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

(10) **DE 602 18 978 T2** 2007.12.20

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 352 310 B1**
(21) Deutsches Aktenzeichen: **602 18 978.0**
(86) PCT-Aktenzeichen: **PCT/US02/00956**
(96) Europäisches Aktenzeichen: **02 707 464.0**
(87) PCT-Veröffentlichungs-Nr.: **WO 2002/056162**
(86) PCT-Anmeldetag: **10.01.2002**
(87) Veröffentlichungstag der PCT-Anmeldung: **18.07.2002**
(97) Erstveröffentlichung durch das EPA: **15.10.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.03.2007**
(47) Veröffentlichungstag im Patentblatt: **20.12.2007**

(51) Int Cl.[8]: ***G06F 1/00*** (2006.01)
H04N 7/16 (2006.01)
H04L 9/32 (2006.01)

(30) Unionspriorität:
758637 **10.01.2001** **US**

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

(73) Patentinhaber:
GeoCodex LLC, Encino, US

(74) Vertreter:
Dr. Weber, Dipl.-Phys. Seiffert, Dr. Lieke, 65183 Wiesbaden

(72) Erfinder:
Sieler, Mark, Los Angeles, CA 90068, US; Glick, Barry J, Warren, VT 05674, US; Karpf, Ronald S, Gaithersburg, MD 20878, US

(54) Bezeichnung: **Kryptographisches System und Verfahren zur geographischen Verriegelung und Sicherung digitaler Information**

Beschreibung

Technischer Hintergrund der Erfindung

1. Technisches Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft die Übertragung von digitaler Information und insbesondere Verfahren und Systeme für das Verschlüsseln digitaler Information unter Verwendung eines Ortsintegritätsattributes.

2. Beschreibung des relevanten Standes der Technik

[0002] Große Schritte in der Computer-Telekommunikations- und Netzwerktechnologie haben eine Lawine von neuen Möglichkeiten und Anwendungen eröffnet, die vor wenigen Jahren noch unmöglich waren. Diese Fortschritte werden anschaulich anhand des explosionsartigen Wachstums der Popularität des Internets. Wie bekannt ist, ist das Internet eine Verbindung von Computernetzwerken, die es Computern aller Art erlaubt, miteinander zu kommunizieren und Informationen auszutauschen. Firmen, Einzelpersonen, Behörden, Wohltätigkeitsorganisationen und wissenschaftliche Zentren aller Größen verwenden regelmäßig das Internet, um Informationen gemeinsam zu nutzen, Dienste auszuliefern und einen großen Bereich von Inhalten auszutauschen. Das Internet fungiert als ein verteiltes Netzwerk aus Systemen, das weder von einer Entität gesteuert noch verwaltet wird. Physikalische und logische Pfade, die den Austausch von Information erleichtern, verbinden diese Netzwerke miteinander.

[0003] Trotz des enormen Wertes, der dieser Informationszugriff der Gesellschaft gebracht hat, bleibt die Kontrolle der Sicherheit der Information einschließlich der Vertraulichkeit, der Authentizität, der Integrität, die unbefugte Verwendung, die Transaktionsgeheimhaltung, der Site-Schutz usw. ein signifikantes Problem. Die große Offenheit des Internets macht es sehr schwer, bestimmt zu wissen, dass Information geschützt ist. Im Ergebnis können Internetbenutzer keine Annahme treffen betreffend der Wahrhaftigkeit oder der Verwendung von Daten, die sie senden oder empfangen.

[0004] Die Wurzel dieses Problems stammt von der inhärenten Konstruktion des Internets. Das TCP/IP-Protokoll, auf das das Internet aufbaut, hat das einfache Ziel der Auslieferung von Informationspaketen zwischen irgendwelchen Computern, die mit dem Internet verbunden sind, ohne die Route der Datenpakete, die diese durch das Netzwerk nehmen, zu leiten. Jeder mit einem Computer und grundlegender Internet-Software kann sich mit dem Internet als ein vollständig leistungsfähiger Host verbinden und Internetdienste für andere Benutzer anbieten.

[0005] Information, die das Internet durchquert, verläuft durch viele Computer entlang des Weges, und jeder Computer kann auf die Information zugreifen. Dieses Problem wird noch größer werden in der Zukunft, wenn neue Netzwerke mit dem Internet verbunden werden (z.B. Mobiltelefonnetz, Breitbandkabel, Laser- und Mikrowellennetzwerke, usw) und neue Informationstypen (z.B. Audio, Video, usw.) sich verbreiten.

[0006] Graphische Systeme, die historisch Informationssicherheit und Zugriffssteuerung bereitstellen, haben mit dem Wachstum des Internets nicht Schritt gehalten. In einem Verschlüsselungssystem wandelt der Sender die ursprünglichen Daten oder den "Plaintext" bzw. "Klartext" in ein codiertes Äquivalent, das "chiffrierter Text" genannt wird, unter Verwendung eines Verschlüsselungsalgorithmus. Der chiffrierte Text kann dann decodiert (oder entschlüsselt) werden von dem Empfänger und dadurch zurück in Klartext verwandelt werden. Der Verschlüsselungsalgorithmus verwendet einen Schlüssel, der eine binäre Zahl ist, die typischerweise eine Länge von 40 (Vierzig) bis 128 (einhundertachtundzwanzig) Bits hat. Je größer die Anzahl von Bits in Schlüsseln, umso mehr mögliche Schlüsselkombinationen gibt es und umso länger würde es brauchen, den Code zu entschlüsseln. Die Daten sind verschlüsselt oder "gesichert" durch mathematisches Kombinieren der Bits in dem Schlüssel mit den Datenbits. Am Empfangsende wird der Schlüssel verwendet, um den Code "zu entsperren" und die ursprünglichen Daten wieder zu gewinnen.

[0007] Vor dem Internet hat sich die Kryptographie hauptsächlich auf private Schlüsselsysteme verlassen, bei denen sowohl der Sender als auch der Empfänger einen geheimen Schlüssel (ebenso bekannt als symmetrischer Schlüssel) verwenden, um die Klartextinformation zu verschlüsseln und zu entschlüsseln. Die Sicherheit hing von dem Sender und dem Empfänger ab, die den privaten Schlüssel kennen und hat sich für Regierungen und große Firmen als angemessen erwiesen zur Sicherung Ihrer vertraulichen Information. Systeme mit privatem Schlüssel arbeiten weniger gut bei der Steuerung des Zugriffs auf die Mengen Informationsverkehr im Internet, im Wesentlichen aufgrund der Schwierigkeit der Verteilung des gemeinen Schlüssels unter den Benutzern ohne dessen Veröffentlichung zu riskieren.

[0008] Eine Alternative zu solchen Systemen mit privatem Schlüssel ist die Kryptographie mit öffentlichem Schlüssel, die zwei Schlüssel verwendet, die bekannt als ein privater und ein öffentlicher Schlüssel sind. Jeder Teilnehmer hat einen privaten Schlüssel, der geheim gehalten wird und nicht mit anderen gemein genutzt wird, und einen öffentlichen Schlüssel, der öffentlich verfügbar gemacht wird. Der öffentliche Schlüssel wird verwendet, um die Klartextinformation

zu verschlüsseln und der private Schlüssel wird verwendet, die chiffrierte Textnachricht zu entschlüsseln. Der private Schlüssel kann nicht mathematisch aus dem öffentlichen Schlüssel abgeleitet werden. Die Teilnehmer an einer Kommunikation können ihre öffentlichen Schlüssel über einen nicht-gesicherten Kommunikationskanal, wie z.B. das Internet, austauschen und danach die öffentlichen Schlüssel verwenden, um ihre Nachrichten zu verschlüsseln. Die Empfänger verwenden dann den privaten Schlüssel, um die Nachricht zu entschlüsseln. Dennoch verbleiben Nachteile mit der Verschlüsselung mit öffentlichem Schlüssel. Die Verschlüsselung mit öffentlichem Schlüssel ist rechnenintensiv und daher langsam im Gebrauch. Systeme mit öffentlichen Schlüssel sind typischerweise etwa 1.000mal langsamer als deren öffentliche Schlüsselgegenstücke, was sie für Audio- und Videosysteme unpraktisch macht, wo auch eine rechenintensive Komprimierung/Dekomprimierung durchgeführt werden muss. Die Verteilung der öffentlichen Schlüssel stellt ein anderes Problem dar, wodurch sich das Wachstum der Firmen (z. B. Verisign, Inc.) vermehrt, die als zentralisierte Registratoren oder unterzeichnende Autoritäten für den Zugriff und die Validierung von öffentlichen Schlüsseln fungieren. Aufgrund dieser Nachteile wird die Verschlüsselung mittels öffentlichem Schlüssel nur für einen kleinen Teil der gesamten Internetkommunikation verwendet. Für die meisten dieser Kommunikationen wird das Sicherheitsproblem nicht als groß genug erachtet, um die Unbequemlichkeit und die Kosten der Waltung des öffentlichen Schlüssels zu rechtfertigen.

[0009] Eine Form der Kryptographie mittels öffentlicher Schlüssel, die einige dieser Nachteile überwindet, ist PGP, was "pretty good privacy" bedeutet. PGP erlaubt es, Individuen sich gegenseitig die Schlüsselzertifikate zu unterzeichnen, wodurch das Vertrauen auf zentralisierter Unterzeichnungsautoritäten eliminiert wird. Während PGP eine wachsende Akzeptanz erreicht hat, wird es immer noch für nur einen Bruchteil des Internetverkehrs verwendet aufgrund der Schwierigkeit der Schlüsselverteilung und -verwaltung. Somit wird eine weit verbreitete Verwendung der Verschlüsselung im Internet nur breit akzeptiert werden, wenn es in einer Art und Weise implementiert wird, die für den Benutzer transparent erscheint.

[0010] Eine andere wichtige Betrachtung für ein Kommunikationssystem ist die Verhinderung des nicht-autorisierten Kopierens von kopie-geschütztem digitalen Inhalt. Mit konventionellen Rechen- und Kommunikationssystemen kann ein skrupelloses Individuum leicht eine unbegrenzte Anzahl von identischen Kopien einer kopiergeschützten Arbeit in digitaler Form (z. B. Musik, Literatur, Fotographie, Video, Software, usw.) herstellen und verteilen. Darüber hinaus erlauben kommerziell verfügbare Datei-Indexdienste es Computerbenutzern, digitale Dateien auf Computersystemen anderer Benutzer leicht zu lokalisieren und auf sie zuzugreifen, wodurch die Möglichkeit einer weit gestreuten Urheberrechts-Verletzung stark ansteigt. Ein solcher Dienst, der von Napster, Inc., of San Mateo, CA, bereit gestellt wird, stellt eine Anwendung zur gemeinsamen Nutzung von Dateien bereit, die in Verbindung mit Napsters Website arbeitet, um Musikdateien im populären MP3-Format zu lokalisieren, die auf anderen Computern residieren, die im Moment im Internet eingeloggt sind. Ein ähnlicher Dienst, bekannt als Gnutella, stellt ein System zur gemeinsamen Nutzung von Dateien bereit, das es Benutzern erlaubt, nach Software und Dokumenten auf dem Gnutella-Net zu suchen, einer losen Vereinigung von Benutzern und Organisationen, die der gesamten Welt eine große Vielfalt von Informationen verfügbar machen. Gnutella unterscheidet sich von Napster, das abgestellt ist auf Musikdateien, und eine zentralisierte Auflistung bereitstellt, während Gnutella-Net ein Peer-to-Peer Netzwerk ist, das alle Dateitypen enthält. Während diese Datei-Sharing-Systeme (Systeme zur gemeinsamen Nutzung von Dateien) den berechtigten Zweck haben, Benutzern zu ermöglichen, nicht copyright-geschützte Dateien gemeinsam zu nutzen, werden sie ebenso verbreitet verwendet, um urheberrechtlich geschützte Dateien unter Verletzung des Urheberrechts zu erhalten. Die verbotene Verwendung dieser Datei-Sharing-Systeme stellt eine ernste Bedrohung der Inhaber der kopier-geschützten Dateien dar.

[0011] Das aktive Kontrollieren des Internets ist keine praktikable Lösung für Inhaber eines Urheberrechts. Solche Überwachungsanstrengungen sind logistisch schwierig aufgrund der weit verzweigten und anonymen Natur der Internet-Urheberpiraterie. Zusätzlich macht die öffentliche Empfindung, dass Informationsinhalt, der über das Internet ausgetauscht wird, frei sein sollte, größere Überwachungsanstrengungen sehr unattraktiv aus Sicht der öffentlichen Darstellung. Um dieses Problem anzugehen, haben sich verschiedene Verwaltungssysteme für digitale Rechte (DRM) zum Schutz des Urheberrechts von digitalem Inhalt, der verteilt wird, heraus gebildet durch Fokussieren auf präventive Maßnahmen. Beispielsweise stellt ein vorgeschlagenes DRM-System für die Aufzeichnungsindustrie, bekannt als die sichere digitale Musikinitiative (SDMI), eine Reihe von Regeln auf für das sichere Verteilen digitaler Musik über das Internet. SDMI stellt Richtlinien für das Entwickeln für verträglicher DRM-Systeme bereit einschließlich eines Behälterformats, das Software- und Hardware-Player unterstützen müssen, um Material abzuspielen. Im Februar 1999 wurde bekanntgegeben, dass SDMI von der Recording Industry Association of America (RIAA) und Sony, Warner, BMG, EMI und Universal, den Top fünf Musikproduktionsfirmen unterstützt wird.

[0012] Ungeachtet dieser Anstrengungen stellen

DRM-Systeme im günstigsten Fall eine unvollständige Lösung aus einer Anzahl von Gründen dar. Als Erstes ist es wegen der Verfügbarkeit von raubkopiertem Material im Internet viel bequemer und günstiger für einen Benutzer, ungesetzlich eine digitale Datei aus dem Internet herunterzuladen als eine legitimierte Kopie des Materials über die konventionellen Verkaufskanäle zu erwerben. Während das ungesetzlich erhaltene Material eine reduzierte Qualität im Vergleich zu der legitimierten Kopie haben kann, wiegen die Bequemlichkeit und die vernachlässigbaren Kosten häufig diesen Nachteil auf. Als Zweites verlassen sich die meisten DRM-Techniken auf eine Form der Verschlüsselung, um die digitale Information zu schützen. Um möglich effektiv zu sein, müssen beide Teilnehmer eines Verschlüsselungsschemas ein persönliches Interesse daran haben, die Geheimhaltung der verschlüsselten Information aufrecht zu halten. Ein legaler Erwerber von Inhalt hat das Recht, den Inhalt anzusehen, hat jedoch kein persönliches Interesse daran, sicher zu stellen, dass die Geheimhaltung, die durch die Verschlüsselung ermöglicht wird, beibehalten wird. Aus diesem Grund verwenden viele DRM-Lösungen digitale Zertifikate oder Lizenzen, die versuchen, den Entschlüsselungsschlüssel gegenüber dem Benutzer zu verbergen. In solchen Systemen werden alle Kopien des Inhaltes in einer identischen Art und Weise verschlüsselt, und der Medienplayer bestätigt das Recht des Benutzers, den entschlüsselten Inhalt anzuzeigen oder abzuspielen. Da der Benutzer dennoch auf den verschlüsselten Inhalt und den Entschlüsselungsschlüsseln zugreifen kann, wenn auch diese versteckt sind, kann ein raffinierter Benutzer die DRM-Lösung umkehren, um die Verschlüsselung zu entfernen, um dadurch ein ungehindertes Kopieren und Verteilen des entschlüsselten Inhaltes zu erlauben. Andere weniger raffinierte Arten des Erhaltens einer unverschlüsselten Kopie des Inhaltes sind ebenso verfügbar für skrupellose Benutzer, wie zum Beispiel das Aufzeichnen jedes Einzelbildes einer digitalen Videodatei, wenn der Inhalt legal während des Abspielens angezeigt wird.

[0013] Die EP 0997808 A2 beschreibt ein System für das Steuern des Zugriffs auf verschlüsselte Dateien, die auf einer CD-ROM gespeichert sind. Die CD-ROM beinhaltet eine Anzahl von Entschlüsselungsschlüsseln, die mit verschiedenen verschlüsselten Dateien verknüpft sind. Ein Benutzer greift auf die Entschlüsselungsschlüssel zu, die auf der CD-ROM gespeichert sind, unter Verwendung eines Vertragspasswortes. Abhängig von dem Ort des Benutzers (bestimmt durch einen Empfänger für ein globales Positionsbestimmungssystem (GPS)) werden andere Entschlüsselungsschlüssel von der CD-ROM abgerufen, so dass ausgewählte verschlüsselte Dateien von dem Benutzer an diesem Ort entschlüsselt werden können.

[0014] Folglich wäre es wünschenswert, einen Weg bereitzustellen, den Austausch von digitaler Information zu steuern, der diese und andere Nachteile überwindet. Genauer gesagt wäre es wünschenswert, ein Informationsaustauschssystem und ein Verfahren bereitzustellen, dass die Steuerung über die Sicherheit und den Zugriff auf die Information ermöglicht und das nicht-autorisierte Kopieren von urheberrechtlich geschütztem Inhalt verhindert

Zusammenfassung der Erfindung

[0015] Die Erfindung wird in den angefügten Ansprüchen definiert.

[0016] Ein vollständigeres Verständnis des Systems und des Verfahrens für die Verwendung der Ortsidentität, um Zugriff auf digitale Information zu steuern, wird den Fachleuten geboten sowie eine Realisierung von zusätzlichen Vorteilen und Zielen hiervon durch eine Betrachtung der folgenden detaillierten Beschreibung der bevorzugten Ausführungsform. Es wird Bezug genommen auf die angehängten Zeichnungsblätter, die als erstes kurz beschrieben werden.

