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

(10) **DE 10 2008 028 881 A1** 2009.01.02

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2008 028 881.0**
(22) Anmeldetag: **18.06.2008**
(43) Offenlegungstag: **02.01.2009**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
***G06F 21/00*** (2006.01)

(30) Unionspriorität:
**60/929,222 18.06.2007 US**

(71) Anmelder:
**Discretix Technologies Ltd., Netanya, IL**

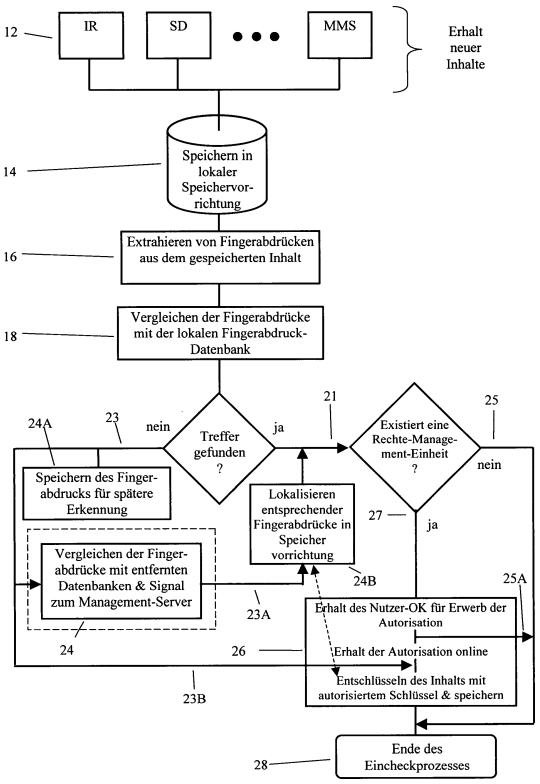
(74) Vertreter:
**Anwaltskanzlei Gulde Hengelhaupt Ziebig & Schneider, 10179 Berlin**

(72) Erfinder:
**Bar-el, Hagai, Rehovot, IL**

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen**

(54) Bezeichnung: **Verfahren und System zum prüfen und autorisieren von Inhalt**

(57) Zusammenfassung: Es werden ein Gerät und ein Verfahren zum Verhindern der Verwendung von nicht zugelassenem empfangenem elektronischem Inhalt auf einer Mobilstation offenbart. Das Gerät und das Verfahren können einschließen: Module zum Extrahieren und Vergleichen von Fingerabdrücken des empfangenen Inhalts auf der Mobilstation mit Fingerabdrücken von nicht zugelassenem Inhalt und für die Aktivierung eines Autorisierungsvorgangs auf der Grundlage der Ergebnisse des Vergleichs sowie der Entscheidungen des Benutzers hinsichtlich des Kaufs der Autorisierung, falls diese erforderlich ist. Es wird eine kryptographiebasierte Eincheckprozedur eingeführt, um sicherzustellen, dass jeglicher Inhalt die Verifizierungsphase durchlaufen hat.



## Beschreibung

### VERWEISUNG AUF VERWANDTE ANMELDUNGEN

**[0001]** Diese Anmeldung beansprucht den Vorteil der vorläufigen US-Anmeldung mit der laufenden Nr. 60/929,222, eingereicht am 18. Juni 2007, mit dem Titel METHOD AND SYSTEM FOR SCREENING AND AUTHORIZING COPYRIGHTED CONTENT, die durch Bezugnahme in ihrer Gesamtheit hierin eingeschlossen ist.

### HINTERGRUND DER ERFINDUNG

**[0002]** Urheberrechtlich geschützter elektronischer Inhalt kann gegen illegale oder nicht autorisierte Verwendung auf bekannte Weise geschützt werden, wie z. B. durch Digital Rights Management (DRM), wobei es sich um einen Sammelbegriff handelt, der von Verlagen oder Urheberrechtsinhabern verwendete Technologien zum Kontrollieren des Zugriffs auf Digitaldaten oder der Nutzung derselben bezeichnet. Solche Technologien schließen häufig die Verschlüsselung der Darstellung von solchem Inhalt ein, um eine bessere Kontrolle über seine Verbreitung zu ermöglichen.

**[0003]** DRM-Systeme unterscheiden sich hinsichtlich ihrer Robustheit. Die Robustheit wird durch die Ausgestaltung der DRM-Konzepte sowie durch Faktoren, die mit den Plattformen, auf denen die DRM-Systeme laufen, zusammenhängen, beeinflusst. Es ist beispielsweise festzustellen, dass geschlossene Plattformen (d. h. Plattformen, in die keine nicht zugelassene Software eingebracht werden kann) für DRM-Anwendungen geeigneter sind als offene Plattformen (d. h. Plattformen, auf denen der Benutzer Software seiner Wahl installieren kann). Wenn ein DRM-System (oder eine DRM-Installation) aufgebrochen wird, kann dies die Verfügbarkeit von zuvor verschlüsseltem Inhalt in (unverschlüsselter) Reintext-Form zur Folge haben. Inhalt in unverschlüsselter (und somit ungeschützter) Form kann gegen den Willen des Inhabers der Verbreitungsrechte hinsichtlich dieses Inhalts und/oder ohne korrekte Vergütung an denselben uneingeschränkt verbreitet werden. Inhalt, dessen Verbreitung der rechtmäßige Verteiler kontrollieren möchte, während solcher Inhalt in unverschlüsselter Form dargestellt wird, wird nachfolgend als „ungeschützter Inhalt" bezeichnet.

**[0004]** Ungeschützter Inhalt kann verbreitet werden und auch in Vorrichtungen eingebracht werden, die mit einem intakten DRM-Modul versehen sind. Das DRM-Modul auf solchen Vorrichtungen, das für die Regelung des Konsums von geschütztem Inhalt konzipiert ist, kann nicht so angepasst werden, dass es den Konsum von solchem ungeschütztem Inhalt einschränkt.

**[0005]** Häufig wird eine Einschränkung des Konsums von Inhalt durch die Verwendung von Datenobjekten erreicht, die den Ausdruck von Beschränkungen hinsichtlich der Nutzung des Inhalts durch die Verwendung einer Bezeichnungsweise einschließen. Diese Datenobjekte, die mitunter auch als Rechte-Objekte bezeichnet werden, enthalten auch einen Schlüssel, der verwendet wird, um das verschlüsselte Inhaltsobjekt zu entschlüsseln. Eine solche Verschlüsselung bildet die Mittel, die den Inhalt an sein Rechte-Objekt binden. Wenn der Inhalt in seiner Reintext-Form (d. h. unverschlüsselt) verfügbar ist, kann er verwendet werden, ohne das Rechte-Objekt hinzuzuziehen, häufig sogar, ohne zu wissen, dass für den Inhalt ein solches Rechte-Objekt existiert.

