(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 08 425 T2** 2004.05.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 153 373 B1**
(21) Deutsches Aktenzeichen: **699 08 425.3**
(86) PCT-Aktenzeichen: **PCT/BY99/00011**
(96) Europäisches Aktenzeichen: **99 965 372.8**
(87) PCT-Veröffentlichungs-Nr.: **WO 01/043086**
(86) PCT-Anmeldetag: **08.12.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **14.06.2001**
(97) Erstveröffentlichung durch das EPA: **14.11.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **28.05.2003**
(47) Veröffentlichungstag im Patentblatt: **06.05.2004**

(51) Int Cl.[7]: **G07F 7/08**

(73) Patentinhaber:
Mischenko, Valentin Alexandrovich, Minsk, BY

(74) Vertreter:
v. Füner Ebbinghaus Finck Hano, 81541 München

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(72) Erfinder:
MISCHENKO, Valentin Alexandrovich, Minsk, BY; HRISHANOVICH, Igor A., Minsk, BY; MISCHENKO, Anatoly Valentinovich, Minsk, BY

(54) Bezeichnung: **VERFAHREN UND SYSTEM ZUR AUTHENTIFIZIERUNG VON ARTIKELN**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf die Technik des Schutzes von Gegenständen vor Fälschung und kann zum Schutz gegen Fälschung und unbefugtes Kopieren von Waren, Dokumenten, Wertpapieren usw. benutzt werden.

Hintergrund der Erfindung

[0002] Es ist eine breite Vielfalt von Verfahren zum Schutz von Dokumenten und anderen Waren vor Fälschung durch Markieren derselben mit speziellen Marken oder Etiketten bekannt.

[0003] In manchen Fällen werden solche Marken aus einem speziellen Material mit spezifischen Eigenschaften hergestellt, z. B. einem Material, das in einem bestimmten Lichtspektrum fluoresziert (US-Patent 5 719 948, Vorrichtung und Verfahren zum fluoreszenten Abbilden und optischen Zeichenlesen), einem Material mit magnetischen Eigenschaften (US-Patent 5 697 649, Gegenstände mit magnetischem Sicherheitsmerkmal) oder einem Material, das bei Absorption, Reflexion und Transmission an-isotrop ist (US-Patent 5 568 251, Authentifizierendes System ...) usw. Solche Materialien können auch im Aufbau einer Marke angewandt oder eingeschlossen werden, die eine bestimmte Figur, Kombination usw. bildet.

[0004] Keines dieser Verfahren bietet jedoch einen vollständigen Fälschungsschutz, da ein Fälscher ein Material erkennen und die gleiche Technik oder sogar eine höherwertige verwenden kann.

[0005] Eine andere Gruppe von Verfahren basiert auf eindeutigen physikalischen oder chemischen Kennmerkmalen der Oberfläche eines Dokuments oder Produkts. Zu diesem Zweck wird ein Abschnitt der zu schützenden Oberfläche entsprechend den gewählten physikalischen Kennmerkmalen einer Oberfläche gescannt (WO97/24699, Authentifizierung von Gegenständen). Das gescannte Bild wird codiert und/oder verschlüsselt und das erhaltene Ergebnis wird auf die Oberfläche eines Gegenstands oder Dokuments in Form einer Zahl oder eines Codes aufgebracht. Beim Prüfen der Authentizität wird die Oberfläche durch ein Testgerät gescannt. Die nach dem Scannen erhaltenen Daten werden nach dem gleichen Verfahren verarbeitet, und der auf die Oberfläche aufgebrachte Code wird decodiert und/oder entschlüsselt und mit dem Ergebnis der Verarbeitung des gescannten Bildes verglichen.

[0006] Das Scannen physikalischer Kennmerkmale erfordert komplizierte physikalische Geräte. Die Kennmerkmale haben einen breiten physikalischen Bereich von Abwandlungen und ein hohes Maß an Hintergrund-Kennmerkmalen. Dies macht ihre Anwendung verhältnismäßig teuer und vermindert das Maß der Gültigkeit der Abschätzung. Ein Hauptproblem besteht in der Bestimmung der Scan-Oberfläche, da die Verwendung der physikalischen Eigenschaften einer Oberfläche die Scan-Fläche nicht auf die eigentlichen physikalischen Kennmerkmale beschränkt, die die Möglichkeit behindern, zum gleichen Bereich zurückzugelangen. Darüber hinaus bieten die derzeit verwendeten Codiersysteme keine ausreichende Krypto-Widerstandsfähigkeit der Codierung, und die verwendeter Schlüssel können zum Fälschen wiederhergestellt werden.

[0007] Zur zuverlässigeren Bestimmung der willkürlichen Kennmerkmale einer Oberfläche werden speziell strukturierte Materialien verwendet, die willkürlich verteilte Fasern oder andere Kontrasteinschlüsse enthalten, die zur Übertragung oder Reflexion leicht durch optische Geräte ausgelesen werden können (WO98/57299, Dokument mit authentifizierendem Merkmal). Dabei wird die Scan-Fläche auf spezielle Muster oder Fenster beschränkt, die auf die Oberfläche eines Etiketts aus einem strukturierten Materialaufgebracht sind.

[0008] Etiketten dieser Art können hergestellt und auf Gegenstände oder Dokumente aufgebracht werden. Beim Wiederauslesen können aber die massige Struktur und die optischen Merkmale der Fasern Fehler hervorrufen, die zu einer unsicheren Identifikation führen können aufgrund von Fehlern bei der Bestimmung der Scan-Flächen als auch wegen Ungenauigkeiten bei der Messung der Kennmerkmale des Mediums. Darüber hinaus erfordert ein solches Identifiziersystem komplizierte Ausrüstungen zur genauen Bestimmung der räumlichen optischen Kennmerkmale. Ein ähnliches System verwendet ein Etikett mit willkürlich (unregelmäßig) angeordneten, dichroitischen Fasern. Informationen über den Hersteller, die Eigenschaften der Waren und Informationen über das codierte Scan-Ergebnis werden nahe beieinander auf einem Etikett angeordnet (WO99/17486, System und Verfahren zur Authentifizierung von Waren). Das System erfordert jedoch spezielle Lesegeräte zur Bestimmung der optischen Kennmerkmale der Dichroität der Fasern. Darüber hinaus können die Anordnung der Fasern im Medium und eine Ungenauigkeit bei der Bestimmung der Bindung der Fasern zu beträchtlichen Ungenauigkeiten beim Auslesen während eines Tests führen.

[0009] Zusätzlich kann während der Analyse einer großen Anzahl von Tags das Codiersystem "geöffnet" werden, und die Tags können gefälscht oder einfach von der Originalware auf die gefälschten Gegenstände übertragen werden.

[0010] Bekannt sind ferner Verfahren zum Kopierschutz von Dokumenten mittels Aufbringen nicht replizierbarer Teilungen auf ein Bild, d. h. aufgedruckte Literaturen usw. (US-Patente 5 108 767, Vor Fälschung geschütztes Dokument; 5 193 853, Nicht replizierbares Dokument und Verfahren zu dessen Herstellung).

[0011] Diese Verfahren erlauben aber keine schnelle Identifizierung eines Gegenstandes, bei dem es sich um eine Fälschung handeln könnte.

[0012] Bekannt sind auch Verfahren und Systeme

zum Schutz von Dokumenten und Postsachen vor Fälschung (US 5 970 151, Verfahren und Anordnung zum Erzeugen und Prüfen von Sicherheitsprägungen). Nach diesem Patent werden speziell codierte Bilder und Ziffern auf ein Dokument oder einen Umschlag aufgebracht; die Daten auf diesen Bildern und Ziffern werden in einem entfernten Kontrollzentrum gespeichert. Beim Prüfen eines Dokuments wird das Bild gescannt, codiert und zum Speicherzentrum übertragen, wo die Daten mit dem gespeicherten Wert verglichen werden. Darauf wird ein Schluss über die Authentizität eines Dokuments gezogen.

[0013] Das gedruckte Kontrastbild erleichtert die Auslesung und erhöht die Zuverlässigkeit der Identifizierung der Markierung. Darüber hinaus bieten solche Verfahren eine recht zuverlässige Kontrolle des Dokumentendurchlaufs. Die Markierung dieser Art kann aber kopiert und auf ein anderes Dokument aufgebracht, d. h. durch Ersetzen eines Dokuments gefälscht werden.

[0014] Die bekannten Authentifizierungssysteme weisen im Allgemeinen wenigstens zwei entfernte Scanner, einen Drucker, Datenverarbeitungseinrichtungen und Nachrichtenübertragungseinrichtungen auf.

[0015] Bei bekannten Systemen druckt eine Druckvorrichtung Information und einen Code. Darüber hinaus druckt nach dem System des US-Patents 5 970 151 die Druckvorrichtung ein codiertes Bild sowie eine Sequenz von Bar-Codes oder Terminal-Codes.

[0016] Die beschriebenen Systeme erfordern komplizierte Scan-Geräte und spezielle Verbundmedien (Materialien) zum zuverlässigen Rückscannen beim Test. Andererseits erhöht eine Vergrößerung des Bildkontrasts und der Reproduzierbarkeit wiederholten Scannens bei bekannten Systemen die Wahrscheinlichkeit für das Kopieren und Fälschen.