Kurze Beschreibung der Figuren

[0017] Fig. 1 ist eine schematische Zeichnung, die Zugriff auf digitale Information darstellt, der bestimmt wird durch die Ortsidentität in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung,

[0018] **Fig.** 2 ist ein Blockdiagramm, das Komponenten eines Ortsidentitätsattributs darstellt,

[0019] Fig. 3 ist ein Blockdiagramm, das Komponenten eines Ortswertes des Ortsidentitätsattributs darstellt,

[0020] Fig. 4 ist ein Flussdiagramm, das ein Verfahren für das Verknüpfen eines Ortsidentitätsattributs mit digitaler Information darstellt,

[0021] Fig. 5 ist ein Flussdiagramm, das ein Verfahren zum Durchführen eines Zugriffes auf geoverriegelte digitale Information unter Verwendung des Ortsidentitätsattributs darstellt,

[0022] Fig. 6A bis Fig. 6D sind Flussdiagramme, die alternative Verfahren für das Bestimmen einer Ortsidentität für eine Anwendung darstellen,

[0023] Fig. 7 ist ein Flussdiagramm, das ein Verfahren für das Erzeugen geoverriegelter digitaler Information aus der Perspektive eines Servers darstellt,

[0024] Fig. 8 ist ein Diagramm, das die Berechnung der Verschlüsselungsparameter aus der Ortsidentität für einen begrenzten rechteckigen Umgebungsbereich darstellt,

[0025] Fig. 9 ist ein Diagramm, das die Berechnung des Verschlüsselungsparameters aus der Ortsidentität für eine kreisförmige Umgebung darstellt,

[0026] Fig. 10 ist ein Flussdiagramm, das ein Verfahren für die Ortsidentität-Verschlüsselungsverarbeitung darstellt,

[0027] Fig. 11 ist ein Flussdiagramm, das ein Verfahren zum Erzeugen eines Geoverriegelungsschlüssels darstellt,

[0028] Fig. 12 ist ein Flussdiagramm, das ein Verfahren zum Betrachten oder Abspielen von geoverriegelter digitaler Information aus der Perspektive eines Clients darstellt,

[0029] Fig. 13 ist ein Flussdiagramm, das ein Verfahren zum Erzeugen eines Geoverriegelungsschlüssels darstellt.

[0030] Fig. 14 ist ein Flussdiagramm, das ein Verfahren für die ortsidentitätsbasierte Entschlüsselungsverarbeitung darstellt,

[0031] Fig. 15 ist ein Diagramm, das ein Beispiel eines begrenzten rechteckigen Umgebungsbereichs darstellt, der für die Berechnung eines entsprechenden Geoverriegelungsschlüssels verwendet wird,

[0032] Fig. 16 ist ein Diagramm, das ein Beispiel eines begrenzten rechteckigen Umgebungsbereichs darstellt, der für das Berechnen eines entsprechenden Geoverriegelungsschlüssels verwendet, bei dem der Ort des Abspielgerätes mit der Ortsidentität der geoverriegelten Daten übereinstimmt,

[0033] Fig. 17 ist ein Diagramm, das ein Beispiel eines begrenzten rechteckigen Umgebungsbereichs darstellt, der verwendet wird für die Berechnung eines entsprechenden Geoverriegelungsschlüssels, in dem der Ort des Abspielgerätes nicht mit der Ortsidentität der geoverriegelten Daten übereinstimmt,

[0034] Fig. 18 ist ein Diagramm, das ein Beispiel eines kreisförmigen Umgebungsbereichs darstellt, der für die Berechnung eines entsprechenden Geoverriegelungsschlüssels verwendet wird, und

[0035] Fig. 19 ist ein Diagramm, das ein Beispiel eines kreisförmigen Umgebungsbereichs darstellt, der für das Berechnen eines entsprechenden Geoverriegelungsschlüssels verwendet wird.

Detaillierte Beschreibung der bevorzugten Ausführungsform

[0036] Die vorliegende Erfindung erfüllt die Notwendigkeit nach einem Weg, den Austausch von digitaler Information zu steuern, der die Steuerung über die Sicherheit und den Zugriff auf die Information erlaubt und die das nicht-autorisierte Kopieren von kopiergeschützten Inhalten verhindert. In der detaillierten Beschreibung, die folgt, werden gleiche Bezugszahlen für Elemente verwendet, um gleiche Elemente zu beschreiben, die in einer oder mehreren der Figuren dargestellt sind.

[0037] Verschiedene Begriffe werden in der detaillierten Beschreibung verwendet einschließlich der folgenden:
Appliance bzw. Gerät: Elektronische Geräte, Systeme, Netzwerke und dergleichen mit der minimalen Kapazität, digitale Information und Ortsinformation zu erfassen. Diese elektronischen Geräte werden häufig eine Verarbeitungsfähigkeit beinhalten, um Programmbefehle auszuführen, und werden eine Speicherkapazität für die kurzzeitige oder langfristige Datenspeicherung haben und können weiterhin die Fähigkeit haben, Information zu übertragen.
Verknüpfen von Ortsidentität: Das Verfahren des Markierens digitaler Information mit einem Ortsidentitätsattribut.
Koordinatensystem: Der Ort wird bezeichnet durch die Breite und die Länge, welches ein Koordinatensystem basierend auf Gradmaßen ist, das eindeutig jeden Ort auf der Erde identifiziert. Die Breite wird gemessen als ein Winkel vom Erdäquator (0 Grad) zum Nordpol (90 Grad Nord) oder zum Südpol (90 Grad Süd). Breitenlinien werden durch Kreise gebildet, die parallel zur Äquatorebene verlaufen. Alle geradzahligen Breitenlinien sind voneinander gleich beabstandet. Die Breite bzw. der Breitengrad eines Ortes ist ein Maß des Winkels zwischen der Äquatorebene und der Linien, die von dem Erdzentrum hinausragen. Längenlinien werden durch große Kreise, die sowohl den Nord- als auch den Südpol schneiden, gebildet. Jede Länge kann als die Erde in zwei Hälften unterteilend gedacht werden. Längen werden in Halbkreisen von 0 Grad bis 180 Grad Ost und von 0 Grad bis 180 Grad West von dem Königlichen Greenwich Observatorium in Greenwich, England gemessen. Die 0°-Längengradlinie wird ebenso als Null-Meridian bezeichnet. Die Länge eines Ortes ist ein Maß des Winkels zwischen der Ebene, die von deren großen Kreis gebildet wird und des Null-Meridians. In dieser detaillierten Beschreibung werden Längen- und Breitenkoordinaten für Orte in Maryland als Beispiele in Bezug auf verschiedene Figuren verwendet. Wenn Längengradkoordinaten als Dezimalgradzahlen dargestellt werden, werden diese in Maryland üblicherweise als negative Zahlen dargestellt. In der folgenden Beschreibung werden diese Längengradkoordinaten jedoch als positive Zahlen dargestellt, um die Erläuterung der der Erfindung zugrunde liegenden Verfahren zu vereinfachen.
Digitale Information: Digitale Information ist Information, die in einem digitalen Format dargestellt wird. Beispiele von Informationen, die digital dargestellt werden kann, beinhaltet Text, Daten, Software, Mu-

sik, Video, Graphik, usw.
Erzwingen der Ortsidentität: Das Verfahren zum Bereitstellen oder Verweigern von Zugriff auf digitale Information über deren verknüpftes Ortsidentitätsattribut.
Geocode: Eine eindeutige Kodierung eines Ortes auf der Erde, die üblicherweise mit einem Koordinatensystem verknüpft ist. Einige Geocodes identifizieren einen punktförmigen Ort, wie z.B. wenn ein Ort durch seinen Längen- und Breitengrad identifiziert wird. Andere Geocodes können einen Bereich, wie z.B. einen Postleitzahlenbereich identifizieren.
Geoverriegelung: Eine erzwungene Verknüpfung zwischen der digitalen Information und einem geographischen Bereich, der durch ein Ortsidentitätsattribut festgelegt ist.
Geoverriegelte Information: Digitale Information, die mit einem Ortsidentitätsattribut verknüpft wurde, und auf die nur innerhalb eines Bereiches zugegriffen werden kann, der durch das Ortsidentitätsattribut festgelegt wird.
Ort: Irgendein geographischer Ort. Es kann, es ist jedoch nicht hierauf beschränkt, ein präziser Punktort, ein Gebiet oder ein Bereich, ein punktförmiger Ort, der in einen Umgebungsbereich enthalten ist oder Kombinationen von Plätzen auf der Welt sein. Der Ort kann ebenso die Höhenlage (oder Flughöhe) beinhalten, um eine Position oberhalb oder unterhalb der Erdoberfläche zu identifizieren, oder kann die Zeit beinhalten, um eine Position in einer zeitlichen Dimension zu identifizieren.
Ortsidentität: Eine präzise Kodierung eines Ortes. Sie kann verwendet werden, wobei es hierauf nicht begrenzt ist, als Informationsattribut, um präzise den Ort festzulegen, von dem auf die Information zugegriffen wird. Die Ortsidentität kann eine Kodierung eines punktförmigen Ortes, eines Bereiches, eines Bereiches mit einem verknüpften punktförmigen Ort, ein Korridor (d. h. eine zentrale Linie mit einer Länge auf beiden Seiten der zentralen Linie) oder irgendeine andere präzise Identifikation eines Ortes in Raum und Zeit sein.
Ortsvarianz: Die minimale Auflösung, bei der ein Geocode eines Ortes diesen nicht mehr exakt von benachbarten Orten unterscheiden kann. Wenn beispielsweise ein militärisches Referenzgittersystem mit zwei Zeichen Genauigkeit verwendet wird, dann ist jeder Ort nur innerhalb von zehn Kilometern genau.
Abspielort: Der Ortsabschnitt des Ortsidentitätsattributs, bei dem der Zugriff auf digitale Information gewährt wird.
Ort des Abspielgerätes: Der Ort eines Gerätes, das versucht, eine geoverriegelte Datei abzuspielen.
Umgebung: Die Zone oder der Bereich, der den Ort beinhaltet.

[0038] Die vorhergehenden Definitionen sind nicht dafür vorgesehen, den Schutzbereich der vorliegenden Erfindung zu begrenzen, sondern sind vielmehr dafür vorgesehen, Begriffe zu klären, die verwendet werden bei der Beschreibung der vorliegenden Erfindung. Es versteht sich, dass die festgelegten Begriffe ebenso andere Bedeutungen haben können für den Fachmann. Diese und andere Begriffe werden in der folgenden detaillierten Beschreibung verwendet.

[0039] In Fig. 1 stellt eine schematische Illustration der vorliegenden Erfindung den Zugriff auf digitale Information dar, der von der Ortsidentität bestimmt wird. Die Ortsidentität bezieht sich auf ein Informationsattribut, dass das geographische Gebiet oder den Bereich, in dem auf die Information zugegriffen werden kann, genau bestimmt. Zwei geographische Gebiete, bezeichnet mit A und B, sind in digitalem Format dargestellt, und haben ein verknüpftes Ortsidentitätsattribut **131**, dass das geographische Gebiet A als die Region festlegt, in der auf die digitale Information zugegriffen werden kann. Wenn ein Gerät **112** innerhalb des geographischen Gebietes A lokalisiert ist, kann von dem Gerät auf die digitale Information **130** zugegriffen werden. Umgekehrt, wenn ein Gerät **122** im geographischen Gebiet B lokalisiert ist (oder irgendwo sonst außerhalb des geographischen Gebietes A), dann kann auf die digitale Information **130** nicht zugegriffen werden. Die Ortsidentität stellt somit ein Attribut der digitalen Information dar, dass den präzisen geographischen Bereich festlegt, innerhalb dessen auf die Information zugegriffen werden kann. Digitale Information, die eine Ortsidentität hat, wird als "geolocked" bzw. "geoverriegelt" bezeichnet und Systeme, die die Ortsidentität erfordern, geoverriegeln die verknüpfte digitale Information mit dem geographischen Bereich, der durch das Ortsidentitätsattribut festgelegt ist.

[0040] **Fig.** 2 stellt ein Ortsidentitätsattribut **140** als zwei Einheiten der Information dar: ein Ortswert **142**, und ein Umgebungswert **143**. Der Ortswert **142** entspricht der eindeutigen Position eines bestimmten Ortes. Viele unterschiedliche Koordinatensysteme, wie z.B. Längen- und Breitengrade, wurden entwickelt, um eine eindeutige numerische Identifikation irgend eines Ortes bereitstellen. Für die Zwecke dieser Erfindung kann jedes Koordinatensystem, dass eindeutig einen Ort identifiziert, für den Ortswert **142** des Ortsidentitätsattributs **140** verwendet werden. Der Umgebungswert **143** entspricht der Ausdehnung einer Zone oder eines Gebietes, die den Ort umgibt. Das Ortsidentitätsattribut **140** kann einen Punktort oder einen exakten Ort aufweisen, wenn der Umgebungswert **143** auf 0, leer, usw. gesetzt wird oder auf irgendeinen anderen Wert, der anzeigt, dass der Bereich, auf der sich das Ortsidentitätsattribut bezieht, ein eindeutiger Punktort ist. Es versteht sich, dass der Umgebungswert **143** sich von der Ortsvarianz unterscheidet. Der Umgebungswert **143** bezieht sich auf die Darstellung eines Bereiches oder einer Region, während die Ortsvarianz die minimale Auflösung ist, der ein Geocode oder ein Ort nicht mehr exakt

von einem benachbarten Ort unterschieden werden kann.

[0041] Fig. 3 stellt den Ortswert **142** im größeren Detail dar. Wie oben erwähnt, gibt es zahlreiche unterschiedliche Koordinatensysteme, die in Gebrauch sind, die einen Satz von Zahlen bereit stellen, der eindeutig jeden Ort innerhalb des Koordinatensystems identifizieren. In der vorliegenden Erfindung wird der Ortswert **142** festgelegt als eindeutige Ortsbezeichnung oder Geocode, wie **142a** gezeigt. Die Höhe **144** und Länge **145** unter Verwendung eines konventionellen Koordinatensystems können dann den Geocode weiter festlegen. Andere bekannte Systeme, wie z.B. das erdzentrierte, erdfeste kartesische Koordinatensystem, das UTM-System (vom engl. Universal Transverse Mercator), das MGRS-System (Military Grid Reference System), das GEOREF-System (World Geographic Reference Systemt) usw. können ebenso mit Vorteil verwendet werden. Zusätzlich zu der Breite **144** und der Länge **145** könnte der Ortswert weiterhin eine Höhenlage **146** beinhalten, wie in **142b** gezeigt, welche der Höhe des Ortes über Normalnull entspricht. Alternativ könnte der Ortswert weiterhin einen Zeitwert **147**, wie in **142c** gezeigt, beinhalten, der als Datum und/oder Zeitbereich festgelegt sein kann. Dies erlaubt die Festlegung der Ortsidentität, um sowohl geographischen und/oder zeitlichen Zugriff auf die Information in Betracht zu ziehen.

[0042] Jeder geographischer Bereich oder Gebiet, der bzw. das den Ortswert **142** der Ortsidentität enthält, kann als Umgebungswert **143** für das Ortsidentitätsattribut **140** dienen. Der Umgebungswert **143** kann einen rechteckigen Bereich aufweisen, der durch zwei benachbarte Längengradlinien (die horizontale Kanten bereitstellen) und zwei benachbarte Breitengradlinien (die vertikale Kanten bereitstellen) festgelegt sein. Alternativ dazu kann der Umgebungswert **143** einen kreisförmigen Bereich aufweisen, der durch eine einzelne Zahl, die den Radius um den Ort festlegt, repräsentiert wird. Die kreisförmige Region kann weiterhin festgelegt werden als ein elliptischer Bereich, der entweder an dem Ort zentriert ist oder einen kreisförmigen oder elliptischen Bereich, der den Ort enthält, jedoch nicht notwendigerweise als Schwerpunkt. In einer anderen Alternative kann der Umgebungswert **143** ein unregelmäßiges geschlossenes Polygon oder ein Korridor aufweisen. In noch einer anderen Alternative kann der Umgebungswert **143** zu einem bekannten geographischen Bereich korrespondieren, wie z.B. das Land Brasilien. Andere Typen von bekannten geographischen Bereichen, die den Umgebungswert **143** festlegen, können Postleitzahlen, Staaten, Landkreise, vereinigte Städte usw. beinhalten.

[0043] In Übereinstimmung mit der Erfindung wird, wann immer geoverriegelte digitale Information gesichert, gespeichert oder kopiert wird, ein Ortsidentitätsattribut **140** mit der digitalen Information verknüpft, so dass der nachfolgende Zugriff auf die digitale Information auf das geographische Gebiet beschränkt ist, das von dem Ortsidentitätsattribut **140** spezifiziert wird. Fig. 4 stellt ein allgemeines Verfahren für das Verknüpfen von digitaler Information mit dem Ortsidentitätsattribut **140** dar, das präzise den Bereich festlegt, in dem der Zugriff oder das Abspielen der digitalen Information erlaubt wird. Es versteht sich, dass dieses Verfahren analog zur Einstellung eines Dateiattributs ist, wie z.B. ein nur Leseattribut für eine Computer-Datei, wenn die Datei abgespeichert wird. Das Verfahren würde von einem System oder einem Gerät durchgeführt mit einer Datenverarbeitungsfähigkeit und ausreichend Speicher, um die digitale Information zu erzeugen, zu handhaben, oder zu verarbeiten, die Endverwendung, die Übertragung oder Verteilung zu einer anderen Partei, wie z.B. ein Personalcomputer, Server, persönlicher digitaler Assistent (PDA), Laptop, Workstation, Netzwerk, Mobiltelefon, usw. Software- oder eingebettete Firmwarebefehle, die auf dem System oder dem Gerät arbeiten, würden veranlassen, dass das Verfahren durchgeführt wird.