**[0006]** Daher basiert die Robustheit des DRM-Systems in einem gewissen Maß auf der Inhaltsverfügbarkeit nur in geschützter (d. h. verschlüsselter) Form. Die Wirksamkeit des DRM-Systems auf einer Vorrichtung kann behindert sein, wenn ungeschützter Inhalt in die Vorrichtung eingebracht wird.

**[0007]** Folglich stellen die DRM-Mechanismen in angemessen geschützten Umgebungen, wie z. B. denen einer Mobilstation, wie z. B. eines Mobiltelefons oder eines Personal Media Player (PMP), möglicherweise nicht die erwarteten Schutzmaßnahmen bereit, wenn nicht autorisierter, d. h. geraubter, ungeschützter, Inhalt empfangen wird. Solcher ungeschützter Inhalt kann von einem weniger geschützten Gerät, wie z. B. einem Personalcomputer (PC), empfangen werden, z. B. in der Folge eines Kompromisses eines DRM-Systems, der möglicherweise auf diesem anderen Gerät aufgetreten ist.

**[0008]** Ungeachtet der Stärke des DRM-Mechanismus auf der MS kann ungeschützter Inhalt allgemein verfügbar sein, beispielsweise zum Erwerb über das Internet. Dieser ungeschützte Inhalt wird zum Download und zum Konsum, z. B. auf PCs, angeboten. Solange ungeschützter Inhalt irgendwie erhältlich ist, kann solcher ungeschützter Inhalt in eine MS eingebracht werden und die Wirksamkeit des Geschäftsmodells der Verbreitung von mobilem Inhalt behindern. Es ist daher von Vorteil, über ein System und ein Verfahren zu verfügen, das eine Lösung zum Schutz einer MS vor dem Empfang, der Speicherung und/oder der Wiedergabe bestimmter Arten von ungeschütztem Inhalt bereitstellen kann. Ein gewünschtes Ergebnis einer solchen Lösung ist, dass die Verfügbarkeit von ungeschütztem Inhalt, beispielsweise in PC-Umgebungen, wie z. B. durch Rippen von CDs oder durch Filesharing über Peer-to-Peer-Netzwerke und dergleichen, nicht zum Konsum von solchem ungeschütztem Inhalt auf einer MS führt und somit das Geschäftsmodell der robusten DRM-Installation auf der MS nicht schwächt.

## ZUSAMMENFASSUNG DER ERFINDUNG

**[0009]** Es werden ein Gerät und ein Verfahren zum Verhindern und Kontrollieren der Verwendung von nicht zugelassenem ungeschützten Inhalt beschrieben. Das Gerät und das Verfahren können einschließen: Module zum Extrahieren von Fingerabdrücken aus den empfangenen elektronischen Inhaltselementen, zum Vergleichen der extrahierten Fingerabdrücke mit Fingerabdrücken von nicht zugelassenem ungeschütztem Inhalt und zur Aktivierung eines Autorisierungsprozesses auf der Grundlage des Vergleichs und der Entscheidungen eines Benutzers hinsichtlich des Kaufs der Autorisierung, falls diese erforderlich ist. Das erfindungsgemäße Gerät und das erfindungsgemäße Verfahren können die Verwendung oder die Wiedergabe von nicht zugelassenem ungeschütztem Inhalt sperren. Das Gerät und das Verfahren können auf verschiedenen Vorrichtungen und in einer Vielzahl von Umgebungen implementiert werden.

## KURZE BESCHREIBUNG DER ZEICHNUNGEN

**[0010]** Der als die Erfindung angesehene Gegenstand ist im abschließenden Teil der Patentschrift konkret ausgewiesen und klar beansprucht. Die Erfindung wird jedoch sowohl hinsichtlich der Organisation als auch des Betriebsverfahrens zusammen mit Zielen, Merkmalen und Vorteilen derselben durch Heranziehen der folgenden detaillierten Beschreibung und der beigefügten Zeichnungen am besten verständlich. Es zeigt:

**[0011]** Fig. 1 einen schematischen Ablaufplan eines Verfahrens gemäß einigen Ausführungsformen der vorliegenden Erfindung und

**[0012]** Fig. 2 ein schematisches Blockdiagramm eines Systems gemäß einigen Ausführungsformen der vorliegenden Erfindung.

**[0013]** Es sollte klar sein, dass der Einfachheit und Klarheit der Darstellung halber die in den Figuren gezeigten Elemente nicht unbedingt maßstabsgerecht gezeichnet wurden. Beispielsweise können die Abmessungen einiger Elemente bezogen auf andere Elemente der Klarheit halber übertrieben sein. Ferner können, wo dies für angemessen erachtet wurde, Bezugszeichen in den Figuren wiederholt verwendet worden sein, um einander entsprechende oder analoge Elemente anzuzeigen. Darüber hinaus können einige der in den Zeichnungen dargestellten Blöcke zu einer einzigen Funktion kombiniert werden.

## DETAILLIERTE BESCHREIBUNG DER VORLIEGENDEN ERFINDUNG

**[0014]** In der folgenden detaillierten Beschreibung sind zahlreiche konkrete Einzelheiten dargelegt, um ein gründliches Verständnis der Erfindung zu ermöglichen. Dem Fachmann sollte jedoch klar sein, dass die vorliegende Erfindung ohne diese konkreten Details praktiziert werden kann. An anderen Stellen wurden gut bekannte Verfahren, Prozeduren und Komponenten nicht detailliert beschrieben, um die vorliegende Erfindung nicht undeutlich zu machen.

**[0015]** In der folgenden detaillierten Beschreibung sind zahlreiche konkrete Einzelheiten dargelegt, um ein gründliches Verständnis der Erfindung zu ermöglichen. Dem Fachmann sollte jedoch klar sein, dass die vorliegende Erfindung ohne diese konkreten Details praktiziert werden kann. An anderen Stellen wurden gut bekannte Verfahren, Prozeduren, Komponenten und Schaltungen möglicherweise nicht detailliert beschrieben, um die vorliegende Erfindung nicht undeutlich zu machen.