[0017] Eine dem erfindungsgemäßen System nahe kommende technische Lösung sind das System und das Verfahren zum Markieren von Waren nach der US-A-5 592 561. Dieses System enthält einen Steuercomputer, einen Hauptcomputer, ein Markiersystem und einen Testleser, die sämtlich kompatibel sind mit und angeschlossen sind an ein Nachrichtensystem. Das Markiersystem enthält einen Drucker, ein Lesegerät und eine Verarbeitungs- und Steuereinheit, die über ein Modem an den Hauptcomputer angeschlossen ist. Markierungen in Form eines zweidimensionalen verschlüsselten Bildes werden auf einen Gegenstand oder auf das Material gedruckt, aus dem das Produkt besteht.

[0018] Das Bild kann durch ein Lesegerät gescannt und in Form verschlüsselter Daten verschlüsselt werden. Die Daten werden dann mit den Authentifizierungsdaten der Datenbank verglichen oder die Daten werden decodiert und mit den in der zentralen Datenbank des Hauptcomputers gespeicherten Daten verglichen.

[0019] Das Markiersystem gewährleistet die Steuerung des Bilddrucks mit Hilfe einer gewissen Anzahl von Authentifizierungscodes, die aufgebracht werden sollten, bevor die Authentisierung erforderlich ist. Nach dem Drucken wird das codierte Bild gescannt und in der zentralen Datenbank als wahres Bild erkannt. Dann kann das Bild in der Datenbank zusammen mit der relevanten Information bezüglich des bestimmten Produkts gespeichert werden.

[0020] Während des Prüfens von Waren werden diese zusammen mit der Authentifizierung hinsichtlich der Duplizierung eindeutiger Codes geprüft, wodurch gefälschte Waren erfasst werden.

[0021] Das System liefert ein recht scharfes und leicht auszulesendes Bild. Gleichwohl ist das System nicht in der Lage, den Hersteller vor Fälschungen vollständig zu schützen, weil ein Bild sich leicht reproduzieren lässt und eine gefälschte Kopie eines Produkts beim Testen von Massenwaren die erste sein könnte.

[0022] Die der vorliegenden Erfindung am nächsten kommende technische Lösung ist ein Verfahren und ein System zum Markieren von Waren, wie es aus der EP-A-0 889 448 bekannt ist. Dieses Verfahren umfasst das Drucken von Etiketten in Form eines zweidimensionalen verschlüsselten Bildes auf einem Gegenstand oder auf einem Material, aus dem das Produkt besteht. Als zusätzliches Kriterium für die Authentifizierung werden nicht reproduzierbare Muster mit magnetischen Fasern verwendet. Ein solches System benötigt ein Magnet-Lesesystem.

[0023] Aufgabe der Erfindung ist die Entwicklung eines zuverlässigen Verfahrens und zuverlässigen Systems zum Erkennen von Markierungen, der Eindeutigkeit von Markierungen sowie zur Steuerung der Bewegung vor. Waren.

[0024] Diese Aufgabe wird erfindungsgemäß durch die in den Ansprüchen 1, 2, 12, 16 und 17 beschriebenen Verfahren sowie die in den Ansprüchen 19 und 20 beschriebenen Systeme gelöst. Bevorzugte Ausführungsformen der Verfahren der Ansprüche 1, 2, 12 und 16, 17 sind in den Ansprüchen 3 bis 11, 13 bis 15 bzw. 18 beschrieben.

Zusammenfassung der Erfindung

[0025] Die vorliegende Erfindung entwickelt neue Verfahren zum Markieren von Gegenständen und zur Authentifizierung derselben sowie ein System zum Prüfen und Authentifizieren, d. h. Prüfen der Echtheit des Ursprungs von Waren, Gegenständen und Dokumenten.

[0026] Hauptziel der Erfindung ist es, eine Markiereinrichtung bereitzustellen, die einerseits eine eindeutige Markierung und die Unmöglichkeit der Fälschung der Markierung gewährleistet und andererseits zufrieden stellend, sicher und einfach in der Technik der Erkennung eindeutiger Markierungen ist.

[0027] Das Ziel der Erfindung wird auf folgende Weise realisiert. Die Markierung von Gegenständen erfolgt aufgrund folgender Schritte:

– Erzeugen privater Schlüssel,

– Speichern der Schlüssel in einer Datenbank,
– Erzeugen eines Bildes für jede Probe eines Gegenstands,
– Aufbringen des Bildes auf eine markierte Oberfläche,
– Lesen des resultierenden Bildes,
– Gewinnen von Daten über das ausgelesene Bild,
– Verschlüsseln der erhaltenen Daten,
– Anbringen des resultierenden Codes auf der markierten Oberfläche.

[0028] Das Verfahren ist ferner dadurch gekennzeichnet, dass ein eindeutiges Bild als wenigstens zweidimensionales Zufallsbild erzeugt und das erzeugte zweidimensionale Zufallsbild auf eine gewählte Fläche aus einem Material aufgebracht wird, das eine raue Oberfläche mit willkürlichen Kennmerkmalen aufweist.

[0029] Verschiedene Materialien können verwendet werden, z. B. Materialien mit einer rauen Oberfläche, faseriges, poröses Material sowie Materialien mit Einschlüssen von Teilchen usw.

[0030] Hierbei sind am billigsten faserige Materialien einschließlich raues Papier, Stoff und andere Haushaltsmaterialien. Die Materialien gewährleisten die Unmöglichkeit jeglichen Kopierens, während ein vollständig anderes Bild erzeugt wird, wenn ein Bild auf eine Oberfläche mit willkürlicher Textur wieder aufgebracht wird. Dies liegt daran, dass beim Färben die Verteilung der Farbe oder eines anderen Markiermittels durch die Textur wesentlich beeinflusst wird. Auf der anderen Seite beeinflusst die Intensität des reflektierten Lichts die Bildeigenschaften während des Lesens wesentlich. So kann ein Bild dieser Art beim Auslesen vollständig unterschiedliche Identifikationsdaten liefern. Hierbei wird ein gefälschter Gegenstand unmittelbar erkannt. Ein Markieren dieser Art liefert einen eindeutigen Charakter der Markierung, und eine Replizierung durch moderne technische Mittel ist ebenfalls unmöglich, wodurch auch neben dem Markierbild der eindeutige Charakter des Identifikationscodes gewährleistet wird.

[0031] Eine weitere Verbesserung der Erfindung erfolgt nach der folgenden Verteilung; von Funktionen für die das System bildenden Teile:

– Das Erzeugen privater Schlüssel, das Verschlüsseln und Speichern der Daten erfolgt in einem entfernten Steuerzentrum,
– das Anbringen des Bildes, Scannen des sich ergebenden Bildes und Anbringen des verschlüsselten Codes erfolgen durch eine Markiereinrichtung,
– der Datenaustausch zwischen der Markiereinrichtung und dem Steuerzentrum erfolgt über Nachrichtenkanäle.

[0032] Die obige Verteilung der Funktionen schützt vor Fälschungen durch sichere Speicherung der Verschlüsselungsschlüssel, die zum Erzeugen von Schutzcodes ausgelegt sind, die neben dem Identifikationsbild auf einem Etikett angebracht sind. Die Individualität der Schlüssel verhindert die Möglichkeit der Verschlüsselung anderer willkürlich erzeugter Fälschungsbilder.

[0033] Nach einer weiteren Ausführungsform der Erfindung kann ein Hersteller oder Lieferant die Herstellung der Schutzmarkierung übernehmen. Dabei können die Funktionen wie folgt verteilt werden:

– Das Erzeugen privater Schlüssel, die Datenverschlüsselung, das Erzeugen eines Zufallsbildes, das Anbringen des Bildes auf der markierten Oberfläche, das Lesen des resultierenden Bildes und das Anbringen des verschlüsselten Codes auf der markierten Oberfläche erfolgen durch die Markiereinrichtung,
– die Datenübertragung zum Kontrollzentrum erfolgt ebenfalls durch die Markiereinrichtung, während wenigstens die Schlüssel zum Kontrollzentrum über einen Weg übertragen werden, der Vertraulichkeit bietet,
– das Kontrollzentrum speichert die Schlüssel und Codes in der Datenbank.

[0034] Dabei übernimmt das Kontrollzentrum nur die Überwachungs- und Prüffunktion.

[0035] Ein anderes Verfahren zur Erzielung eines eindeutigen Markierbildes, das Bedingungen für die Unmöglichkeit der Reproduktion und Fälschung bietet, ist eine Variante der Ausführungsform, nach der unter Anwendung der gleichen Schritte und Datenverarbeitungsfolge ein Zufallsbild auf eine Oberfläche aufgebracht wird und das zur Ausbildung einer Textur mit willkürlichen Parametern weiter modifiziert wird. Hierbei wird ein zweidimensionales Zufallsbild auf die Oberfläche aufgebracht, das weiter modifiziert wird. Dabei wird ein Ergebnis erzielt mit ähnlichen Antifälschungsmerkmalen wie im vorherigen Fall. Dabei wird die Oberfläche vorzugsweise modifiziert, bis eine ständige Textur mit Zufallsparametern gebildet ist.

[0036] Die zuvor erwähnte Oberflächenmodifikation kann nach einem der im Folgenden beschriebenen Verfahren oder äquivalente Techniken ausgeführt werden, z. B. durch Perforation. Hierbei werden die Textur und ihre Zufallsparameter an der Kante von Öffnungen gebildet, und zwar sowohl durch Erosion der Kante und ihre Anpassung an Zufalls-Bildelemente und ihre Teile.

[0037] Die Perforation kann auch durch Elektrofunkenbearbeitung erzielt werden. Dabei ist die Verteilung der Öffnungen ebenfalls zufällig und nicht reproduzierbar.