[0044] Genauer gesagt beginnt das Verfahren in Schritt **200** mit einem Befehl, digitale Information mit einem Ortsidentitätsattribut abzuspeichern oder zu speichern. In Schritt **202** wird ein Ortswert **142** für die digitale Information abgerufen und für die spätere Verwendung gespeichert. Der Ortswert **142** ist nicht notwendigerweise der geographische Ort, an dem das Verfahren auf dem Gerät aufgerufen wird, sondern entspricht vielmehr dem Ortsidentitätsattribut (oben beschrieben) für ein Gerät, bei dem Zugriff auf die digitale Information erlaubt wird. In Schritt **204** wird ein Umgebungswert **143** des Ortsidentitätsattributs des Gerätes abgerufen und für die spätere Verwendung gespeichert. Verschiedene Verfahren zur Erzeugung des Orts- und Umgebungswertes **142**, **143**, werden unten genauer beschrieben. Zusätzlich zu solchen Verfahren können die Orts- und Umgebungswerte **142**, **143** ebenso vorher gespeichert und vom Speicher abgerufen werden oder der Endbenutzer kann gefragt werden, um die Information bereitzustellen. Den Schritt **206** werden die abgerufenen Orts- und Umgebungswerte **142**, **143** verwendet, um das Ortsidentitätsattribut **140** zu erzeugen. Dann, in Schritt **210**, wird die digitale Information **216** mit dem Ortsidentitätsattribut **140** verknüpft, um geoverriegelte digitale Information **218** bereitzustellen.

[0045] Versuche, auf geoverriegelte Information über eine Lese- oder Kopieroperationen, die von dem Abspielgerät durchgeführt werden, zuzugreifen, werden abgelehnt, bis das Gerät eine gültige Ortsidentität bestätigt. Dies wird durchgeführt durch Bewerten der verknüpften Ortsidentität der digitalen Information gegenüber dem Ort des Abspielgeräts, um zu be-

stimmen, ob es eine Übereinstimmung gibt. Fig. 5 zeigt ein allgemeines Verfahren für das Ermöglichen des Zugriffs auf digitale Information durch die Ortsidentität. Logischerweise ist dieses Verfahren analog zu der Art, wie Betriebssysteme ein nur Leseattribut auf Dateien erzwingen, d.h. dem Benutzer den Zugriff auf die Datei zum Lesen erlauben, jedoch den Zugriff für das Schreiben ablehnen. Das Verfahren würde von einem System oder einem Gerät durchgeführt mit einer Datenverarbeitungskapazität und ausreichend Speicher, um den Empfang von digitaler Information zu empfangen, die von jemand Drittes übertragen oder verteilt wird, wie z.B. einen Personalcomputer, Server, Router, persönlichem digitalem Assistenten (PDA), Workstation, Netzwerk, Mobiltelefon, Laptop und dergleichen. Software- oder eingebettete Firmwarebefehle, die auf dem System oder Gerät arbeiten, würden veranlassen, dass das Verfahren durchgeführt wird.

[0046] Genauer gesagt startet das Verfahren in Schritt **220** mit einem Befehl, auf die digitale Information zuzugreifen. In Schritt **222** wird auf die geoverriegelte digitale Information **218** zugegriffen, um das verknüpfte Ortsidentitätsattribut **140** zu lesen und zu speichern. Es versteht sich, dass nur auf den Ortsidentitätsabschnitt der geoverriegelten Information zugegriffen wird und nicht auf die digitale Information selbst. Die Ortsidentität **140** der geoverriegelten Information wird für die weitere Verwendung in den Verfahren gespeichert. In Schritt **224** bestimmt das Verfahren den Ort des Gerätes, dass auf die digitale Information zugreift. Wie unten beschrieben wird, gibt es zahlreiche Möglichkeiten, um den Ort des Geräts **160** zu bestimmen. Der Geräteort **160** wird für die weitere Verwendung in dem Verfahren gespeichert. In Schritt **226** bestimmt das Verfahren, ob der Ort des Gerätes mit dem Bereich konsistent ist, der durch die Ortsidentität **140** festgelegt wird. Wenn der Geräteort **160** mit der Ortsidentität **140** übereinstimmt, dann wird der Zugriff auf die geoverriegelte digitale Information **218** den Schritt **228** gewährt. Umgekehrt, falls der Geräteort **160** nicht mit der Ortsidentität **140** übereinstimmt, dann wird in Schritt **230** der Zugriff verweigert.

[0047] Die Fig. 6A bis Fig. 6D stellen eine Mehrzahl von beispielhaften Verfahren dar, um den Abspielort des Gerätes, dass Zugriff auf die geoverriegelte digitale Information ersucht, zu bestimmen. Dieses Verfahren würden von einem System als Teil des Prozesses des Erzwingen der Ortsidentität mit digitaler Information durchgeführt, wie oben in Bezug auf Fig. 5 beschrieben. Es versteht sich, dass andere Verfahren zur Bestimmung des Abspielortes des Gerätes ebenso mit Vorteil verwendet werden könnten.

[0048] Fig. 6A zeigt ein Adressdekodierverfahren **240**, in dem ein Geocode aus der Straßenadresse für das Gerät aufgelöst wird, das die geoverriegelte digitale Information erhalten wird. In Schritt **242** wird die Adresse des Gerätes abgerufen. Die Adreßinformation kann von dem Speicher abgerufen werden, basierend auf einer vorherigen Kommunikation mit dem Gerät, in der die Adresse erhalten wurde. Alternativ kann das Gerät veranlassen, dass die Adressinformation als ursprünglicher Teil einer Informationstransaktion bereit gestellt wird. Sobald die Adreßinformation abgerufen wurde, kann die Adressinformation dekodiert werden, um einen spezifischen Geocode den Schritt **244** abzuleiten. Dieser Schritt kann ein kommerziell verfügbares Softwareprogramm verwenden, dass einen koordinaten-spezifischen Geocode von einer Adresse erzeugen kann, wie z.B. die MapMarker OCX Component Version 4.2 von der Mapinfo Corporation mit Sitz in Troy, New York. Falls es gewünscht ist, ein Zeitelement in das Ortsidentitätsattribut zu integrieren, dann würde in Schritt **246** die gegenwärtige Zeit von dem Gerät abgerufen, wie z.B. durch Lesen der Zeit aus der Systemuhr des Gerätes. Es versteht sich, dass dieser Schritt **246** optional ist und in vielen Anwendungen ein Zeitelement nicht erforderlich sein wird. Schließlich werden in Schritt **248** der Geocode und die Zeit in ein Format umgewandelt, dass als Ortswert **142** für das Ortsidentitätsattribut **140** verwendbar ist.

[0049] Fig. 6B zeigt ein Gerätelizenzverfahren **250**, bei dem der Ortswert von einer Lizenz, die im Gerät abgelegt ist, abgeleitet wird. Ein Lizenzierungspäckchen ist ein übliches Merkmal vieler Systeme und wird im Allgemeinen verwendet, um den Zugriff auf Anwendungsprogramme zu validieren. Lizenzpäckchen sind digitale Dateien, die Informationen enthalten betreffend den Benutzer/Lizenznehmer. Obgleich nicht unverletzlich sind sie geordnet und verschlüsselt in einer Art und Weise, die sie zu einem zuverlässigen Weg der Validierung des Benutzers machen. In dieser Ausführungsform der Erfindung würde das Lizenzpäcken einen koordinaten-spezifischen Geocode beinhalten, der den Ort des Gerätes identifiziert. In Schritt **252** wird auf das Lizenzpäckchen, das auf dem Gerät gespeichert ist, zugegriffen und es abgerufen. Dann wird ein Geocode aus der Lizenz in Schritt **252** wieder erlangt. Wenn es gewünscht ist, ein Zeitelement in das Ortsidentitätsattribut zu integrieren, dann würde in Schritt **256** die gegenwärtige Zeit von dem Gerät abgerufen, beispielsweise durch Auslesen der Zeit von der Systemuhr des Gerätes. Es versteht sich, dass dieser Schritt **256** optional ist und in vielen Anwendungen ein Zeitelement nicht erforderlich wäre. Schließlich wird in Schritt **258** der Geocode und die Zeit in ein Format umgewandelt, dass als Ortswert **142** für das Ortsidentitätsattribut **140** nutzbar ist.

[0050] Fig. 6C zeigt ein GPS Datenwiederherstellungsverfahren **260**, bei dem der Ortswert aus einem GPS-Empfänger, der in das Gerät eingebettet ist, gewonnen wird. Wie in der Technik bekannt, ist das Glo-

bale Positionsbestimmungssystem (GPS) ein satellitenbasiertes Funknavigationssystem, das entwickelt und betrieben wird von dem US-Verteidigungsministerium. GPS erlaubt es Benutzern, auf dem Land, auf dem Meer oder in der Luft, ihre dreidimensionale Position, ihre Geschwindigkeit und die Zeit 24 Stunden am Tag während aller Wetterlagen irgendwo in der Welt zu bestimmen. Das GPS-System stellt zivilen Benutzern weltweit dies mit einer Genauigkeit von besser als 100 Metern zur Verfügung, während militärische und zivile Benutzer in den Vereinigten Staaten sogar noch eine höhere Genauigkeit haben. Die GPS-Positionsinformation basiert auf einem System von Koordinaten, die das World Geodetic System 1984 (WGS 84) genannt wird und ist ähnlich der Breiten- und Längenkoordinaten. Die kommerzielle Verfügbarkeit von GPS-Empfängern steigt allgemein und in dieser Ausführungsform wird vorausgesetzt, dass das Gerät einen eingebetteten GPS-Empfänger enthält. Beispielsweise sind GPS-Empfänger als PCMCIA-Karten erhältlich, wie z.B. die NavCard hergestellt von der Rockwell Corporation oder die GPScard von der Trimble Navigation, und die Novalel Corporation stellt einen GPS-Empfänger für einen Allzweck-IBM-PC her. In Schritt **262** wird auf den GPS-Empfänger, der im Gerät eingebettet ist, zugegriffen. Ein Geocode wird in Schritt **264** von dem eingebetteten GPS-Empfänger erhalten. Optional kann ebenso ein Zeitwert von dem GPS-Empfänger erhalten werden. Schließlich werden in Schritt **266** der Geocode und der optionale Zeitwert in ein Format umgewandelt, dass als Ortswert **142** für das Ortidentitätsattribut **140** verwendet werden kann.

[0051] Fig. 6D zeigt ein Triangulationsdatengewinnungsverfahren **270**, um den Ort des Gerätes zu bestimmen. Wie in der Technik bekannt ist, ist die Triangulation ein Verfahren, das häufig von Satelliten, Mobiltelefonen, Navigationssystemen und anderen Funksignaloperatoren eingesetzt wird, um genaue Positionsinformationen bereitzustellen. Das Loran-C-System ist ein Beispiel eines kommerziell verfügbaren Navigationssystems, das Ortsinformation durch das Triangulieren von Hochfrequenzsignalen von einer Mehrzahl von Hochfrequenzsendern mit fester Position bereitstellt. In Schritt **272** wird das System die Richtung des Gerätes bestimmen durch Zugreifen auf ein Hochfrequenzsignal, das von dem Gerät gesendet wird. Ein Geocode wird aus dem RF-Signal berechnet unter Verwendung eines Triangulationsalgorithmus in Schritt **274**. Schließlich wird in Schritt **276** der Geocode in ein Format umgewandelt, das als Ortswert **142** für das Ortsidentitätsattribut **140** verwendbar ist. Falls ein Zeitelement in dem Ortsidentitätsattribut **140** benötigt wird, dann würde die gegenwärtige Zeit aus der Systemuhr des Gerätes in der gleichen Art und Weise wie oben beschrieben, ausgelesen.

[0052] In Übereinstimmung mit einer Ausführungsform der Erfindung wird die digitale Information verschlüsselt, bevor sie zu einem Gerät übertragen wird und das Ortsidentitätsattribut **140** wird verwendet, um einen ortsidentitätsbasierten Schlüssel zu erzeugen, der verwendet wird, um die digitale Information zu verschlüsseln. Die Verschlüsselungsschicht, die der digitalen Information zugefügt wird, erzwingt die Zugriffsbeschränkung, die durch das Ortsidentitätsattribut **140** festgelegt wird. Fig. 7 stellt ein Verschlüsselungsverfahren für das Verknüpfen von digitaler Information mit dem Ortsidentitätsattribut **140** dar, dass verwendet wird, um eine digitale Klartextinformation (Medien) in geoverriegelte verschlüsselte digitale Information umzuwandeln. Dieses Verfahren kann von einem Server, der mit einem Netzwerk, z.B. das Internet, verbunden ist, durchgeführt werden für das Verteilen von verschlüsselter digitaler Information zu Benutzern, die mit dem Netzwerk verbunden sind. Auf digitale Information wird von dem Server von einem Medienspeicher **152** zugegriffen. Auf Vorschauinformation, wie z.B. Werbung oder andere ähnliche Materialien in digitaler Form, kann ebenso von dem Server aus zugegriffen werden von einem Vorschauspeicher **154**. Die digitale Information und die Vorschauinformation werden in Klartextform in dem Medienspeicher **152** und im Vorschauspeicher **154** gespeichert. Diese spezifische digitale Information, die geoverriegelt wird, wird eine eindeutige Medien-ID **150** zugewiesen, die verwendet wird, um die digitale Klartextinformation innerhalb des Medienspeichers **152** zu indexieren.

[0053] Das Verfahren startet in Schritt **300** mit einem Befehl, um digitale geoverriegelte Information zu erzeugen, die in Übereinstimmung mit einem Identitätsattribut verschlüsselt ist. In Schritt **302** wird auf die angeforderte digitale Information (oder die Medien) vom Medienspeicher **152** in Verbindung mit einer entsprechenden Medien-ID **150** zugegriffen. Da die digitale Information maßgeschneidert verschlüsselt ist für einen geographischen Umgebungsbereich, kann die Vorschauinformation maßgeschneidert für den entsprechenden geographischen Umgebungsbereich sein und in den verschlüsselten Medien enthalten sein. Alternativ könnte demographische Information über den Zielkunden bekannt sein und verwendet werden, um die eingeschlossene Vorschauinformation weiter zu verfeinern. Wenn zusätzliche Vorschauinformation eingeschlossen werden soll, wird von dem Vorschauspeicher **154** zugegriffen und sie mit der angeforderten digitalen Information in Schritt **304** verkettet. Die digitale Klarinformation und die verkettete Vorschauinformation wird dann als Eingang in die Verschlüsselungsverarbeitung, die in Schritt **306** durchgeführt wird, verwendet.

[0054] Die Verschlüsselungsverarbeitung in Schritt **306** verwendet ein Ortsidentitätsattribut **140**, das eine Form der geographischen Region, die von den Orts- und Umgebungswerten festgelegt wird, fest-

legt. Das Ortsidentitätsattribut **140** wird verwendet, um einen Geoverriegelungsschlüssel **166** zu erzeugen, der für die Verschlüsselung verwendet wird, wie in größerem Detail unten beschrieben wird. Dann wird in Schritt **380** der Klartext verschlüsselt und die geoverriegelte Information gepackt durch Anfügen eines Parameters, der als Shape-Parm bezeichnet wird, an den Beginn des kodierten Textes. Genauer gesagt wird der Geoverriegelungsschlüssel verwendet, um die digitale Klartextinformation und die verkettete Vorschauinformation deterministisch zu modifizieren unter Verwendung eines Verschlüsselungsalgorithmus, um die geoverriegelte digitale Information **156** bereitzustellen, die die digitale Information und die verkettete Vorschauinformation in verschlüsselter Form **158** und den Shape-Parm **157** in Klartextform beinhaltet. Der Shape-Parm legt eine Form eines interessierenden Bereiches fest ohne den spezifischen Ort, der dem Bereich von Interesse entspricht, zu identifizieren. Der Shape-Parm ist eine ortslose Übersetzung des Umgebungsbereiches des Ortsidentitätsattributs **140**. Ortslos bzw. ortsfrei bezieht sich auf die Charakteristik des Shape-Parm, die Form eines Umgebungsbereiches festzulegen ohne auf einen tatsächlichen Ort Bezug zu nehmen.

[0055] Abhängig davon, ob die Ortsidentität **140** einen kreisförmigen oder begrenzten rechteckigen Umgebungsbereich festlegt, werden die entsprechenden Shape-Parms unterschiedliche charakteristische Größen haben. Die unterschiedlichen Größen werden von dem Client verwendet, der die geoverriegelte digitale Information **156** empfängt, um zu bestimmen, ob die Datei für einen kreisförmigen oder begrenzten rechteckigen Umgebungsbereich verarbeitet wird.

[0056] Alternativ kann das Format des Shape-Parm als ein Feld in der geoverriegelten digitalen Information enthalten sein.

[0057] In einer bevorzugten Ausführungsform der vorliegenden Erfindung wird eine Abbildungsfunktion verwendet, um unterschiedliche Koordinaten innerhalb eines Umgebungsbereiches in die gleichen Werte abzubilden. Die Abbildungsfunktion ist wie folgt:

$$f(x) = \Delta \cdot int(x/\Delta)$$

wobei int eine Funktion ist, die den ganzzahligen Teil ihres Klammer-Argumentes zurückgibt. Unter Verwendung von x als Breitengrad des Geocodeortes und Δ als die Länge der Seite zwischen den begrenzten Breitengraden, oder von x als Längengrad des Geocodeortes und Δ als die Länge der Seite zwischen den begrenzenden Längengraden, kann ein Gitter über das gesamte Längen-/Breitenkoordinatensystem konstruiert werden. Jeder Geocode innerhalb einer Gitterzelle wird in den selben Wert transformiert, wenn die obige Funktion auf ihren Längengrad und Breitengrad angewendet wird. Da die "großen rechteckigen" Grenzen nicht direkt auf Grenzen fallen müssen, die exakte Vielfache der Längen der Begrenzungsseiten sind, wird ein ortsfreies Verschiebungsmaß berechnet unter Verwendung der unteren Begrenzungsseite und wird verwendet, um das Gitter linear zu verschieben.