**[0016]** Es wird angenommen, dass der Besitz von ungeschütztem Inhalt sowie von nicht zugelassenem ungeschütztem Inhalt, wie z. B. illegal kopiertem Inhalt, auf einigen Plattformen und/oder in einigen Umgebungen, bei denen es sich nicht um eine MS handelt, immer möglich sein wird. Somit kann der Schutz einer MS vor dem Speichern und/oder Verwenden von nicht zugelassenem ungeschütztem Inhalt vorzugsweise beim Einbringen von solchem Inhalt in eine MS und auf eine Weise, bei der nicht angenommen wird, dass der eingebrachte Inhalt eine geschützte Form aufweist, erfolgen. Eine der Möglichkeiten, um zu verhindern, dass scheinbar zugelassener Reintext-Inhalt auf einer MS in nicht zugelassener Weise verwendet wird, ist die Verwendung der Basis „sichere Ausführung", die mitunter auf mobilen Plattformen verfügbar ist, um die Verwendung von nicht zugelassenem ungeschütztem Inhalt zu erkennen und zu verhindern, wie hierin offenbart.

**[0017]** Obwohl die vorliegende Erfindung in dieser Hinsicht nicht beschränkt ist, kann solcher nicht zugelassener ungeschützter Inhalt Inhalt sein, der auf Verbraucherplattformen nur in geschützter Form verfügbar sein soll, z. B. so, dass seine Nutzung eingeschränkt werden kann, wie z. B. durch die Verwendung eines auf der MS implementierten Digital-Rights-Management-(DRM-)Konzepts.

**[0018]** Obwohl die vorliegende Erfindung in dieser Hinsicht nicht beschränkt ist, kann solcher nicht zugelassener ungeschützter Inhalt Inhalt sein, dessen Verwendung aus anderen rechtlichen und/oder moralischen Gründen nicht gestattet ist.

**[0019]** Obwohl die vorliegende Erfindung in dieser Hinsicht nicht beschränkt ist, kann solcher nicht zugelassener ungeschützter Inhalt in Form von Soundtracks oder Videoclips vorliegen.

**[0020]** Nicht zugelassener ungeschützter Inhalt

kann auf einer MS gefiltert werden. Eine solche Filterung kann erfordern, dass nicht zugelassener ungeschützter Inhalt als solcher identifiziert wird. Die Identifizierung eines elektronischen Medieninhalts kann durch die Verwendung von akustischen und/oder Video-Fingerabdrücken dieses Inhalts erreicht werden. Die Fingerabdruck-Technologie, wie auf dem Fachgebiet bekannt, ermöglicht die Zuordnung eines Inhalts zu einem oder mehreren entsprechenden „Fingerabdruck/Fingerabdrücken" und den Vergleich von Fingerabdrücken eines ersten Inhaltselements mit Fingerabdrücken eines zweiten Inhaltselements. Die Zuordnung von Fingerabdrücken zu einem konkreten Inhaltselement kann gemäß einem von mehreren Extraktionsverfahren erfolgen. Der Vergleich zwischen Fingerabdrücken kann gemäß einem gegebenen Schwellenwert und einem oder mehreren Kriterium/Kriterien erfolgen. Eine Übereinstimmung zwischen zwei Fingerabdrücken kann als Situation definiert werden, in welcher der Grad der Ähnlichkeit zwischen diesen zwei Fingerabdrücken basierend auf diesem einen Kriterium oder diesen mehreren Kriterien zum Bestimmen der Ähnlichkeit, den gegebenen Schwellenwert übersteigt. Die Bestimmung des Grads der Ähnlichkeit kann gemäß auf dem Fachgebiet bekannten Verfahren erfolgen. Bei dem zweiten Inhaltselement handelt es sich üblicherweise um ein bekanntes Inhaltsobjekt. Ein solcher Fingerabdruckvergleich kann in seiner Wirkung einem bitweisen Vergleich von Inhaltsdateien ähneln, ausgenommen, dass er nicht durch eine einfache Veränderung des getesteten Inhaltselements, wie z. B. durch leichtes Trunkieren oder durch Verändern seiner Digitalisierungseigenschaften, vereitelt werden kann. Dieser Vergleich kann einen Indikationswert ergeben, der die Ähnlichkeit des ersten Inhaltselements und des zweiten Inhaltselements anzeigen kann. Im Fall, dass ein geprüftes Inhaltselement mit einem Referenz-Inhaltselement verglichen wird, kann der Indikationswert einen „Ja/Nein"-Wert aufweisen, der anzeigt, ob die zwei Inhaltselemente miteinander „übereinstimmen" oder „nicht übereinstimmen". Der Indikationswert kann einen von zwei oder mehr diskreten Werten aufweisen, der die Zuordnung des Vergleichsergebnisses zu einem einer Gruppe möglicher Ergebnisse anzeigt.

**[0021]** Es wird jetzt Bezug genommen auf Fig. 1, die ein schematischer Ablaufplan eines Verfahrens gemäß einigen Ausführungsformen der vorliegenden Erfindung ist, und Fig. 2, die ein schematisches Blockdiagramm eines Systems **100** gemäß einigen Ausführungsformen der vorliegenden Erfindung ist.