[0038] Die Oberfläche kann auch durch eine Texturprägung modifiziert werden, analog mit Siegeln, Presseinrichtungen usw.

[0039] Weitere Mittel der Bildmodifikation, die eine Reproduktion verhindern, kann die Verwendung eines porösen Materials mit Kapillareigenschaften sein. Hierbei führt die Porosität zu einer Textur, wäh-

rend das Bild aufgrund der unregelmäßigen Wiederverteilung eines flüssigen Färbmittels über das unregelmäßige Bild der Kapillaren modifiziert wird.

[0040] Die nach der vorliegenden Erfindung markierten Gegenstände werden im Prüfterminal identifiziert. Dabei werden die folgenden bekannten Operationen ausgeführt:

– Lesen eines Markierbildes,
– Lesen eines verschlüsselten Codes,
– Entschlüsseln des verschlüsselten Codes zur Datenrückgewinnung,
– Vergleichen der der rückgewonnenen Daten mit den ausgelesenen Daten.

[0041] Ungleich den bekannten Authentifizierungsverfahren wird erfindungsgemäß das Kriterium der Gegenwart einer jeweiligen Textur auf einem Bild beim Identifizieren spezifiziert, wonach das Bild ausgelesen wird. Gemäß einer Ausführungsform werden die Funktionen zwischen dem Prüfterminal und dem Steuerzentrum wie folgt verteilt:

– Das Spezifizieren des Merkmals der Existenz einer Textur, das Lesen des Markierbildes und das Lesen des verschlüsselten Codes werden im Prüfterminal ausgeführt, wobei die ausgelesenen Bilddaten zum Kontrollzentrum übertragen werden,
– das Entschlüsseln (Wiedergewinnung der Bilddaten gegen den ausgelesenen Code), das Vergleichen des wiedergewonnenen Bildes mit den Daten des ausgelesener Bildes erfolgen im entfernten Kontrollzentrum.

[0042] Nach einer weiteren Ausführungsform werden

– Das Lesen des Markierbildes, das Lesen des verschlüsselten Codes und das Spezifizieren des Kriteriums der Gegenwart einer Textur am Prüfterminal ausgeführt, wobei die ausgelesenen Bilddaten zum Kontrollzentrum übertragen werden,
– das Entschlüssen (Wiedergewinnung der Bilddaten gegen den ausgelesenen Code) erfolgt im entfernten Zentrum, und das wiedergewonnene Ergebnis wird zum Prüfterminal übertragen,
– das Vergleichen der wiedergewonnenen Daten mit den ausgelesenen Identifikaitions-Bilddaten erfolgt im Prüfterminal.

[0043] Bei den beschriebenen Authentifikationssystemen ist das zusätzliche Kriterium, d. h. die Gegenwart einer Textur auf einer Oberfläche, das entscheidende Kriterium zum Starten des Identifikationsvorgangs. Dieses Kriterium schließt eine Markierungsimitation durch genaue Reproduktion einer flachen Probe (Kopie) der ursprünglichen Markierung aus. Die Gegenwart der Textur macht jegliche Fälschung unmöglich, weil beim Anbringen eines Bildes auf die Texturoberfläche sich das resultierende Bild in zufälliger Weise ändert und nicht dem Originalbild entsprechen kann.

[0044] Während der Bildauslesung können tatsächlich einige Abweichungen zwischen der ersten und der zweiten Auslesung auftreten. Die Abweichungen werden sowohl durch die Haltbarkeit des Etiketts als auch durch die Kennmerkmale des Lesers konditioniert. Die Abweichungsgrenzen können nach der Praxis oder Tests festgelegt werden. Daher vergleichen moderne Identifikationsverfahren generell die Kennmerkmale der erhaltenen Bilder und nicht der erhaltenen Codes. Beim Vergleichen werden Fehler abgeschätzt. Entschieden wird auf der Grundlage des voreingestellten Kriteriums.

[0045] Generell umfasst erfindungsgemäß der gesamte Vorgang der Identifikation von Gegenständen, ausgehend vom Markieren bis zur Entscheidung über die Authentizität eines Gegenstandes, zusammen mit dem Test durchlaufender Produkte und der Suche nach gefälschten Produkten die folgenden Schritte:

– Vormarkieren von Gegenständen,
– Lesen des resultierenden Bildes,
– Datenverschlüsselung,
– Datenspeicherung in der Datenbank des Kontrollzentrums,
– wiederholtes Lesen (Prüfen) des eindeutigen Bildes,
– Datenübertragung zum Kontrollzentrum,
– Vergleich der Daten mit den in der Datenbank gespeicherten Daten.

[0046] Dieses Verfahren unterscheidet sich von den bekannten dadurch, dass ein Markierbild. durch folgende Schritte erhalten wird:

– Erzeugen eines eindeutigen Zufallsbildes als wenigstens zweidimensionales Bild,
– Anbringen des erzeugten Zufallsbildes auf einer Oberfläche mit einer Rauheit mit Zufallsparametern,
– Lesen des sich ergebenden Bildes,
– Übertragen der Daten über das ausgelesene Bild zum entfernten Kontrollzentrum,
– Erzeugen privater Schlüssel,
– Codieren der erhaltenen eindeutigen Bilddaten mittels privater Schlüssel
– Übertragen des sich ergebenden Codes zur Markierstation und Anbringen des Codes auf der Markierfläche,
– Speichern der Schlüssel in der Datenbank des Kontrollzentrums,
– Verifizieren der Gegenwart und des Musters der Textur auf der Markierfläche im Prüfterminal, und darauf
– Testlesen des markierten Bildes und des angebrachten Codes,
– Übertragen der Daten über den Code zum Kontrollzentrum,
– Entschlüsseln der Daten über den Code und Wiedergewinnen der Daten über das ausgelesene Bild,
– Übertragen der wiedergewonnenen Daten zum

Prüfterminal zum Vergleich mit den Daten über das ausgelesene Bild und Entscheiden über die Authentizität des Gegenstandes.

[0047] Hierbei handelt es sich um eine bevorzugte Ausführungsform der Erfindung, weil hierdurch der Verkehr über das Nachrichtennetzwerk vermindert wird. Gleichzeitig lässt sich, während die Bilddaten am Prüfterminal verglichen werden, d. h. an der Einheit zum Speichern direkter Information über den geprüften Gegenstand und seinen Zustand, die Situation objektiver einschätzen. Zusätzlich ist es, wenn beträchtliche Abweichungen in den quantitativen Kennmerkmalen registriert werden, möglich, dass einige andere Gegenstände aus der Serie geprüft werden.

[0048] Andererseits lassen sich die Bilddaten auch zum Kontrollzentrum übertragen, um die beim Prüf-Scannen erhaltenen Daten mit den Daten zu vergleichen, die unter Anwendung des erhaltenen Codes wiedergewonnen wurden.

[0049] Dieses Verfahren zeichnet sich dadurch aus, dass ein eindeutiges Markierbild durch folgende Schritte erhalten wird:

– Erzeugen eines eindeutigen Bildes als zumindest zweidimensionales Zufallsbild,
– Anbringen des erzeugten Zufallsbildes auf eine Oberfläche mit einer Textur mit unregelmäßigen Parametern,
– Lesen des resultierenden Bildes,
– Übertragen der Daten über das ausgelesene Bild zum entfernten Kontrollzentrum,
– Erzeugen privater Schlüssel,
– Verschlüsseln der erhaltenen eindeutigen Bilddaten mittels der privaten Schlüssel,
– Anbringen des resultierenden Code auf der Markieroberfläche,
– Speichern der Schlüssel und der eindeutigen Bilddaten in der Datenbank des Kontrollzentrums,
– Verifizieren der Gegenwart und des Musters der Textur auf der Markierfläche im Prüfterminal, und dann
– Testlesen des Markierbildes und des aufgebrachten Codes,
– Übertragen der ausgelesenen Daten zum Kontrollzentrum,
– Entschlüsseln der Daten über den Code und Wiedergewinnen der Daten über das ausgelesene Bild,
– Vergleichen der wiedergewonnenen Daten mit den nach dem Testlesen erhaltenen Bilddaten,
– Übertragen der Vergleichsergebnisse zum Prüfterminal.

[0050] Eine weitere Verbesserung des Verfahrens zur Identifikation von Gegenständen und Überwachung durchlaufender Produkte im Hinblick auf die Feststellung von gefälschten Gegenständen und die rechtzeitige Verhinderung einer Verletzung ist dadurch gekennzeichnet, dass das Kontrollzentrum Daten über die ausgeführten Prüfungen speichert, wobei eine Anzahl von Prüfungen ein und desselben Codes registriert wird, wenn der gesetzte Wert der Prüfungen überschritten wird, wobei ein Informationssignal über die wiederkehrende Anforderung erzeugt wird.

[0051] Zur technischen Implementation der beschriebenen Verfahren lassen sich Systeme zur Identifikation von Waren einrichten, die aus einem Ausrüstungskomplex bestehen, wobei ihre Struktur umfasst:

– Eine Markierstation,
– ein Kontrollzentrum,
– Prüfterminals,
– Nachrichteneinrichtungen,
– Datenübertragungsmedien.