[0058] Fig. 8 stellt die Bestimmung des Shape-Parm-Parameters aus der Ortsidentität für einen rechteckig begrenzten Umgebungsbereich dar. Die horizontalen Linien in der Figur entsprechen den Breitenlinien und die vertikalen Linien entsprechen den Längenlinien. Der Äquator (Breite) und Greenwich (Länge) sind gezeigt. Ein gepunktetes Gitter stellt die Linien der Breitengrade und Längengrade für ein rechteckiges Gitter dar mit der selben Größe wie die des rechtwinkligen Umgebungsbereichs. Das Gitter ist zentriert bei Null Grad Breite (d. h. Äquator) und Null Grad Länge (d. h. Greenwich). Die Ortsidentität für eine rechteckige Grenze beinhaltet einen Ortsabschnitt, die Breite (lat) und Länge (ing) des Abspielortes. Der Umgebungsbereich wird durch zwei Koordinatensätze dargestellt. Der erste Koordinatensatz stellt die Linie des Breitengrades dar, die den unteren Abschnitt des Rechteckes definiert, und die Linie des Längengrades dar, die die linke Seite des Rechtecks festlegt, und wird dargestellt durch (βlat1, βlng1). Der zweite Koordinatensatz stellt die Breitengradlinie, die die Oberseite des Rechteckes und die rechte Seite des Rechteckes festlegt, dar und wird dargestellt durch (βlat2, βlng). Von der Ortsidentität wird der Shape-Parm berechnet durch zunächst Berechnen der Länge der Seiten des begrenzten Rechtecks. Der Abstand zwischen den Breitengradlinien wird als Δlat bezeichnet und ist die absolute Differenz zwischen βlat2 und βlat1 (oder abs(βlat2 – βlat1)). Der Abstand zwischen Längengradlinien wird als Δlng bezeichnet und ist die absolute Differenz zwischen βlng2 und βling1 (oder abs(βlng2 – βling1)).

[0059] Als nächstes werden die Translationsfaktoren berechnet, die die Abbildungsfunktion, die oben beschrieben wurde, verwendet. Der Breitentranslationsfaktor (olat) wird berechnet in Übereinstimmung mit der folgenden Gleichung:

$$olat = \beta lat1 - \Delta lat \cdot int(\beta lat1/\Delta lat)$$

[0060] Der Längengradtranslationsfaktor (olng) wird berechnet in Übereinstimmung mit der Gleichung:

$$olng = \beta lng1 - \Delta lng \cdot int(\beta lng1/\Delta lng)$$

[0061] Diese Gleichungen werden verwendet, um die Koordinatenwerte linear zu verschieben. Der Shape-Parm ist dann die zwei Zahlensätze (Δlat, Δlng) und (olat, olng). Bemerkenswert ist, dass der Shape-Parm ortsfrei ist, d. h. er hängt nur von der Größe des rechtwinkligen Umgebungsbereich ab

und nicht von dem genauen Ort des rechtwinkligen Umgebungsbereichs. Wenn die Abbildungsfunktion mit dem Shape-Parm verwendet wird, werden die folgenden Funktionen den gleichen Wert für jede Breiten-/Längengradkoordinaten (plat, plng) in dem rechteckigen Umgebungsbereich haben:

f(plat) = Δlat·(int((plat – olat)/Δlat)

f(ping) = Δlng·(int((plng – olng)/Δlng)

[0062] Genauer gesagt werden die Wertepaare (f(plat), f(plng)) identische Werte für alle Koordinaten innerhalb auf der unteren und linken Kante des begrenzten Rechteckes haben und die Werte werden nur von den Shape-Parm und den Koordinaten (plat, plng) abhängen. Diese Funktionen werden verwendet, um den Verschlüsselungsschlüssel zu konstruieren, der für die Geoverriegelung der digitalen Information verwendet wird.

[0063] Fig. 9 stellt die Bestimmung des Shape-Parm-Parametes aus der Ortsidentität für einen kreisförmigen Umgebungsbereich dar. Wie in der vorherigen Figur entsprechen die horizontalen Linien den Breitengraden und die vertikalen Linien entsprechen den Längengraden. Ein gepunktetes Gitter stellt die Linien der Breitengrade und Längengrade für ein Quadratgitter der Größe eines Quadrates, dass exakt den kreisförmigen Umgebungsbereich umgibt, dar. Die Ortsidentität für einen kreisförmigen Umgebungsbereich beinhaltet einen Ortsabschnitt, der durch die Breite (lat) und Länge (lng) des Abspielortes festgelegt wird, und ein Umgebungsbereich wird durch eine einzelne Zahl festgelegt, d.h. den Radius des kreisförmigen Umgebungsbereichs. Aus der Ortsidentität wird der Shape-Parm berechnet durch zunächst Bestimmen des Durchmessers des kreisförmigen Umgebungsbereichs als der doppelte Radius. Dieser Wert stellt die Größe für ein Quadratgitter bereit, wie in Fig. 9 gezeigt. Als nächstes werden die Translationsfaktoren berechnet und die Abbildungsfunktion wie oben beschrieben verwendet. Der Breitengradtranslationsfaktor (olat) und der Längengradtranslationsfaktor (olng) werden berechnet in Übereinstimmung mit den folgenden Gleichungen:

olat = lat – radius – (Δlatling·int(lat/Δlatlng))

olng = lng – radius – (Δlatling·int(lng/Δlatling))

wobei Δlatlng den Durchmesser des kreisförmigen Umgebungsbereichs entspricht. Diese Gleichungen werden verwendet, um die Koordinatenwerte linear zu verschieben. Der Shape-Parm ist dann die beiden Zahlensätze (olat, oling) und der Radius. Wenn die Abbildungsfunktionen mit dem Shape-Parm verwendet wird, werden die folgenden Funktionen den selben Wert für jede Breitengrad-/Längengradkoordinate (plat, plng) in dem Rechteck haben, dass den kreisförmigen Umgebungsbereich begrenzt:

f(plat) = Δlatlng·(int((plat – olat)/Δlating)

f(pling) = Δlnging·(int((plng – oing)/Δlating)

[0064] Genauer gesagt wird das Wertepaar (f(plat), f(plng)) identische Werte für alle Koordinaten innerhalb und auf der unteren und linken Kante des Quadratgitters haben, und die Werte hängen nur von dem Shape-Parm und den Koordinaten (plat, pling) ab. Diese Funktionen werden verwendet, um den Geoverriegelungsschlüssel zu konstruieren, der für das Verschlüsseln der digitalen Information verwendet wird. Schließlich können die Koordinaten (plat, plng) bewertet werden, um zu bestimmen, ob sie innerhalb des kreisförmigen Umgebungsbereichs liegen unter Verwendung der folgenden Gleichung:

$dist = sqrt((plat – (f(plat) + radius + olat))^2 + (plng – (f(plng) + radius + olng))^2$

für die dist kleiner als oder gleich dem Radius ist und innerhalb oder auf dem Umfang des kreisförmigen Umgebungsbereiches liegt.

[0065] In Übereinstimmung mit einer alternativen Ausführungsform der Erfindung wird die digitale Information verschlüsselt vor der Übertragung oder der Speicherung durch ein Gerät, und das Ortsidentitätsattribut **140** wird verwendet, um einen auf der Ortsidentität basierenden Geoverriegellungsschlüssel zu erzeugen, der verwendet wird, um die digitale Information zu verschlüsseln. Das Verschlüsselungslayer, dass der digitalen Information zugefügt wurde, erzwingt den beschränkten Zugriff, der durch das Ortsidentitätsattribut **140** festgelegt wird.

[0066] Fig. 10 stellt ein Verschlüsselungsverfahren für das Verknüpfen von digitaler Information mit dem Ortsidentitätsattribut **140** dar, dass verwendet wird, um digitale Klartextinformation (Medien) in geoverriegelte verschlüsselte digitale Information umzuwandeln. Dieses Verfahren kann von einem Gerät durchgeführt werden vor dem Speichern der digitalen Information innerhalb eines lokalen Speichers (z.B. der Festplatte) oder dem Weiterleiten der digitalen Information zu einem anderen Gerät oder Netzwerk.

[0067] Das Ortsidentitätsattribut **140**, das verwendet wird, um die digitale Klartextinformation **170** geozuverriegeln, wird verwendet, um zwei Parameter zu berechnen: (a) einen Abspielortparameter **162**, und (b) einen Shape-Parm-Parameter **157**. Der Ortsparameter **162** ist der Ortsabschnitt des Ortsidentitätsattributs **140**. Der Shape-Parm **157** ist eine ortslose Translation des Umgebungsabschnittes der Ortsidentität, die für einen rechtwinklig begrenzten Bereich oder einen kreisförmig begrenzten Bereich berechnet wurde, wie oben beschrieben. Sowohl der

Ortsparameter als auch der Shape-Parm-Parameter werden verwendet als Eingabe in einen Schlüsselerzeugungsprozess **310**, um einen Geoverriegelungsschlüssel **166** zu konstruieren, der nicht erraten oder rekonstruiert werden kann. In einer bevorzugten Ausführungsform der Erfindung ist der Geoverriegelungsschlüssel **166** vierundsechzig Bits lang, wobei es sich jedoch versteht, dass jede Länge mit Vorteil verwendet werden könnte. Die resultierende Sequenz wird verwendet, um die Klartextdaten **170** durch Durchführen einer bitweisen XOR durch einen Verschlüsselungsprozess **312** zu verschlüsseln. Diese Ergebnisse in den verschlüsselten Bytes sind gleich in der Länge mit der Anzahl von Datenbytes im Klartext **170**. Die verschlüsselten Daten (oder der codierte Text) **158** wird mit dem Shape-Parm-Parameter **157** verkettet und als geoverriegelte digitale Information **156** gespeichert. Es versteht sich, dass jeder andere Verschlüsselungsalgorithmus ebenso mit Vorteil verwendet werden könnte.

[0068] Der beispielhafte Verschlüsselungsprozess **312** ist ähnlich zu anderen häufig verwendeten Verschlüsselungsverfahren mit einer bedeutenden Ausnahme. Die Verwendung eines 64 Bit kryptografischen Schlüssel kombiniert mit Klartext unter Verwendung einer exklusiven ODER-Funktion (XOR) wird kommerziell in solchen Protokollen verwendet, wie z.B. Wired Equivalent Privacy (WEP). Implementierungen von WEP müssen das Schlüsselverwaltungsproblem angehen wie die Schlüssel zu Stationen verteilt wird, die an der Konversation teilnehmen, so dass die Verschlüsselung/Entschlüsselung stattfinden kann. In der vorliegenden Erfindung gibt es jedoch kein Schlüsselverteilungsproblem. Der Verschlüsselungs-/Entschlüsselungsschlüssel kann konstruiert werden nur aus der ortsfreien Information, die in der digitalen Information enthalten ist, den Abspielort für das Gerät. Nur ein Gerät, dass innerhalb des Umgebungsbereiches lokalisiert ist, der durch das Ortsidentitätsattribut festgelegt wird, wenn die Datei verschlüsselt wird, kann die digitale Information sehen oder abspielen. Alternativ dazu kann der Zeitparameter des Ortsidentitätsattributes **140** statt dessen oder mit dem Umgebungsparameter verwendet werden, um den Verschlüsselungsschlüssel zu konstruieren.

[0069] Der vorerwähnte Schlüsselerzeugungsprozess **310**, der verwendet wird, um einen Geoverriegelungsschlüssel **166** aus den Shape-Parm-Werten und einem Abspielortswert (lat, lng) zu erzeugen, ist ausführlicher in Fig. 11 gezeigt. Ein ursprünglicher Schlüsselerzeugungsprozess **322** verwendet den Shape-Parm **157** und den Ortsparameter **162**, um einen ursprünglichen kryptografischen 64-Bit-Schlüssel **174** zu erzeugen. Der ursprüngliche Schlüssel **124** wird dann in einem Geheimschlüsselerzeugungsprozess **324** (d.h. einer verborgenen Funktion) verwendet, die eine deterministische mathematische Transformation des ursprünglichen Schlüssels **174** verwendet, um den Geoverriegelungsschlüssel **166** weiter zu sichern und zu erzeugen. Der ursprüngliche Schlüsselerzeugungsprozess **322**, der verwendet wird, um den ursprünglichen Schlüssel zu erzeugen, und der Geheimschlüsselerzeugungsprozess **324** werden weiter unten in Bezug auf Fig. 13 beschrieben.

[0070] Nachdem die digitale Information in Übereinstimmung mit einer der vorhergehenden Ausführungsformen der Erfindung verschlüsselt wurde, führt ein Gerät einen Entschlüsselungsprozess durch, um die digitale Klarinformation wieder zu erhalten und erlaubt dadurch, das Ansehen oder Abspielen der digitalen Information. Fig. 12 zeigt ein Dechiffrierverfahren für das Wiedererhalten von digitaler Klartextinformation aus geo-verriegelter digitaler Information. Das Verfahren startet in Schritt **320** mit einem Befehl, auf geoverriegelte digitale Information, die in Übereinstimmung mit einem Identitätsattribut verschlüsselt wurde, zuzugreifen. In Schritt **322** wird der Geräteort **160** bestimmt, zum Beispiel unter Verwendung eines der oben in Bezug auf die Fig. 6A bis Fig. 6D beschriebenen Verfahren. Der Geräteort **160** kann durch das Gerät für die weitere Verwendung in dem Verfahren gespeichert werden. Auf die geoverriegelte digitale Information **156** wird in Schritt **324** zugegriffen. Wie oben beschrieben weist die geoverriegelte digitale Information **156** den Shape-Parm-Parameter **157** und den chiffrierten Text **158** auf. Die Dechiffrierungsverarbeitung wird in Schritt **326** durchgeführt, in dem der Shape-Parm **157** und der Abspielort **160** verwendet werden, um den Geoverriegelungsschlüssel zu bestimmen, der verwendet wird, um die verschlüsselte Information zu entschlüsseln und die digitale Klartextinformation **170** zu erhalten. Danach kann die digitale Klartextinformation **170** von dem Gerät in irgendeiner gewünschten Art und Weise verwendet werden, z.B. Abspulen der digitalen Information an einem Drucker, Ansehen der digitalen Information auf einem Anzeige-/Abspielgerät, usw. Der Entschlüsselungsverarbeitungsschritt **326** wird unten ausführlicher in Bezug auf Fig. 15 beschrieben.

[0071] In Fig. 13 ist ein beispielhafter Prozess für das Erzeugen des Geoverriegelungsschlüssels gezeigt, der entweder für die Verschlüsselung oder die Entschlüsselung verwendet wird. Die Werte (flat(plat), fling(plng)), die oben für jede der rechteckigen und kreisförmigen Umgebungsbereiche berechnet wurden, werden als Eingaben verwendet, um den Geoverriegelungsschlüssel zu erzeugen. Wie oben in Bezug auf die Fig. 8 und Fig. 9 beschrieben, werden diese Werte berechnet aus den Shape-Parm und dem Ortswert. Der Breitengradwert flat(plat) **182** wird als 10-Zeichen-Breitengradstring **184** im Prozessschritt **332** formatiert, um das Format sll.dddddd, in dem s das Vorzeichen ist, zu erzielen. In gleicher Weise wird der Längengradwert flng(plng) **183** als ein

11-Zeichen-Längengradstring **185** im Prozessschritt **334** formatiert, um das Format slll.dddddd zu erzielen. Dann werden im Prozessschritt **336** alle nichtnumerischen Zeichen (d. h. das Vorzeichen und der Dezimalpunkt) aus dem Breitengradstring **184** und dem Längengradstring **185** entfernt und der resultierende Längengradstring **185** wird mit dem resultierenden Breitengradstring **184** verkettet, um einen 17-Zeichen-String **186** zu erzielen mit dem Format llddddddlllddddddd. Im Prozeßschritt **338** wird der 17-Zeichen-String **186** in einen 64-Bit-Binärstring umgewandelt. Genauer gesagt, wird das Endzeichen des 17-Zeichen-Strings fallen gelassen, was zu einem 16-Zeichen-String führt, in dem alle Zeichen numerisch sind. Da jedes numerische Zeichen durch ein 4-Bit-Oktett (z.B. "1" ist das Oktett "0001" und "2" ist das Oktett "0010", usw. dargestellt werden kann) werden die Oktettdarstellungen für jedes Zeichen in dem 16-Zeichen-String zusammen verkettet, um den 64-Bitbinärstring zu erzielen. Der 64-Bitbinärstring stellt den ursprünglichen Schlüssel **174** bereit, der für das Verschlüsseln der digitalen Information wie oben beschrieben verwendet wird.

[0072] Der ursprüngliche Schlüssel **174** wird dann mit einer versteckten Funktion **340** verarbeitet, die ihn in einen geheimen oder Geoverriegelungsschlüssel **166** umwandelt. In der bevorzugten Ausführungsform der Erfindung wird eine relativ einfache versteckte Funktion verwendet, obgleich es sich versteht, dass andere und kompliziertere versteckte Funktionen ebenso verwendet werden können. Gemäß der versteckten Funktion **340** wird der ursprüngliche Schlüssel **174** mit einem 64-Bitbinärstring kombiniert, der mit der Oktetterweiterung des 16-Zeichen-Strings 1234567890123456 verknüpft ist unter Verwendung einer ausschließlichen ODER-Funktion (d.h. XOR). Dies erzeugt einen Geoverriegelungsschlüssel **166**, der sowohl für die Verschlüsselung als auch die Entschlüsselung verwendet wird. Bezeichnenderweise wird der Wert dieses Geoverriegelungsschlüssels **166** der gleiche für alle Orte innerhalb des Umgebungsbereiches sein entsprechend der geoverriegelten digitalen Information. In einer bevorzugten Ausführungsform der Erfindung wird die versteckte Funktion als eine Softwareroutine implementiert, es versteht sich jedoch, dass eine stärkere Verschlüsselung resultieren wird durch Implementieren des gesamten Verschlüsselungsalgorithmus, einschließlich der versteckten Funktion im elektronischen Schaltkreis.