**[0022]** Fig. 2 stellt ein System **100** dar, das eine MS **50**, wie z. B. eine Mobiltelefonvorrichtung oder dergleichen, und (eine) Fingerabdruck-Einheit(en) **62** umfassen kann. Die MS **50** kann eine lokale Speichereinheit **52** zum Speichern ankommender elektronischer Inhaltselemente (auch als Inhaltsobjekte bezeichnet) umfassen, die von einem beliebigen verfügbaren Eingangskanal, wie z. B. einem Infrarot-(IR-)Eingang, Speicherkarten, wie z. B. SD-Karten (Speicherkarten laut Spezifikation der SD Association (SDA)) oder MMC-Karten (Speicherkarten laut Spezifikation der Multi Media Card Association (MMCA)), Multimedia Messaging System (MMS), direktes Download und dergleichen, verfügbar sind. Die MS **50** kann ferner umfassen: eine Fingerabdruck-Extraktionseinheit **53**, um Fingerabdrücke aus den in der lokalen Speichereinheit **52** gespeicherten ankommenden elektronischen Inhaltselementen zu extrahieren, und eine lokale Datenbank **54**, um Fingerabdrücke von nicht zugelassenen ungeschützten Inhaltselementen zu speichern. Die MS **50** kann ferner eine Fingerabdruck-Vergleichseinheit **56** umfassen, um durch die Fingerabdruck-Extraktionseinheit **53** extrahierte Fingerabdrücke mit in der lokalen Bank **54** gespeicherten Fingerabdrücken zu vergleichen. Die Fingerabdruck-Vergleichseinheit **56** kann ferner mit (einer) entfernten Fingerabdruck-Speichereinheit(en) **62** verbindbar sein, beispielsweise über eine Mobilfunkverbindung, zum Vergleichen des extrahierten Fingerabdrucks mit in der/den entfernten Fingerabdruck-Speichereinheit(en) **62** gespeicherten Fingerabdrücken. Die Fingerabdruck-Speichereinheit(en) **62** kann/können Teil eines Management-Servers (nicht gezeigt) sein; in anderen Ausführungsformen können sie jedoch auch voneinander getrennt sein. Der Management-Server kann dafür zuständig sein, die Server-Seite anderer relevanter Wartungsvorgänge auf der MS **50** auszuführen, wie nachstehend erläutert. Die MS **50** kann ferner eine Rechte-Management-Einheit **58** umfassen, damit der Benutzer nach einem Autorisationszyklus, der eine erfolgreiche finanzielle Transaktion umfassen kann, eine Freigabe hinsichtlich der Verwendung empfangener Inhaltsobjekte erhalten kann. Die erfolgreiche finanzielle Transaktion kann sicherstellen, dass für das Recht, die betreffenden Inhaltsobjekte zu nutzen, eine Vergütung erhalten wurde. Die MS **50** kann ferner eine Inhaltsverschlüsselungseinheit **60** umfassen, um mit einem Autorisierungsschlüssel zu verschlüsseln: Inhaltsobjekte, für deren Fingerabdrücke ermittelt wurde, dass sie nicht mit Fingerabdrücken von nicht zugelassenen ungeschützten Inhaltselementen übereinstimmen, die entweder lokal in der lokalen Bank (**54**) und/oder entfernt in (einer) Fingerabdruck-Speichereinheit(en) **62** gespeichert sind, und Inhaltselemente, die bereits durch die Rechte-Management-Einheit **58** freigegeben wurden. Schließlich kann die MS **50** eine Speichereinheit **61** umfassen, um mit einem Autorisierungsschlüssel verschlüsselte Inhaltselemente zu speichern. Es sollte dem Fachmann klar sein, dass einige oder alle Einheiten oder Module, die ähnliche Funktionen aufweisen, wie z. B. Speicher oder Speichereinheiten, in einer einzigen Vorrichtung und/oder einem einzigen Bereich implementiert sein können, in anderen Ausführungsformen jedoch ebenso in verschiedenen

physischen Einheiten implementiert sein können.

**[0023]** Die in Fig. 1 dargestellte Abfolge von Vorgängen kann beginnend mit dem Einbringen von elektronischem Inhalt in die MS **50** ausgeführt werden. Elektronischer Inhalt kann von einer oder mehreren einer Vielzahl von Quellen, wie bei Block **12** angezeigt, empfangen werden, wie z. B. einem Infrarot-(IR-)-Kommunikationskanal, einem SD-Kanal, einem Multimedia-Messaging-System-(MMS-)Kanal und dergleichen. Der ankommende Inhalt kann in einer lokalen Speichervorrichtung **52** (wie bei Block **14** angegeben) gespeichert werden. Dann können durch die Fingerabdruck-Extraktionseinheit **53** Fingerabdrücke aus dem gespeicherten Inhalt extrahiert werden (wie bei Block **16** angegeben) und ferner durch die Fingerabdruck-Vergleichseinheit **56** mit Fingerabdrücken in einer lokalen Bank von Fingerabdrücken nicht zugelassener ungeschützter Inhaltsdateien, die beispielsweise in der lokalen Bank **54** auf der MS **50** gespeichert sind, verglichen werden (wie bei Block **18** angegeben). Eine solche lokal gespeichert Bank von Fingerabdrücken, die lokale Bank **54**, kann typischerweise Fingerabdrücke mehrerer tausend nicht zugelassener ungeschützter Inhaltselemente umfassen. Die lokale Bank **54** kann beispielsweise Fingerabdrücke ausgewählter Inhaltselemente umfassen, wie z. B. eine oder mehrere Hot-List(s) nicht zugelassener ungeschützter Inhaltselemente, die aufgrund ihrer Popularität oder beliebiger anderer gewünschter Kriterien darin eingeschlossen sind. Der Vergleich des extrahierten Fingerabdrucks mit denen, die lokal in der lokalen Bank **54** gespeichert sind, kann ein positives Ergebnis erbringen (d. h. eine Übereinstimmung des extrahierten Fingerabdrucks mit einem lokal gespeicherten Fingerabdruck wurde ermittelt, was die Wahrscheinlichkeit zeigt, dass der ankommende Inhalt dem Inhaltselement ähnelt, das dem lokal gespeicherten Fingerabdruck zugeordnet ist), wie durch den Pfad **21** angezeigt. Dieser Vergleich kann in anderen Fällen jedoch ein negatives Ergebnis erbringen, d. h. es wurde keine solche Übereinstimmung gefunden, wie durch den Pfad **23** angegeben.

**[0024]** Der Vergleich des extrahierten Fingerabdrucks mit denen, die in der lokalen Bank **54** gespeichert sind, kann die Form des Einander-Zuordnens anhand eines Schwellenwerts statt durch bitweisen Vergleich aufweisen. Ein Erkennungsschwellenwert-Parameter kann durch den Management-Server auf der MS **50** festgelegt sein und geregelt werden. Ein solcher Erkennungsschwellenwert-Parameter kann das Gleichgewicht zwischen falschen positiven und falschen negativen Erkennungsraten herstellen, wie auf dem Fachgebiet bekannt.

**[0025]** Der Management-Server kann den Wert des Erkenungsschwellenwert-Parameters willkürlich festlegen und kann verschiedene Werte für den Erkennungsschwellenwert-Parameter für verschiedene Exemplare der MS **50** aufrechterhalten. Die Regelung des Erkennungsschwellenwert-Parameters durch den Management-Server kann durch jedes Kommunikationsprotokoll, wie auf dem Fachgebiet bekannt, erfolgen, einschließlich, jedoch nicht beschränkt auf vorhandene Vorrichtungsmanagementprotokolle, die möglicherweise bereits verwendet werden. Im Fall, dass eine Übereinstimmung mit lokal gespeicherten Fingerabdrücken gefunden wurde, und im Fall, dass eine Rechte-Management-Einheit **58** in der MS **50** existiert, kann dem Benutzer durch die MS **50** eine Option angeboten werden, die Autorisierung zum Verwenden des identifizierten elektronischen Inhaltselements zu erhalten (wie durch den Pfad **27** angezeigt). Wenn der Benutzer den Erhalt der Autorisierung bestätigt hat, um das elektronische Inhaltselement zu verwenden, kann ein Autorisierungszyklus zwischen dem Benutzer und dem Inhaber der Verbreitungsrechte hinsichtlich dieses Inhaltselements oder zwischen dem Benutzer und einer anderen geeigneten Stelle ausgelöst werden. Dieser Zyklus kann eine erfolgreiche finanzielle Transaktion umfassen, die sicherstellt, dass für das Recht, das Inhaltselement zu nutzen, eine Vergütung erhalten wurde. Nachdem die Autorisierung zur Verwendung des Inhaltselements erhalten wurde, wird das Element durch die Inhaltsverschlüsselungseinheit **60** mit einem Autorisierungsschlüssel verschlüsselt (wie bei Block **26** angezeigt) und kann als solches in der Speichereinheit **61** gespeichert werden. Wenn jedoch in der MS **50** keine Rechte-Management-Einheit **58** existiert (wie durch den Pfad **25** angezeigt) oder der Benutzer keine Autorisierung zur Verwendung des identifizierten Inhaltselements kauft (wie durch den Pfad **25A** angezeigt), wird keine Autorisierung zur Verwendung des Inhaltselements empfangen und es erfolgt keine Verschlüsselung des Inhaltselements mit einem Autorisierungsschlüssel.