[0052] Das System zur Authentifizierung von Gegenständen umfasst Markiereinrichtungen mit einem Drucker, einer Druckersteuerung, einem Auslesegerät, einer Bildverarbeitungseinheit, einer Nachrichteneinrichtung und ein entferntes Kontrollzentrum sowie ein Prüfterminal mit einer Schlüsselerzeugungseinheit, einer Codier-/Decodiereinheit, einer Speichereinheit, einer Vergleichseinrichtung (Entscheidungseinheit) und Rohlingen für Etiketten. Die erfindungsgemäße Markiereinrichtung umfasst ferner eine Zufallsbild-Erzeugungseinrichtung, Einrichtungen zum Anbringen eines verschlüsselten Codes. Als Etikettrohlinge werden Substrate aus einem Material mit einer Textur mit Zufallsparametern verwendet.

[0053] Insgesamt resultiert die Implementierung des vorgeschlagenen Verfahrens in einem neuen positiven Effekt, der durch Folgendes gekennzeichnet ist.

[0054] Einerseits wird die Zuverlässigkeit mehrfacher Auslesungen vergrößert, weil auf der identifizierten Oberfläche des Bildes Merkmale erzeugt und aufgebracht werden, die für eine qualitative mehrfache Auslesung optimal sind.

[0055] Dabei wird die Scan-Fläche des Schutzbildes genau lokalisiert, da das aufgebrachte Bild einen guten Kontrast im Vergleich mit der restlichen Oberfläche hat.

[0056] Andererseits erhöht das Speichern der privaten Schlüssel im entfernten Verarbeitungszentrum das Maß der Zuverlässigkeit für das Speichern privater Schlüssel, die nie zu offenen Prüfterminals übertragen werden und im Allgemeinen nirgendwohin übertragen werden können.

[0057] Darüber hinaus schließt die Verwendung eines Textursubstrats oder jeglicher anderer dreidimensionaler Zufallsbildtransformation praktisch jegliche Möglichkeit für ein einfaches Kopieren der Etiketten aus. Dabei dient die Struktur der Oberfläche selbst als zusätzliches Kriterium für eine Voridentifikation (visuelle Identifikation).

[0058] Weiterbildungen der vorliegenden Erfindung bieten darüber hinaus weitere Vorteile.

[0059] Ein zusätzliches Testen der Etiketten im Hinblick auf eine Replikationsverhinderung verbessert

weiter das Maß des Antireplikationsschutzes, wodurch Fälschungen wirkungsvoll erfasst werden. Hat z. B. der Verletzer eine Möglichkeit zum Reproduzieren oder sonstigen Fälschen der Etiketten in einer oder mehreren Varianten "gewählt", lässt sich das häufige Auftreten identischer Etiketten erfassen und lokalisieren.

Beschreibung der Zeichnungen

[0060] **Fig.** 1 zeigt ein Etikett mit einem aufgebrachten Bild und einem Bar-Code,
[0061] **Fig.** 2 zeigt ein Gesamtschema des Systems zur Authentifizierung von Gegenständen oder Dokumenten,
[0062] **Fig.** 3 zeigt ein Blockschaltbild der Markierstation,
[0063] **Fig.** 4 zeigt ein Blockschaltbild des Prüfterminals,
[0064] **Fig.** 5 zeigt ein Blockschaltbild des Kontrollzentrums.
[0065] Das erfindungsgemäße Verfahren und das erfindungsgemäße System werden anhand des in **Fig.** 1 gezeigten Beispiels eines Etiketts erläutert.
[0066] Ein Etikett ist eine an einem Gegenstand oder Dokument befestigte Karte und kann mit diesem einteilig verbunden sein.
[0067] Ein Etikett kann allgemeine Information **2** enthalten, z. B. eine Marke, Art des Gegenstands, Parameter usw. Ferner kann ein Etikett ein Identifikationsbild **3** und sein codiertes Bild in Form eines Bar-Codes **4** enthalten. Der Bar-Code kann auch weitere Service-Informationen über Schlüssel, Seriennummer usw. enthalten. Die Oberfläche im Bereich des Identifikationsbildes kann mit einem speziellen Material abgedeckt sein, das der Oberfläche Rauigkeit verleiht.
[0068] Generell kann das in **Fig.** 2 gezeigte Identifikationssystem in einer Computervariante mit speziellen oder universellen Prozessoren geliefert werden. Das System enthält eine Markiereinrichtung mit wenigstens einem Drucker **5**, einem Scanner **6** und einem Markierprozessor **7**, der Zufallsbilder erzeugt, Daten verarbeitet und eine Druckersteuerung beinhaltet, sowie eine Einrichtung **8** zur Datenübertragung über ein verteiltes oder lokales Netzwerk **9**. Das Steuerzentrum enthält eine zentrale Datenverarbeitungseinheit **10** und wenigstens eine Speichereinrichtung **11** zum Speichern von Datenbanken und eine Codier-/Decodiereinheit. Über die Nachrichteneinrichtung **8** ist das Zentrum auch mit dem weltweiten oder einem lokalen Datenübertragungsnetzwerk **9** verbunden (online).
[0069] Das Zentrum ist ferner mit entfernten Prüfeinrichtungen verbunden, die je wenigstens eine Nachrichteneinrichtung **8**, einen Scanner **6** und einen Datenprozessor **13** zum Prüfen umfassen.
[0070] Das System kann auch eine Gruppe von Etikettenrohlingen umfassen.
[0071] Erfindungsgemäß wird durch einen Bildgenerator **14** in der Markierstation ein Bild erzeugt (**Fig.** 3). Das Bild enthält Punkte, die zufällig innerhalb der Grenzen der festgelegten Punktefläche (Pixel) verteilt sind, oder es besteht vollständig aus diesen Punkten. Jedem Punkt ist eine eigene Farbe zugeordnet, die jedes Mal von einer n Farben umfassenden Palette zufällig verteilt werden.
[0072] Das erzeugte Bild wird auf eine Oberfläche des Etiketts mit Hilfe eines Tintenstrahl- oder Laserdruckers **5** mit einer Auflösung von 300 dpi gedruckt.
[0073] Das Substrat **15** des Etiketts besteht aus einem Material mit einer Reliefoberfläche, z. B. bröseligem Papier, Stoff oder porösem Material. Das erhaltene Bild kann während des Druckens oder danach mittels einer speziellen Einrichtung zufällig transformiert werden. Die Oberflächenstruktur dieser Materialien ist in zufälliger Weise verteilt. Daher werden ungleich einem erzeugten Bild Farbstoffe oder Druckertoner, die die Unregelmäßigkeit der Oberfläche ausfüllen, rückverteilt. Ferner variieren beim weiteren Auslesen Reflexionsmerkmale entsprechend der Texturneigung.
[0074] Das Bild hat einen weiteren Vorteil. Beim Replizieren auf eine ähnliche Oberfläche treffen die Tonerpartikel auf andere Bedingungen, so dass das Bild wiederum variiert und nicht in Faksimile auf eine ähnliche Oberfläche kopiert werden kann, weil eine zufällige Oberflächentextur nicht mit dem Bildelement des Originals übereinstimmt.
[0075] Das aufgedruckte Bild kann auch in anderer Weise transformiert werden, z. B. durch Perforieren, Expandieren, Komprimieren, Wärmebehandlung usw.
[0076] In diesen Fällen ist die räumliche Struktur eines Substrats wichtig, da die Struktur das Haupthindernis für ein identisches Kopieren ist, was ein weiteres Authentifizierungskriterium darstellt.
[0077] Wenn das Bild gedruckt wird, wird die Fläche durch den Scanner **16** mit einer Auflösung von 300 dpi und 256 Graustufen gescannt.
[0078] Das gescannte Ergebnis ist ein Raster mit 8 bpp Farbtiefen.
[0079] Die resultierende Reihe wird in einem DIB (Device Independent Bitmap)-Prozessor **16** nach der eingestellten Regel verarbeitet, z. B. durch Verschachteln auf Fraktionen entsprechend den Farben. Pixel der gleichen Fraktion werden aus der Gesamtzahl der Reihenpixel ausgeschlossen. Die Zahl N_1 der anderen Pixel wird zusammen mit ihrer mittleren Farbintensität wie folgt definiert:

$$N_2 = (C_1 + C_2 + ... C_{N1})/N_1$$

[0080] Die Linie der durch Verknüpfung der Linienausdrücke hexadezimaler Darstellung von N_1 und N_2 erhaltenen Symbole ist die Bilddarstellung. Die Linie von Symbolen wird durch einen privaten Schlüssel verschlüsselt, z. B. gemäß PCT/99BY/00004 (MZ4).
[0081] Ein privater Schlüssel kann entweder in der Markierstation erzeugt oder zum Kontrollzentrum

übertragen werden, oder er kann von dem in **Fig.** 4 gezeigten Kontrollzentrum erhalten werden. Dabei wird durch den Schlüsselgenerator **19** für jedes Markierterminal ein individueller privater Schlüssel erzeugt. Um eine höhere Sicherheit zu erzielen, insbesondere zum Markieren einzelner Objekte, kann eine Bilddarstellung zum Verschlüsseln zum Kontrollzentrum gesandt werden. Dann wird die erhaltene verschlüsselte Bilddarstellung vom Kontrollzentrum zur Markierstation übertragen. Wie in **Fig.** 1 gezeigt, transformiert der Bar-Code-Generator **17** die verschlüsselte Bilddarstellung in einen Bar-Code, der durch einen Drucker **18** neben das Bild als Bar-Code **3** auf die Etikettenoberfläche gedruckt wird.