[0073] Fig. 14 ist ein Flußdiagramm gezeigt, dass ein Entschlüsselungsverfahren zeigt, dass bei einem Gerät anwendbar ist, dass versucht, die Geoverriegelung abzurufen. In diesem Verfahren kann der Abspielgerätort **160** bekannt sein oder aus dem Speicher abgerufen werden oder bestimmt werden, wie vorher in Bezug auf die Fig. 6A bis Fig. 6D gezeigt. Das Verfahren startet in Schritt **342**, in dem der Shape-Parm **157** von der geoverriegelten digitalen Information **156** verwendet wird im Zusammenhang mit dem Abspielgerätort **160**, um einen Geoverriegelungsschlüssel **166** zu erzeugen. Die digitale Chiffriertextinformation **158** wird dann in Schritt **344** entschlüsselt und zwar unter Verwendung des Geoverriegelungsschlüssels **166**, um die digitale Klartextinformation **170** zu erhalten. Wie oben beschrieben, kann der Entschlüsselungsschritt **344** eine exklusive ODER-Funktion zwischen dem Geoverriegelungsschlüssel **166** und der digitalen Chiffriertextinformation **158** durchführen.

[0074] Es wird nun auf die Fig. 15 bis Fig. 17 Bezug genommen. Dort sind verschiedene Beispiele des begrenzten rechteckigen Umgebungsbereiches gezeigt. Die Figuren sind ähnlich zu Fig. 8 (oben beschrieben), werden aber verwendet, um die Berechung der Geoverriegelungsschlüssel für einen begrenzten rechteckigen Umgebungsbereich zu zeigen unter Verwendung der bevorzugten Verfahren, die oben präsentiert wurden. Fig. 15 zeigt ein erstes begrenztes rechteckiges Umgebungsgebiet, dass verwendet wird für die Erzeugung eines Geoverriegelungsschlüssels. Das Ortsidentitätsattribut ist wie folgt:

Ortsidentität = (Ort, Umgebung) =
((39.102479, 77.235771), ((39.102100, 77.235000), (39.103100, 77.237000)))

[0075] Der Shape-Parm-Parameter wird abgeleitet aus der Ortsidentität wie folgt:

Shape-Parm = ((Δlat, Δlng), (olat, olng)) =
((.001,.002), (.0001,.001))

[0076] Der Shape-Parm wird dann von den vorher gehenden Abbildungsfunktionen verwendet, um f(plat) und f(plng) zu bestimmen:

f(plat) = .001·(int(plat – .0001)/.001)

f(plat) = .001·(int(39.102479 – .0001)/.001) =
39.102000

f(plng) = .002·(int(plng – .0001)/.0001)

f(plng) = .002·(int(77.235771 – .001)/.0001) =
77.234000

[0077] Die acht signifikantesten Zeichen von f(plat) und f(plng) werden verwendet, um den 16-Zeichenstring 3910200007723400 zu erzielen. Jedes einzelne Zeichen des 16-Zeichenstrings wird als nächstes in ein 4-Bit-Oktett umgewandelt, um den folgenden ursprünglichen 64-Bitstringschlüssel zu erhalten:
0011100100010000001000000000000000011101
1100100011010000000000

[0078] Der ursprüngliche 64-Bitstringschlüssel wird dann mit der Oktetterweiterung des 16-Zeichenstrings 123456789123456 kombiniert unter Verwendung einer exklusiven Oder-Funktion (d. h. XOR), um den Geoverriegelungsschlüssel zu erzeugen. Genauer gesagt ist die Oktetterweiterung des 16-Zeichenstrings 1234567890123456 wie folgt:
0001001000110100010101100111100010010000000100100011010001010110

[0079] Der Geoverriegelungsverschlüsselungsschlüssel, der erzeugt wird durch Kombinieren der zwei 64-Bitstrings unter der Verwendung der exklusiven ODER-Funktion ist wie folgt:
0010101100100100011101100111100010010111011000000000000001010110

[0080] Fig. 16 zeigt die Erzeugung des Geoverriegelungsschlüssels für einen begrenzten rechteckigen Umgebungsbereich, wenn der Abspielgerätort konsistent ist mit der Ortsidentität der geoverriegelten Daten, d.h. innerhalb des rechteckigen Umgebungsbereichs liegt. In diesem Beispiel unterscheidet sich der Abspielgerätort (d.h. 39.102120, 77.236120) von dem Abspielgerätort, der in dem obigen Beispiel in Bezug auf Fig. 15 gegeben ist. Dennoch, wie gezeigt werden wird, führen beide Sätze von Berechnungen zum selben kryptografischen Schlüsseln, was demonstriert, dass die digitale Chiffriertextinformation von jedem Abspielgerätort innerhalb des rechteckigen Umgebungsbereiches wiederhergestellt werden kann. Für den spezifizierten Abspielgerätort sind die Shape-Parmparameter diesselben wie oben beschrieben. Die Abbildungsfunktionen f(plat) und f(plng) sind wie folgt:

f(plat) = .001·(int(plat – .0001)/.001)

f(plat) = .001·(int(39.102120 – .0001)/.001) = 39.102000

f(plng) = .002·(int(plng – .001)/.0001)

f(plng) = .002·(int(77.236120 – .001)/.0001) = 77.234000

[0081] Es versteht sich, dass die Abbildungsfunktionen f(plat) und f(plng) die gleichen sind für diesen Abspielgerätort wie für das Ortsidentitätsattribut, dass oben beschrieben wurde. Folglich werden der ursprüngliche Schlüssel und der Geoverriegelungsschlüssel ebenso die gleichen sein wie oben berechnet. Ein Abspielgerät wird somit in der Lage sein, erfolgreich die digitale geoverriegelte Information von dem spezifizierten Abspielgerätort zu entschlüsseln.

[0082] Im Gegensatz dazu zeigt Fig. 17 die Erzeugung eines Geoverriegelungsschlüssels für einen begrenzten rechteckigen Umgebungsbereich, wenn der Abspielgerätort nicht konsistent mit der Ortsidentität der geoverriegelten Daten ist, d.h. außerhalb des Umgebungsbereiches liegt, der von der Ortsidentität festgelegt wurde. Der Abspielgerätort (d.h. 28.543212, 73.543456) unterscheidet sich von dem Abspielort, der im vorherigen Beispiel gegeben wurde. Für diesen speziellen Abspielgeräteort sind die Shape-Parmparameter einmal mehr die gleichen wie im vorherigen Beispiel, die Abbildungsfunktionswerte ergeben jedoch unterschiedliche Werte für f(plat) und f(plng). Genauer gesagt sind die Abbildungsfunktionen f(plat) und f(plng) wie folgt:

f(plat) = .001·(int(plat – .0001)/.001)

f(plat) = .001·(int 28.543212 – .0001)/.001) = 28.543000

f(plng) = .002·(int(plng – .001)/.0001)

f(plng) = .002·(int(73.543456 – .001)/.0001) = 73.542000

[0083] Die acht signifikantesten Zeichen von f(plat) und f(plng) werden verwendet, um den 16-Zeichenstring 2854300007354200 zu erzielen. Jedes einzelne Zeichen des 16-Zeichenstrings wird als nächstes in ein 4-Bitoktett umgewandelt, um den folgenden ursprünglichen 64-Bitstring-Key zu erhalten:
0010100001010100001100000000000000000011001101010100001000000000

[0084] Wie vorher wird der ursprüngliche 64-Bitstringschlüssel dann mit der Oktetterweiterung des 16-Zeichenstrings 1234567890123456 kombiniert unter Verwendung der ausschließlichen ODER-Funktion (d. h. XOR), um den Geoverriegelungsschlüssel zu erzeugen und zwar wie folgt:
0011101001100000011001100111100010010111001001110111011001010110

[0085] Der ursprüngliche Schlüssel und damit der Geoverriegelungsschlüssel sind somit nicht in die gleichen wie vorher berechnet. Somit wird ein Abspielgerät nicht in der Lage sein, die digitale geoverriegelte Information von dem spezifizierten Abspielgerät zu entschlüsseln.

[0086] Es wird nun Bezug genommen auf die Fig. 18 und Fig. 19, die Beispiele der Berechnungen des Verschlüsselungs-/Entschlüsselungsschlüssel für einen kreisförmigen Umgebungsbereich bereitstellen. Die Figuren sind ähnlich zu Fig. 9 (oben beschrieben), werden aber verwendet, um die Berechnung der Verschlüsselungs-/Entschlüsselungsschlüssel für einen kreisförmigen Umgebungsbereich zu zeigen unter Verwendung des bevorzugten oben präsentierten Verfahrens. Fig. 18 zeigt die Erzeugung des Verschlüsselungsschlüssels für eine kreisförmigen Umgebungsbereich. Das Ortsidentitätsattribut ist wie folgt:

Ortsidentität = (Ort, Umgebung) = ((lat, lng), (radius)) =
((39.102479, 77.235711), 0.0001)

[0087] Der Shape-Parmparameter wird aus der Ortsidentität abgeleitet wie folgt:

Shape-Parm = ((olat, olng), radius) = ((–.000021, 000071), 0.0001)

[0088] Der Durchmesser des kreisförmigen Umgebungsbereich Δlatlng beträgt 0,0002. Der Shape-Parm wird dann in den vorhergehenden Abbildungsfunktionen verwendet, um f(plat) and f(plng) zu bestimmen:

f(plat) = .0002·(int(plat – (–.000021)/.0002)

f(plat) = .0002·(int(39.102479 + .000021)/.000) = 39.102400

f(plng) = .0002·(int(plng – .000071)/.0002

f(plng) = .0002·(int((77.235711 – .000071)/.0002) = 77.235600

[0089] Die acht signifikanten Zeichen von f(plat) und f(plng) werden verwendet, um den 16-Zeichen-String 3910240007723560 zu erhalten. Jedes einzelne Zeichen des 16-Zeichen-Strings wird als nächstes in ein 4-Bit-Oktett umgewandelt, um den folgenden ursprünglichen 64-Bitstringschlüssel zu erhalten:
0011100100010000001000000000000000000011100100011010101100000

[0090] Der ursprüngliche 64-Bitstringschlüssel wird dann mit der Oktetterweiterung des 16-Zeichenstrings 1234567890123456 unter Verwendung einer ausschließlichen Oder-Funktion (d.h. XOR) kombiniert, um den folgenden Geoverriegelungsschlüssel zu erzeugen:
0010101100100100011100100111100010010111011000000000000100110110

[0091] Fig. 19 zeigt die Erzeugung des Geoverriegelungsschlüssels für einen kreisförmigen Umgebungsbereich, wenn der Abspielgeräteort innerhalb der Ortsidentität der geoverriegelten Daten liegt, d.h. innerhalb des kreisförmigen Umgebungsbereichs. Der Abspielgeräteort (d.h. 39,102420; 77.235699) unterscheidet sich von dem Abspielort, der in der Ortsidentität festgelegt ist, die oben in Bezug auf Fig. 18 dargestellt ist. Wie gezeigt wird, liefern jedoch beide Berechnungssätze denselben kryptographischen Schlüssel. Für den spezifizierten Abspielgerätort sind die Shape-Parmparameters die gleichen wie oben in Bezug auf Fig. 18 beschrieben. Der Shape-Parm wird dann in den vorhergehenden Abbildungsfunktionen verwendet, um f(plat) und f(plng) zu bestimmen:

f(plat) = .0002·(int(plat – (–.000021)/.0002)

f(plat) = .0002·(int(39.102420 + .000021)/.0002) = 39.102400

f(plng) = .0002·(int(plng – .000071)/.0002)

f(plng) = .0002·(int(77.235699 – .000071)/.0002) = 77.235600

[0092] Die Abbildungsfunktionen führen zu denselben Ergebnissen bei dem spezifizierten Abspielgeräteort als sie es unter Verwendung des Ortsabschnittes der Ortsidentität tun. Die Koordinate (plat, plng) wird als nächstes bewertet, um zu bestimmen, ob sie innerhalb des kreisförmigen Umgebungsbereiches liegt und zwar unter Verwendung der Gleichung:

$dist = sqrt((plat – (f(plat) + radius + olat))^2 + (plng – (f(plng) + radius + olng))^2)$

$dist = sqrt((39.1024202 – (39.102400 + .00001 – .000021))^2 + (77.235699 – (77.235600 + .00001 + .000071))^2)$
dist = .00008414

[0093] Wenn die Abstandsfunktion einen Wert zurückgibt, der kleiner oder gleich dem Radius ist, dann liegt das Abspielgerät innerhalb oder auf dem Umfang des kreisförmigen Bereichs. Umgekehrt, wenn die Abstandsfunktion größer als der Radius ist, dann wird der Geoverriegelungsschlüssel auf einen 64-Bitstring aus nur "0"-en gesetzt, was ein ungültiger Schlüssel ist und nicht korrekt die digitale geoverriegelte Information entschlüsseln wird. Wie oben beschrieben, sind die Abbildungsfunktionen f(plat) und f(plng) für diesen Abspielgeräteort die gleichen wie für das Ortsidentitätsattribut. Folglich werden der ursprüngliche Schlüssel und der Geoverriegelungsschlüssel ebenso die gleichen sein wie vorher berechnet. Somit wird ein Abspielgerät in der Lage sein, die digitale geoverriegelte Information von dem spezifizierten Abspielgeräteort erfolgreich zu entschlüsseln.

[0094] Es gibt viele Vorteile für das vorhergehende kryptographische Ortsidentitäts-System und Verfahren. Die Ortsidentität stellt einen Weg bereit, digitale Informationssicherheitsprobleme zu überwinden und kryptographische Schlüssel in einer Art und Weise zu verwalten, die für den Benutzer völlig transparent sind. Dies erlaubt es, dass verschlüsselte digitale Informationen einfach über öffentliche Netzwerke, wie z.B. das Internet, verbreitet wird. Ein Benutzer innerhalb eines Umgebungsbereiches, für den die digitale Information erzeugt wurde, wird in der Lage sein, auf die Information zuzugreifen und die Information zu verwenden, während Benutzern außerhalb dieses Gebietes der Zugriff verweigert wird. In dieser Hinsicht stellt die Erfindung eine "maßgeschneiderte"

oder "Einzel"-Verschlüsselung bereit, durch die digitale Information speziell für einen Zielort verschlüsselt wird, in dem sie abgespielt wird. Maßgeschneiderte Verschlüsselung erlaubt es ebenso, dass digitale Information maßgeschneidert wird, um Vorschau- und Werbematerialien, die in der geoverriegelten Information enthalten sind, zu planen. Wenn eine Datei für einen bestimmten Ort verschlüsselt ist, können demographische Daten dieses Gebietes verwendet werden, um maßgeschneiderte Vorschaumaterialien aufzunehmen. Beispielsweise können Materialien, die für Mexiko-City verschlüsselt sind, Vorschaumaterialien in Spanisch beinhalten, während ähnliche Materialien für Gaithersburg, Maryland in Englisch sein würden.

[0095] Die Ortsidentität basierte Verschlüsselung nimmt einen charakteristisch anderen Ansatz gegenüber vorherigen kryptographischen Verfahren in Bezug auf die gemeinsame Nutzung der kryptographischen Schlüsseln an. Es gibt zwei Stücke von notwendiger Information für das Konstruieren der symmetrischen Entschlüsselung, einschließlich: a) den Abspielort, der dem Abspielgerät bekannt ist, und b) den Shape-Parmparameter, der in der entschlüsselten digitalen Information beinhaltet ist. Kein Stück der Information allein ist ausreichend, einen Entschlüsselungsschlüssel zu konstruieren. Die Verschlüsselung ist spezifisch für ein geographisches Gebiet und der Verschlüsselungsalgorithmus muss nichts über den Benutzer oder das Gerät wissen, auf dem die Entschlüsselung erfolgen wird. Die Entschlüsselung derselben digitalen Information kann auf irgendeiner Maschine erfolgen mit einem Ort, der als innerhalb des Bereiches identifiziert wird, die von dem Ortsidentitätsattribut festgelegt wird. Die Ortidentitätsverschlüsselung unterscheidet sich von vorherigen kryptographischen Algorithmen darin, dass sie das Schlüsselverteilungsproblem vermeidet, dass die Verwendbarkeit der bekannten Verfahren begrenzt. Es besteht nicht die Notwendigkeit, kryptographische Schlüssel zu verteilen oder gemeinsam zu nutzen, wie in symmetrischen kryptographischen Verfahren, wie z.B. Wired Equivalent Privacy (WEP) oder asymmetrischen Verfahren, wie z.B. Diffie-Hellman. Ebenso gibt es nicht das Erfordernis, einen Geheimschlüsselaustausch auszuhandeln wie in Secure Sockets Layer (SSL) oder Secure Multipurpose Internet Mail Exchange (S/MIME).

