensatz erstellt. Der erste Spektralbereich unterscheidet sich von dem zweiten Spektralbereich. Basierend zumindest auf dem ersten Datensatz und dem zweiten Datensatz wird die Echtheit des Sicherheitsdokuments und/oder des Sicherheitselements überprüft.

[0008] Die US 2005/010776 A1 beschreibt Systeme und Verfahren zum Sichern eines Identifikationsdokuments das mindestens ein Speicherelement aufweist, das

in der Lage ist, Informationen zu speichern. Ein Verschlüsselungsschlüssel wird bereitgestellt, wobei der Verschlüsselungsschlüssel einen öffentlichen Schlüssel und einen privaten Schlüssel umfasst. Ein optisch variables Element (OVD) in einem maschinenlesbaren Format wird erstellt, wobei das OVD dem öffentlichen Schlüssel zugeordnet ist. Eine Nutzlast von Daten wird zum Speichern in dem Speicherelement erzeugt. Mindestens ein Teil der Nutzdaten wird mit dem privaten Schlüssel verschlüsselt, und die verschlüsselten Nutzdaten werden an mindestens eine Stelle auf dem Identifikationsdokument übertragen. Mindestens ein Teil der Nutzdaten kann auf Daten basieren, die zufällig aus Daten ausgewählt werden, die in dem Speicherelement gespeichert sind, oder die aus Daten verschlüsselt sind, die in dem Speicherelement gespeichert sind. Das Speicherelement kann ein optisch variables Element (OVD), optische Speichermedien, ein Hologramm, ein Kinegramm, ein Exelgramm, ein Pixelgramm, einen dreidimensionalen Strichcode, einen zweidimensionalen Strichcode, einen Magnetstreifen und einen Chip umfassen. Das Übertragen der verschlüsselten Nutzlast kann mindestens eines von Einbetten, digitalem Wasserzeichen, Drucken und Codieren verschlüsselter Daten an mindestens einer Stelle auf dem Identifikationsdokument umfassen.

[0009] Die WO 2020/004633 A1 beschreibt einen Authentifizierungskörper, welcher ein blattförmiges Laminierungsblatt umfasst mit einem ersten Bereich, der in dem Laminierungsblatt ausgebildet ist und in dem persönliche Identifikationsinformationen aufgezeichnet sind, und einem zweiten Bereich, der in dem Laminierungsblatt ausgebildet ist und eine Hologrammstruktur aufweist, in welcher Prüfdaten aufgezeichnet sind, die ersten individuellen Informationen zugeordnet sind.

[0010] Es muss vielmehr ferner sichergestellt werden, dass die optisch erfassbaren, personenbezogenen Daten des Dokuments nicht manipuliert sind bzw. eine entsprechende Manipulation schnell und zuverlässig identifiziert werden kann.

Gegenstand der Erfindung

[0011] Der Erfindung liegt die Aufgabe zugrunde, einen verbesserten Ansatz zum Bereitstellen eines Wert- oder Sicherheitsdokument zu schaffen.

[0012] Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Ansprüchen angegeben. Die im Folgenden aufgeführten Ausführungsformen sind frei miteinander kombinierbar, sofern sie sich nicht gegenseitig ausschließen.

[0013] In einem Aspekt betrifft die Erfindung eine Verwendung einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument zur Herstellung des Wert- oder Sicherheitsdokuments. Die elektronische Dokumentenvorlage für das Wert- oder Sicherheitsdokument ist mit einem computerimplementierten Verfahren

erzeugt. Das Verfahren weist auf eine

- Zurverfügungstellung einer Datenbank, in der verschiedenen Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet sind, wobei das optische Lesegerät zur Trennung der Kanäle ausgebildet ist,
- Auswahl einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank und Instanziierung der ausgewählten Typen jeweils durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht des Wert- oder Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs,
- Prüfung des Layoutentwurfs, wobei für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft wird, ob diese einen gemeinsamen der Kanäle belegen, und
- wenn dies der Fall ist, Ausgabe eines Signals und Eingabe einer Korrektur des Layoutentwurfs als Antwort auf das Signal,
- Speicherung des resultierenden korrigierten Layoutentwurfs als die elektronische Dokumentenvorlage.

[0014] Ausführungsformen können den Vorteil haben, dass sie es ermöglichen bereits beim Entwurf eine solcher Dokumente darauf zu achten, dass eine Integritätsprüfung des fertigen Dokuments unter Verwendung eines optischen Lesegerätes auch tatsächlich, insbesondere mit vertretbaren Fehlerwahrscheinlichkeiten, sichergestellt werden kann. Somit kann sichergestellt werden, dass das fertige Dokument bezüglich des optischen Lesegerätes optimiert wird, wodurch es Vermieden werden kann, dass wichtige Merkmale des Dokuments nicht sicher erkannt werden können. Es wird ein Designprozess bereitgestellt, der das System aus Dokument und Inspektions- bzw. Lesegerät berücksichtigt, so dass schon beim Entwurf der Dokumente die Möglichkeiten und Begrenzungen des optischen Lesegerätes und des Herstellungsprozesses berücksichtigt werden können. Insbesondere können so beispielsweise systematische Pseudofehler während der Prozessierung im Feld aufgrund widersprüchlicher Gestaltung von Sicherheitsmerkmalen vermieden werden.

[0015] Ausführungsformen können den Vorteil haben, dass sie es erlauben die zur Verfügung stehenden optischen Sicherheitsmerkmale im Zuge des Entwerfens des Dokumentenlayouts unter Verwendung der Datenbank frei auszuwählen und miteinander zu kombinieren. Falls im Zuge des Entwerfens Sicherheitsmerkmale so instan-

ziiert werden, dass sie räumlich überlappend oder aneinander angrenzend und zugleich einen gemeinsamen Kanal belegen, besteht die Gefahr, dass das optische Lesegerät diese Sicherheitsmerkmale nicht sauber voneinander trennen bzw. voneinander isoliert erfassen kann. Beispielsweise vermag das optische Lesegerät nur eine Überlagerung der entsprechenden Sicherheitsmerkmale zu erfassen, aus welchen es die zugrundeliegenden Sicherheitsmerkmale nicht individuell extrahieren kann. Beispielsweise können in diesem Fall ein oder mehrere dieser Sicherheitsmerkmale von dem optischen Lesegerät nicht oder nicht vollständig erfasst werden.

[0016] Im Zuge einer Validitätsprüfung des Dokuments bestünde die Gefahr, dass die entsprechenden Sicherheitsmerkmale von dem optischen Lesegerät beispielsweise als unvollständig oder als Ganzes fehlend eingestuft werden. Mithin würden die Sicherheitsmerkmale, obwohl vorhanden und valide, durch das optische Lesegerät als invalide eingestuft werden, was zur Folge haben könnte, dass das die Sicherheitsmerkmale aufweisende Dokument fälschlicher Weise als invalide eingestuft werden könnte.

[0017] Würden die entsprechenden Sicherheitsmerkmale bei einer Validitätsprüfung aufgrund der Gefahr einer Falschrückweisung ("False Rejection") vernachlässigt bzw. außer Acht gelassen werden, wäre der Aufwand des Einbringens der entsprechenden Sicherheitsmerkmale in das Dokument umsonst gewesen. Ferner würde durch das Außerachtlassen von Sicherheitsmerkmalen das Sicherheitsniveau des entsprechenden Dokuments beeinträchtigt werden, die Sicherheit des entsprechenden Dokuments könnte aufs Spiel gesetzt werden. Insbesondere bestünde eine erhöhte Gefahr einer Falschakzeptanz eines invaliden Dokuments, welches die entsprechenden Sicherheitsmerkmale gar nicht, in unvollständiger und/oder fehlerhafter Form umfasst. Werden die entsprechenden Sicherheitsmerkmale aber als notwendig für eine Bestätigung der Validität des Dokuments vorausgesetzt, wäre das Dokument durch ein entsprechendes optisches Lesegerät nicht validierbar bzw. verifizierbar. Eine erfolgreiche Validitätsprüfung wäre entweder von vorneherein ausgeschlossen oder aber zumindest störanfällig, da eine hohe Wahrscheinlichkeit einer Falschrückweisung bestehen würde.

[0018] Für ein Sicherheitsmerkmal kann es erforderlich sein, dass durch das optische Lesegerät eine Mehrzahl von vordefinierten charakteristischen Details des zu prüfenden Sicherheitsmerkmals als vorhanden erfasst werden. Beispielsweise wird das Sicherheitsmerkmal mit einer Referenzvorlage verglichen. Ist die Übereinstimmung ausreichend, d.h. stimmt das erfasste Sicherheitsmerkmal und/oder die erfassten charakteristischen Details des Sicherheitsmerkmals mit der Referenzvorlage überein, wird das Sicherheitsmerkmal als vorhanden bzw. valide eingestuft. Eine Übereinstimmung kann beispielsweise eine Identität und/oder eine Übereinstimmung innerhalb eines vordefinierten Toleranzbereichs umfassen.

[0019] Ausführungsformen können den Vorteil haben, dass für ein vorgegebenes optisches Lesegerät bzw. für einen vorgegebenen optischen Lesegerätetyp im Zuge eines Layoutentwurfs geprüft werden kann, ob die instanziierten Sicherheitsmerkmale im Zuge einer Validitätsprüfung mit dem entsprechenden optischen Lesegerät bzw. dem entsprechenden optischen Lesegerätetyp auch tatsächlich erfassbar sind. Falls die Prüfung des Layoutentwurfs positiv ausfällt, d.h. keine potentiell problematischen Sicherheitsmerkmalskombinationen erfasst werden, wird der geprüfte Layoutentwurf als elektronische Dokumentenvorlage gespeichert. Falls die Prüfung negativ ausfällt, d.h. falls im Zuge der Prüfung instanziierte Sicherheitsmerkmale identifiziert werden, welche das Lesegerät nicht individuell auflösen und mithin nicht zu prüfen vermag, wird eine Korrektur des Layoutentwurfs initiiert und der resultierenden korrigierten Layoutentwurf als elektronische Dokumentenvorlage gespeichert.

[0020] Beispielsweise wird der resultierende korrigierte Layoutentwurf nach einer Korrektur als elektronische Dokumentenvorlage gespeichert. Beispielsweise ist ein positives Prüfungsergebnis Voraussetzung für die Speicherung des resultierenden korrigierten Layoutentwurfs. Die Prüfung und Korrektur können im Fall eines negativen Prüfungsergebnisses, beispielsweise mehrmals hintereinander wiederholt werden, bis die Prüfung des korrigierten Layoutentwurfs positiv ausfällt und dieser ohne weitere Korrektur als elektronische Dokumentenvorlage gespeichert wird.

[0021] Ausführungsformen können den Vorteil haben, dass vor der Herstellung eines Dokuments sichergestellt werden kann, dass alle Sicherheitsmerkmale des entsprechenden Dokuments mit dem optischen Lesegerät, welches zur Prüfung des Dokuments vorgesehen ist, validierbar bzw. verifizierbar sind. Insbesondere erübrigen sich Validierungstests des entsprechenden Dokuments mit ein oder mehreren entsprechenden optischen Lesegeräten, welche zum Validieren bzw. Verifizieren des entsprechenden Dokuments vorgesehen sind. Entsprechende Validierungstests können vielmehr durch die Prüfung des Layoutentwurfs noch vor der Herstellung des physischen Dokuments ersetzt werden.

[0022] Nach Ausführungsformen ist es vorgesehen, dass das optische Lesegerät eine gegebene optische Auflösung aufweist und die Prüfung des Layoutentwurfs so erfolgt, dass sie für räumlich durch das optische Lesegerät nicht auflösbare benachbarte Bereiche des Layoutentwurfs durchgeführt wird. Nach Ausführungsformen ist es vorgesehen, dass die Prüfung des Layoutentwurfs so erfolgt, dass sie für räumlich durch das optische Lesegerät nicht auflösbare benachbarte instanziierte Typen von Sicherheitsmerkmalen durchgeführt wird. Nach Ausführungsformen ist es vorgesehen, dass die Prüfung des Layoutentwurfs so erfolgt, dass sie für räumlich durch das optische Lesegerät nicht auflösbare überlappende Bereiche des Layoutentwurfs durchgeführt wird. Nach Ausführungsformen ist es vorgesehen, dass die

Prüfung des Layoutentwurfs so erfolgt, dass sie für räumlich durch das optische Lesegerät nicht auflösbare überlappende instanziierte Typen von Sicherheitsmerkmalen durchgeführt wird.

[0023] Ausführungsformen können den Vorteil haben, dass das optische Auflösungsvermögen des optischen Lesegeräts bei der Prüfung des Layoutentwurfs berücksichtigt wird. Unter Verwendung des optischen Auflösungsvermögens des optischen Lesegeräts können beispielsweise Bereiche des Layoutentwurfs und/oder von dem Layoutentwurf umfasste instanziierte Sicherheitsmerkmale identifiziert werden, für welche eine Prüfung relevant ist. Solange das Auflösungsvermögen des optischen Lesegeräts ausreicht zwei instanziierte Sicherheitsmerkmale als getrennte Sicherheitsmerkmale bzw. zwei Sicherheitsmerkmale umfassende Bereiche des Layoutentwurf als getrennte Bereiche erfassen zu können, wird die Erfassung und Validierung bzw. Verifizierung der entsprechenden Sicherheitsmerkmale beispielsweise nicht dadurch gestört, dass die Sicherheitsmerkmale denselben optischen Kanal belegen. Die räumliche Trennung kann beispielsweise ausreichend sein zur Trennung der entsprechenden Sicherheitsmerkmale. Falls andererseits das optische Auflösungsvermögen für eine räumliche Trennung nicht ausreicht, kann eine Trennung beispielsweise über eine Belegung unterschiedlicher optischer Kanäle erfolgen.

[0024] Beispielsweise handelt es sich bei dem herzustellenden Dokument um ein mehrschichtiges Dokument, welches aus einer Mehrzahl von Schichten aufgebaut ist. Beispielsweise definiert der Layoutentwurf eine Mehrzahl von Schichten, in welchen die Sicherheitsmerkmale instanziiert werden. Beispielsweise werden Sicherheitsmerkmale in unterschiedlichen Schichten, d.h. auf unterschiedlichen Ebenen, des Layoutentwurfs instanziiert. Sicherheitsmerkmale, welche sich überlappen bzw. auf unterschiedlichen Ebenen in überlappenden Bereichen des Layoutentwurfs des Layoutentwurfs angeordnet sind, können von dem optischen Lesegerät beispielsweise nicht räumlich getrennt werden.