**[0026]** Im Fall, dass keine Übereinstimmung gefunden wurde (wie durch den Pfad **23** angezeigt), können Fingerabdrücke von Inhaltselementen, für die keine Übereinstimmung gefunden wurde, für eine spätere Verifizierung gespeichert werden (wie bei Block **24A** angezeigt), und die MS **50** kann sich, beispielsweise über eine Mobilfunkverbindung, mit externen Ressourcen verbinden, um den Vergleich der gespeicherten extrahierten Fingerabdrücke von ankommenden Inhaltselementen mit entfernten Datenbanken von Fingerabdrücken auszulösen, die in einem Exemplar oder mehreren Exemplaren von Fingerabdruck-Speichereinheit(en) **62** gespeichert sind. Wenn eine Übereinstimmung mit einem Fingerabdruck/Fingerabdrücken in (einer) entfernten Fingerabdruck-Speichereinheit(en) **62** gefunden wurde (wie durch den Pfad **23A** angezeigt), kann die betreffende Datei, die in Block **24** identifiziert und in Block **26** verschlüsselt und gespeichert wurde, aufgefunden werden, wie in Block **24B** angezeigt, und die Abfolge

kann zur weiteren Verarbeitung, wie oben beschrieben, wie angezeigt mit dem Pfad **21** zusammenfließen. Ebenfalls im Fall, dass keine Übereinstimmung gefunden wird (wie durch den Pfad **23**, **23B** angezeigt), wird das geprüfte Element durch die Inhaltsverschlüsselungseinheit **60** mit einem Autorisierungsschlüssel verschlüsselt (wie bei Block **26** angezeigt) und kann als solches in der Speichereinheit **61** gespeichert werden. Man beachte, dass der Verschlüsselungsvorgang und der Entschlüsselungsvorgang in umgekehrter Reihenfolge ausgeführt werden können. Der Verschlüsselungs- und der Entschlüsselungsvorgang können nachstehend allgemein als kryptographische Vorgänge definiert sein. Dementsprechend kann die Inhaltsverschlüsselungseinheit **60** so betrieben werden, dass sie einen Entschlüsselungsvorgang ausführt, und die Entschlüsselungseinheit (nicht gezeigt) kann so betrieben werden, dass sie einen Verschlüsselungsvorgang ausführt. Beide Vorgänge können als kryptographische Vorgänge bezeichnet werden.

**[0027]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann der Management-Server die Inhalte der lokalen Bank **54** gelegentlich ändern. Beispielsweise kann der Management-Server die Inhalte der lokalen Bank **54** in Übereinstimmung mit einer oder mehreren Hot-List(s) nicht zugelassener ungeschützter Inhaltselemente halten, beispielsweise entsprechend ihrer Popularität.

**[0028]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann der Management-Server sicherstellen, dass die lokale Bank **54** Fingerabdrücke nicht zugelassener ungeschützter Inhaltselemente enthält, für die eine sofortige Erkennung, d. h. vor einem einzigen Konsumfall, am meisten gewünscht ist, während er erlaubt, dass die entfernte(n) Fingerabdruck-Speichereinheit(en) **62** auch Fingerabdrücke nicht zugelassener ungeschützter Inhaltselemente enthält/enthalten, die auf der MS **50** möglicherweise erst erkannt werden, nachdem sie mindestens einmal konsumiert wurden.

**[0029]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann der Management-Server sicherstellen, dass die lokale Bank **54** Fingerabdrücke nicht zugelassener ungeschützter Inhaltselemente enthält, für die festgestellt wird, dass sie für den konkreten Benutzer der MS **50** mit höherer Wahrscheinlichkeit von Interesse sind. Der Management-Server kann beispielsweise bestimmen, dass ein konkreter Benutzer wahrscheinlich versuchen wird, eine bestimmte Art von nicht zugelassenem ungeschütztem Inhalt zu nutzen, und kann somit die Inhalte der lokalen Bank **54** gemäß einer solchen Bestimmung zusammenstellen.

**[0030]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann der Management-Server sicherstellen, dass die lokale Bank **54** Fingerabdrücke nicht zugelassener ungeschützter Inhaltselemente enthält, für die festgestellt wird, dass ihr Konsum einen größeren finanziellen Schaden verursacht. Der Management-Server kann beispielsweise sicherstellen, dass die lokale Bank **54** Fingerabdrücke der aktuellen Titel der Unterhaltungsbranche, wie z. B. derjenigen, die als „Premium-Inhalt" angesehen werden, enthält, um zu verhindern, dass der Benutzer ungeschützte, d. h. geraubte, Kopien dieser Titel konsumiert.

**[0031]** Der Management-Server kann die Inhalte der lokalen Bank **54** willkürlich ändern und kann für verschiedene Exemplare der MS **50** verschiedene Inhalte in der lokalen Bank **54** aufrechterhalten, z. B. durch das Unterscheiden zwischen Benutzerprofilen, und somit beispielsweise Fingerabdrücke bereitstellen, die aus einer MS-spezifischen Liste von Inhaltselementen extrahiert sind. Die Verwaltung der Inhalte der lokalen Bank **54** durch den Management-Server kann durch ein beliebiges Kommunikationsprotokoll erfolgen, wie auf dem Fachgebiet bekannt, einschließlich, jedoch nicht beschränkt auf vorhandene Vorrichtungsmanagementprotokolle, die möglicherweise bereits verwendet werden.