[0096] Es gibt sehr zahlreiche Anwendungen und Datenformate, bei denen das Ortsidentitätsattribut verwendet werden kann, um den Zugriff auf digitale Information zu steuern. Ein Benutzer kann geoverriegelte digitale Information in elektronischer Form empfangen unter Verwendung irgendeiner konventionellen Methode, einschließlich über die Telefonleitung, Faseroptik, Kabelfernsehen, Satellitenempfang, per Funk oder über andere Medien. Ein Benutzer kann ebenso speziell erzeugte geoverriegelte digitale Information physikalisch von einem Geschäft oder Verkäufer in Form von magnetischen oder anderen kodierten Medien, z. B. CD-ROM, Diskette, Videokassette oder Band, erhalten. In gleicher Weise kann geoverriegelte digitale Information über ein Netzwerk übertragen werden, einschließlich Weitbereichsnetzwerke, wie z.B. das Internet, lokale Netzwerke, wie z.B. Intranets, Einwahl-Zugriff zwischen persönlichen und Servern-Computern, als eine Anlage an eine E-Mail oder über ein digitales Mobiltelefon oder andere Funkgeräte. Geoverriegelte digitale Information kann auf Diskette, CD-ROM, Band, festeingebaute oder entfernbare Festplatten, DVD-CD-ROMs, Flashspeicher/-Platten, EEPROMs, usw. gespeichert werden. die Typen von digitaler Information, die auf diese Weise geschützt werden können, beinhalten Musikdateien (z.B. MP3), Software, literarische Arbeiten, kommerzielle Transaktionsdateien, Textdateien, Video/Graphik, Paging-Nachrichten, Mobiltelefonkonversation, kommerzielle und digitale Filme, um nur ein paar zu nennen.

[0097] In einer beispielhaften Anwendung bestellt ein Kunde einen digitalen Film oder Audio über einen Katalog eines Verkäufers. Der Katalog kann gedruckt oder internet-basiert sein und der Auftrag kann über Post, Telefon, Faxübertragung oder internet-basierte Transaktionen aufgegeben werden. Egal welches Verfahren zur Aufgabe der Bestellung verwendet wird, der Auftrag des Kunden zeigt den Ort der Abspielung an. Wenn der Verkäufer den Auftrag erfüllt, wird das Ortsidentitätsattribut, dass mit dem Käufer verknüpft ist, bestimmt und verwendet, um einem Verschlüsselungsschlüssel zu erzeugen, der dann verwendet wird, um die digitale Informationsdatei für das Medium zu verschlüsseln. Die verkauften Medien sind dann speziell für den Auftrag verschlüsselt, kopiert in ein Format, wie z.B. DVD oder CD-Rom und mit einem Betrachter zusammengepackt, der ebenso speziell angepasst ist für das Ortsidentitätsattribut. Selbst wenn die gesamten Inhalte der verkauften Medien kopiert werden, verhindert der Betrachter und die Medien, die mit dem Ortsidentitätsattribut versehen sind, das Betrachten außer in den erlaubten Bereich. In dieser beispielhaften Anwendung stellt die Verwendung der Ortsidentität und der speziell angepassten Verschlüsselung und die Betrachter eine sichere Lösung der für die Probleme der Piraterie und der nicht-autorisierten Verwendung und des Kopierens von digitalen Medien.

[0098] In einer anderen beispielhaften Anwendung der Erfindung wird die Ortsidentität verwendet, um Informationen über öffentliche Netzwerke "eng" auszusenden. Das enge Senden bezieht sich in diesem Kontext auf die Übertragung von Information an ein Publikum an spezifischen Orten im Gegensatz zu den Punkt zu Punktübertragungen oder einer Sendeübertragung in unbeschränkte Orte. Viele Informationstypen sind nutzbar nur innerhalb eines Ortskon-

textes, z.B. lokales Wetter, Verkehrsinformation, Kinoprogramme, Geschäftsinformationen, usw. Anwendungen, die solche ortsabhängigen Informationen verwenden, können als ortsbasierte Anwendungen bezeichnet werden. Die Ortsidentität stellt einen Weg bereit, ein Sendetyp-Protokoll zu verwenden, um Information über ein Netzwerk zu senden, die von dem Ort für die sie vorgesehen ist, identifiziert wird, z.B. einen lokalen Bereich für das Wetter, Geschäftsort für den Verkauf und Werbeinformation, usw. Unter Verwendung des Orts des Clients-Gerätes können die Anwendungen des Clients die Ortsidentität verwenden, die der Information angehängt ist, um Information selektiv basierend auf ihren gegenwärtigen Ort auszusuchen. Es kann ebenso einen Weg bereitstellen, einen eindeutigen ortsbasierten, gemeinsam genutzten kryptographischen Schlüssel zu errichten, um sichere vertrauliche Kommunikationen für geographisch begrenzte enge Sendeanwendungen beizubehalten.

[0099] In einer anderen beispielhaften Anwendung der vorliegenden Erfindung wird die Ortsidentität verwendet, um die Vertraulichkeit und Sicherheit für Funknetzwerk-Verbindungen zu erhöhen. Netzwerke sind erwachsen geworden mit dem Aufkommen von Netzwerkgeräten und Protokollen, wie z. B. die "Bluetooth"-Technologie, die es drahtlosen, tragbaren oder Workstations erlaubt, sich mit einem Netzwerk zu verbinden. "Bluetooth" ist ein offener Standard für Kurzbereichsübertragung von digitaler Sprache und Daten zwischen mobilen Geräten (z.B. Laptops, PDAs, Mobiltelefon) und Desktopgeräten, die Punkt zu Punkt Mehrpunktanwendungen unterstützen. Da jede Funkanwendung, die über das Netzwerk kommuniziert, einen eindeutigen Ort haben wird, kann die Ortsidentität verwendet werden, um einen eindeutigen gemeinsam genutzten kryptographischen Schlüssel zu errichten, der verwendet werden kann, um sichere vertrauliche Kommunikationen für Funkgeräte, die sich über ein öffentliches Netzwerk verbinden, sicherzustellen.

[0100] In jeder der vorhergehenden Ausführungsformen und beispielhaften Anwendungen gibt es zumindest vier logische Grenzen, die zwischen dem Anwendungsprogramm, das auf digitale geoverriegelte Information zugreift und externen Geräten und der Netzwerkumgebung, in der diese Anwendungen arbeiten. Diese Grenzen beinhalten: (1) die Datenerfassungs-/Gerätegrenze, (2) die Speicher-/Gerätegrenze, (3) die Benutzerschnittstelle/Gerätegrenze und (4) die Geräte-/Ortserfassungsgrenze. Die Datenerfassung/Gerätegrenze bezieht sich auf die Durchführung der Ortsidentität am Punkt der Erfassung der digitalen Information durch ein Gerät, z.B. kann das Gerät nicht die digitale Information von einer anderen Quelle erhalten, es sei denn, das Ortsidentitätsattribut ist erfüllt. Die Speicher-/Gerätegrenze bezieht sich auf die Durchführung der Ortsidentität am Speicherpunkt der digitalen Information durch ein Gerät, z. B. kann das Gerät eine gespeicherte Datei aus dem Speicher nicht wieder aufrufen, es sei denn, das Ortsidentitätsattribut ist erfüllt. Die Benutzerschnittstelle/Gerätegrenze bezieht sich auf die Durchführung der Ortsidentität an dem Punkt der Darstellung der Information für den Benutzer, z.B. kann der Benutzer die digitale Information auf dem Monitor des Gerätes nicht ansehen, es sei denn, das Ortsidentitätsattribut ist erfüllt. Die Geräte/Erfassungsortgrenze bezieht sich auf die Beschränkungen mit Zugriff auf geoverriegelte Daten durch Validieren des Geräteortes, z.B. kann der Benutzer die digitale Information nicht sehen, speichern, abrufen oder auf andere Weise verwenden in irgendeiner Art und Weise, es sei denn, der Geräteort wird erfasst unter Verwendung eines eingebetteten GPS-Empfängers. Es versteht sich, dass die relative Sicherheit, die durch irgendeine bestimmte Implementierung der vorliegenden Erfindung bereitgestellt, wird, sich auf die Grenzen bezieht, an denen die Zugriffssteuerung durchgeführt wird.

[0101] Es wurde eine bevorzugte Ausführungsform eines Systems und ein Verfahren für die Verwendung der Ortsidentität beschrieben, um Zugriff auf digitale Informationen zu steuern. Es sollte für den Fachmann klar sein, dass verschiedene Vorteile der Erfindung erzielt wurden. Es versteht sich ebenso, dass verschiedene Modifikationen, Anpassungen und alternative Ausführungsformen hiervon durchgeführt werden können innerhalb des Schutzbereiches der vorliegenden Erfindung.

Patentansprüche

1. Verfahren zum Steuern des Zugriffs auf digitale Information (**170**), das aufweist:
Identifizieren eines Ortsidentitätsattributs (**140**), das zumindest einen spezifischen geographischen Ort festlegt,
Erzeugen eines Schlüssels zur geographischen Verriegelung bzw. eines Geolockingschlüssels (**166**), zumindest teilweise basierend auf dem Ortsidentitätsattribut (**140**),
Verschlüsseln der digitalen Information (**170**) unter Verwendung des Geolockingschlüssels (**166**) und
Übertragen der verschlüsselten digitalen Information zu einer Empfangseinrichtung, die angepaßt ist, um ihren Ort zu bestimmen und einen entsprechenden Geolockingschlüssel basierend auf ihrem bestimmten Ort zu erzeugen, so daß auf die verschlüsselte digitale Information (**158**) nur zugegriffen werden kann, wenn die Empfangseinrichtung an dem spezifischen geographischen Ort ist, ohne daß die Übertragung des Geolockingschlüssels notwendig ist.

2. Verfahren nach Anspruch 1, bei dem der Identifizierungsschritt weiterhin das Identifizieren von zumindest einem Ortswert (**142**) und einem Annähe-

rungswert (**143**) aufweist.

3. Verfahren nach Anspruch 2, bei dem der Ortswert (**142**) einem Ort einer vorgesehenen bzw. geplanten Empfängereinrichtung der digitalen Information (**170**) entspricht.

4. Verfahren nach Anspruch 2, bei dem der Ortswert (**142**) weiterhin einen Breitengrad und einen Längengrad aufweist.

5. Verfahren nach Anspruch 2, bei dem der Annäherungswert (**143**) einer Zone entspricht, die den Ort umgibt.

6. Verfahren nach Anspruch 2, das weiterhin das Erzeugen eines Formparameters (**157**) basierend auf dem Annäherungswert (**143**) aufweist, wobei der Formparameter (**157**) eine Form eines Bereichs festlegt, der den spezifischen geographischen Ort umfaßt.

7. Verfahren nach Anspruch 6, das weiterhin das Erzeugen eines ursprünglichen Schlüssels (**174**), basierend auf dem Formparameter (**157**), aufweist.

8. Verfahren nach Anspruch 7, das weiterhin das Erzeugen des Geolockingschlüssels (**166**) basierend auf dem ursprünglichen Schlüssel (**174**) aufweist, wobei der Verschlüsselungsschritt weiterhin das Verschlüsseln der digitalen Information (**170**) unter Verwendung des Geolockingschlüssels (**166**) aufweist.

9. Verfahren nach Anspruch 6, das weiterhin das Packen des Formparameters (**157**) mit der verschlüsselten digitalen Information (**158**) aufweist.

10. Verfahren nach Anspruch 9, das weiterhin das Senden des Formparameters (**157**) und der verschlüsselten digitalen Information (**158**) zu einem Endbenutzer aufweist.

11. Verfahren nach Anspruch 1, das weiterhin das Auswählen einer Vorschauinformation und Einschließen der Vorschauinformation in die digitale Information (**170**) vor dem Verschlüsselungsschritt aufweist.

12. Verfahren nach Anspruch 1, das weiterhin das Speichern der verschlüsselten digitalen Information (**158**) in einem festen Format aufweist, einschließlich CD-ROM, DVD, Diskette, Videokassette oder Band.

13. Verfahren nach Anspruch 10, bei dem der Übertragungsschritt weiterhin das Übertragen der verschlüsselten digitalen Information (**158**) in elektronischer Form aufweist, und zwar über eine Telefonleitung, ein Videokabel, eine Satellitensendung, eine Faseroptik oder drahtlos.

14. Verfahren nach Anspruch 1, bei dem das Zugreifen auf die verschlüsselte digitale Information (**158**) aufweist:
Abrufen der Ortsdaten (**160**), die einen spezifischen geographischen Ort einer Abspielvorrichtung identifizieren,
Zugreifen auf geoverriegelte Daten (**156**), die die verschlüsselte digitale Information (**158**) und einen Formparameter (**157**) beinhalten, welcher eine Form eines Bereiches festlegt, der den spezifischen geographischen Ort umgibt,
Erzeugen eines Geolockingschlüssels (**166**) unter Verwendung von zumindest dem Formparameter (**157**) und den Ortsdaten (**160**) und
Verschlüsseln der digitalen Information (**158**) unter Verwendung des Geolockingschlüssels (**166**).

15. Verfahren nach Anspruch 14, bei dem die Ortsdaten (**160**) weiterhin einen Breiten- (**144**) und einen Längengrad (**145**) aufweisen.

16. Verfahren nach Anspruch 14, bei dem der Erzeugungsschritt weiterhin das Erzeugen eines ursprünglichen Schlüssels (**174**), basierend auf dem Formparameter (**157**), aufweist.

17. Verfahren nach Anspruch 16, bei dem der Erzeugungsschritt weiterhin das Erzeugen des Geolockingschlüssels (**166**), basierend auf dem ursprünglichen Schlüssel (**174**), aufweist.

18. Verfahren nach Anspruch 14, bei dem der Zugriffsschritt weiterhin das Empfangen der geographisch verriegelten Daten (**156**) von einem entfernten Sender aufweist.

19. Verfahren nach Anspruch 14, bei dem die geoverriegelten Daten (**156**) weiterhin Vorschauinformationen aufweisen.

20. Verfahren nach Anspruch 14, bei dem der Zugriffsschritt weiterhin das Abrufen der geographisch verriegelten Daten (**156**) von einem Speichermedium aufweist, das zumindest eine CD-ROM, eine DVD, eine Diskette, eine Videokassette oder ein Band beinhaltet.

21. Verfahren nach Anspruch 14, bei dem der Zugriffsschritt weiterhin das Empfangen der geographisch verriegelten Daten (**156**) in elektronischer Form über die Telefonleitung, ein Videokabel, eine Satellitenausstrahlung, eine Faseroptik und/oder per Funk aufweist.

22. System für das Steuern des Zugriffs auf digitale Information (**170**), das eine Vorrichtung und eine Empfangseinrichtung aufweist, wobei die Vorrichtung aufweist:
einen Prozessor mit einem Speicher, der angepaßt ist, um Softwarebefehle zu speichern, die betreibbar

sind, um zu veranlassen, daß der Prozessor die folgenden Funktionen ausführt:
Identifizieren eines Ortsidentifizierungsattributes (**140**), das zumindest einen spezifischen geographischen Ort festlegt,
Erzeugen eines Geolockingsschlüssels (**166**), zumindest teilweise basierend auf dem Ortsidentifizierungsattribut (**140**),
Verschlüsseln der digitalen Information (**170**) unter Verwendung des Geolockingschlüssels (**166**) und
Übertragen der verschlüsselten digitalen Daten zu der Empfangseinrichtung, wobei die Empfangseinrichtung angepaßt ist, so daß sie ihren Ort bestimmt und einen korrespondierenden Geolockingschlüssel basierend auf ihrem bestimmten Ort erzeugt, so daß auf die verschlüsselten digitalen Informationen nur ohne die Notwendigkeit, den Geolockingschlüssel zu übertragen, zugegriffen werden kann, wenn die Empfangseinrichtung an dem speziellen geographischen Ort angeordnet ist.

23. System nach Anspruch 22, bei dem die Identifizierungsfunktion weiterhin das Identifizieren von zumindest einem Ortswert (**142**) und einem Näherungswert (**143**) aufweist.

24. System nach Anspruch 23, bei dem der Ortswert (**142**) einem Ort einer beabsichtigten Empfangseinrichtung der digitalen Information entspricht.

25. System nach Anspruch 23, bei dem der Ortswert (**142**) weiterhin einen Breiten- (**144**) und einen Längengrad (**145**) aufweist.

26. System nach Anspruch 23, bei dem der Annäherungswert (**143**) einer Zone entspricht, die den Ort umfaßt.

27. System nach Anspruch 23, das weiterhin die Funktion des Erzeugens eines Formparameters (**157**) basierend auf dem Annäherungswert (**143**) aufweist, wobei der Formparameter (**157**) eine Form eines Bereichs festlegt, der den spezifischen geographischen Ort umfaßt.

28. System nach Anspruch 27, das weiterhin die Funktion des Erzeugens eines ursprünglichen Schlüssels (**174**), basierend auf dem Formparameter (**157**), aufweist.

29. System nach Anspruch 28, das weiterhin die Funktion des Erzeugens des Geolockingschlüssels (**166**), basierend auf dem ursprünglichen Schlüssel (**174**), aufweist.

30. System nach Anspruch 27, das weiterhin die Funktion des Packens des Formparameters (**157**) mit der verschlüsselten digitalen Information (**158**) aufweist.

31. System nach Anspruch 30, das weiterhin die Funktion des Übertragens des Formparameters (**157**) und der verschlüsselten digitalen Information (**158**) zu einem Endbenutzer aufweist.

32. System nach Anspruch 22, das weiterhin die Funktion des Auswählens von Vorschauinformation und des Einfügens der Vorschauinformation in die digitale Information (**170**) vor der Ausführung der Verschlüsselungsfunktion aufweist.

33. System nach Anspruch 22, das weiterhin einen Server aufweist, der mit dem Prozessor verbunden ist und angepaßt ist, um die verschlüsselte digitale Information (**158**) über eine Netzwerkverbindung zu Endbenutzern zu senden.

34. System nach Anspruch 22, bei dem die Empfangseinrichtung aufweist:
einen Prozessor mit Speicher, der angepaßt ist, um Softwarebefehle zu speichern, die betreibbar sind, um zu veranlassen, daß der Prozessor die folgenden Funktionen ausführt:
Abrufen von Ortsdaten (**160**), die einen spezifischen geographischen Ort der Empfangseinrichtung identifizieren,
Zugreifen auf geographisch verriegelte Daten (**156**), die die verschlüsselte digitale Information (**158**) und einen Formparameter (**157**), der eine Form eines Bereiches, der einen spezifischen geographischen Ort umfaßt, festlegt, beinhalten,
Erzeugen eines Geolockingschlüssels (**166**) unter Verwendung des Formparameters (**157**) und/oder der Ortsdaten (**160**) und
Verschlüsseln der digitalen Information unter Verwendung des Geolockingschlüssels (**166**).