[0025] Nach Ausführungsformen handelt es sich bei ein oder mehreren der Kanäle um lesergerätspezifische Kanäle, welche jeweils einem oder mehreren optischen Lesegerätetypen zugeordnet sind. Nach Ausführungsformen umfasst das Verfahren ferner ein Auswählen von ein oder mehreren der Lesegerätetypen für welche der Layoutentwurf geprüft wird. Das Prüfen, ob räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen einen gemeinsamen Kanal belegen, erfolgt jeweils lesergerätetypspezifisch. Das bedeutet, es werden nur gemeinsame Kanäle berücksichtigt, welche einem gemeinsamen Lesegerätetyp zugeordnet sind. Belegen überlappende oder aneinander angrenzende instanziierte Typen von Sicherheitsmerkmalen denselben Kanal, aber jeweils für unterschiedliche Lesegerätetypen, wird beispielsweise kein Signal ausgegeben und mithin keine Korrektur eingegeben.

[0026] Ausführungsformen können den Vorteil haben, dass ein Layoutentwurf für eine Mehrzahl von unterschiedlichen optischen Lesegerätetypen geprüft werden kann. Es kann mithin sichergestellt werden, dass die instanziierten Sicherheitsmerkmale von allen optischen Lesegeräten der Mehrzahl von unterschiedlichen optischen Lesegerätetypen erfasst und für eine Dokumentenvalidierung bzw. -verifizierung verwendet werden können.

[0027] Nach Ausführungsformen ist es vorgesehen, dass eine Herstellung des Wert- oder Sicherheitsdokuments gemäß der elektronischen Dokumentenvorlage hinsichtlich der räumlichen Anordnung der instanziierten optischen Sicherheitsmerkmale Fertigungstoleranzen unterliegt, wobei diese Fertigungstoleranzen in die Ermittlung der räumlich durch das optische Lesegerät nicht auflösbaren überlappenden oder benachbarten Bereiche eingehen. Beispielsweise gehen diese Fertigungstoleranzen in die Ermittlung räumlich durch das optische Lesegerät nicht auflösbarer überlappend oder benachbarter Sicherheitsmerkmale ein.

[0028] Toleranzen können nicht nur empfängerseitig, beispielsweise in Form des Auflösungsvermögens des optischen Lesegeräts auftreten, sondern auch senderseitig. Senderseitige Toleranzen umfassen beispielsweise Fertigungstoleranzen der Sicherheitsmerkmale. Ausführungsformen können den Vorteil haben, dass der senderseitige Einfluss der Fertigungstoleranzen der instanziierten Sicherheitsmerkmale auf die Erfassbarkeit bzw. die Trennbarkeit von Sicherheitsmerkmalen, welche denselben Kanal belegen, bei der Prüfung des Layoutentwurfs berücksichtigt werden können.

[0029] Nach Ausführungsformen ist es vorgesehen, dass den Typen von optischen Sicherheitsmerkmalen in der Datenbank jeweils eine Prüfungsfehlerrate bei Prüfung auf Validität durch das optische Lesegerät zugeordnet ist, wenn das betreffende Sicherheitsmerkmal vereinzelt auftritt, und wobei das Verfahren eine Berechnung einer Gesamtprüfungsfehlerrate für den Layoutentwurf und/oder den resultierenden korrigierten Layoutentwurf. Ausführungsformen können den Vorteil haben, dass anhand der Prüfungsfehlerraten der einzelnen instanziierten Sicherheitsmerkmale eine Gesamtprüfungsfehlerrate für den Layoutentwurf berechnet werden kann. Beispielsweise kann die Prüfung des Layoutentwurfs eine Prüfung der Gesamtprüfungsfehlerrate umfassen. Falls eine für einen Layoutentwurf berechnete Gesamtprüfungsfehler einen vordefinierten Schwellwert überschreitet, erfolgt beispielsweise eine Ausgabe eines Signals und Eingabe einer Korrektur des entsprechenden Layoutentwurfs als Antwort auf das Signal. Der resultierende korrigierte Layoutentwurf wird beispielsweise als die elektronische Dokumentenvorlage gespeichert. Beispielsweise werden die Prüfungsfehlerraten der einzelnen instanziierten Sicherheitsmerkmale zu Berechnung der Gesamtprüfungsfehlerrate aufsummiert. Ein den Prüfungsfehlerraten handelt es sich beispielsweise um Falschakzeptanzraten ("False Acceptance Ra-

tes"/FARs) und/oder Falschrückweisungsrate ("False Rejection Rate"/FRRs). Bei der Gesamtprüfungsfehler-rate handelt es sich beispielsweise um eine Gesamtfalschakzeptanzrate oder um eine Gesamtfalschrückweisungsrate. Beispielsweise werden eine Gesamtfalschakzeptanzrate und eine Gesamtfalschrückweisungsrate berechnet.

[0030] Nach Ausführungsformen ist es vorgesehen, dass die Kanäle ausgewählt sind aus der Gruppe, die gebildet wird von Frequenzkanälen, Kippwinkeln, Anregungswellenlängen, Farbeindrücken und deren Kombinationen. Ein Kanal kann beispielsweise durch eine Frequenz bzw. einen Frequenzbereich, in welchem Sicherheitsmerkmale erfasst werden, definiert sein. Ein Kanal kann beispielsweise durch einen Kippwinkel einer Oberfläche des Dokuments relativ zu einer dem optischen Lesegerät zugeordneten Ebene, unter welchem Sicherheitsmerkmale erfasst werden, definiert sein. Bei der zugeordneten Ebene handelt es sich beispielsweise um eine Bildebene. Der Kippwinkel definiert beispielsweise eine relative Verkippung der Oberfläche des Dokuments, d.h. der Objektebene, relativ zu der Bildebene. Ein Kanal kann beispielsweise durch ein oder mehrere Wellenlängen und/oder Wellenlängenbereiche, mit welchen Sicherheitsmerkmale angeregt werden, definiert sein. Ein Kanal kann beispielsweise durch eine Farbeindruck, mit welchem Sicherheitsmerkmale erfasst werden, definiert sein.

[0031] Nach Ausführungsformen ist es vorgesehen, dass die optischen Sicherheitsmerkmale ausgewählt sind aus der Gruppe, die gebildet wird von Guillochen, Mikro-Schrift, metamere Systeme, Aufdrucken mit Fluoreszenz, Phosphoreszenz und/oder Up-Conversion-Farben, Aufdrucken mit Infrarot-Farbe, Barcodes, insbesondere ein- oder zweidimensionale Barcodes, optisch variablen Farben, transparenten oder reflektierenden Hologrammen oder Kinegrammen, Wasserzeichen, insbesondere digitale Wasserzeichen, die eine maschinell auslesbare Information tragen, Passerdruckelementen, insbesondere Durchsichtspasser, Durchsichtsfenster, Melierfasern, Sicherheitsfäden, Mikroperforationen und deren Kombinationen.

[0032] Nach Ausführungsformen ist es vorgesehen, dass das Verfahren zusätzlich eine Optimierung der Dokumentenvorlage aufweist, vorzugsweise mit Hilfe eines Optimierungsalgorithmus unter Verwendung einer ROC-Kurve oder einer Performance-Kurve unter Berücksichtigung von Fertigungstoleranzen. Beispielsweise wird eine zu optimierende Funktion definiert, welche eine Eigenschaft des Layoutentwurfs definiert, wie etwa eine Erfassbarkeit individueller Sicherheitsmerkmale oder eine Gesamtfehlerrate. Beispielsweise handelt es sich bei der definierten Funktion um eine ROC-Kurve oder einer Performance-Kurve. Die entsprechende Funktion kann beispielsweise unter Berücksichtigung von Fertigungstoleranzen der instanziierten Sicherheitsmerkmale und/oder des Auflösungsvermögens des optischen Lesegeräts definiert werden. Die entsprechende Funktion

wird als Zielfunktion im Zuge des Ausführens des Optimierungsalgorithmus minimiert oder maximiert.

[0033] Ausführungsformen können den Vorteil haben, dass der Layoutentwurf und damit die Dokumentenvorlage optimiert werden können. Mit anderen Worten können Parameter der instanziierten Sicherheitsmerkmale automatisch optimiert und das Ergebnis der Optimierung zur Korrektur bzw. Anpassung des Layoutentwurfs verwendet werden. Beispielsweise kann ein Abstand zwischen Sicherheitsmerkmalen, welche denselben Kanal belegen, optimiert werden. Beispielsweise wird der Abstand minimiert auf einen Minimalabstand, bei welchem die entsprechenden Sicherheitsmerkmale von dem optischen Lesegerät gerade noch trennbar sind. Beispielsweise werden dabei Fertigungstoleranzen der Sicherheitsmerkmale und/oder das Auflösungsvermögen des optischen Lesegeräts berücksichtigt.

[0034] Nach Ausführungsformen ist es vorgesehen, dass das Verfahren zusätzlich eine Platzierung und Skalierung von Sicherheitsmerkmalen aufweist, denen multivariate getrennte Kanäle zugeordnet sind, vorzugsweise unter Kombination der Kanäle Anregungswellenlänge und Farbeindruck, zur Optimierung der Dokumentenvorlage.

[0035] Ausführungsformen können den Vorteil haben, dass bei der Optimierung Platzierung und Skalierung des Sicherheitsmerkmale berücksichtigt wird. Beispielsweise kann ein Abstand zwischen Sicherheitsmerkmalen durch Anpassung der Platzierung und/oder Skalierung ein oder mehrerer der entsprechenden Sicherheitsmerkmale angepasst und mithin optimiert werden. Bei den entsprechenden Sicherheitsmerkmalen handelt es sich um Sicherheitsmerkmale, welche denselben Kanal belegen. Beispielsweise handelt es sich bei den entsprechenden Sicherheitsmerkmalen um Sicherheitsmerkmale, welche getrennte Kanäle belegen. Bei den Kanälen handelt es sich beispielsweise um multivariante Kanäle. Die Optimierung der Dokumentenvorlage hinsichtlich der Platzierung und Skalierung von Sicherheitsmerkmalen kann beispielsweise darauf abzielen, ein Übersprechen zwischen getrennten Kanälen, zu verhindern.

[0036] Beispielsweise wird das Wert- oder Sicherheitsdokument unter Verwendung der elektronischen Dokumentenvorlage hergestellt. Die elektronische Dokumentenvorlage wird beispielsweise einem Fertigungssystem für Dokumente, wie etwa Wert- oder Sicherheitsdokumente, zur Verfügung gestellt. Beispielsweise umfasst das Fertigungssystem ein elektronisches Entwurfssystem, auf welchem die Dokumentenvorlage erstellt wird. Beispielsweise wird die Dokumentenvorlage vom dem Entwurfssystem über ein Netzwerk an das Fertigungssystem gesendet. Beispielsweise wird die Dokumentenvorlage dem Fertigungssystem auf einem Wechselspeichermedium zur Verfügung gestellt.

[0037] Ein elektronische Entwurfssystem umfasst beispielsweise ein Drucksystem zum Drucken des Dokuments. Falls es sich bei dem Dokument um ein personalisiertes Dokument, wie etwa ein Ausweisdokument, han-

delt umfasst das Entwurfssystem beispielsweise ein Personalisierungssystem zur Personalisierung eines Dokumentenrohlings zur Herstellung des entsprechenden personalisierten Dokuments, wie etwa einem personalisierten Wert- oder Sicherheitsdokument. Nach Ausführungsformen der Erfindung kann der Dokumentenkörper eine Mehrzahl von Materialschichten umfassen, wobei ein oder mehrere der Materialschichten jeweils einzelnen personalisiert werden. Beispielsweise werden alle Materialschichten der Mehrzahl von Materialschichten jeweils einzeln personalisiert. Beispielsweise umfasst die Mehrzahl von Materialschichten ein oder mehrere Materialschichten, welche nicht personalisiert werden. Die Mehrzahl von Materialschichten wird beispielsweise nach der Personalisierung der ein oder mehreren Materialschichten zu dem Dokumentkörper zusammengefügt. Beispielsweise wird die Mehrzahl von Materialschichten laminiert, um den Dokumentenkörper aus der Mehrzahl von Materialschichten zu formen. Der resultierende Dokumentenkörper umfasst somit ein oder mehrere jeweils einzeln personalisierte Materialschichten. Beispielsweise sind alle Materialschichten des resultierenden Dokumentenkörpers jeweils einzeln personalisiert. Beispielsweise umfasst der resultierende Dokumentenkörper ein oder mehrere Materialschichten, welche nicht personalisiert sind. Nach Ausführungsformen der Erfindung kann der Dokumentenkörper aus mehreren Materialschichten bestehen, die jeweils einzeln personalisiert und dann laminiert werden, um den Dokumentenkörper aus den personalisierten Schichten zu formen. Beispielsweise ist das Personalisierungssystem dazu konfiguriert Personalisierungsdaten in den zu personalisierenden Dokumentenrohling einzubringen. Die Personalisierungsdaten umfassen beispielsweise Attribute eines Inhabers des Dokuments, wie etwa einen Namen, eine Anschrift etc. Ferner umfassen die Personalisierungsdaten beispielsweise biometrische Daten des Inhabers, wie etwa ein Gesichtsfoto oder Fingerabdruckdaten. Beispielsweise werden die Personalisierungsdaten auf das Dokument bzw. auf eine Dokumentenschicht gedruckt. Beispielsweise umfassen ein oder mehrere der Sicherheitsmerkmale jeweils Personalisierungsdaten des Inhabers. Beispielsweise umfasst das Drucksystem das Personalisierungssystem zum Drucken von Personalisierungsdaten. Beispielsweise umfasst das Dokument einen Speicher, in welchem das Personalisierungssystem die Personalisierungsdaten speichert.

[0038] Beispielsweise handelt es sich bei dem Dokument um einen Verbundkörper, welcher eine Mehrzahl von Materialschichten bzw. Materialbögen umfasst. Beispielsweise sind die Sicherheitsmerkmale auf ein oder mehrere der Materialschichten angeordnet. Beispielsweise werden Sicherheitsmerkmale in ein oder mehrere der Materialschichten eingebracht. Beispielsweise werden Sicherheitsmerkmale auf ein oder mehrere der Materialschichten aufgedruckt. Die Mehrzahl von Materialbögen wird im Zuge der Herstellung des Dokuments beispielsweise in einer dokumentenspezifischen Reihenfol-

ge aufeinander angeordnet zu einem Materialbogenheft, aus welchem, beispielsweise mittels Laminierens, ein Verbundkörper erzeugt wird.

[0039] Beispielsweise umfassen ein oder mehrere der Sicherheitsmerkmale Daten, welche für einen Zugriff auf einen von dem Dokument umfassten Speicher benötigt werden. Beispielsweise handelt es sich bei einem oder mehreren der geprüften Sicherheitsmerkmale um ein Sicherheitsmerkmal, welches entsprechende Daten umfasst. Das optische Lesegerät erfasst beispielsweise die entsprechenden Sicherheitsmerkmale. Ein das optische Lesegerät umfassendes Daten-Lesegerät extrahiert die entsprechenden Daten aus dem erfassten Sicherheitsmerkmal. Unter Verwendung der entsprechenden Daten leitet das Daten-Lesegerät beispielsweise einen kryptographischen Schlüssel ab. Diesen kryptographischen Schlüssel verwendet das Daten-Lesegerät bei einem Ausführen eines kryptographischen Protokolls zum Aufschließen des Speichers des Dokuments, d.h. zum Erlangen eines Zugriffs auf den Speicher, aus welchem das Daten-Lesegerät Daten unter Verwendung einer kontaktbehafteten oder kontaktlosen Kommunikationsschnittstelle ausliest.