[0082] Wie in **Fig.** 4 gezeigt, enthält das Kontrollzentrum Ein-/Ausgabe-Nachrichteneinheiten (Modem) **8**, einen Code-Generator **19**, einen Codierer/Decodierer **20**, einen Komparator **22** (der sich auch am Prüfterminal befinden kann), eine Speichereinheit **23** zum Speichern der Daten über die ausgeführten Tests usw.

[0083] Wenn Daten über das Testbild vom Markierterminal am Eingang des Kontrollzentrums eintreffen, erzeugt der Schlüsselgenerator **19** einen privaten Schlüssel, der in der Datenbank **21** gespeichert wird. Dann wird der private Schlüssel zum Codierer/Decodierer **20** übertragen, wo die Bilddarstellung codiert und zum Drucken auf ein Etikett als Bar-Code **3** zur Markierstation zurückübertragen wird.

[0084] Wenn die Codedaten am Eingang des Kontrollzentrums vom Prüfterminal eingehen, fordert der Codierer/Decodierer **20** von der Datenbank einen Schlüssel entsprechend der ID des Bar-Codes. Der entsprechende Schlüssel trifft am Decodierer **20** ein, der die Bilddaten wiedergewinnt (decodiert). Danach werden die Daten über den Komparator **22** zur Entscheidungseinheit **25** des Prüfterminals übertragen (**Fig.** 5).

[0085] Die Testdaten werden in der Datenbank **23** gespeichert. Falls gewisse Bar-Codes oft auftreten, sperrt die Einheit **22** die Übertragung der wiedergewonnenen Bilddarstellung und gibt ein Fälschungssignal.

[0086] Wie in **Fig.** 5 gezeigt, ist das Prüfterminal mit einem Bar-Code-Leser **24**, einem Bild-Scanner **6**, einem DIB-Prozessor **16** zur Bildidentifizierung, einer Ein-/Ausgabeeinheit des Nachrichtenkanals **8** und einer Vergleichs- und Entscheidungseinrichtung **25** ausgerüstet. Im Prüfterminal wird das schützende Bild **2** gescannt, und der schützende Bar-Code **3** wird ausgelesen.

[0087] Der Wert eines Bar-Codes **3** der verschlüsselten Bilddarstellung wird ausgelesen und über einen Nachrichtenkanal **9** zum Kontrollzentrum gesendet.

[0088] Das Kontrollzentrum wählt den relevanten Schlüssel vom Speicher **21** der Schlüsseldatenbank und decodiert den eingestellten Wert, wobei die Bilddarstellung, ausgedrückt durch die Parameter N_1' und N_2', wiedergewonnen wird.

[0089] Die gewonnene Bilddarstellung wird zum Prüfterminal zurückübertragen. Die Vergleichs- und Entscheidungseinheit **25** vergleicht das Bild mit der Bilddarstellung, die als Ergebnis des Prüf-Scannens mittels des Scanners **6** des aufgedruckten Bildes und der Verarbeitung im DIB-Prozessor **16** durch die Parameter N_1 und N_2 gewonnen wurde. Das Ergebnis des Vergleichs der Parameter N_1' und N_2' mit den Parametern N_1 und N_2 wird zur Herbeiführung der Entscheidung über die Authentizität oder die Fälschung eines Gegenstandes analysiert. Dabei werden zulässige Abweichungen der Parameterwerte abgeschätzt, die durch die Abnutzung eines Etiketts, Ungenauigkeiten beim Scannen usw. hervorgerufen werden.

[0090] Eine Markierstation kann entweder beim Hersteller in einem zentralen Lager oder in einer speziellen Station zum Beglaubigen von Dokumenten, z. B. im Büro eines Notars, usw. angeordnet sein.

[0091] Die Identifikationsstation sollte vernünftig sicher sein, um einen Schutz der gespeicherten Information, der Schlüssel, der Testdaten und anderer Informationen zu gewährleisten.

[0092] Das Prüfterminal kann als öffentlich zugängliches Terminal ausgeführt sein, z. B. als Bankautomat, der sich in einem großen Kaufhaus oder anderen öffentlich zugänglichen Einrichtungen befindet.

[0093] Zur Nachrichtenverbindung können erfindungsgemäß das Internet, das Telefonnetz, bestimmte lokale oder andere Netzwerke verwendet werden. Geschützte Verbindungskanäle sind vorzuziehen.

[0094] Somit wird mit Hilfe des vorgeschlagenen Verfahrens und des vorgeschlagenen Systems, das auf dem Verfahren beruht, mit technischen Standardeinrichtungen eine Authentifizierung von Gegenständen und/öder Dokumenten erreicht. Gleichzeitig wird ein Fälschungsschutz mittels eindeutiger Bilder gewährleistet, die auf einen Träger mit zufälliger dreidimensionaler Struktur gedruckt sind. Diese Kombination zusammen mit der Verwendung eines Systems des entfernten Sicherheitskontrollzentrums mit theoretisch entschlüsselungsresistenten privaten Schlüsseln bietet eine zuverlässigen Fälschungsschutz.

[0095] Schließlich ermöglicht das System einen Fälschungsschutz von Waren und Dokumenten ohne die Verwendung jeglicher komplexer und spezifischer physikalischer Schut zeinrichtungen. Diese Tatsache macht das System preiswert und leicht erhältlich.

Patentansprüche

1. Verfahren zum Markieren von Gegenständen zur sicheren Authentifizierung, mit folgenden Schritten:

– Erzeugen privater Schlüssel,

– Speichern der Schlüssel in einer Datenbank,

– Erzeugen eines Bildes für jede Probe eines Gegenstandes,

– Aufbringen des Bildes auf eine markierte Oberflä-

che,
– Lesen des resultierenden Bildes,
– Gewinnen von Daten über das ausgelesene Bild,
– Verschlüsseln,
dadurch gekennzeichnet, dass
– je Probe eines Gegenstandes ein Bild als eindeutiges und zumindest zweidimensionales Zufallsbild erzeugt wird,
– das erzeugte zweidimensionale Zufallsbild auf eine gewählte Fläche aus einem Material mit rauer Oberfläche mit Zufallsparametern aufgebracht wird,
– die Daten über das ausgelesene Bild verschlüsselt werden und
– der sich ergebende Code auf die Markieroberfläche aufgebracht wird.

2. Verfahren zum Markieren von Gegenständen zur sicheren Authentifizierung, mit folgenden Schritten:
– Erzeugen privater Schlüssel,
– Speichern der Schlüssel in einer Datenbank,
– Erzeugen eines Bildes für jede Probe eines Gegenstandes,
– Aufbringen des Bildes auf eine markierte Oberfläche,
– Lesen des resultierenden Bildes,
– Gewinnen von Daten über das ausgelesene Bild,
– Verschlüsseln,
dadurch gekennzeichnet, dass
– je Probe eines Gegenstandes ein Bild als eindeutiges und zumindest zweidimensionales Zufallsbild erzeugt wird,
– das erzeugte zweidimensionale Zufallsbild auf eine gewählte Oberfläche aufgebracht wird und danach,
– die Oberfläche mit dem aufgebrachten Bild modifiziert wird, bis eine unregelmäßige dreidimensionale Textur gebildet wird,
– das sich ergebende Bild nach Modifizieren der Oberfläche ausgelesen wird und danach
– die Daten über das ausgelesene Bild verschlüsselt werden und
– der sich ergebende Code auf die Markieroberfläche aufgebracht wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Oberfläche modifiziert wird, bis eine beständige Textur von Zufallsparametern gebildet ist.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Oberfläche durch Perforation modifiziert wird.

5. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Oberfläche durch Prägen modifiziert wird.

6. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Oberfläche durch Funkenbehandlung modifiziert wird.

7. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass als Markiermaterial ein Aufkleber mit einer gewählten Fläche eines dreidimensionalen gemusterten Materials verwendet wird, z. B. poröses Material mit Kapillareigenschaften.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass
– das Erzeugen privater Schlüssel, die Datenverschlüsselung und die Datenspeicherung in einem entfernten Kontrollzentrum erfolgen,
– das Aufbringen des Bildes, Abtasten des sich ergebenden Bildes und Aufbringen des verschlüsselten Code durch eine Markiereinrichtung erfolgen,
– die Markiereinrichtung Daten über das Bild zum Kontrollzentrum überträgt, während das Kontrollzentrum das Verschlüsselungsergebnis zur Markiereinrichtung überträgt, wobei die Datenübertragung zwischen der Markiereinrichtung und dem Kontrollzentrum über Nachrichtenkanäle erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass
– die Erzeugung privater Schlüssel, die Datenverschlüsselung, die Erzeugung eines Zufallsbildes, das Anbringen des Bildes auf der markierten Oberfläche, das Lesen des resultierenden Bildes und das Anbringen des verschlüsselten Code auf der markierten Oberfläche durch eine Markiereinrichtung erfolgen,
– die Datenübertragung zum Kontrollzentrum ebenfalls durch die Markiereinrichtung ausgeführt wird, während zumindest Schlüssel zum Kontrollzentrum über einen Vertraulichkeit gewährleistenden Weg übertragen werden,
– das Kontrollzentrum die Schlüssel und Codes in der Datenbank speichert.

10. Verfahren nach einem der Ansprüche 2 bis 6, dadurch gekennzeichnet, dass
– das Erzeugen privater Schlüssel, die Datenverschlüsselung und die Speicherung in einem entfernten Kontrollzentrum erfolgen,
– das Anbringen des Bildes, das Modifizieren der Oberflächentextur mit dem aufgebrachten Bild, das Abtasten des sich ergebenden Bildes und das Anbringen des Code durch die Markiereinrichtung ausgeführt werden,
– ein Datenaustausch zwischen der Markiereinrichtung und dem Kontrollzentrum über Nachrichtenkanäle erfolgt.

11. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass
– das Erzeugen privater Schlüssel, die Datenverschlüsselung sowie das Anbringen des Bildes, das Abtasten des sich ergebenden Bildes und das Anbringen des Code durch eine Markiereinrichtung erfolgen,
– die Markiereinrichtung die Daten über das Bild zum Kontrollzentrum überträgt, die sie in der Datenbank

speichert, wobei wenigstens die Schlüssel über den Vertraulichkeit gewährleistenden Übertragungskanal zum Kontrollzentrum übertragen werden.

12. Verfahren zur Authentifizierung von nach einem der Ansprüche 1 bis 11 markierten Gegenständen an einem Gegenstands-Prüfterminal, mit folgenden Schritten:
– Lesen eines Markierbildes und Transformieren desselben in Daten,
– Lesen eines verschlüsselten Code,
– Entschlüsseln zur Wiedergewinnung der Bilddaten vom ausgelesenen Code,
– Vergleichen der gewonnenen Daten mit den ausgelesenen Bilddaten, dadurch gekennzeichnet, dass
– die Existenz einer jeweiligen Textur auf dem Bild als zusätzliches Kriterium spezifiziert wird, wenn Authentifizierung ausgeführt wird, wonach das Bild ausgelesen wird.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass
– das Lesen des Markierbildes, das Lesen des verschlüsselten Code und das Spezifizieren des Kriteriums der Texturgegenwart am Prüfterminal ausgeführt werden, die ausgelesenen Bilddaten und der ausgelesene verschlüsselte Code zum Kontrollzentrum übertragen werden,
– das Entschlüsseln zur Wiedergewinnung der Bilddaten aus dem ausgelesenen Code und das Vergleichen des gewonnenen Bildes mit den Daten des ausgelesenen Bildes im entfernten Kontrollzentrum erfolgen.

14. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass
– das Lesen des Markierbildes, das Lesen des verschlüsselten Code und das Spezifizieren des Kriteriums der Texturgegenwart am Prüfterminal erfolgen, wobei die ausgelesenen Codedaten zum Kontrollzentrum übertragen werden,
– das Entschlüsseln zur Gewinnung der Bilddaten aus dem Auslesecode im entfernten Zentrum erfolgt und das gewonnene Prüfergebnis zum Prüfterminal übertragen wird,
– das Vergleichen der gewonnenen Daten mit den Daten des ausgelesenen Authentifizierungsbildes im Prüfterminal erfolgt.

15. Verfahren nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass im Verlauf des Vergleichs Fehler geschätzt werden und eine Entscheidung auf der Basis eines vorgegebenen Kriteriums erfolgt.

16. Verfahren zur Authentifizierung und Erfassung gefälschter Gegenstände mit folgenden Schritten:
– Erzeugen eines eindeutigen Bildes als wenigstens zweidimensionales Zufallsbild,
– Aufbringen des erzeugten Zufallsbildes auf eine Oberfläche mit einer Textur mit unregelmäßigen Parametern,
– Lesen des resultierenden Bildes,
– Übertragen der Daten über das ausgelesene Bild zu einem entfernten Kontrollzentrum,
– Erzeugen privater Schlüssel,
– Verschlüsseln der erhaltenen eindeutigen Bilddaten durch die privaten Schlüssel,
– Übertragen des sich ergebenden Code zu einer Markierstation,
– Aufbringen des resultierenden Code auf die Markieroberfläche,
– Speichern der Schlüssel in der Datenbank des Kontrollzentrums,
– Verifizieren der Gegenwart und des Texturmusters auf der Markieroberfläche in einem Prüfterminal und darauf
– Test-Lesen des Markierbildes und des aufgebrachten Code,
– Übertragen der Codedaten zum Kontrollzentrum,
– Entschlüsseln der Codedaten und Gewinnen der Daten über das ausgelesene Bild,
– Übertragen der gewonnenen Daten zum Prüfterminal,
– Vergleichen der gewonnenen Daten mit den Daten über das ausgelesene Bild,
– Entscheiden über die Authentizität Gegenstandes.

17. Verfahren zur Authentifizierung und Erfassung gefälschter Gegenstände mit folgenden Schritten:
– Erzeugen eines eindeutigen Bildes als wenigstens zweidimensionales Zufallsbild,
– Aufbringen des erzeugten Zufallsbildes auf eine Oberfläche mit einer Textur mit unregelmäßigen Parametern,
– Lesen des resultierenden Bildes,
– Übertragen der Daten über das ausgelesene Bild zu einem entfernten Kontrollzentrum,
– Erzeugen privater Schlüssel,
– Codieren der erhaltenen eindeutigen Bilddaten durch die privaten Schlüssel,
– Übertragen des sich ergebenden Code zu einer Markierstation,
– Aufbringen des resultierenden Code auf die Markieroberfläche,
– Speichern der Schlüssel in der Datenbank des Kontrollzentrums,
– Verfizieren der Gegenwart und des Texturmusters auf der Markieroberfläche und darauf
– Test-Lesen des Markierbildes und des aufgebrachten Code,
– Übertragen der ausgelesenen Bilddaten und des Code zum Kontrollzentrum,
– Entschlüsseln der Codedaten und Gewinnen der Daten über das ausgelesene Bild,
– Übertragen der gewonnenen Daten zum Prüfterminal,
– Vergleichen der gewonnenen Daten mit dem nach

dem Test-Lesen empfangenen Bild,
– Übertragen der Vergleichsergebnisse zum Prüfterminal.

18. Verfahren nach Anspruch 16 oder 17, dadurch gekennzeichnet, dass die Daten über die ausgeführten Tests im Kontrollzentrum gespeichert werden, wobei die Anzahl der gleichen Codetests zusammengefasst wird, und, wenn ein voreingestellter Wert überschritten wird, ein Alarmsignal über die Überschreitung erzeugt wird.

19. System zur Authentifizierung von nach Anspruch 1 markierten Gegenständen, mit einer Markiereinrichtung enthaltend:
– einen Drucker (**5**),
– eine Druckersteuerung,
– ein Auslesegerät (**6**),
– eine Bildverarbeitungseinheit (**16**),
– eine Kommunikationseinrichtung (**8**, **9**), und
– ein entferntes Verarbeitungs- und Speicherzentrum mit
– einer Schlüssel-Erzeugungseinheit (**19**),
– einer Verschlüsselungs-/Entschlüsselungseinheit (**20**),
– einer Speichereinheit (**23**),
– einer Vergleichseinrichtung (**22**) und freie Teile für Aufkleber (**1**),
dadurch gekennzeichnet, dass die Markiereinrichtung ferner enthält:
– eine Zufallsbild-Erzeugungseinrichtung (**14**),
– eine Einrichtung (**18**) zum Anbringen eines verschlüsselten Code, und
– Substrate aus einem Material mit einer Textur mit Zufallsparametern, die als leere Teile für Aufkleber verwendet werden.

20. System zur Authentifizierung von nach Anspruch 2 markierten Gegenständen, mit einer Markiereinrichtung enthaltend:
– einen Drucker (**5**),
– eine Druckersteuerung,
– ein Auslesegerät (**6**),
– eine Bildverarbeitungseinheit (**16**),
– eine Kommunikationseinrichtung (**8**, **9**), und
– ein entferntes Verarbeitungs- und Speicherzentrum mit
– einer Schlüssel-Erzeugungseinheit (**19**),
– einer Verschlüsselungs-/Entschlüsselungseinheit (**20**),
– einer Speichereinheit (**23**),
– einer Vergleichseinrichtung (**22**) und freie Teile für Aufkleber (**1**),
dadurch gekennzeichnet, dass die Markiereinrichtung ferner enthält:
– eine Zufallsbild-Erzeugungseinrichtung (**14**),
– eine Einrichtung (**18**) zum Anbringen eines verschlüsselten Code, und
– Einrichtungen zum Umformen von Aufkleberflächen in eine dreidimensionale Textur mit Zufallsparametern.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