35. System nach Anspruch 34, bei dem die Ortsdaten (**160**) weiterhin einen Breiten- (**144**) und einen Längengrad (**145**) aufweisen.

36. System nach Anspruch 34, bei dem die Erzeugungsfunktion weiterhin das Erzeugen eines ursprünglichen Schlüssels (**174**), basierend auf dem Formparameter (**157**), aufweist.

37. System nach Anspruch 36, bei dem die Erzeugungsfunktion weiterhin das Erzeugen des Geolockingschlüssels (**166**), basierend auf dem ursprünglichen Schlüssel, aufweist.

38. System nach Anspruch 34, bei dem die Zugriffsfunktion weiterhin das Empfangen der geographisch verriegelten Daten (**156**) von einem entfernten Sender aufweist.

39. System nach Anspruch 34, bei dem die geographisch verriegelten Daten (**156**) weiterhin eine Vorschauinformation aufweisen.

40. System nach Anspruch 34, bei dem die Zugriffsfunktion weiterhin das Abrufen der geographisch verriegelten Daten (**156**) von einem Speichermedium aufweist, das zumindest eine CD-ROM, eine DVD, eine Diskette, eine Videokassette oder ein Band beinhaltet.

41. System nach Anspruch 34, bei dem die Zugriffsfunktion weiterhin das Empfangen der geographisch verriegelten Daten (**156**) in elektronischer Form aufweist über eine Telefonleitung, ein Videokabel, eine Satellitensendung, eine Faseroptik und/oder drahtlos.

42. System nach Anspruch 34, das weiterhin einen GPS-Empfänger aufweist, der mit dem Prozessor verbunden ist und angepaßt ist, um die Ortsdaten (**160**) bereitzustellen.

Es folgen 14 Blatt Zeichnungen

Anhängende Zeichnungen

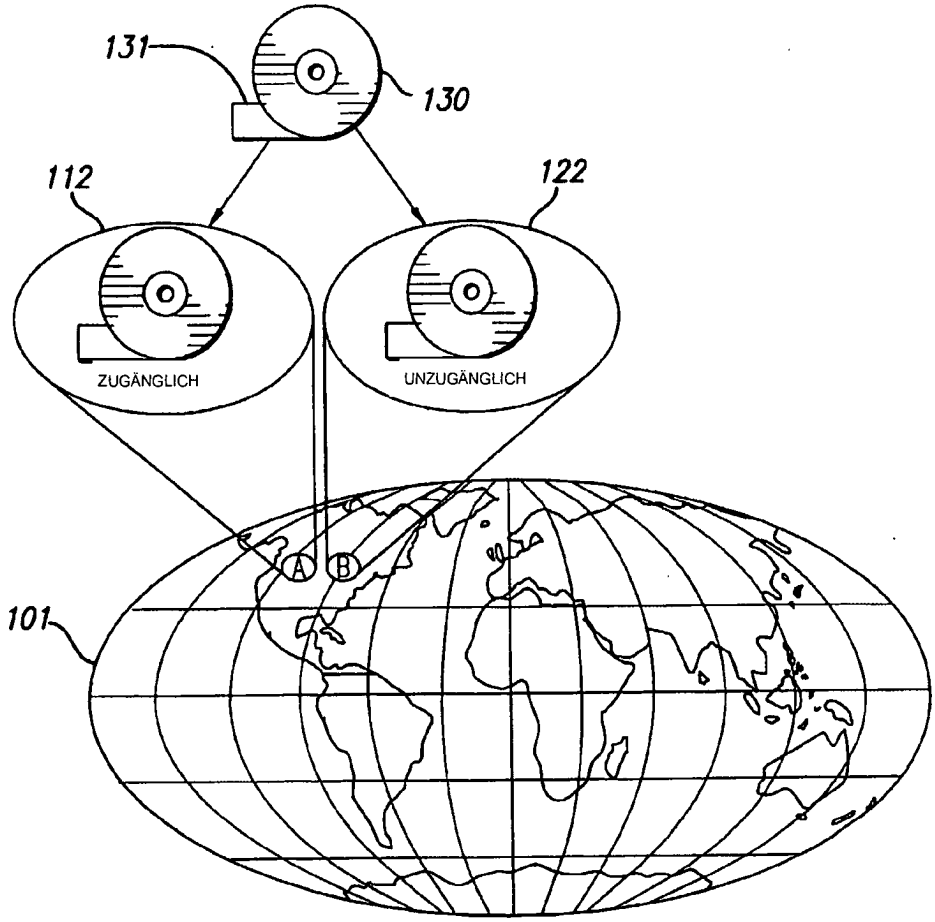


FIG. 1

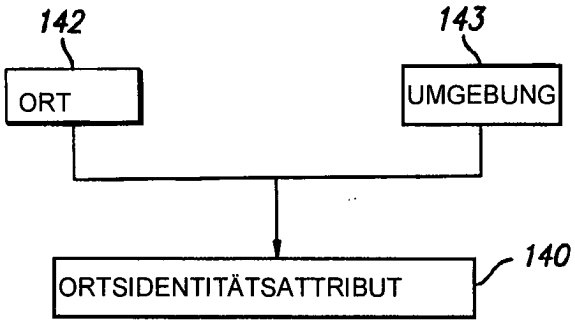


FIG. 2

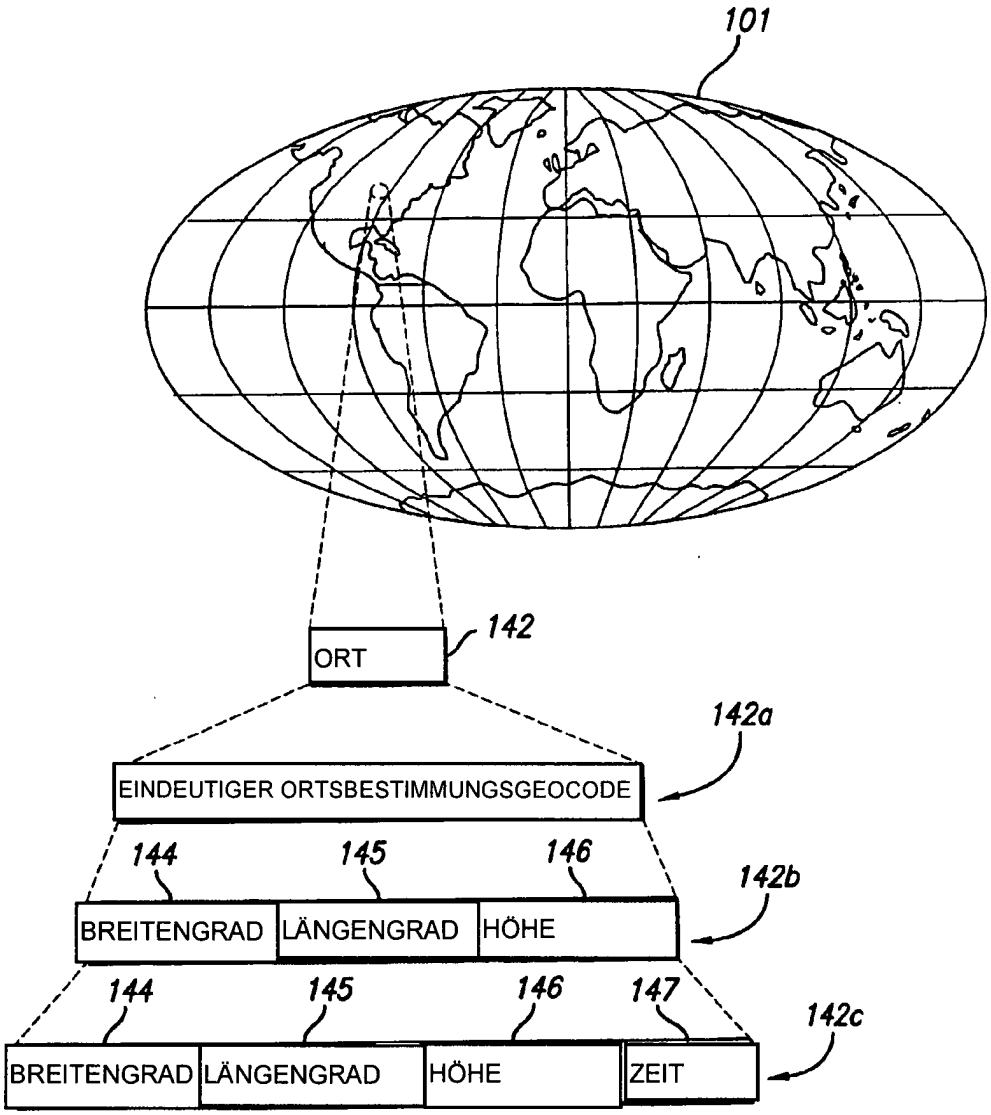

101
142
ORT
142a
EINDEUTIGER ORTSBESTIMMUNGSGEOCODE
144
145
146
142b
BREITENGRAD
LÄNGENGRAD
HÖHE
144
145
146
147
142c
BREITENGRAD
LÄNGENGRAD
HÖHE
ZEIT

FIG. 3

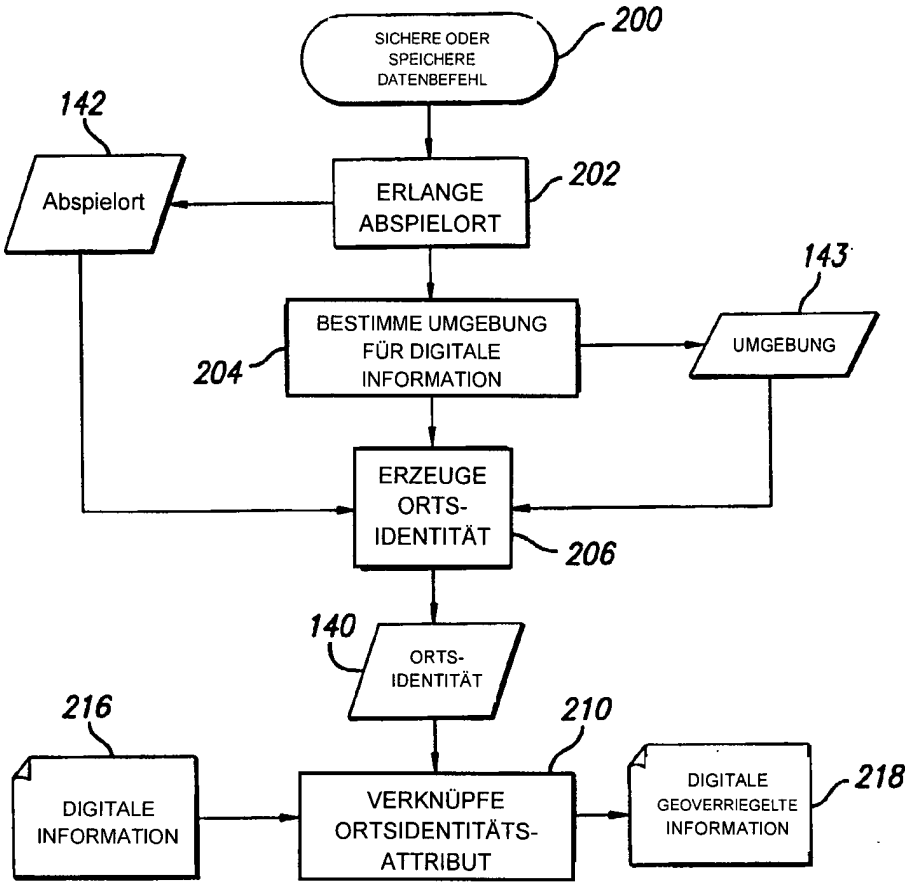

SICHERE ODER SPEICHERE DATENBEFEHL
200
142
Abspielort
ERLANGE ABSPIELORT
202
143
BESTIMME UMGEBUNG FÜR DIGITALE INFORMATION
204
UMGEBUNG
ERZEUGE ORTS-IDENTITÄT
206
140
ORTS-IDENTITÄT
216
DIGITALE INFORMATION
210
VERKNÜPFE ORTSIDENTITÄTS-ATTRIBUT
DIGITALE GEOVERRIEGELTE INFORMATION
218

FIG. 4

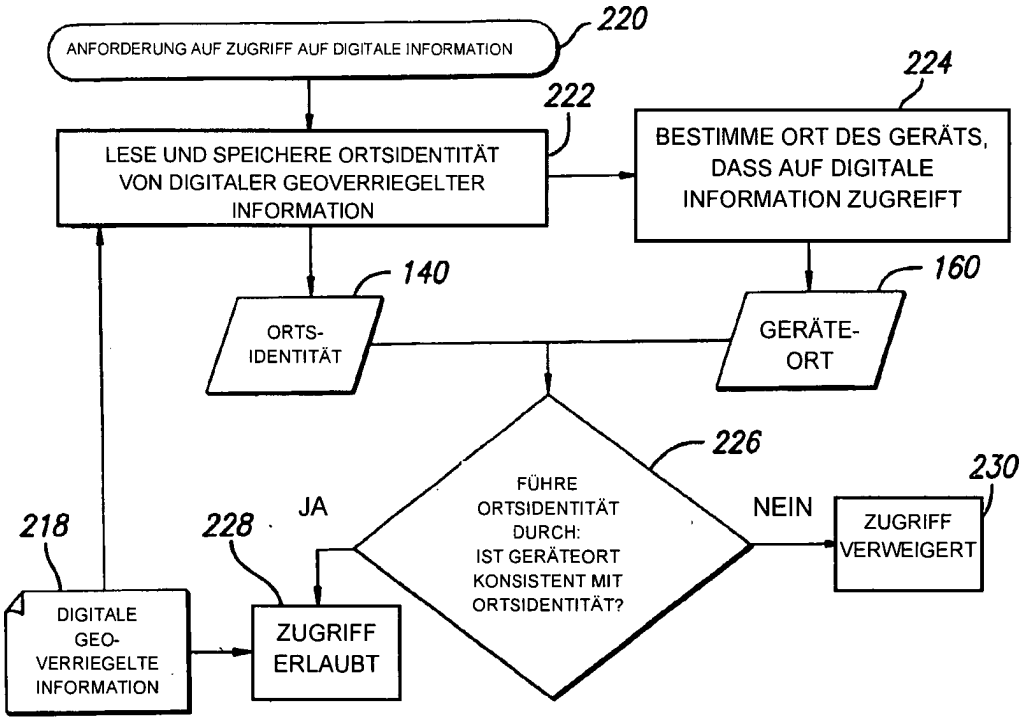

ANFORDERUNG AUF ZUGRIFF AUF DIGITALE INFORMATION
220
LESE UND SPEICHERE ORTSIDENTITÄT VON DIGITALER GEOVERRIEGELTER INFORMATION
222
BESTIMME ORT DES GERÄTS, DASS AUF DIGITALE INFORMATION ZUGREIFT
224
ORTS-IDENTITÄT
140
GERÄTE-ORT
160
FÜHRE ORTSIDENTITÄT DURCH: IST GERÄTEORT KONSISTENT MIT ORTSIDENTITÄT?
226
JA
NEIN
ZUGRIFF VERWEIGERT
230
218
DIGITALE GEO-VERRIEGELTE INFORMATION
228
ZUGRIFF ERLAUBT

FIG. 5

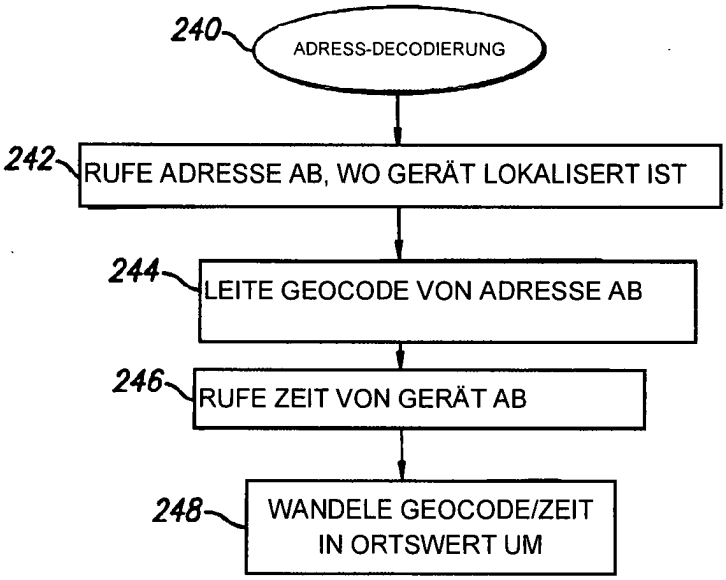

240
ADRESS-DECODIERUNG
242
RUFE ADRESSE AB, WO GERÄT LOKALISERT IST
244
LEITE GEOCODE VON ADRESSE AB
246
RUFE ZEIT VON GERÄT AB
248
WANDELE GEOCODE/ZEIT IN ORTSWERT UM