[0040] In einem weiteren Aspekt betrifft die Erfindung eine Kombination aus einer elektronischen Dokumentenvorlage für ein Wert -oder Sicherheitsdokument und dem Wert -oder Sicherheitsdokument, welches hergestellt ist unter Verwendung der Dokumentenvorlage. Die elektronische Dokumentenvorlage für das Wert -oder Sicherheitsdokument ist mit einem Verfahren erzeugt, welches aufweist

- Zurverfügungstellung einer Datenbank, in der verschiedenen Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet sind, wobei das optische Lesegerät zur Trennung der Kanäle ausgebildet ist,
- Auswahl einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank und Instanziierung der ausgewählten Typen jeweils durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht des Wert- oder Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs,
- Prüfung des Layoutentwurfs, wobei für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft wird, ob diese einen gemeinsamen der Kanäle belegen, und
- wenn dies der Fall ist, Ausgabe eines Signals und Eingabe einer Korrektur des Layoutentwurfs als Antwort auf das Signal,

- Speicherung des resultierenden korrigierten Layoutentwurfs als die elektronische Dokumentenvorlage.

[0041] Das Wert- oder Sicherheitsdokument ist hergestellt unter Verwendung einer solchen Dokumentenvorlage. Das Wert- oder Sicherheitsdokument umfasst beispielsweise eine mehrschichtigen Verbundkörper.

[0042] Das Wert- oder Sicherheitsdokument weist beispielsweise einen integrierten elektronischen Schaltkreis und einen elektronischen Speicher zur Speicherung von schutzbedürftigen Daten und Mittel zur Ausführung eines kryptographischen Protokolls auf und eine Schnittstelle zu einem Daten-Lesegerät, die einen Zugriff des Daten-Lesegeräts auf die schutzbedürftigen Daten nach Ausführung des kryptographischen Protokolls ermöglicht.

[0043] Gemäß einer bevorzugten Ausführungsform ist die Ausführung des kryptographischen Protokolls nur unter Verwendung eines optischen Sicherheitsmerkmals dieses Dokuments möglich.

[0044] Beispielsweise ist in einem elektronischen Entwurfssystem für Dokumentenvorlagen mit einem Prozessor und einer Speichereinrichtung ein Computerprogramm gespeichert, dessen Ausführung durch den Prozessor die Durchführung eines erfindungsgemäßen Verfahrens bewirkt.

[0045] Beispielsweise weist ein Fertigungssystem für Wert- oder Sicherheitsdokumente ein elektronisches Entwurfssystem sowie ein Drucksystem für den Wert- oder Sicherheitsdruck und/oder ein Personalisierungssystem zur Personalisierung von Dokumentenrohlingen zur Herstellung der Wert- oder Sicherheitsdokumente auf.

[0046] Beispielsweise ist das Wert- oder Sicherheitsdokument mit einem Verfahren hergestellt, welches ein Prozess zur Erstellung eines prüfoptimierten Dokumenten-Layouts ist, dessen Basis vorzugsweise die Darstellung aller Merkmale anhand von Trägern (Supports), belegter Empfangskanäle und Prüfausprägung ist.

[0047] Dieser Prozess stellt Merkmale, Formulare und/oder Produktionsdaten in Datenbanken zur Verfügung. Das gewünschte Layout wird erstellt und der Anwender kann dabei unterstützt werden. Innerhalb einer Prüfroutine wird vorzugsweise die lokale Belegung aller Kanäle und die zu erwartende Performance anhand einer ROC Kurve oder einer Merit Funktion analysiert. Ist das Ergebnis prozesssicher, kann das Layout verwendet werden und die vorhandenen Daten werden vorzugsweise direkt an die Druckvorstufe bzw. ein Drucksystem zum Drucken des Dokuments gesendet. Ansonsten bietet sich die Möglichkeit einer Nacharbeit bis zur Zielerreichung. Beispielsweise erfolgt eine iterative Wiederholung von Korrektur und Prüfung des Layoutentwurfs, bis die Prüfung auf potentiell problematische Merkmalskombinationen positiv ausfällt und keine problematische Merkmalskombinationen gefunden werden. Die Prüfroutine beinhaltet vorzugsweise auch Tests zur maximalen Flächen- und Kanalbelegung des Dokuments, des Ver-

hältnisses von personenbezogenen Daten zu statischen Merkmalen und reinen ästhetischen Emblemen, beispielsweise Designelementen, eine Abschätzung der Prozessierbarkeit und der erwarteten Falschakzeptanzrate (FAR("False Acceptance Rate")) Wert) und der Falschrückweisungsrate (FRR("False Rejection Rate")) Wert) im Feld anhand bekannter externer Daten und Performance Kurven, zur Fertigbarkeit aufgrund von Flächenbelegung und Verwendung von Sondermaterialien und/oder zu den zu erwarteten Kosten des finalen Dokuments.

[0048] Im Zusammenhang mit der Beschreibung der vorliegenden Erfindung und ihrer Ausführungsbeispiele werden die nachstehenden Begriffe wie folgend definiert: Ein "Dokument" ist ein physisches Objekt, zum Beispiel eine papierbasierte oder kunststoffbasierte Karte mit oder ohne einen integrierten Schaltkreis, wie etwa einen Chip, welche eine Identität oder eine Eigenschaft oder ein Recht des Inhabers des Dokuments nachweist. Ein Dokument kann insbesondere ein Wert- oder Sicherheitsdokument sein.

[0049] Beispiele für Wertaspekte sind Geldscheine. Ein Identitätsdokument ist ein Dokument, welches Angaben bezüglich der Identität seines Besitzers (Name, Adresse, Gesichtsbild, Unterschrift, etc.) beinhaltet. Ein Identitätsdokument kann zum Beispiel einen Personalausweis, ein Reisepass, ein Mitarbeiterausweis oder ein personalisiertes Wertaspekte (zum Beispiel Kreditkarte) sein. Dokumente beinhalten oftmals Sicherheitsmerkmale wie zum Beispiel Gesichtsbilder, Hologramme, Prüfschlangen, kryptographische Schlüssel oder dergleichen.

[0050] Eine "Dokumentenvorlage" ist ein elektronisch auf einem Entwurfssystem gespeichertes Daten-Objekt mit dessen Hilfe ein Dokument erzeugt werden kann, dessen Eigenschaften durch die Dokumentvorlage bestimmt sind.

[0051] Ein "Layoutelement" ist ein Element eines Layouts eines Dokuments bzw. einer Dokumentenvorlage, das optische Sicherheitsmerkmale aufweist. Unterschiedliche Typen von Layoutelementen weisen unterschiedliche optische Sicherheitsmerkmale oder Kombinationen solcher Sicherheitsmerkmale auf.

[0052] "Optische Sicherheitsmerkmale" sind Eigenschaften eines Dokuments, mit deren Hilfe die Echtheit oder die Integrität eines Dokuments unter Verwendung eines optischen Lesegeräts geprüft werden kann, das solche Sicherheitsmerkmale aufweist. Beispiele für solche Sicherheitsmerkmale sind Guillochen, Mikro-Schrift, metamere Systeme, Aufdrucken mit Fluoreszenz-, Phosphoreszenz- und/oder Up-Conversion-Farben, Aufdrucken mit Infrarot-Farben, Barcodes, insbesondere ein- oder zweidimensionale Barcodes, optisch variable Farben, transparente oder reflektierende Hologramme oder Kinegramme, Wasserzeichen, insbesondere digitale Wasserzeichen, die eine maschinell auslesbare Information tragen, Passerdruckelemente, insbesondere Durchsichtspasser, Durchsichtsfenster, Melierfasern, Sicher-

heitsfäden, Mikroperforationen und deren Kombinationen. Ein Merkmal belegt einen oder mehrere Kanäle je nach Definition (CMYK vs. RGB). Ein Merkmal hat eine Fläche, die als Träger (Support) benötigt wird, um das Merkmal aufzubringen und ungestört darzustellen. Ein Merkmal hat pro Kanal eine Struktur, die es zu prüfen gilt. Merkmale sind in einer Datenbank mit Information zu belegten Kanälen, Flächenausprägung, Struktur und Prüfbedingung hinterlegt. Merkmale können im Layout grundsätzlich beliebig angeordnet werden, wobei ein Überlapp von Merkmalen verboten sein kann.

[0053] Unter einer "Datenbank" wird hier ein Container und/oder System zur Speicherung und Verwaltung elektronischer Daten verstanden. Vorzugsweise ist die Datenbank eine dokument-externe Datenbank, die die Bildreferenzdaten und optional auch weitere Referenzdaten für eine Vielzahl von Dokumenten speichert. Eine Datenbank kann also z.B. als Verzeichnis oder Verzeichnisbaum ausgebildet sein. Vorzugsweise handelt es sich bei einer Datenbank jedoch um ein Datenbanksystem, das dafür ausgebildet ist, große Datenmengen effizient, widerspruchsfrei und dauerhaft zu speichern und benötigte Teilmengen in unterschiedlichen, bedarfsgerechten Darstellungsformen für Benutzer und Anwendungsprogramme bereitzustellen. Nach Ausführungsformen besteht ein Datenbanksystem aus zwei Teilen: der Verwaltungssoftware, genannt Datenbankmanagementsystem (DBMS), und der Menge der zu verwaltenden Daten, der Datenbank (DB) im engeren Sinn, zum Teil auch "Datenbasis" genannt. Die Verwaltungssoftware organisiert intern die strukturierte Speicherung der Daten und kontrolliert alle lesenden und schreibenden Zugriffe auf die Datenbank. Zur Abfrage und Verwaltung der Daten bietet ein Datenbanksystem eine Datenbanksprache an. Beispiel für Datenbanken sind eine Merkmalsdatenbank (Kanäle, Träger (Support), Ausprägung), eine Formulardatenbank (Formular, Datengruppen) und eine Fertigungsdatenbank (Fertigungstoleranzen, Prozessgrenzen).

[0054] Ein "Optisches Lesegerät" ist eine Vorrichtung zur optischen Erfassung eines Dokuments, insbesondere zur optischen Erfassung eines Sicherheitsmerkmals eines solchen Dokuments.

[0055] Ein "Daten-Lesegerät" ist eine Vorrichtung zum Lesen von Daten aus einem elektronischen Speicher. Ein Daten-Lesegerät kann mit einem optischen Lesegerät in einem Lesegerät, etwa in Form eines Terminals, untergebracht sein.

[0056] Ein "Kanal zur optischen Erfassung eines Sicherheitsmerkmals" ist durch die spezifischen optischen Eigenschaften eines Sicherheitsmerkmals definiert. Beispiele für Kanäle in diesem Sinne sind Frequenzkanälen, Kippwinkeln, Anregungswellenlängen, Farbeindrücken und deren Kombinationen. Typischerweise (z.B. gemäß der "ICAO - Best Practice Guidelines for Optical Machine Authentication", Version 1.2, Februar 2018) werden Bilder im Vis, UV und IR aufgenommen. Erweiterungen insbesondere im Bereich holographischer Darstellungen

sind denkbar. Damit ergeben sich im Sichtbaren ("Visible" = Vis) beispielsweise 3 Kanäle VisR, VisG, VisB, d.h. Rot, Grün und Blau. Der UV-Bereich kann ebenfalls in Teilbereiche aufgeteilt werden. Beispielsweise wird der UV-Bereich in drei Teilbereiche analog zu den sichtbaren Kanälen VisR, VisG, VisB aufgeteilt, welche als UVR, UVG, UVB bezeichnet werden. Der UV-Teilbereich mit den größten Wellenlängen wird als "roter" UV-Bereich UVR bezeichnet, der mittlere UV-Teilbereich mit mittleren Wellenlängen als "grüner" UV-Bereich UVG und der UV-Teilbereich mit den kleinsten Wellenlängen als "blauer" UV-Bereich UVB. Ferner ergeben sich der IR Kanal und ein Holo-Kanal. Da in jedem Kanal sowohl statische als auch personalisierte Merkmale auftreten können, ergeben sich insgesamt in dieser Ausprägung beispielsweise 16 Kanäle.

[0057] Unter der "Trennung der Kanäle" ist eine nach Kanälen getrennte Erfassung der optischen Sicherheitsmerkmale durch ein optisches Lesegerät zu verstehen. Beispielsweise können unterschiedliche optische Sensoren Signale unterschiedlicher Kanäle getrennt erfassen und verarbeiten oder einer getrennten Verarbeitung zuführen. Die Trennung von Kanälen wird u.a. durch das sogenannte Übersprechen oder Nebensprechen erschwert. Ein Merkmal besetzt regelmäßig eine bestimmte Anzahl von Kanälen. Eine gelbe UV-Farbe kann beispielsweise die Kanäle UVG und UVR belegen, ein gelaserter Text belegt beispielsweise alle Kanäle. Die Anforderung an die Trennbarkeit bedeutet nun, dass innerhalb der einzelnen Kanäle Merkmale nicht überlappen oder zu nahe aneinander Angrenzen. Eine Ausnahme bilden gelegentlich Texte und Codes, die direkt decodiert werden. Diese können aus den entsprechenden Kanälen mit einem Vorwissen über ein Formular, einen Decoder und/oder eine Ausprägung auch wieder herausgerechnet werden. Eine formale Beschreibung der Trennbarkeit zweier Merkmale M_i und M_j mit den Trägern (Supports) $\text{supp}(M_{\text{Channel}_i})$ bzw. $\text{supp}(M_{\text{Channel}_j})$ führt dann innerhalb eines Kanals (Channel) auf eine Bedingung der Form: $\text{supp}(M_{\text{Channel}_i}) \cap \text{supp}(M_{\text{Channel}_j}) = \emptyset$, wobei $\text{supp}(M_{\text{Channel}_i}) = \{x_{\text{Channel}_i}, y_{\text{Channel}_i} | M_{\text{Channel}_i} > 0\}$ und x_{Channel_i} bzw. y_{Channel_i} die Koordinaten von Bildpunkten in einer zweidimensionalen Dokumentenebene bzw. Erfassungsebene sind.

[0058] "Übersprechen oder Nebensprechen", ist ein Begriff aus der Telefonie und bezeichnet ursprünglich einen Effekt, durch den man am Telefon ein anderes Gespräch leise mithören kann - daher der Name. Heute wird der Begriff in der Nachrichtentechnik allgemein für die unerwünschte gegenseitige Beeinflussung eigentlich unabhängiger Signalkanäle verwendet.