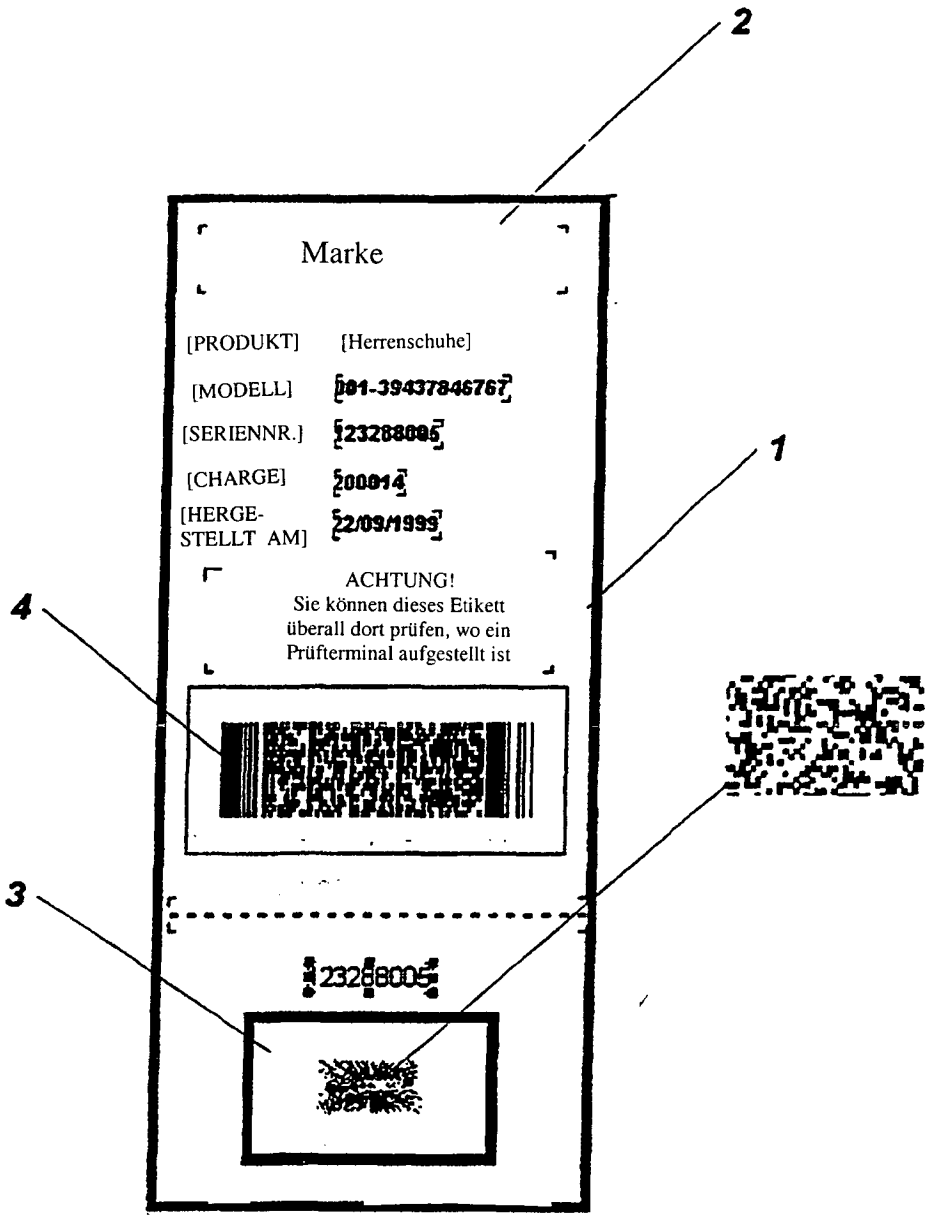

Fig. 1

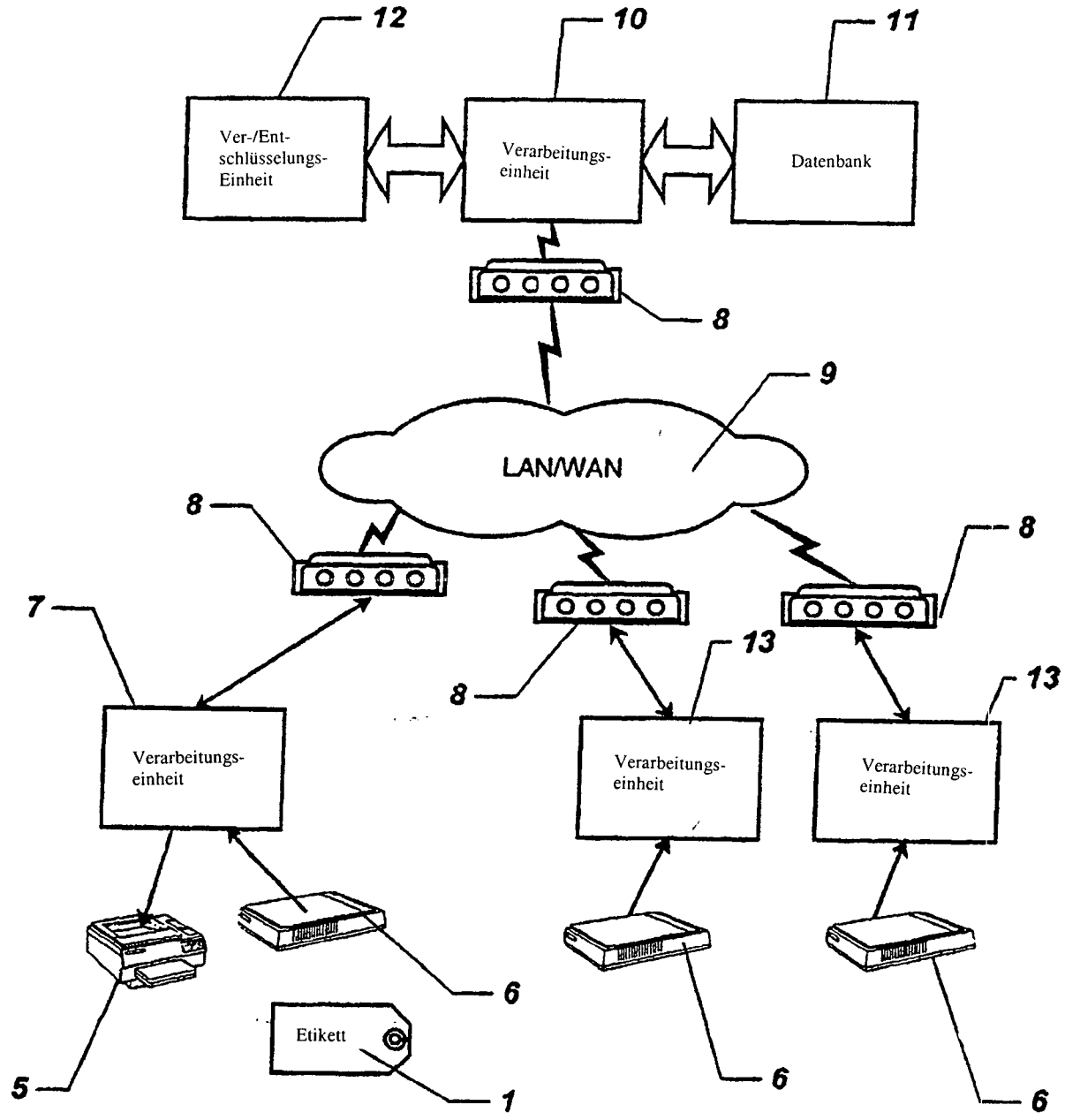
12
10
11
Ver-/Ent-schlüsselungs-Einheit
Verarbeitungs-einheit
Datenbank
8
9
LAN/WAN
8
8
8
7
13
13
Verarbeitungs-einheit
Verarbeitungs-einheit
Verarbeitungs-einheit
6
Etikett
5
1
6
6

Fig. 2

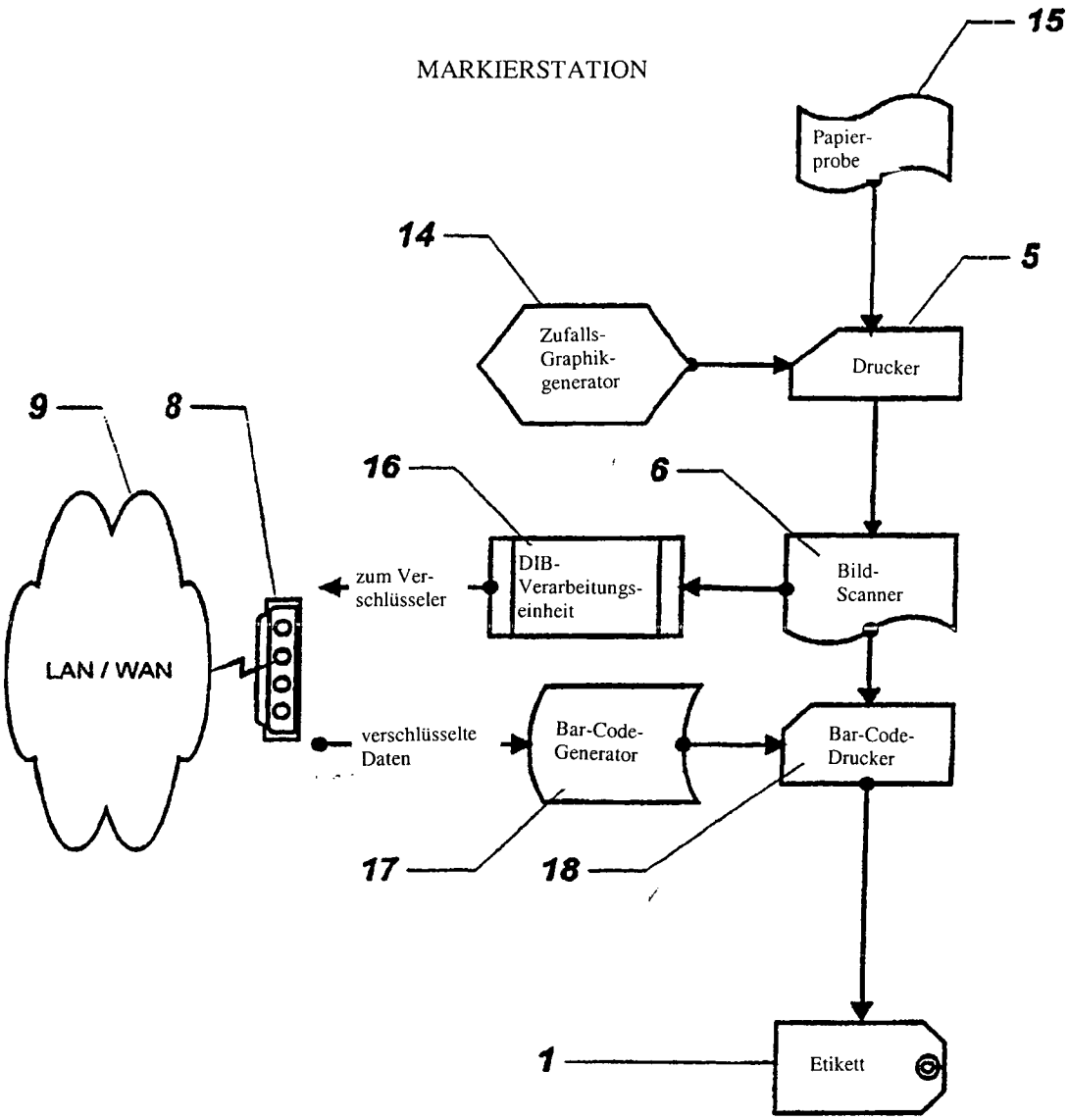
MARKIERSTATION
15
Papier-probe
14
Zufalls-Graphik-generator
5
Drucker
9
8
16
6
LAN / WAN
zum Ver-schlüsseler
DIB-Verarbeitungs-einheit
Bild-Scanner
verschlüsselte Daten
Bar-Code-Generator
Bar-Code-Drucker
17
18
1
Etikett