**[0032]** Um sicherzustellen, dass auf der MS **50** nur autorisierter Inhalt wiedergegeben wird, kann schließlich ein Entschlüsselungseinheitsmodul (nicht gezeigt) in die MS **50** integriert sein. Ankommende Inhaltselemente, die am Ende des oben beschriebenen Prozesses autorisiert wurden und nachfolgend mit einem Autorisierungsschlüssel verschlüsselt wurden, können somit über das Entschlüsselungseinheitsmodul an der MS **50** wiedergegeben werden. Nicht autorisierte Inhaltselemente wurden gemäß der obigen Vorgehensweise nicht mit dem Autorisierungsschlüssel verschlüsselt, und jeder Versuch, sie wiederzugeben, wird scheitern. Der oben beschriebene Eincheckprozess kann, wie angezeigt, am Block **28** enden.

**[0033]** Es ist zu erkennen, dass ein in der MS **50** empfangenes Inhaltselement direkt gespeichert werden kann, ohne einen Schritt des oben beschriebenen Eincheckprozesses zu durchlaufen; in diesem Fall wird es gespeichert, ohne zuerst mit einem Autorisierungsschlüssel verschlüsselt zu werden, und ist somit auf einer MS **50** nicht wiedergabefähig. In einem solchen Fall kann der Benutzer der MS **50** die Option haben, den Eincheckprozess später zu veranlassen. Alternativ kann der Eincheckprozess unmittelbar nach dem Speichern des ankommenden elektronischen Inhaltselements folgen.

**[0034]** Die sichere Ausführung des oben vorgestellten Verfahrens, einschließlich, jedoch nicht beschränkt auf die Fingerabdruck-Extraktion, den Ver-

gleich, das Einchecken des Inhalts, die Entschlüsselung und die Wiedergabe, kann mittels vertrauenswürdiger Ausführungsumgebungen und/oder beliebiger anderer Sicherheitsmechanismen sichergestellt werden.

**[0035]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung können andere Formen der Bindung zwischen der oben beschriebenen Eincheckprozedur und dem Konsum (z. B. der Wiedergabe) des eingecheckten Inhaltselements verwendet werden. Die oben beschriebene Eincheckprozedur kann beispielsweise einen Schritt einschließen, in dem eine digital signierte „Quittung" oder ein digital signiertes „Ticket", wie auf dem Fachgebiet bekannt, für eingecheckten Inhalt ausgestellt werden kann, und die Routinen, welche die Wiedergabe des Inhalts vornimmt, können so ausgelegt sein, dass sie solche „Quittungen" oder „Tickets" prüfen, bevor sie den für den Konsum nötigen relevanten Vorgang ausführen. Die digitale Signierung der „Quittung" oder des „Tickets" kann ebenfalls als kryptographischer Vorgang bezeichnet werden. Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung können andere Formen der Bindung zwischen der oben beschriebenen Eincheckprozedur und dem Konsum (z. B. der Wiedergabe) des eingecheckten Inhaltselements verwendet werden. Die oben beschriebene Eincheckprozedur kann beispielsweise einen Schritt einschließen, in welchem dem eingecheckten Inhaltselement ein Identifizierungswert zugeordnet wird und dieser aufgezeichnet wird, um anzuzeigen, dass das Inhaltselement eingecheckt wurde. Die Identifizierungswerte können in einem beliebigen der Speichermittel in der MS **50** gespeichert werden, wie z. B. der lokalen Speichereinheit **52**, der lokalen Bank **54** und dergleichen. Die Routine, welche die Wiedergabe des Inhalts vornimmt, kann so ausgelegt sein, dass sie prüft, ob Inhaltselemente als erlaubt eingestuft wurden, bevor sie die notwendigen Wiedergabevorgänge ausführt. Diese Prüfung kann als Freigabevorgang bezeichnet werden. In einigen Ausführungsformen der Erfindung können auch Vorgänge der Entschlüsselungseinheit als Freigabevorgänge bezeichnet werden. Gemäß Ausführungsformen der Erfindung können die Freigabevorgänge beim Konsum des Inhaltselements ausgelöst werden und die Verweigerung des Konsums zum Ergebnis haben.

**[0036]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann das Ergebnis der oben beschriebenen Eincheckprozedur nicht die Genehmigung des Konsums des geprüften Inhaltselements durch den Verschlüsselungsvorgang sein, sondern vielmehr ein Vermerk zur späteren Meldung an den Management-Server oder eine beliebige andere Stelle, die diese Information weiter verwenden kann. Gemäß solchen Ausführungsformen der Erfindung wird die Einbringung von nicht zugelassenem ungeschütztem Inhalt in die MS **50** aufgezeichnet, und diese Information kann durch eine beliebige Komponente der MS **50** an die Fingerabdruck-Speichereinheit(en) **62**, den Management-Server oder eine beliebige andere entfernte Stelle, die solche Informationen sammelt, gesendet werden. Obwohl die vorliegende Erfindung in dieser Hinsicht nicht beschränkt ist, können solche Daten zum Zweck der Rechnungslegung verwendet werden.

**[0037]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann der lokale Fingerabdruckvergleich, wie bei Block **18** angezeigt, entfallen. Inhaltselemente können eingecheckt werden, indem ihr Fingerabdruck extrahiert wird, wie bei Block **16** angezeigt, und der extrahierte Fingerabdruck mit Fingerabdrücken in der/den Fingerabdruck-Speichereinheit(en) **62** verglichen wird, wie bei Block **24** angezeigt. Inhaltselemente können während des Zeitrahmens von dem Zeitpunkt, zu dem ihre Fingerabdrücke extrahiert werden, bis von der/den Fingerabdruck-Speichereinheit(en) **62** eine Antwort angekommen ist, entweder verwendbar sein (folglich eingecheckt werden) oder nicht verwendbar sein.

**[0038]** Gemäß einigen veranschaulichenden Ausführungsformen der Erfindung kann der Eincheckvorgang, der mit der Fingerabdruckextraktion, wie bei Block **16** angezeigt, beginnt, durch das Entschlüsselungseinheitsmodul oder durch ein beliebiges anderes Modul auf der MS **50** ausgelöst werden, die das Inhaltselement bei seinem Konsum verarbeitet. Gemäß solchen Ausführungsformen wird der durch die MS **50** empfangene Inhalt nicht wie oben beschrieben verarbeitet, bis zum ersten Mal versucht wird, ihn zu verwenden (z. B. zu konsumieren); erst zu diesem Zeitpunkt wird er durch das Entschlüsselungseinheitsmodul verarbeitet. Sobald das Entschlüsselungseinheitsmodul versucht, das Inhaltselement zu entschlüsseln, zeigt ein Scheitern dieses Versuchs an, dass das Inhaltselement nicht die Prozedur durchlaufen hat, die seine Verschlüsselung durch die Inhaltsverschlüsselungseinheit **60** beinhaltete, wie bei Block **26** angezeigt, und kann den Prozess auslösen, der mit der Fingerabdruckextraktion beginnt, wie bei Block **16** angezeigt.