[0059] Unter der "Instanziierung ausgewählter Typen von optischen Sicherheitsmerkmalen" ist die Inklusion von Vertretern solcher Typen von optischen Sicherheitsmerkmalen in eine Dokumentvorlage beim Entwurf dieser Dokumentvorlage zu verstehen.

[0060] Unter der "Platzierung und Skalierung" ist die örtliche Platzierung und Wahl einer konkreten Dimensi-

onierung der Abmessungen eines optischen Sicherheitsmerkmals im Layout einer Dokumentenvorlage bei dessen Instanziierung zu verstehen.

[0061] Eine "Dokumententrägerschicht eines Wert- oder Sicherheitsdokuments" ist eine Schicht in, an oder auf dem Körper des Wert- oder Sicherheitsdokuments, welche die Informationen des Dokuments, insbesondere dessen optische Sicherheitsmerkmale trägt.

[0062] Eine "elektronische Repräsentation einer Dokumententrägerschicht" ist der Layoutentwurf der Dokumententrägerschicht eines Dokuments, der in einer Speichereinrichtung eines Entwurfssystems für Dokumentenvorlagen gespeichert ist.

[0063] Eine "Layoutentwurf" ist ein Datensatz, in dem die instanziierten optischen Sicherheitsmerkmale eines Dokuments und deren Platzierung und Skalierung gespeichert sind.

[0064] "Gemeinsame Kanäle" sind Kanäle, die in einer Datenbank, in der verschiedenen Typen von optischen Sicherheitsmerkmalen Kanäle zugeordnet sind, mehr als nur einem dieser Typen von optischen Sicherheitsmerkmalen zugeordnet sind.

[0065] Eine "Eingabe einer Korrektur des Layoutentwurfs" ist die Neuangabe eines berichtigten oder die Korrektur eines vorhandenen, korrekturbedürftigen Layoutentwurfs durch den Entwerfer (den "Designer") des Layoutentwurfs.

[0066] Die "Optische Auflösung eines optischen Lesegeräts" ist hier der minimale Abstand zweier Strukturen insbesondere von Sicherheitsmerkmalen in einem Dokumentenlayout, der gerade noch die räumliche Auflösung (Trennung) dieser beiden Strukturen in einem von diesem optischen Lesegerät aufgenommen Bild erlaubt. Das Auflösungsvermögen wird beispielsweise durch Angabe eines Winkelabstandes bzw. einer Winkelauflösung oder durch Angabe eines Abstandes zwischen gerade noch trennbaren Strukturen quantifiziert.

[0067] "Fertigungstoleranzen" sind hier ungewollte Abweichungen der tatsächlichen Werte von Layoutparametern wie beispielsweise Lagen, Größen oder optischen Merkmalen von den Sollwerten dieser Layoutparameter.

[0068] Eine "Prüfungsfehlerrate" (auch Fehlerrate, Fehlerquotient, Fehlerdichte, Fehlerquote oder Fehlerhäufigkeit) ist bei der Prüfung von Dokumenten oder Dokumentenvorlagen der relative Anteil von fehlerhaften Elementen im Verhältnis zur Gesamtheit, also die relative Häufigkeit, mit der ein Fehler vorliegt. Dabei wird häufig insbesondere zwischen falsch positiven und falsch negativen Prüfungsergebnissen unterschieden. Den Typen von optischen Sicherheitsmerkmalen in der Datenbank ist beispielsweise jeweils eine Prüfungsfehlerrate bei Prüfung auf Validität durch das optische Lesegerät zugeordnet.

[0069] Eine "Gesamtprüfungsfehlerrate" für einen Layoutentwurf und/oder ein resultierendes Layout wird aus den einzelnen Prüfungsfehlerraten der in dem Layout(entwurf) instanziierten Typen von Sicherheitsmerk-

malen nach den Regeln der Wahrscheinlichkeitsrechnung berechnet. Ein Layout wird erstellt und in Prüfkä-
nälen dargestellt. Aufgrund bekannter Performance Er-
fahrungen (ROC-Kurve oder ähnliches) wird ein Erwart-
ungswert für Feldtests erstellt. Herstellungsspezifisches
Know-how kann bei der Anordnung von Merkmalen
ebenfalls mit bewertet werden (z.B. Farbdeckung). Ins-
besondere biometrische Merkmale können besonders
gewichtet werden.

[0070] Eine "ROC-Kurve" (ROC: englisch für receiver
operating characteristic bzw. deutsch Operationscharak-
teristik eines Beobachters), auch Grenzwertoptimie-
rungskurve oder Isosensitivitätskurve genannt, ist eine
Methode zur Bewertung und Optimierung von Analyse-
strategien. Die ROC-Kurve stellt visuell die Abhängigkeit
der Effizienz mit der Fehlerrate für verschiedene Para-
meterwerte dar. Sie ist eine Anwendung der Signalent-
deckungstheorie.

[0071] Die ROC-Kurve kann eingesetzt werden, um
den bestmöglichen Wert eines Parameters zu finden,
beispielsweise bei einem dichotomen (semi-)quantitati-
ven Merkmal oder Zwei-Klassen-Klassifizierungsprob-
lem. Für jeden möglichen Parameterwert (z. B. Sende-
geschwindigkeit, Frequenz, ...) ermittelt man die resul-
tierenden relativen Häufigkeitsverteilungen in Form von
Sensitivität (Richtig-Positiv-Rate) und Falsch-Positiv-
Rate. In einem Diagramm oder in einer digital gespei-
cherten Tabelle trägt man vorzugsweise die Sensitivität
(Richtig-Positiv-Rate) als Ordinate ("y-Achse") und die
Falsch-Positiv-Rate als Abszisse ("x-Achse") ein. Der
Parameterwert selbst taucht dabei nicht auf, kann aber
als Beschriftung oder digitales Label der Punkte verwen-
det werden. Es resultiert typischerweise ein Zusammen-
hang, der einer gekrümmten, aufsteigenden Kurve ent-
spricht. Eine ROC-Kurve nahe der Diagonalen deutet auf
einen Zufallsprozess hin: Werte nahe der Diagonalen be-
deuten eine gleiche Trefferquote und Falschpositivquo-
te, was der zu erwartenden Trefferhäufigkeit eines Zu-
fallsprozesses entspricht. Die ideale ROC-Kurve steigt
zunächst (fast) senkrecht an (die Trefferquote liegt nahe
bei 100 %, während die Fehlerquote anfangs noch nahe
bei 0 % bleibt), erst danach steigt die Falsch-Positiv-Rate
an. Eine ROC-Kurve, die deutlich unterhalb der Diago-
nalen bleibt, deutet darauf hin, dass die Werte falsch in-
terpretiert wurden. Das theoretische Optimum (im Sinne
eines Kompromisses aus Treffer- und Fehlerrate) des
getesteten Wertes ermittelt man dann visuell oder com-
putergestützt aus dem Kontaktpunkt einer diagonal an-
steigenden Tangente mit der ROC-Kurve.

[0072] Zeichnet man die Testwerte (beispielsweise in
Abhängigkeit von der Falsch-Positiv-Rate) in das gleiche
Diagramm, findet sich der Grenzwert als Lot des Kon-
taktpunktes der Tangente auf die Testwertekurve. Alter-
nativ können die Punkte der Kurve mit dem Testwert be-
schrieben werden. Rechnerisch sucht man den Testwert
mit dem höchsten Youden-Index. Dieser berechnet sich
aus Sensitivität+Spezifität-1.

[0073] Eine "Merit Funktion" bzw. Leistungsfunktion

bezeichnet eine Funktion, welche eine Übereinstimmung zwischen Daten und einem Anpassungsmodell bzw. Fitting Modell für eine bestimmte Auswahl der Parameter misst. Gemäß allgemeiner Konvention ist die Leistungsfunktion beispielsweise klein, wenn die Übereinstimmung hoch ist. Beispielsweise im Zuge einer Regression können Parameter basierend auf dem Wert der Merit Funktion angepasst werden, bis ein kleinster Wert erhalten wird, wodurch eine optimale Anpassung der entsprechenden Parameter erzeugt wird, die den kleinsten Wert der Merit Funktion ergibt. Mit anderen Worten können die entsprechenden Parameter optimiert werden, indem die Merit Funktion minimiert wird. Das Resultat der entsprechenden Optimierung sind optimale bzw. optimierte Parameterwerte.

[0074] Zum Bestimmen der Einflüsse von Parametern der instanziierten Sicherheitsmerkmale des Layoutentwurfs und/oder von Parametern des optischen Lesegeräts auf die Trennbarkeit der instanziierten Sicherheitsmerkmale durch das optische Lesegerät wird beispielsweise ein bayessches Netzwerk bzw. Modell verwendet. Ein bayessches Netzwerk bezeichnet einen gerichteten azyklischen Graphen, in dem die Knoten Zufallsvariablen und die Kanten bedingte Abhängigkeiten zwischen den Variablen beschreiben. Jedem Knoten des Netzes ist eine bedingte Wahrscheinlichkeitsverteilung der durch ihn repräsentierten Zufallsvariable gegeben, die Zufallsvariablen an den Elternknoten zuordnet. Ein bayessches Netz dient dazu, die gemeinsame Wahrscheinlichkeitsverteilung aller beteiligten Variablen unter Ausnutzung bekannter bedingter Unabhängigkeiten möglichst kompakt zu repräsentieren. Dabei wird die bedingte (Un)abhängigkeit von Untermengen der Variablen mit A-priori-Wissen kombiniert. Ist von manchen der Variablen der Wert bekannt, d. h. liegt Evidenz vor, so kann mit Hilfe verschiedener Algorithmen auch die bedingte Wahrscheinlichkeitsverteilung von Zufallsvariablen mit den gegebenen Variablen berechnet und damit Inferenz betrieben werden. Für eine approximative Inferenz kann beispielsweise ein Monte-Carlo-Algorithmus verwendet werden.

[0075] Eine "Frequenzkanal" ist ein optischer Kanal, der durch eine Frequenz, durch mehrere Frequenzen oder durch ein Spektrum von optischen Frequenzen in oder außerhalb des sichtbaren Bereichs elektromagnetischer Strahlung definiert ist.

[0076] "Kippwinkel" sind im Zusammenhang mit dem Kippeffekt von Bedeutung, der ein mögliches Sicherheitsmerkmal von Wert- oder Sicherheitsdokumenten, insbesondere von Banknoten sein kann. Dadurch kann man einerseits erreichen, dass die betreffende Stelle des Geldscheins aus verschiedenen Blickwinkeln unterschiedlich aussieht (unterschiedliche Farbtöne oder Motive); andererseits können auf das linke und das rechte Auge unterschiedliche Bilder geworfen werden, um einen 3D-Effekt zu bewirken. Der Kippeffekt kann durch Prägedruck oder Linsenrasterbilder erzeugt werden; ein wichtiges Beispiel ist das sogenannte Kinegramm. Ein

Kinegramm oder Kinegram ist eine Technologie zum Schutz gegen Fälschungen von Banknoten, Metallbarren, Reisepässen, Visa und Identitätskarten mittels Kippeffekt. Es wird sicherheitstechnisch als "OVD" (Optically Variable Device = optisch variables Merkmal) bezeichnet. Anders als beim Hologramm, das dreidimensionale Elemente besitzt, stellen die meist silbrig glänzenden Kinegramme einen zweidimensionalen Bewegungsablauf dar. Der Name ist vom Begriff Kinematik abgeleitet, weil je nach Winkel der Betrachtung des Kinegramms ein fest definierter filmähnlicher Ablauf stattfindet.

[0077] Ein durch "Anregungswellenlängen" definierter Kanal ist durch die Wellenlängen des diskreten oder kontinuierlichen Spektrums einer Lichtquelle definiert, mit der ein Dokument im optischen Lesegerät beleuchtet wird. Diese Anregungswellenlängen müssen nicht mit den vom beleuchteten Dokument emittierten Spektren identisch sein. Dies ist beispielsweise bei der Fluoreszenz, der Phosphoreszenz und/oder bei den Up-Conversion-Farben nicht der Fall.

[0078] Ein durch "Farbeindrücke" definierter Kanal ist durch die optischen Farbeindrücke eines Beobachters definiert. Der optische Eindruck eines Beobachters ergibt sich dabei als das Produkt aus der Reflektion oder Remission, der Beleuchtungsstärke und der spektralen Empfindlichkeit.

[0079] Unter einem "optischen Sensor" wird hier ein Sensor bezeichnet, welcher dazu ausgebildet ist, ein oder mehrere Bilder eines physischen Objekts, z.B. eines Dokuments oder eines Teils eines Dokuments, zu erfassen. Die Bilder können insbesondere digitale Bilder sein. Der optische Sensor kann z.B. eine Kamera oder eine Videokamera sein. Der optische Sensor kann z.B. dazu ausgebildet sein, selektiv Licht eines bestimmten Wellenlängenbereichs zu erfassen, z.B. Infrarotlicht (IR-Licht) oder Licht im für das menschliche Auge sichtbaren Wellenlängenbereich (Weißlicht, Tageslicht). Vorzugsweise handelt es sich bei den erfassten Bildern um digitale Bilder, die elektronisch gespeichert und/oder ein das Bild weiterverarbeitendes System gesendet werden.

[0080] Unter einem "Gesichtsbild" wird hier ein Bild, insbesondere ein digitales Bild, verstanden, welches das Gesicht einer Person abbildet.

[0081] Ein "digitales Bild" ist ein Datensatz, in dem Bildinhalte repräsentiert und gespeichert werden. Insbesondere kann es sich bei dem digitalen Bild um einen Datensatz handeln, in dem der Inhalt eines Bildes durch ganze Zahlen repräsentiert wird. Insbesondere kann es sich bei dem digitalen Bild um eine Rastergraphik handeln.

[0082] Unter einem "System" ist hier eine Gesamtheit aus ein oder mehreren System-Elementen zu verstehen, die in der Lage ist, Daten zu verarbeiten. Beispielsweise kann ein System einen Computer umfassen, oder ein verteiltes Computersystem, das z.B. als Cloud-Computersystem ausgebildet ist. Es ist auch möglich, dass einzelne Komponenten des Systems oder das gesamte System in einer dezidierten Hardware implementiert

sind. Beispielsweise kann das Prüfsystem komplett in ein Terminal integriert sein, welches neben einer oder mehreren Kameras auch ein oder mehrere Beleuchtungssysteme und eine Kopie der Datenbank mit den Referenzdaten beinhaltet. Es ist aber auch möglich, dass einzelne Komponenten, wie z.B. die Datenbank, von einer Terminal-externen Komponente bereitgestellt werden, beispielsweise über einen per Netzwerkverbindung mit dem Terminal verbundenen Datenbankserver.