Fig.3

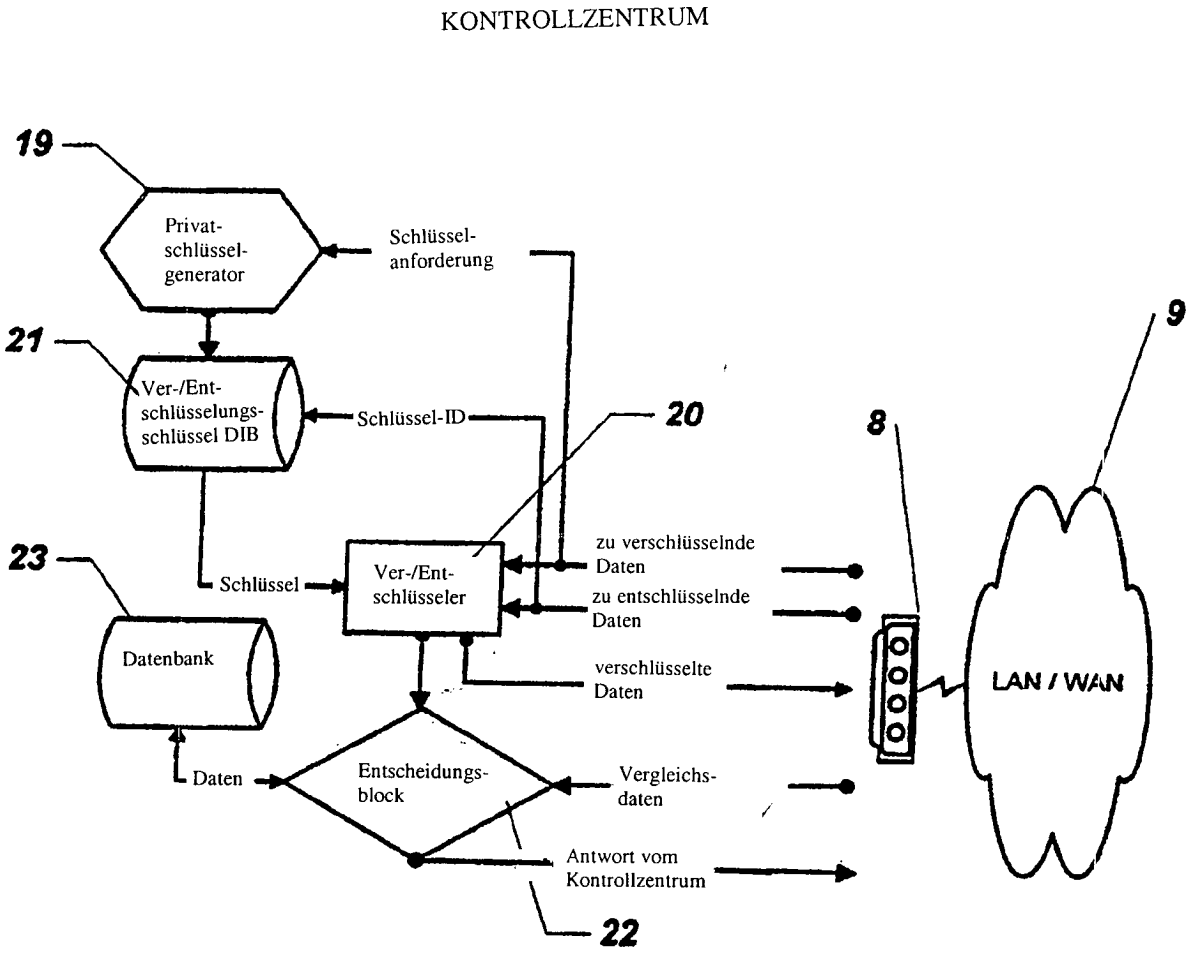
KONTROLLZENTRUM
19
Privat-schlüssel-generator
Schlüssel-anforderung
21
Ver-/Ent-schlüsselungs-schlüssel DIB
Schlüssel-ID
20
8
9
23
Schlüssel
Ver-/Ent-schlüsseler
zu verschlüsselnde Daten
zu entschlüsselnde Daten
Datenbank
verschlüsselte Daten
LAN / WAN
Daten
Entscheidungs-block
Vergleichs-daten
Antwort vom Kontrollzentrum
22

Fig. 4

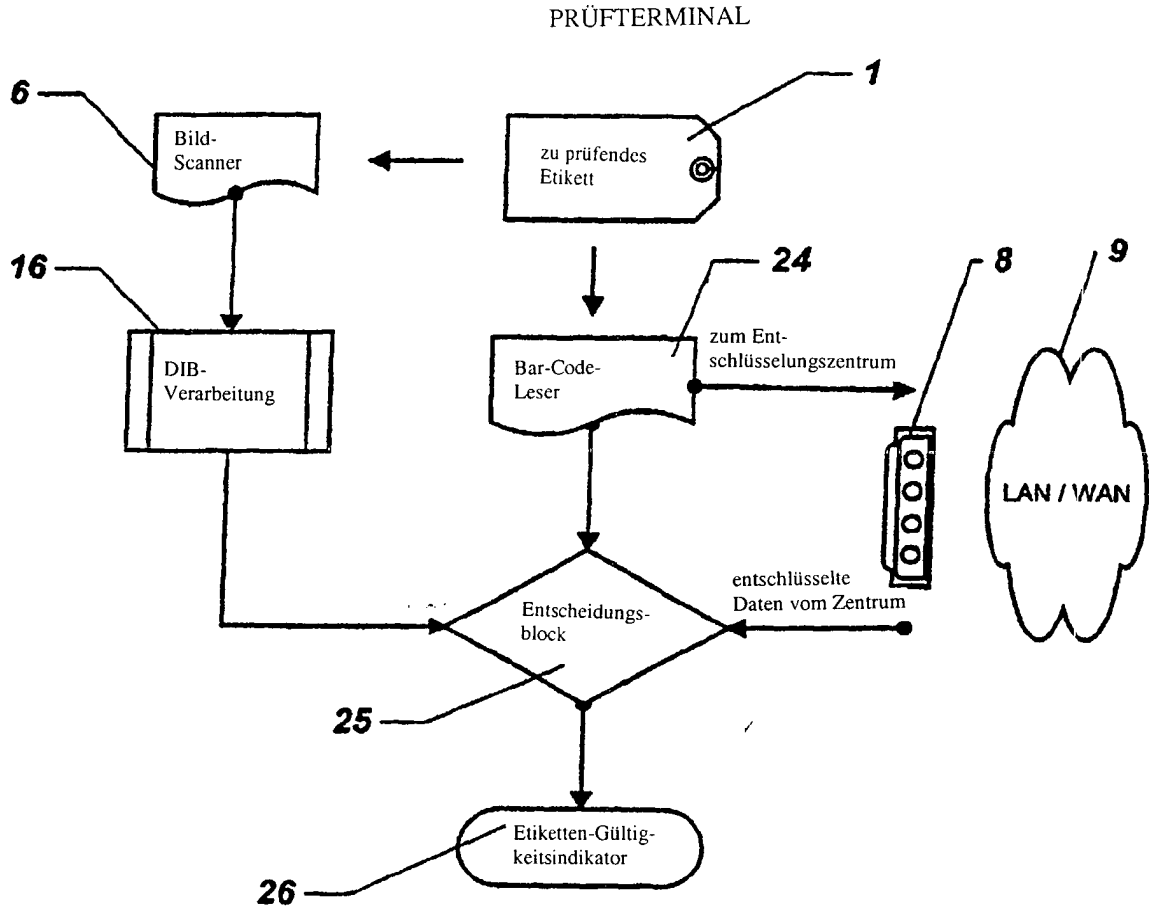
PRÜFTERMINAL
6
Bild-
Scanner
1
zu prüfendes
Etikett
16
DIB-
Verarbeitung
24
Bar-Code-
Leser
zum Ent-
schlüsselungszentrum
8
9
LAN / WAN
entschlüsselte
Daten vom Zentrum
Entscheidungs-
block
25
Etiketten-Gültig-
keitsindikator
26

Fig. 5