**[0039]** Zwar wurden hierin bestimmte Merkmale der Erfindung illustriert und beschrieben, jedoch sind für den Fachmann viele Abwandlungen, Ersetzungen, Änderungen und Äquivalente denkbar. Es sollte daher klar sein, dass die angehängten Ansprüche alle solchen Abwandlungen und Änderungen, die dem eigentlichen Geist der Erfindung entsprechen, erfassen sollen.

## Patentansprüche

1. Mobile Vorrichtung, umfassend:

eine Fingerabdruck-Extraktionseinheit, um einen ersten Fingerabdruck eines ankommenden ersten elektronischen Inhaltselements zu extrahieren, und
eine Fingerabdruck-Vergleichseinheit, um einen Fingerabdruckvergleich des extrahierten ersten Fingerabdrucks mit mindestens einem Referenz-Fingerabdruck vorzunehmen, bei dem es sich um einen zweiten Fingerabdruck handelt,
wobei:
der Fingerabdruckvergleich einen Indikationswert bestimmen soll, der den Grad der Ähnlichkeit des ersten Inhaltselements mit dem zweiten Inhaltselement anzeigt.

2. Vorrichtung nach Anspruch 1, ferner umfassend:
eine Verbindung mit einer entfernten Speichereinheit, um den Vergleich des ersten Fingerabdrucks mit mindestens einem in der entfernten Speichereinheit gespeicherten Fingerabdruck zu ermöglichen, bei dem es sich um einen dritten Fingerabdruck handelt.

3. Vorrichtung nach Anspruch 1, die ferner eine lokale Bank umfasst, um den zweiten Fingerabdruck und ferner Fingerabdrücke ausgewählter Inhaltselemente zu speichern.

4. Vorrichtung nach Anspruch 1, wobei die Fingerabdruck-Vergleichseinheit ferner so angepasst ist, dass sie den ersten Fingerabdruck und den zweiten Fingerabdruck gemäß mindestens einem gegebenen Kriterium vergleicht.

5. Vorrichtung nach Anspruch 1, die ferner eine Inhaltsverschlüsselungseinheit umfasst, um einen ersten kryptographischen Vorgang auszuführen, um den Indikationswert an das erste Inhaltselement zu binden.

6. Vorrichtung nach Anspruch 1, die ferner eine Entschlüsselungseinheit umfasst, um den Konsum eines Inhaltselements auf der Grundlage des Indikationswerts zu ermöglichen.

7. Vorrichtung nach Anspruch 1, wobei die Vorrichtung ferner so angepasst ist, dass sie einen Freigabevorgang ausführt, wenn das erste Inhaltselement konsumiert wird, und wobei der Konsum auf einer Genehmigung durch den Freigabevorgang basiert.

8. Vorrichtung nach Anspruch 3, wobei die in der lokalen Datenbank gespeicherten Fingerabdrücke aus vorrichtungsspezifischen Listen von Inhaltselementen extrahiert sind.

9. Verfahren zum Prüfen von Inhalt in einer mobilen Vorrichtung, das folgende Schritte umfasst:
Empfangen mindestens eines ersten Inhaltselements an der mobilen Vorrichtung,
Extrahieren eines ersten Fingerabdrucks aus dem mindestens einem ersten Inhaltselement und
Vergleichen des extrahierten ersten Fingerabdrucks mit mindestens einem Referenz-Fingerabdruck, bei dem es sich um einen zweiten Fingerabdruck handelt, wobei der zweite Fingerabdruck aus einem zweiten Inhaltselement extrahiert wurde,
wobei das Vergleichen einen Indikationswert bestimmen soll, der den Grad der Ähnlichkeit des ersten Inhaltselements mit einem zweiten Inhaltselement anzeigt.

10. Verfahren nach Anspruch 9, ferner umfassend:
Kommunizieren mit einer entfernten Speichereinheit, um den ersten Fingerabdruck zum Vergleich mit mindestens einem in der entfernten Speichereinheit gespeicherten Fingerabdruck zu senden.

11. Verfahren nach Anspruch 9, das ferner das Speichern von Fingerabdrücken einer ausgewählten Liste von Inhaltselementen in einer lokalen Speichereinheit umfasst.

12. Verfahren nach Anspruch 9, das ferner das Ausführen eines ersten kryptographischen Vorgangs umfasst, um den Indikationswert an das erste Inhaltselement zu binden.

13. Verfahren nach Anspruch 9, das ferner das Ermöglichen des Konsums des Inhaltselements durch eine Entschlüsselungseinheit auf der Grundlage des Indikationswerts umfasst.

14. Verfahren nach Anspruch 9, das ferner das Ausführen eines Freigabevorgangs umfasst, wenn das erste Inhaltselement konsumiert wird,
wobei der Konsum auf einer Genehmigung durch den Freigabevorgang basiert.

15. Verfahren nach Anspruch 9, das ferner das Speichern von aus einer vorrichtungsspezifischen Liste von Inhaltselementen extrahierten Fingerabdrücken in der lokalen Bank umfasst.