Kurze Beschreibung der Figuren

[0083] Nachfolgend werden Ausführungsformen der Erfindung mit Bezug auf die Figuren beschrieben. Es zeigen:

Figur 1 ein schematisches Diagramm eines exemplarischen Layoutentwurfs eines Dokuments oder einer Dokumentvorlage,

Figur 2 ein schematisches Diagramm einer exemplarischen Zuordnung von Kanälen zu Merkmalen;

Figur 3 ein Flussdiagramm eines exemplarischen Verfahrens,

Figur 4 ein schematisches Diagramm eines exemplarischen Dokuments mit einem integrierten elektronischen Schaltkreis,

Figur 5 ein schematisches Diagramm eines exemplarischen Entwurfssystems zum Erzeugen von elektronischen Dokumentenvorlagen und

Figur 6 ein schematisches Diagramm eines exemplarischen Fertigungssystems zum Herstellen eines Dokuments unter Verwendung einer elektronischen Dokumentenvorlagen.

[0084] Wie in der Figur 1 beispielhaft und in schematischer Weise dargestellt, weist ein exemplarischer Layoutentwurf 100 eines Dokument 101 oder einer elektronischen Dokumentvorlage eine Mehrzahl von Layoutelementen auf. Beispielsweise umfasst der Layoutentwurf 100 eine Mehrzahl von Typen von optischen Sicherheitsmerkmalen 104 bis 108, welche in dem Layoutentwurf 100 instanziiert sind. Die Sicherheitsmerkmale können auf derselben Ebene bzw. Schicht des Dokuments platziert und gegebenenfalls skaliert werden oder, im Fall eines mehrschichtigen Dokuments, auf verschiedenen übereinander angeordneten Schichten. Ein optisches Lesegerät erfasst beispielsweise die Oberseite eines entsprechenden Dokuments. Dabei sind die Sicherheitsmerkmale beispielsweise in einer Erfassungsebene einer Dokumententrägerschicht verteilt, welche durch zwei Achsen 102, 103 eines x-, y-Koordinatensystems aufgespannt wird. Dabei können ein oder mehrere Sicherheitsmerkmale beispielsweise überlappend angeordnet sein,

wie etwa die exemplarischen Sicherheitsmerkmale 105 und 107 bzw. 106 und 108 in der Figur 1. Die optischen Sicherheitsmerkmalen können beispielsweise textuelle Merkmale (Textfelder) 104 oder andere Typen von optischen Sicherheitsmerkmalen umfassen. Sicherheitsmerkmale können beispielsweise aneinander angrenzend angeordnet sein, wie etwa die exemplarischen Sicherheitsmerkmale 107 und 108, sodass sie sich berühren. Sicherheitsmerkmale können ferner auch vollständig disjunkte Träger aufweisen, wie beispielsweise die Sicherheitsmerkmale 106 und 105 bzw. 107 und 106 in Figur 1.

[0085] Falls sich überlappende optische Sicherheitsmerkmale, wie beispielsweise die Sicherheitsmerkmale 106 und 108, denselben Kanal belegen, besteht die Gefahr, dass ein optisches Lesegerät, welches versucht ein Dokument mit den entsprechend instanziierten Sicherheitsmerkmalen zu validieren bzw. zu verifizieren, die Sicherheitsmerkmale nicht auseinander zu halten bzw. voneinander zu trennen vermag. Beispielsweise kommt das optische Lesegerät zu dem Ergebnis, dass eines oder beide Sicherheitsmerkmale unvollständig und damit invalide sind. Dasselbe Problem kann beispielsweise bei aneinander angrenzend angeordneten Sicherheitsmerkmalen, wie etwa den Sicherheitsmerkmalen 107 und 108, auftreten. Ist ein Auflösungsvermögen des optischen Lesegerätes nicht ausreichend, um die Grenze bzw. einen geringfügigen Abstand zwischen den entsprechenden Sicherheitsmerkmalen aufzulösen, vermag das optische Lesegerät diese Sicherheitsmerkmale ebenfalls nicht auseinander zu halten bzw. voneinander zu trennen. Auch in diesem Fall könnte das optische Lesegerät zu dem Ergebnis gelangen, dass eines oder beide Sicherheitsmerkmale unvollständig und damit invalide sind.

[0086] Wie in der Figur 2 beispielhaft und in schematischer Weise dargestellt, belegen die optischen Sicherheitsmerkmale M_1 und M_2 unterschiedlichen Kanäle. Das optische Sicherheitsmerkmal M_1 ist beispielsweise den Kanälen mit den Kanalnummern 6 und 11 zugeordnet, während das optische Sicherheitsmerkmal M_2 beispielsweise dem Kanal mit der Kanalnummer 5 zugeordnet ist. Bei den optischen Sicherheitsmerkmalen M_1 und M_2 handelt es sich beispielsweise um Sicherheitsmerkmale, welche vollständig disjunkte Träger aufweisen, d.h. vollständig überlappings- und berührungsfreie (disjunkte) Bereiche des Layoutentwurfs belegen. Die Kanalnummern sind an der vertikalen Achse 201 aufgetragen. Die horizontalen x- bzw. y-Achsen 203 bzw. 202 spannen die Erfassungsebene auf.

[0087] Wie in der Figur 3 beispielhaft und in schematischer Weise dargestellt, weist das exemplarische Verfahren zur Erzeugung einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument die folgenden Schritte auf:

In Schritt 301 wird eine Datenbank DB zur Verfügung gestellt. Die Datenbank ordnet verschiedene Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung mit einem optischen

Lesegerät zu. Das entsprechende optische Lesegerät ist beispielsweise zur Trennung der Kanäle ausgebildet. In Schritt 302 wird eine einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank ausgewählt. Die ausgewählten optischen Sicherheitsmerkmale werden im Zuge ihrer Instanziierung auf einer elektronischen Repräsentation einer Dokumententrägerschicht des zu entwerfenden Dokuments, beispielsweise eines Wert- oder Sicherheitsdokuments, zur Erzeugung eines Layoutentwurfs platziert und gegebenenfalls skaliert.

[0088] Der so erstellte Layoutentwurf mit den instanziierten optischen Sicherheitsmerkmalen wird in Schritt 303 geprüft. Im Zuge der Prüfung wird für räumlich überlappende oder aneinander angrenzende der instanziierten Sicherheitsmerkmale geprüft, ob diese einen gemeinsamen der Kanäle belegen. Falls das Ergebnis negativ ist und die Prüfung ergibt, dass potentiell problematische überlappende oder aneinander angrenzende Sicherheitsmerkmale vorhanden sind, erfolgt in Schritt 304 eine Korrektur des Entwurfs. Beispielsweise wird ein Signal ausgegeben bzw. gesendet, welches mögliche problematische Kombinationen von Sicherheitsmerkmalen identifiziert. In Antwort auf das entsprechende Signal wird beispielsweise eine Korrektur des Layoutentwurf eingegeben bzw. empfangen. Beispielsweise wird das Signal in Form eines Konflikthinweises, welcher die möglichen problematischen Kombinationen von Sicherheitsmerkmalen identifiziert, auf einer Anzeigevorrichtung einer Nutzerschnittstelle angezeigt. Über eine Eingabevorrichtung der Nutzerschnittstelle werden beispielsweise Korrekturbefehle empfangen. Eine Korrektur problematischer Kombinationen von Sicherheitsmerkmalen kann beispielsweise ein Beabstanden der entsprechenden Sicherheitsmerkmale auf der Dokumententrägerschicht voneinander umfassen. Dabei wird der Abstand beispielsweise so gewählt, dass die entsprechenden Sicherheitsmerkmale unter Berücksichtigung von Fertigungstoleranzen und/oder Auflösungsvermögen des optischen Lesegerätes von dem entsprechenden Lesegerät getrennt werden können, obwohl sie denselben Kanal belegen. Eine entsprechende Beanstandung kann beispielsweise durch Anpassung der Platzierung der Sicherheitsmerkmale erfolgen und/oder durch ein Reskalieren der Sicherheitsmerkmale, im Zuge dessen sie verkleinert werden. Ferner kann die Korrektur ein Ersetzen ein oder mehrerer der Sicherheitsmerkmale durch Sicherheitsmerkmale anderen Typs umfassen, welcher einen anderen Kanal belegt. Schließlich kann eine Korrektur ein Weglassen bzw. ein Entfernen eines der instanziierten Sicherheitsmerkmale aus dem Layoutentwurf umfassen.

[0089] Beispielsweise kann der Konflikthinweis ein oder mehrere automatisch erstellte Korrekturvorschläge umfassen. Die Korrekturvorschläge können beispielsweise hierarchisch geordnet erstellt und ausgegeben werden. Soweit möglich kann ein erster Vorschlag beispielsweise eine Änderung der Platzierung von instanziierten Sicherheitsmerkmalen vorschlagen, ein zweiter

Vorschlag kann beispielsweise eine Änderung der Skalierung von instanziierten Sicherheitsmerkmalen vorschlagen, ein dritter Vorschlag kann beispielsweise Ersetzungsvorschläge zum Ersetzen von instanziierten Sicherheitsmerkmalen mit Sicherheitsmerkmalen eines anderen Typs, welcher einen anderen Kanal belegt, umfassen, ein vierter Vorschlag kann beispielsweise ein Entfernen von ein oder mehreren der instanziierten Sicherheitsmerkmale vorschlagen. Die in Antwort auf den Konflikthinweis empfangene Eingabe identifiziert beispielsweise einen der Korrekturvorschläge, welcher zur Korrektur des Layoutentwurfs zu implementieren ist. Auf den Empfang der entsprechenden Eingabe wird der Layoutentwurf gemäß der Eingabe korrigiert.

[0090] Nach Ausführungsformen können die Prüf- und Korrekturschritte 303, 304 beispielsweise auch in den Auswahlschritt 302 integriert sein, d.h. während des Erstellens des Layoutentwurfs ausgeführt werden. Beispielsweise erfolgt eine entsprechende Prüfung im Zuge des Instanziiierens jedes der Sicherheitsmerkmale. Wird ein optisches Sicherheitsmerkmal ausgewählt und auf der elektronischen Repräsentation der Dokumententrägerschicht angeordnet, wird beispielsweise geprüft, ob dieses optische Sicherheitsmerkmal ein weiteres optisches Sicherheitsmerkmal überlappt oder an ein weiteres optisches Sicherheitsmerkmal angrenzt, welches denselben Kanal wie das ausgewählte Sicherheitsmerkmal belegt. Ist dies der Fall, wird ein Signal mit einem Konflikthinweis ausgegeben. Beispielsweise werden die potential konfliktbelasteten Sicherheitsmerkmale in einer visuellen Darstellung der elektronischen Repräsentation der Dokumententrägerschicht auf der Ausgabevorrichtung der Nutzerschnittstelle visuell, etwa farblich, hervorgehoben. Beispielsweise werden zusätzlich ein oder mehrere Korrekturvorschläge zur Behebung des Konflikts angezeigt. Dies könnte den Vorteil haben, dass der Layoutentwurf schrittweise im Zuge seiner Erstellung korrigiert werden kann. Somit kann sichergestellt werden, dass der fertiggestellte Layoutentwurf konfliktfrei ist und in Schritt 305 ohne weitere Korrekturen als Dokumentenvorlage gespeichert werden kann.

[0091] Beispielsweise wird nach jeder Korrektur des Layoutentwurfs in Schritt 304 die Prüfung gemäß Schritt 303 wiederholt, um zu prüfen, ob durch die Korrektur sämtliche Konflikte hinsichtlich überlappender oder aneinander angrenzender Sicherheitsmerkmale desselben Kanals behoben wurden. Dies kann es ermöglichen, dass die Korrektur des Layoutentwurfs iterativ erfolgt.

[0092] Falls die Prüfung in Schritt 303 positiv ausfällt, d.h. keine überlappenden oder aneinander angrenzenden Sicherheitsmerkmale desselben Kanals vorliegen, erfolgt in Schritt 305 eine Speicherung des Layoutentwurfs als elektronische Dokumentenvorlage. Bei dem gespeicherten Layoutentwurf kann es sich um einen unveränderten Layoutentwurf handeln, falls die Prüfung in Schritt 303 positiv ausgefallen ist, d.h. keine Konflikte aufgetreten sind, oder um einen ein oder mehrfach korrigierten Layoutentwurf, falls in vorangegangenen Prü-

fungsschritten Konflikte aufgefunden und korrigiert wurden.

[0093] Wie in der Figur 4 beispielhaft und in schematischer Weise dargestellt, weist eine Ausführungsform eines Dokuments 101, etwa eines Wert- oder Sicherheitsdokuments, einen integrierten elektronischen Schaltkreis 402 auf. Der integrierten elektronischen Schaltkreis 402 umfasst beispielsweise einen elektronischen Speicher 403 zur Speicherung von schutzbedürftigen Daten sowie einen Prozessor 404, welcher zum Ausführen eines kryptographischen Protokolls 407 konfiguriert ist. Das kryptographische Protokoll 407 ist beispielsweise in Form von ausführbaren Programminstruktionen implementiert. Ferner umfasst das Dokument 101 eine Kommunikationsschnittstelle 405 zur Kommunikation mit einem Terminal 411 bzw. mit einer Kommunikationsschnittstelle 415 eines als Daten-Lesegerät konfigurierten bzw. ein Daten-Lesegerät umfassenden Terminals 411. Schließlich umfasst das Dokument 101 eine Mehrzahl von optischen Sicherheitsmerkmalen 408, welche beispielsweise unter Verwendung einer gemäß dem Verfahren der Figur 3 erzeugten elektronischen Dokumentenvorlage, in dem Dokuments 101 instanziiert wurden. Die Mehrzahl von optischen Sicherheitsmerkmalen 408 umfasst beispielsweise verschiedene Typen optischer Sicherheitsmerkmale, welche verschiedene Kanäle belegen bzw. über verschiedene Kanäle erfassbar sind.

[0094] Das exemplarische Terminal 411 umfasst beispielsweise einen elektronischen Schaltkreis 412 mit einem elektronischen Speicher 413 zum Speichern von Daten sowie einen Prozessor 414, welcher zum Ausführen eines kryptographischen Protokolls 417 konfiguriert ist. Das kryptographische Protokoll 417 ist beispielsweise in Form von ausführbaren Programminstruktionen implementiert. Ferner umfasst das Terminal 411 beispielsweise eine Kommunikationsschnittstelle 415 zur Kommunikation mit dem Dokument 101 bzw. mit der Kommunikationsschnittstelle 405 des Dokuments 101. Schließlich umfasst das Terminal 411 ein optisches Lesegerät 416 bzw. optischen Sensor zur Erfassung optischer Sicherheitsmerkmale 408 des Dokuments 101. Das optische Lesegerät 416 ist dazu konfiguriert optische Sicherheitsmerkmale unter Verwendung unterschiedlicher Kanäle zu erfassen. Beispielsweise umfasst das optische Lesegerät 416 eine Mehrzahl unterschiedlicher optischer Sensoren, welche dazu konfiguriert sind optische Sicherheitsmerkmale jeweils über unterschiedliche Kanäle zu erfassen. Beispielsweise umfasst das optische Lesegerät 416 ein oder mehrere optische Sensoren, welche jeweils dazu konfiguriert eine Mehrzahl von Kanälen zur Erfassung von optischen Sicherheitsmerkmalen zu verwenden.

[0095] Beispielsweise ist der Prozessor 414 des Terminals 411 dazu konfiguriert das optische Lesegerät 416 zur Erfassung der Mehrzahl von optischen Sicherheitsmerkmalen 408 zu steuern. Die erfassten Sicherheitsmerkmale 408 werden von dem Terminal 411 auf ihre

Validität hin überprüft. Beispielsweise werden die erfassten optischen Daten der Sicherheitsmerkmalen 408 mit Referenzdaten verglichen, welche in dem Speicher 413 des Terminals hinterlegt sind. Bei einer ausreichenden Übereinstimmung der erfassten optischen Daten mit den hinterlegten Referenzdaten werden die Sicherheitsmerkmale 408 und damit das Dokument 101 als valide und authentisch eingestuft. Beispielsweise umfassen ein oder mehrere der Sicherheitsmerkmale 408 Daten, welche von dem Terminals 411 aus den mittels des optischen Lesegeräts 416 erfassten Daten extrahiert werden. Unter Verwendung der extrahierten Daten leitet der Prozessor 414 im Zuge des Ausführens des kryptographischen Protokolls 417 beispielsweise einen kryptographischen Schlüssel ab, welcher das Dokument 101 aufschließt und dem Terminal 411 einen Zugriff auf die schutzbedürftigen Daten in dem elektronischen Speicher 403 des Dokuments 411 erlaubt. Unter Verwendung des abgeleiteten Schlüssels kann das Terminal 411 nachweisen, dass das Dokument 101 tatsächlich für eine optische Prüfung vorliegt. Somit können heimliche Leseversuche, etwa ohne dass das Dokument 101 von dem Besitzer willentlich für diesen Zweck vorgelegt wird, verhindert werden.

[0096] Beispielsweise muss das Terminal zusätzlich ein Berechtigungszertifikat vorweisen, welches Zugriffsrechte des Terminals 411 definiert. Beispielsweise legt das Berechtigungszertifikat Datenkategorien fest, für welche das Terminal 411 Leserechte besitzt. Beispielsweise sendet das Terminal 411 das Berechtigungszertifikat im Zuge einer Authentisierung gegenüber dem Dokument 101 über die Kommunikationsschnittstelle 415 an die Kommunikationsschnittstelle 405 des Dokuments 101. Ferner weist das Terminal 411 beispielsweise unter Verwendung eines Challenge-Response-Verfahrens einen Besitz eines privaten kryptographischen Schlüssels nach dessen zugehöriger öffentlicher kryptographischer Schlüssel den in dem Berechtigungszertifikat definierten Leserechten zugeordnet ist. Falls das Terminal 411 seine Leseberechtigung und/oder den aus den Sicherheitsmerkmalen 408 abgeleiteten Schlüssel vorlegen kann, erhält es beispielsweise einen Lesezugriff auf die schutzbedürftigen Daten in dem Speicher 403 des Dokuments 101 und kann diese über die Kommunikationsschnittstellen 405, 415 auslesen. Seitens des Dokuments 101 erfolgt eine Prüfung der von dem Terminal 411 vorgelegten Daten zum Nachweis der Zugriffs- bzw. Leseberechtigung beispielsweise durch den Prozessor 404 unter Verwendung des kryptographischen Protokolls 407.

[0097] Wie in der Figur 5 beispielhaft und in schematischer Weise dargestellt, weist eine Ausführungsform eines elektronischen Entwurfssystems 500 zum Erzeugen von elektronischen Dokumentenvorlagen beispielsweise einen Prozessor 502 auf, welcher dazu konfiguriert ist Programminstruktionen 504 eines Computerprogramms zum Erzeugen einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument auszuführen. Ferner umfasst das elektronische Entwurfs-

system 500 beispielsweise eine Speichereinrichtung 503 und eine Kommunikationsschnittstelle 504. Des Weiteren umfasst das elektronische Entwurfssystem 500 beispielsweise eine Ausgabevorrichtung 505, wie etwa ein Display, sowie Eingabevorrichtungen 506, wie etwa Maus und/oder Tastatur. Ferner hat das elektronische Entwurfssystem 500 beispielsweise Zugriff auf eine Datenbank 507. Die Datenbank 507 kann beispielsweise von der Speichereinrichtung 503 des elektronischen Entwurfssystems 500 umfasst sein oder es kann sich um eine entfernte Datenbank handeln, auf welche das elektronische Entwurfssystem 500 über die Kommunikationsschnittstelle 503 und beispielsweise ein Netzwerk, etwa ein Intranet oder das Internet, zugreift. In der Datenbank 507 sind beispielsweise verschiedenen Typen von optischen Sicherheitsmerkmalen T1, T2, T3, ..., TN gespeichert. Den verschiedenen Typen von optischen Sicherheitsmerkmalen T1, T2, T3, ..., TN sind beispielsweise jeweils ein oder mehrere Kanäle K1, K2, K3 zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet. Beispielsweise können den verschiedenen Typen von optischen Sicherheitsmerkmalen T1, T2, T3, ..., TN für verschiedene Typen von optischen Lesegeräten verschiedene Kanäle zur optischen Erfassung zugeordnet sein. Beispielsweise kann die Datenbank 507 ferner Angaben zu Fertigungstoleranz der optischen Sicherheitsmerkmalen T1, T2, T3, ..., TN und/oder zum Auflösungsvermögen des oder der optischen Lesegeräte umfassen. Schließlich kann die Datenbank 507 Angaben zu Prüfungsfehlerraten für die verschiedenen Typen von optischen Sicherheitsmerkmalen T1, T2, T3, ..., TN, wie etwa Falschakzeptanzraten und/oder Falschrückweisungsrate, umfassen. Beispielsweise sind die Prüfungsfehlerraten der verschiedenen Typen von optischen Sicherheitsmerkmalen T1, T2, T3, ..., TN jeweils einem bestimmten Typ von optischem Lesegerät zugeordnet bzw. gelten nur für den entsprechenden Typ. Entsprechende Angaben können beispielsweise auch in verschiedenen Datenbanken gespeichert sein. Beispielsweise kann das elektronische Entwurfssystem 500 neben der Datenbank 507, bei welcher es sich beispielsweise um eine Merkmalsdatenbank handelt, Zugriff auf eine separate Formulardatenbank besitzen, welche für herzustellende Dokumente Formularvorgaben bereitstellt, wie etwa Vorgaben zur inhaltlichen Anordnung und Strukturierung von Daten des Dokuments sowie zu Datengruppen, welche das entsprechende Dokument umfassen soll. Ferner kann das elektronische Entwurfssystem 500 beispielsweise Zugriff auf eine separate Fertigungsdatenbank besitzen, welche beispielsweise Angaben zu Fertigungstoleranzen und/oder Prozessgrenzen umfasst.

[0098] Das elektronische Entwurfssystem 500 ist dazu konfiguriert, einem Nutzer eine Auswahl einer Mehrzahl von Typen der optischen Sicherheitsmerkmale T1, T2, T3, ..., TN aus der Datenbank 507 zu ermöglichen sowie eine Instanziierung der ausgewählten Typen jeweils

durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht eines Wert- oder Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs. Hierzu kann der Nutzer über die Eingabevorrichtungen 506 Eingaben vornehmen, deren Ergebnis, etwa in Form des Layoutentwurfs, dem Nutzer mittels der Ausgabevorrichtung 505 angezeigt werden. Das elektronische Entwurfssystem 500 ist ferner dazu konfiguriert eine Prüfung des Layoutentwurfs auszuführen. Dabei wird beispielsweise für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft, ob diese einen gemeinsamen der Kanäle belegen. Falls dies der Fall ist, erfolgt eine Ausgabe eines Signals, beispielsweise über die Ausgabevorrichtung 505, und ein Empfang einer Eingabe einer Korrektur des Layoutentwurfs als Antwort auf das Signal über die Eingabevorrichtungen 506. Der resultierende korrigierte Layoutentwurf wird beispielsweise als elektronische Dokumentenvorlage zur Herstellung eines entsprechenden Dokuments, d.h. Wert- oder Sicherheitsdokuments, in der Speichereinrichtung 503 gespeichert.

[0099] Wie in der Figur 6 beispielhaft und in schematischer Weise dargestellt, weist eine Ausführungsform eines Fertigungssystems 600 für Wert- oder Sicherheitsdokumente 101 ein elektronisches Entwurfssystem 500, wie beispielsweise aus Figur 5, auf. Ferner weist das Fertigungssystem 600 beispielsweise ein Drucksystem 602 für den Wert- oder Sicherheitsdruck auf. Das elektronische Entwurfssystem 500 stellt dem Drucksystem 602 die elektronische Druckvorlage bereit. Ferner werden Materialbögen 601 zur Herstellung des Dokuments 101 bereitgestellt. Das Drucksystem 602 bedruckt die Materialbögen 601 gemäß den Vorgaben der elektronischen Druckvorlage. Diese Materialbögen 601 werden im Falle eines mehrschichtigen Dokuments beispielsweise zu einem Materialbogenheft zusammengefügt, aus welchem beispielsweise mittels Laminierens das Dokument 101 bzw. den Dokumentenkörper des Dokuments 101 erzeugt wird. Falls es sich bei dem Dokument 101 um ein personalisiertes Dokument handelt, welches einem individuellen Inhaber zugeordnet ist, umfasst das Fertigungssystem 600 beispielsweise ferner ein Personalisierungssystem 604 zur Personalisierung von Dokumentenrohlingen 605 zur Herstellung personalisierter Dokumente 101, wie etwa Wert- oder Sicherheitsdokumente. Beispielsweise werden im Zuge der Personalisierung persönliche bzw. personenbezogene Daten des Inhabers auf den Dokumentenrohlingen 605 oder einen der Materialbögen 603 gedruckt. In diesem Fall kann das Personalisierungssystem 604 beispielsweise in das Drucksystem 602 integriert sein. Zusätzlich oder alternativ können von dem Personalisierungssystem 604 persönliche bzw. personenbezogene Daten des Inhabers in einen elektronischen Speicher des Dokumentenrohlings 605 eingebracht werden.

[0100] Beispiele können die folgenden Merkmalskom-

binationen umfassen:

1. Verfahren zur Erzeugung einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument, aufweisend eine
 - Zurverfügungstellung einer Datenbank, in der verschiedenen Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet sind, wobei das optische Lesegerät zur Trennung der Kanäle ausgebildet ist,
 - Auswahl einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank und Instanziierung der ausgewählten Typen jeweils durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht des Wert- oder Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs,
 - Prüfung des Layoutentwurfs, wobei für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft wird, ob diese einen gemeinsamen der Kanäle belegen, und
 - wenn dies der Fall ist, Ausgabe eines Signals und Eingabe einer Korrektur des Layoutentwurfs als Antwort auf das Signal,
 - Speicherung des resultierenden korrigierten Layoutentwurfs als die elektronische Dokumentenvorlage.
2. Verfahren nach Merkmalskombination 1, wobei das optische Lesegerät eine gegebene optische Auflösung aufweist und wobei die Prüfung des Layoutentwurfs so erfolgt, dass sie für räumlich durch das optische Lesegerät nicht auflösbare überlappende oder benachbarte Bereiche des Layoutentwurfs durchgeführt wird.
3. Verfahren nach Merkmalskombination 2, wobei eine Herstellung des Wert- oder Sicherheitsdokuments gemäß der elektronischen Dokumentenvorlage hinsichtlich der räumlichen Anordnung der instanziierten optischen Sicherheitsmerkmale Fertigungstoleranzen unterliegt, wobei diese Fertigungstoleranzen in die Ermittlung der räumlich durch das optische Lesegerät nicht auflösbaren überlappenden oder benachbarten Bereiche eingehen.
4. Verfahren nach einem der vorhergehenden Merkmalskombinationen, wobei den Typen von optischen Sicherheitsmerkmalen in der Datenbank jeweils eine Prüfungsfehlerrate bei Prüfung auf Validität durch das optische Lesegerät zugeordnet ist, wenn das

betreffende Sicherheitsmerkmal vereinzelt auftritt, und mit einer Berechnung einer Gesamtprüfungsfehlerrate für den Layoutentwurf und/oder den resultierenden korrigierten Layoutentwurf.

5. Verfahren nach einem der vorhergehenden Merkmalskombinationen, wobei die Kanäle ausgewählt sind aus der Gruppe, die gebildet wird von Frequenzkanälen, Kippwinkeln, Anregungswellenlängen, Farbeindrücken, optischer Auflösung und deren Kombinationen.

6. Verfahren nach einem der vorhergehenden Merkmalskombinationen, wobei die optischen Sicherheitsmerkmale ausgewählt sind aus der Gruppe, die gebildet wird von Guillochen, Mikro-Schrift, metamere Systeme, Aufdrucken mit Fluoreszenz, Phosphoreszenz und/oder Up-Conversion-Farben, Aufdrucken mit Infrarot-Farbe, Barcodes, insbesondere ein- oder zweidimensionale Barcodes, optisch variablen Farben, transparenten oder reflektierenden Hologrammen oder Kinegrammen, Wasserzeichen, insbesondere digitale Wasserzeichen, die eine maschinell auslesbare Information tragen, Passerdruckelementen, insbesondere Durchsichtspasser, Durchsichtsfenster, Melierfasern, Sicherheitsfäden, Mikroperforationen und deren Kombinationen.

7. Verfahren nach einem der vorhergehenden Merkmalskombinationen, aufweisend eine Optimierung der Dokumentenvorlage, vorzugsweise mit Hilfe eines Optimierungsalgorithmus unter Verwendung einer ROC-Kurve oder einer Performance-Kurve unter Berücksichtigung von Fertigungstoleranzen.

8. Verfahren nach Merkmalskombination 7, aufweisend eine Platzierung und Skalierung von Sicherheitsmerkmalen, denen multivariate getrennte Kanäle zugeordnet sind, vorzugsweise unter Kombination der Kanäle Anregungswellenlänge und Farbeindruck, zur Optimierung der Dokumentenvorlage.

9. Verfahren nach einem der vorhergehenden Merkmalskombinationen, ferner aufweisend eine Herstellung des Wert- oder Sicherheitsdokument unter Verwendung der elektronischen Dokumentenvorlage.

10. Elektronische Dokumentenvorlage für ein Wert- oder Sicherheitsdokument, erzeugt mit einem Verfahren nach einem der vorhergehenden Merkmalskombinationen.