Es folgen 2 Blatt Zeichnungen

**Anhängende Zeichnungen**

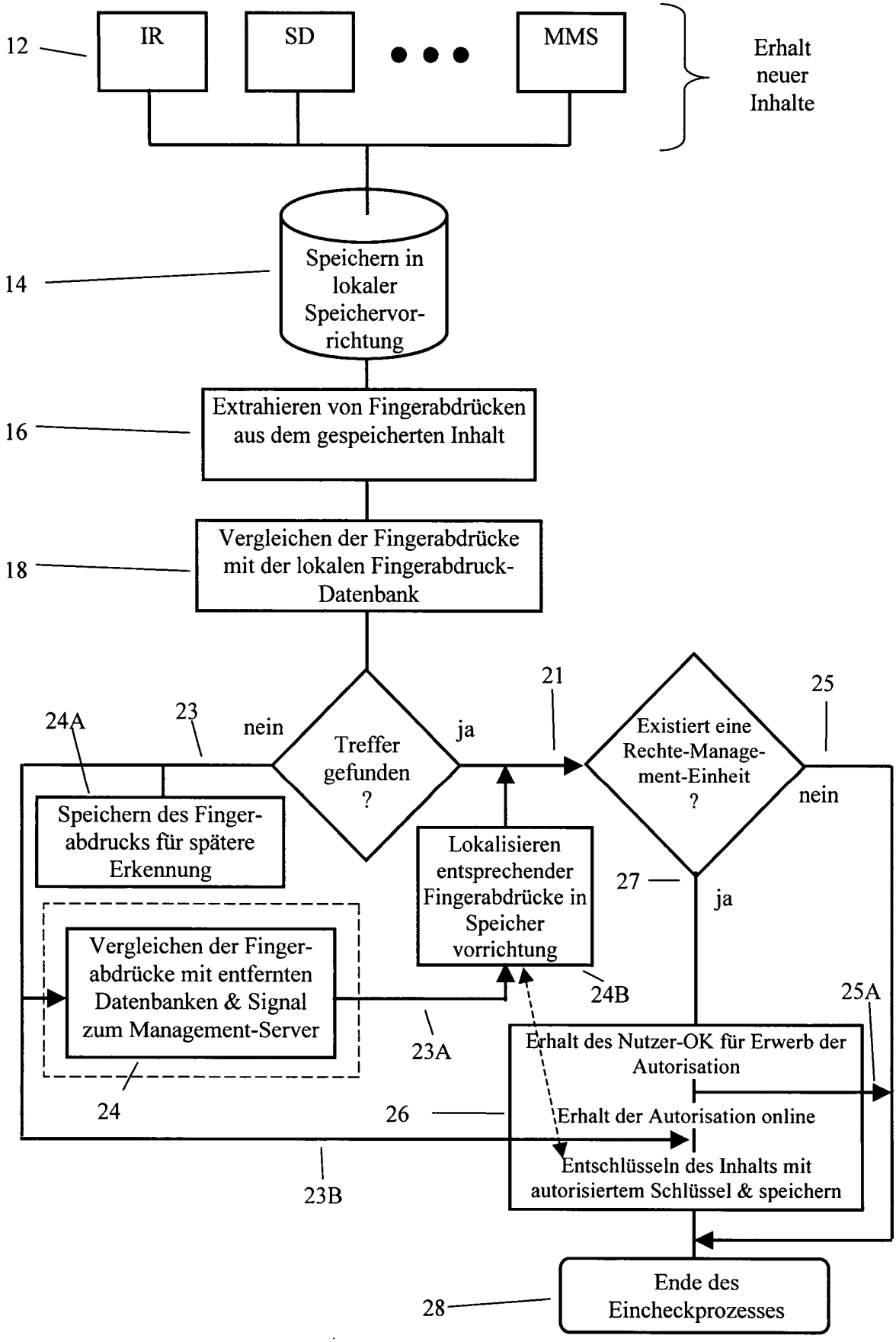



Fig. 1

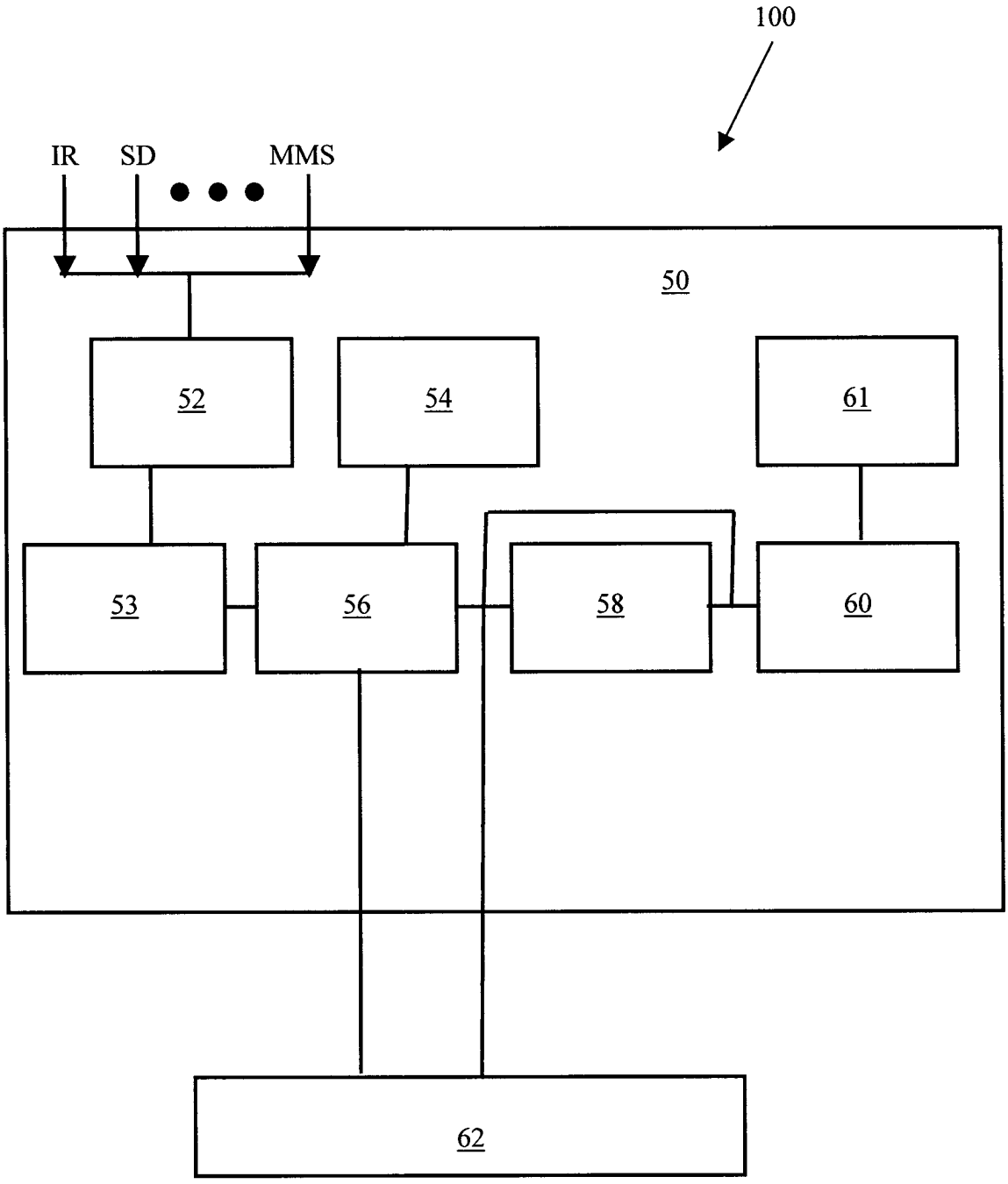



Fig. 2