11. Wert- oder Sicherheitsdokument, hergestellt unter Verwendung einer Dokumentenvorlage nach Merkmalskombination 10.

12. Wert- oder Sicherheitsdokument nach Merkmalskombination 10, aufweisend einen integrierten

elektronischen Schaltkreis und einen elektronischen Speicher zur Speicherung von schutzbedürftigen Daten und Mittel zur Ausführung eines kryptographischen Protokolls, und mit einer Schnittstelle zu einem Daten-Lesegerät, die einen Zugriff des Daten-Lesegeräts auf die schutzbedürftigen Daten nach Ausführung des kryptographischen Protokolls ermöglicht.

13. Wert- oder Sicherheitsdokument nach Merkmalskombination 12, bei dem die Ausführung des kryptographischen Protokolls nur unter Verwendung eines optischen Sicherheitsmerkmals dieses Dokuments möglich ist.

14. Elektronisches Entwurfssystem für Dokumentenvorlagen mit einem Prozessor und einer Speichereinrichtung, in der ein Computerprogramm gespeichert ist, dessen Ausführung durch den Prozessor die Durchführung eines Verfahrens nach einem der Merkmalskombinationen 1 bis 9 bewirkt.

15. Fertigungssystem für Wert- oder Sicherheitsdokumente gemäß einem der Merkmalskombinationen 11 bis 13 mit einem elektronischen Entwurfssystem nach Merkmalskombination 14, aufweisend ein Drucksystem für den Wert- oder Sicherheitsdruck und/oder ein Personalisierungssystem zur Personalisierung von Dokumentenrohlingen zur Herstellung der Wert- oder Sicherheitsdokumente.

Bezugszeichenliste

[0101]

100	Layoutentwurf	
101	Dokument	
102	y-Achse eines Koordinatensystems in der Dokumentebene	
103	x-Achse eines Koordinatensystems in der Dokumentebene	40
104	Textfeld, Sicherheitsmerkmal in Textform	
105 bis 108	optische Sicherheitsmerkmale	
M ₁ ^{6,11}	optisches Sicherheitsmerkmal 1 mit den Kanälen 6 und 11	45
M ₂ ⁵	optisches Sicherheitsmerkmal 2 mit Kanal 5	
201	Achse der Kanalnummern	
202	y-Achse eines Koordinatensystems in der Dokumentebene	50
203	x-Achse eines Koordinatensystems in der Dokumentebene	
301 bis 305	Verfahrensschritte	
DB	Datenbank	55
402	integrierter Schaltkreis	
403	Speicher	
404	Prozessor	

405	Kommunikationsschnittstelle
407	kryptographisches Protokoll
408	optische Sicherheitsmerkmale
411	Terminal
5 412	Schaltkreis
413	Speicher
414	Prozessor
415	Kommunikationsschnittstelle
417	kryptographisches Protokoll
10 416	optische Lesegerät
500	elektronisches Entwurfssystem
501	Prozessor
502	Programminstruktionen
503	Speichereinrichtung
15 504	Kommunikationsschnittstelle
505	Ausgabevorrichtung
506	Eingabevorrichtung
507	Datenbank
T1 bis TN	Typen von Sicherheitsmerkmalen
20 K1 bis KN	Kanäle
600	Fertigungssystem 600
601	Materialbogen
602	Drucksystem
604	Personalisierungssystem
25 605	Dokumentenrohling

Patentansprüche

- 30 1. Verwendung einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument zur Herstellung des Wert- oder Sicherheitsdokuments, wobei die elektronische Dokumentenvorlage für das Wert- oder Sicherheitsdokument erzeugt ist mit einem Verfahren, aufweisend eine
- 35
- Zurverfügungstellung (301) einer Datenbank (DB), in der verschiedenen Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet sind, wobei das optische Lesegerät zur Trennung der Kanäle ausgebildet ist,
 - Auswahl (302) einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank und Instanziierung der ausgewählten Typen jeweils durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht des Wert- oder Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs,
 - Prüfung (303) des Layoutentwurfs, wobei für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft wird, ob diese einen gemeinsamen der Kanäle belegen, und

- wenn dies der Fall ist, Ausgabe eines Signals und Eingabe einer Korrektur (304) des Layoutentwurfs als Antwort auf das Signal,
- Speicherung (305) des resultierenden korrigierten Layoutentwurfs als die elektronische Dokumentenvorlage.
2. Verwendung nach Anspruch 1, wobei bei dem Erzeugen der elektronischen Dokumentenvorlage das optische Lesegerät eine gegebene optische Auflösung aufweist und wobei die Prüfung des Layoutentwurfs so erfolgt, dass sie für räumlich durch das optische Lesegerät nicht auflösbare überlappende oder benachbarte Bereiche des Layoutentwurfs durchgeführt wird. 10
 3. Verwendung nach Anspruch 2, wobei die Herstellung des Wert- oder Sicherheitsdokuments gemäß der elektronischen Dokumentenvorlage hinsichtlich der räumlichen Anordnung der instanziierten optischen Sicherheitsmerkmale Fertigungstoleranzen unterliegt, wobei diese Fertigungstoleranzen in die Ermittlung der räumlich durch das optische Lesegerät nicht auflösbaren überlappenden oder benachbarten Bereiche eingehen. 20
 4. Verwendung nach einem der vorhergehenden Ansprüche, wobei bei dem Erzeugen der elektronischen Dokumentenvorlage den Typen von optischen Sicherheitsmerkmalen in der Datenbank jeweils eine Prüfungsfehlerrate bei Prüfung auf Validität durch das optische Lesegerät zugeordnet ist, wenn das betreffende Sicherheitsmerkmal vereinzelt auftritt, und mit einer Berechnung einer Gesamtprüfungsfehlerrate für den Layoutentwurf und/oder den resultierenden korrigierten Layoutentwurf. 30
 5. Verwendung nach einem der vorhergehenden Ansprüche, wobei die Kanäle ausgewählt sind aus der Gruppe, die gebildet wird von Frequenzkanälen, Kippwinkeln, Anregungswellenlängen, Farbeindrücken, optischer Auflösung und deren Kombinationen. 40
 6. Verwendung nach einem der vorhergehenden Ansprüche, wobei die optischen Sicherheitsmerkmale ausgewählt sind aus der Gruppe, die gebildet wird von Guillochen, Mikro-Schrift, metamere Systeme, Aufdrucken mit Fluoreszenz, Phosphoreszenz und/oder Up-Conversion-Farben, Aufdrucken mit Infrarot-Farbe, Barcodes, insbesondere ein- oder zweidimensionale Barcodes, optisch variablen Farben, transparenten oder reflektierenden Hologrammen oder Kinegrammen, Wasserzeichen, insbesondere digitale Wasserzeichen, die eine maschinell auslesbare Information tragen, Passerdruckelementen, insbesondere Durchsichtspasser, Durchsichtsfenster, Melierfasern, Sicherheitsfäden, Mikroperforationen und deren Kombinationen. 50
 7. Verwendung nach einem der vorhergehenden Ansprüche, wobei das Erzeugen der elektronischen Dokumentenvorlage eine Optimierung der Dokumentenvorlage aufweist, vorzugsweise mit Hilfe eines Optimierungsalgorithmus unter Verwendung einer ROC-Kurve oder einer Performance-Kurve unter Berücksichtigung von Fertigungstoleranzen. 5
 8. Verwendung nach Anspruch 7, wobei das Erzeugen der elektronischen Dokumentenvorlage eine Platzierung und Skalierung von Sicherheitsmerkmalen aufweist, denen multivariate getrennte Kanäle zugeordnet sind, vorzugsweise unter Kombination der Kanäle Anregungswellenlänge und Farbeindruck, zur Optimierung der Dokumentenvorlage. 15
 9. Verwendung nach einem der vorhergehenden Ansprüche, wobei das Wert- oder Sicherheitsdokument (401) einen integrierten elektronischen Schaltkreis (402) und einen elektronischen Speicher (403) zur Speicherung von schutzbedürftigen Daten und Mittel (404) zur Ausführung eines kryptographischen Protokolls aufweist, und mit einer Schnittstelle (405) zu einem Daten-Lesegerät (406), die einen Zugriff des Daten-Lesegeräts auf die schutzbedürftigen Daten nach Ausführung des kryptographischen Protokolls ermöglicht. 25
 10. Verwendung nach Anspruch 9, wobei die Ausführung des kryptographischen Protokolls nur unter Verwendung eines optischen Sicherheitsmerkmals dieses Dokuments möglich ist. 35
 11. Kombination aus einer elektronischen Dokumentenvorlage für ein Wert- oder Sicherheitsdokument und dem Wert- oder Sicherheitsdokument, welches hergestellt ist unter Verwendung der Dokumentenvorlage, wobei die elektronische Dokumentenvorlage für das Wert- oder Sicherheitsdokument erzeugt ist mit einem Verfahren, aufweisend eine
 - Zurverfügungstellung (301) einer Datenbank (DB), in der verschiedenen Typen von optischen Sicherheitsmerkmalen jeweils ein oder mehrere Kanäle zur optischen Erfassung des betreffenden Sicherheitsmerkmals mit einem optischen Lesegerät zugeordnet sind, wobei das optische Lesegerät zur Trennung der Kanäle ausgebildet ist,
 - Auswahl (302) einer Mehrzahl von Typen der optischen Sicherheitsmerkmale aus der Datenbank und Instanzierung der ausgewählten Typen jeweils durch Platzierung und Skalierung von Sicherheitsmerkmalen der ausgewählten Typen auf einer elektronischen Repräsentation einer Dokumententrägerschicht des Wert- oder

Sicherheitsdokuments zur Erzeugung eines Layoutentwurfs,

- Prüfung (303) des Layoutentwurfs, wobei für räumlich überlappende oder aneinander angrenzende der instanziierten Typen von Sicherheitsmerkmalen geprüft wird, ob diese einen gemeinsamen der Kanäle belegen, und 5
- wenn dies der Fall ist, Ausgabe eines Signals und Eingabe einer Korrektur (304) des Layoutentwurfs als Antwort auf das Signal, 10
- Speicherung (305) des resultierenden korrigierten Layoutentwurfs als die elektronische Dokumentenvorlage.

12. Kombination nach Anspruch 11, wobei das Wert- oder Sicherheitsdokument (401) einen integrierten elektronischen Schaltkreis (402) und einen elektronischen Speicher (403) zur Speicherung von schutzbedürftigen Daten und Mittel (404) zur Ausführung eines kryptographischen Protokolls aufweist, und 20
mit einer Schnittstelle (405) zu einem Daten-Lesegerät (406), die einen Zugriff des Daten-Lesegeräts auf die schutzbedürftigen Daten nach Ausführung des kryptographischen Protokolls ermöglicht. 25

13. Kombination nach Anspruch 12, wobei die Ausführung des kryptographischen Protokolls nur unter Verwendung eines optischen Sicherheitsmerkmals dieses Dokuments möglich ist. 30

35

40

45

50

55

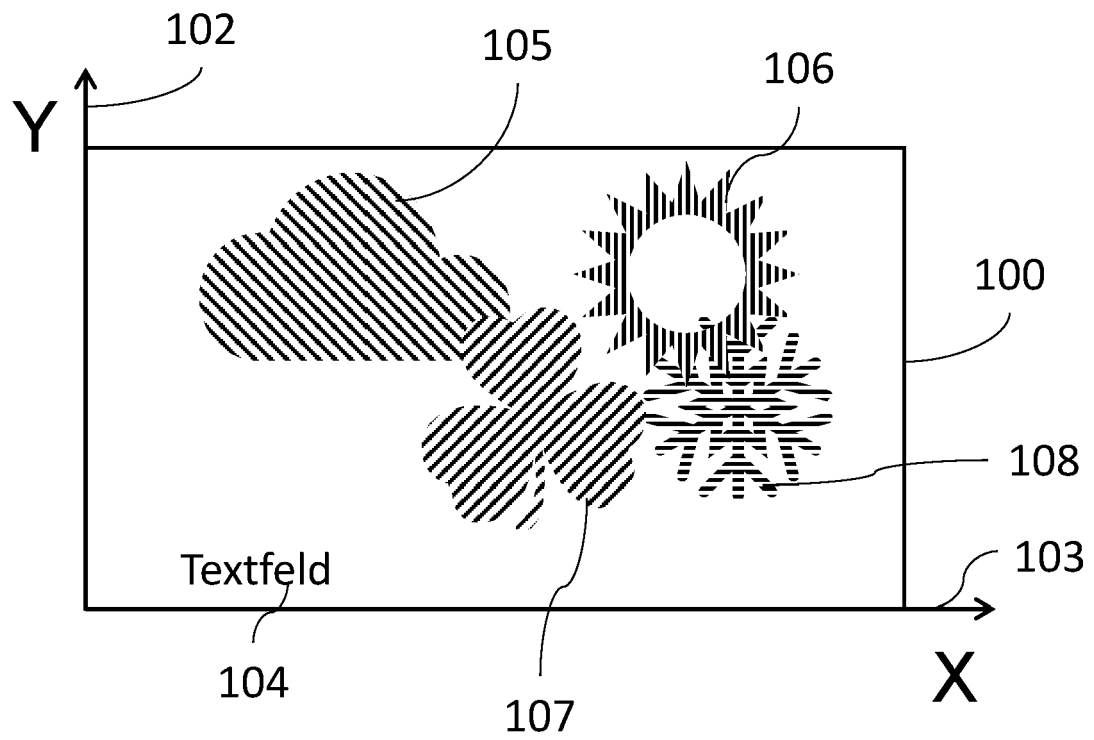


Fig. 1

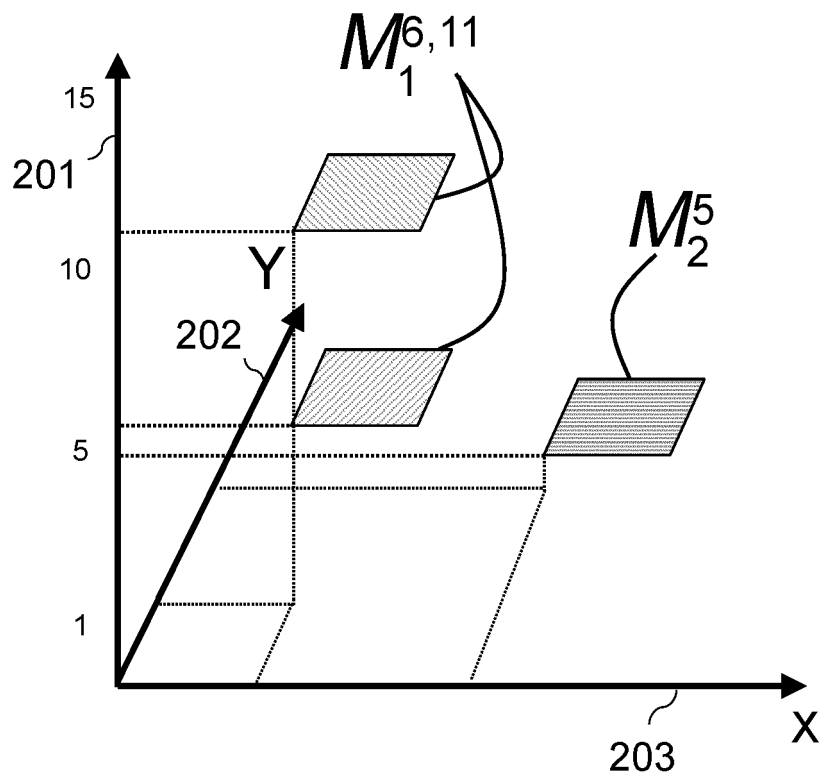


Fig. 2

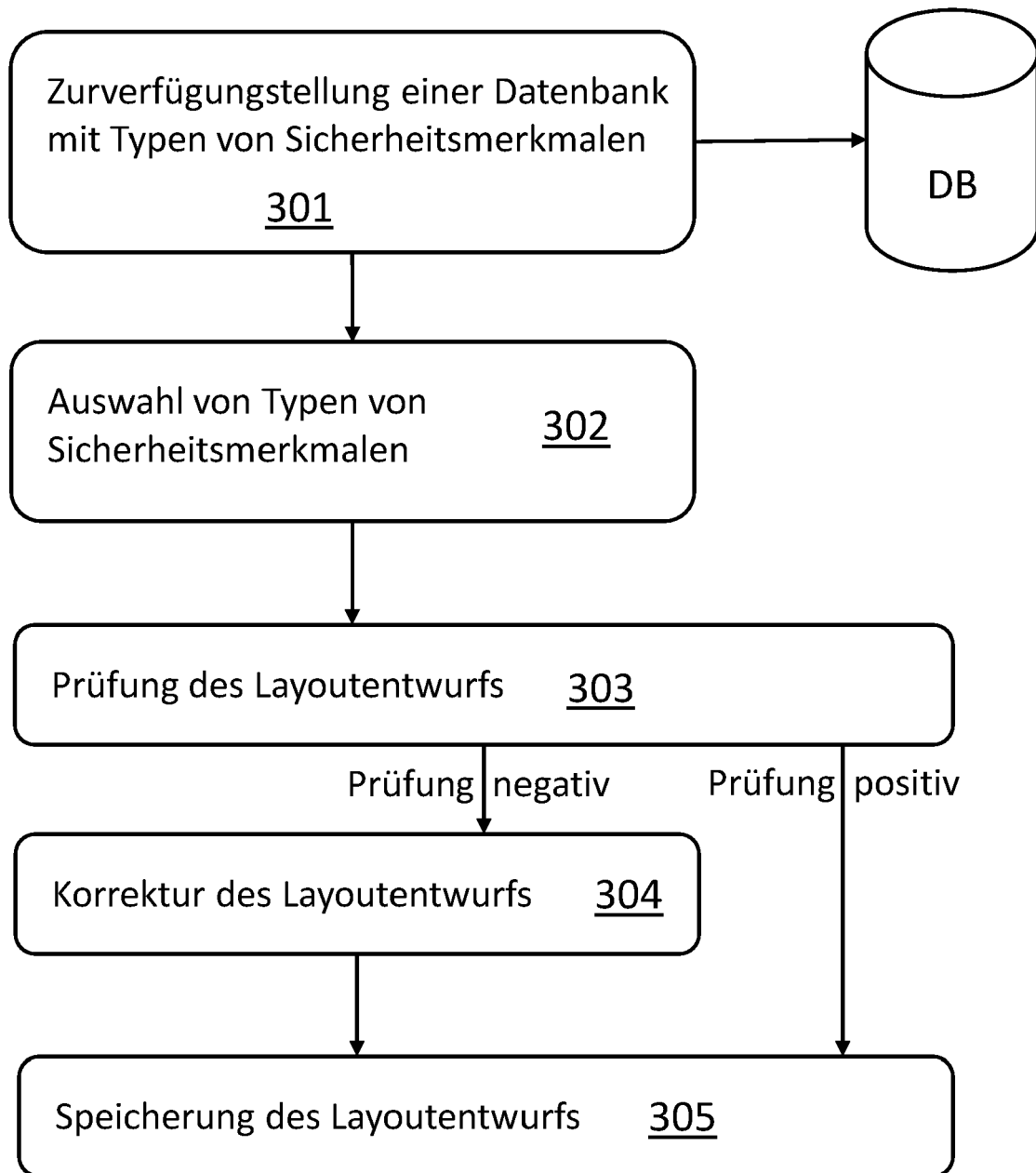


Fig. 3

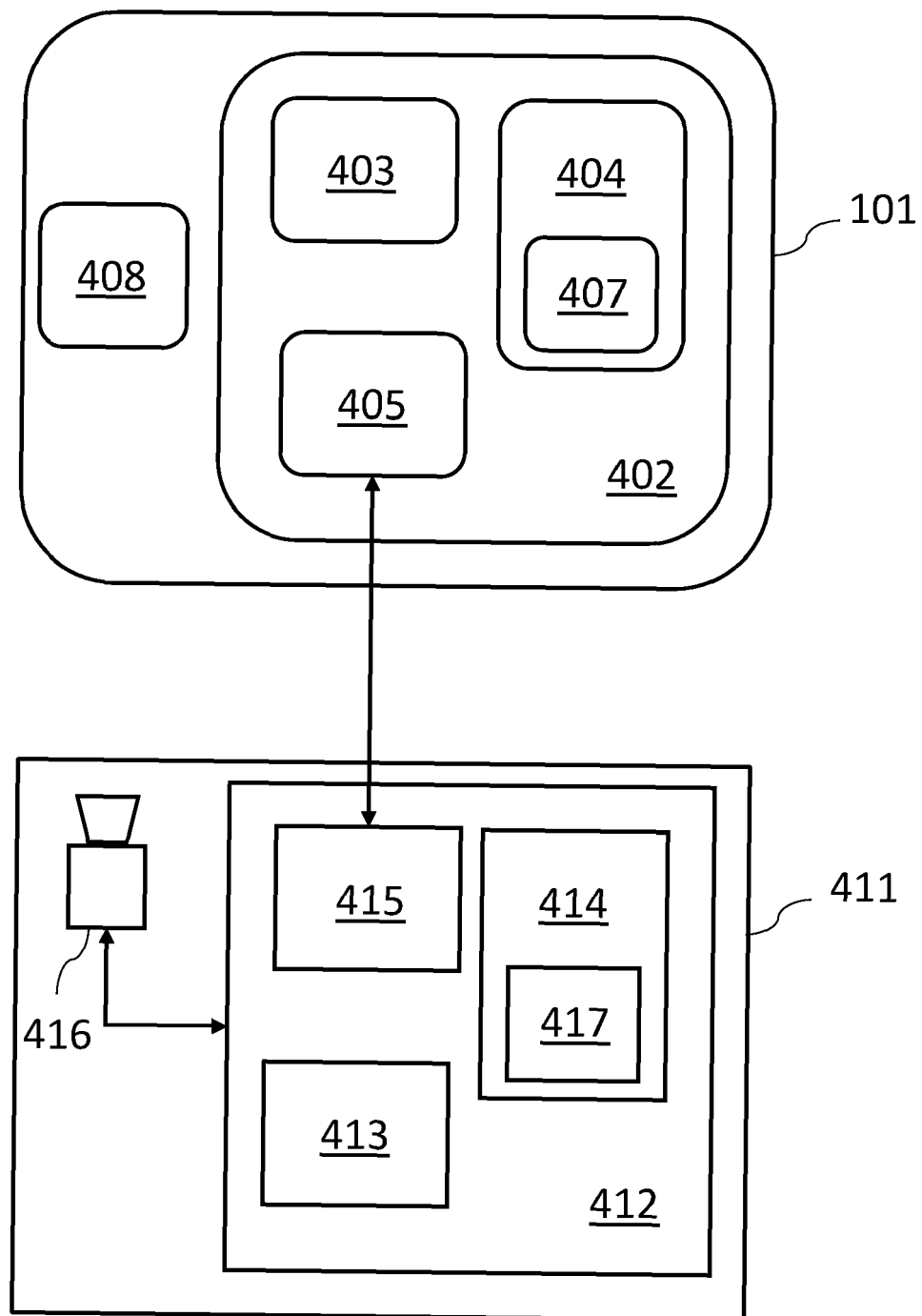


Fig. 4

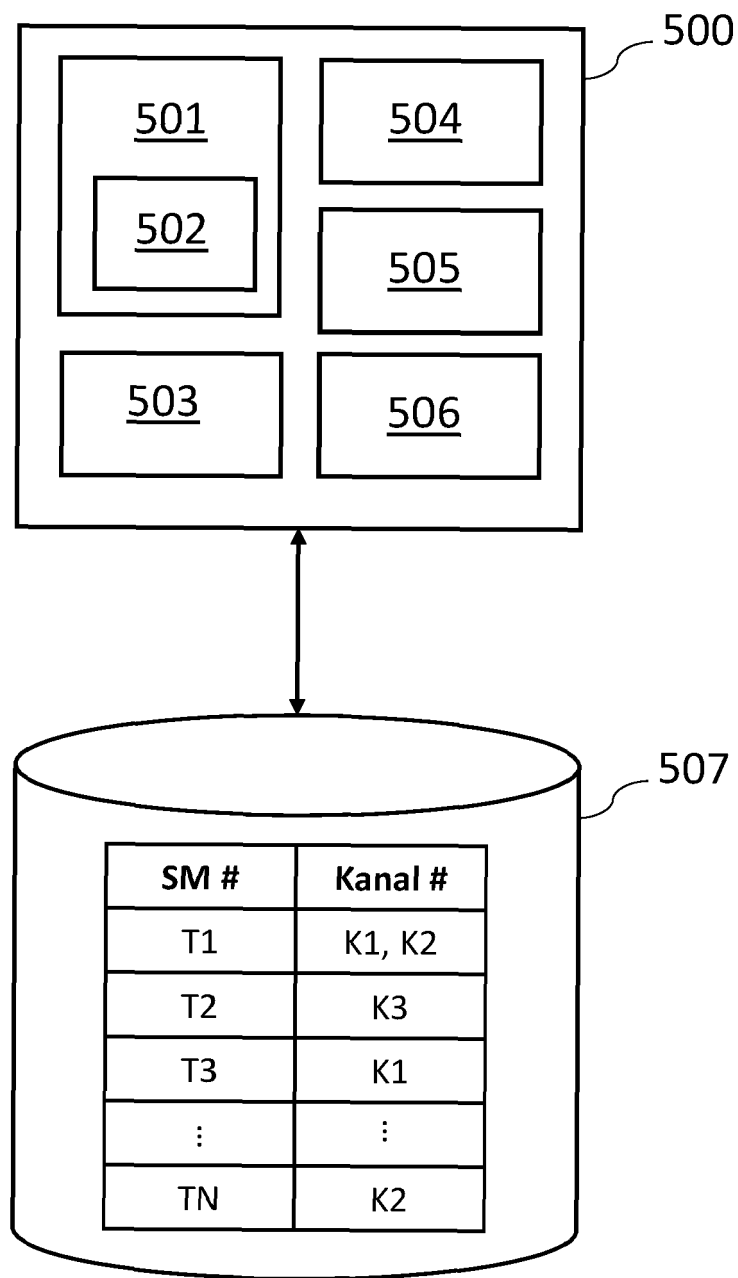


Fig. 5

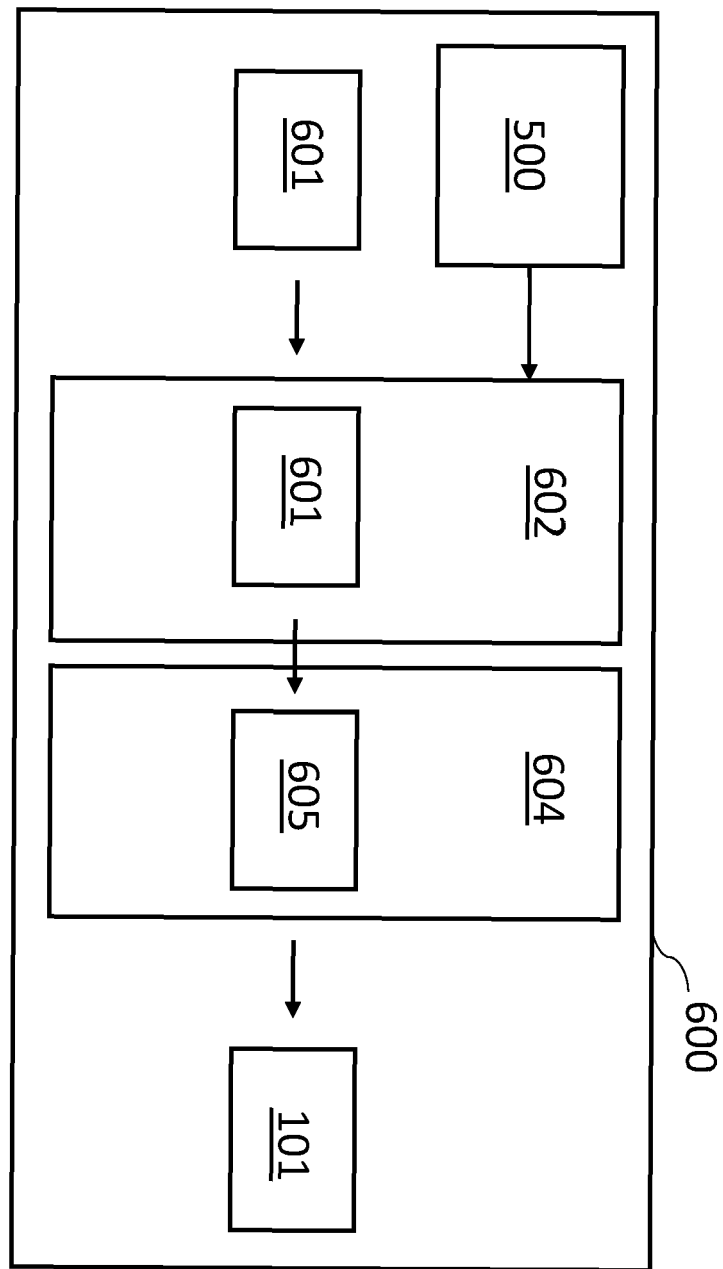


Fig. 6

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

- GB 2352708 A **[0005]**
- WO 0038932 A1 **[0006]**
- WO 2018109035 A2 **[0007]**
- US 2005010776 A1 **[0008]**
- WO 2020004633 A1 **[0009]**