FIG. 6A

FIG. 6B

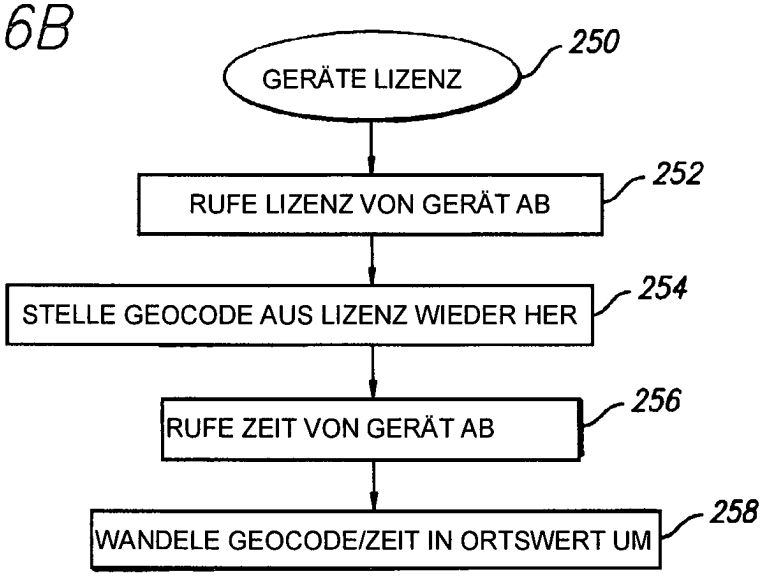


FIG. 6C

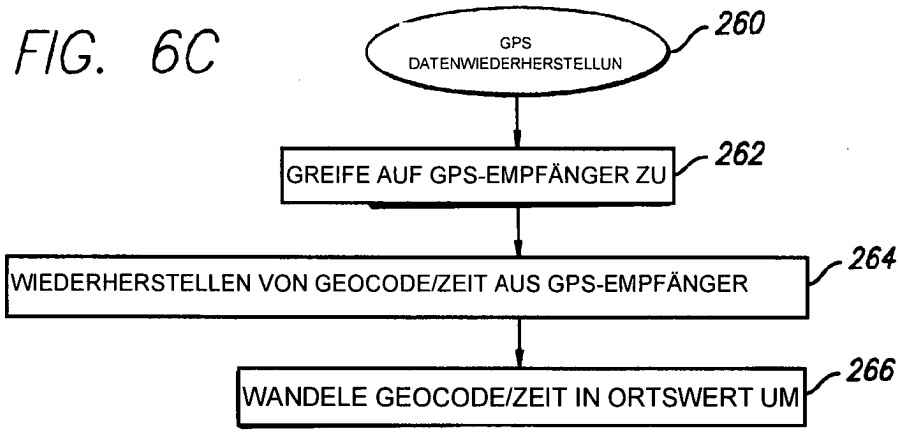


FIG. 6D

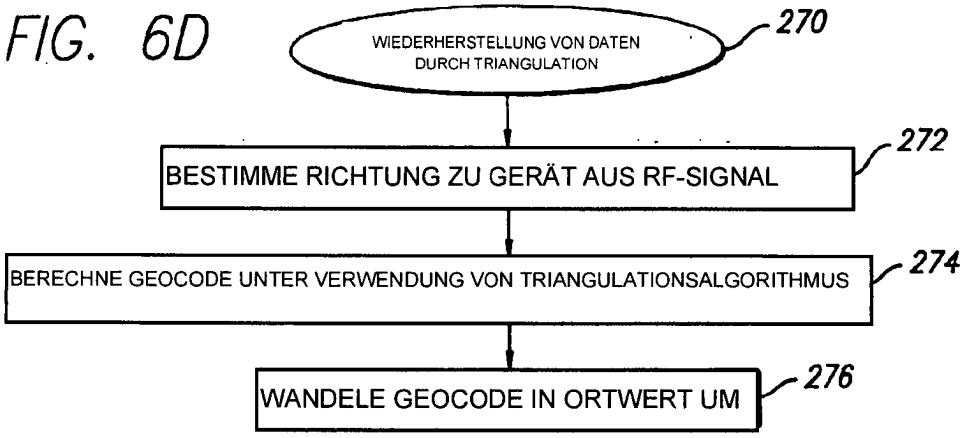


FIG. 7

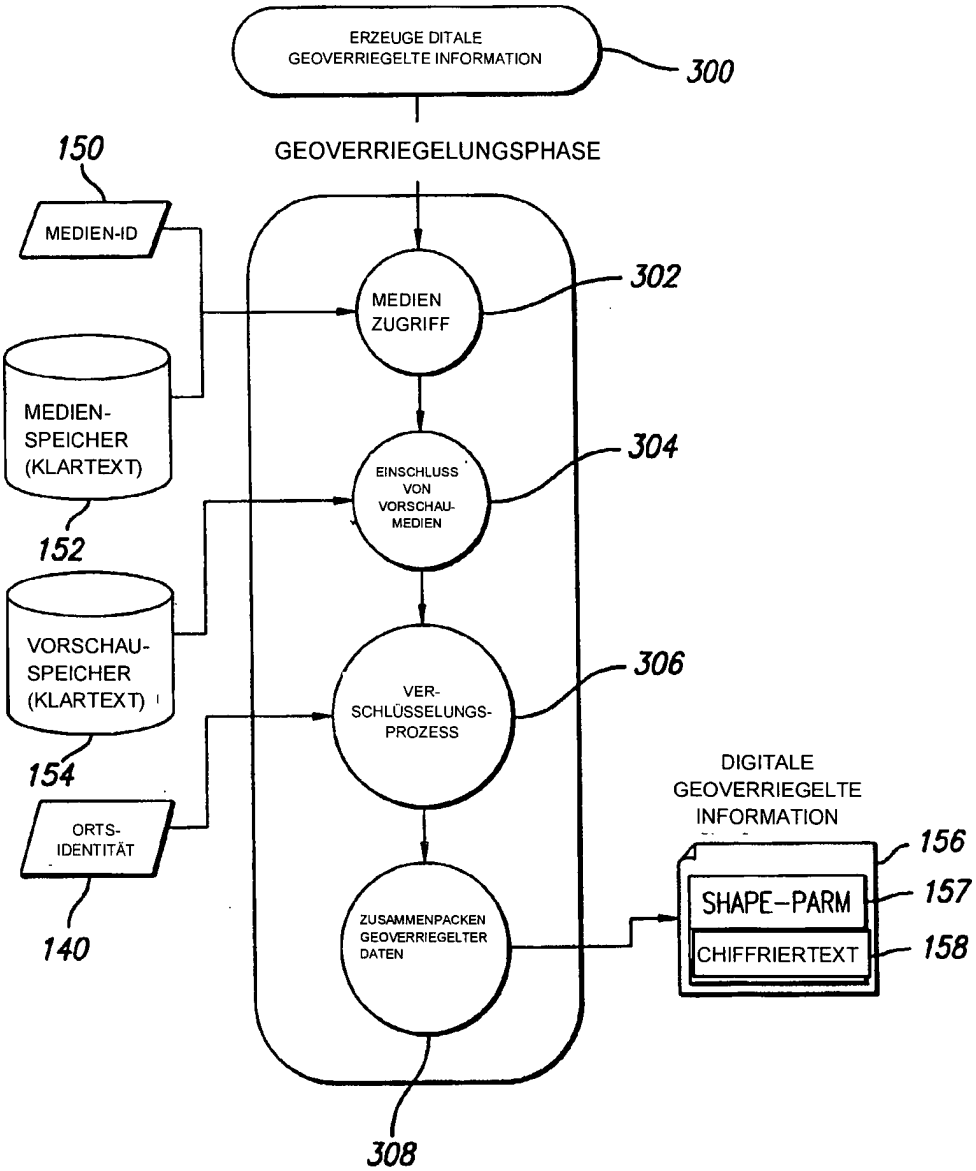
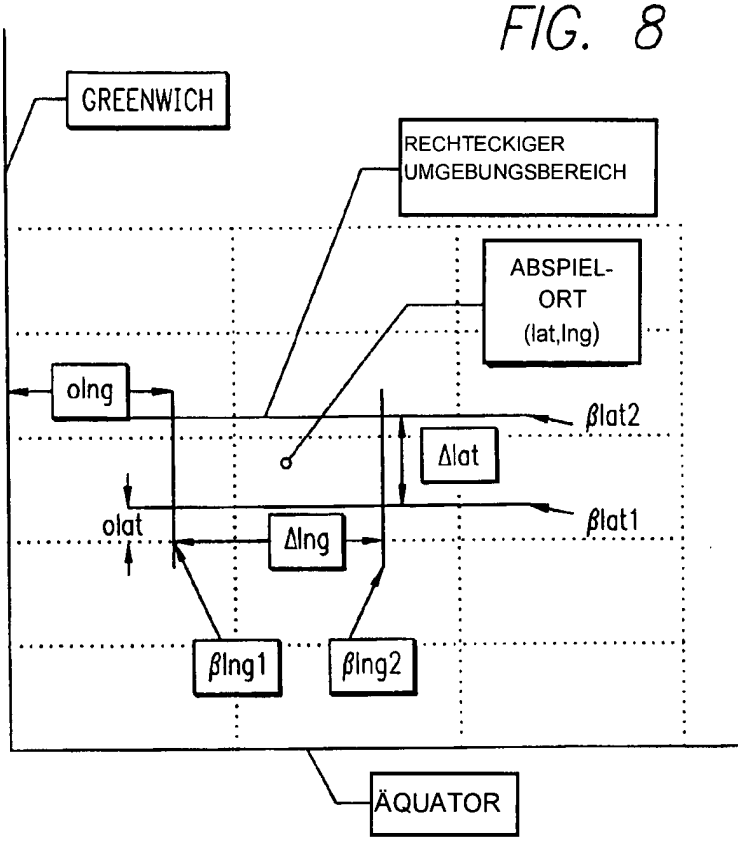

ERZEUGE DITALE GEOVERRIEGELTE INFORMATION
300
GEOVERRIEGELUNGSPHASE
150
MEDIEN-ID
MEDIEN ZUGRIFF
302
MEDIEN-SPEICHER (KLARTEXT)
152
EINSCHLUSS VON VORSCHAU-MEDIEN
304
VORSCHAU-SPEICHER (KLARTEXT)
154
VER-SCHLÜSSELUNGS-PROZESS
306
ORTS-IDENTITÄT
140
ZUSAMMENPACKEN GEOVERRIEGELTER DATEN
DIGITALE GEOVERRIEGELTE INFORMATION
156
SHAPE-PARM
157
CHIFFRIERTEXT
158
308

FIG. 8


GREENWICH
RECHTECKIGER UMGEBUNGSBEREICH
ABSPIEL-ORT (lat,lng)
olng
βlat2
Δlat
βlat1
olat
Δlng
βlng1
βlng2
ÄQUATOR

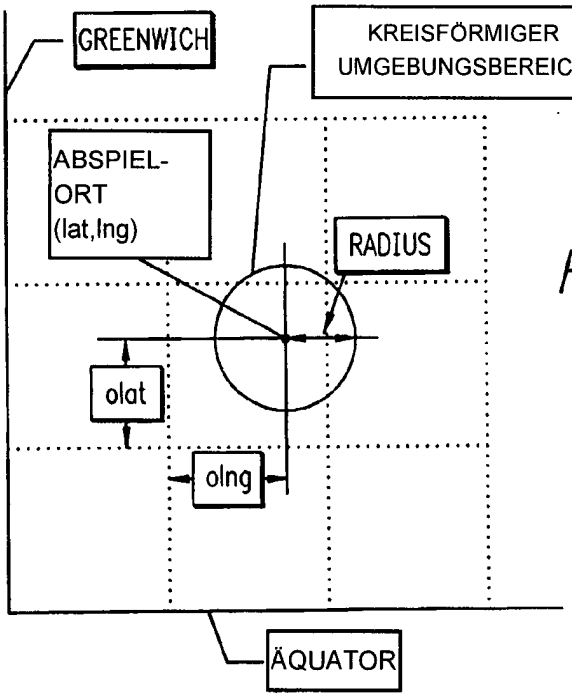

GREENWICH
KREISFÖRMIGER UMGEBUNGSBEREICH
ABSPIEL-ORT (lat,lng)
RADIUS
olat
olng
ÄQUATOR

FIG. 9

FIG. 10

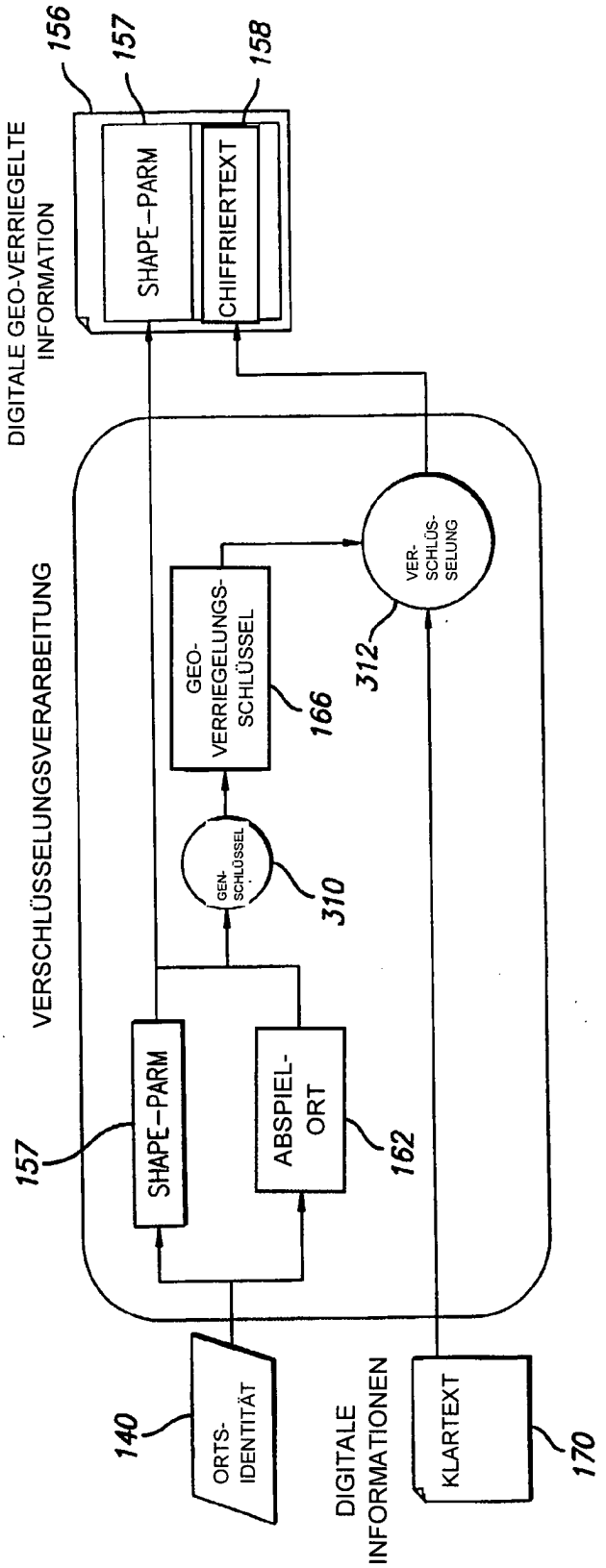

DIGITALE GEO-VERRIEGELTE INFORMATION
156
157
158
SHAPE-PARM
CHIFFRIERTEXT
VERSCHLÜSSELUNGSVERARBEITUNG
VER-SCHLÜS-SELUNG
312
GEO-VERRIEGELUNGS-SCHLÜSSEL
166
GEN-SCHLÜSSEL
310
157
SHAPE-PARM
ABSPIEL-ORT
162
140
ORTS-IDENTITÄT
DIGITALE INFORMATIONEN
KLARTEXT
170

FIG. 11

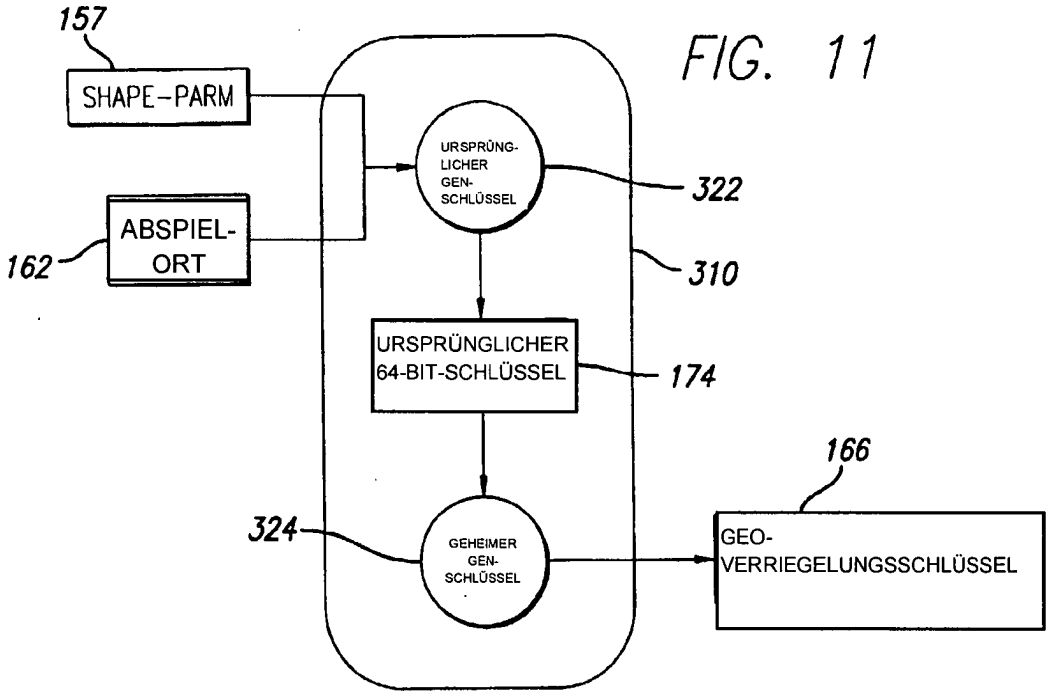

157
SHAPE-PARM
ABSPIEL-ORT
162
URSPRÜNG-LICHER GEN-SCHLÜSSEL
322
310
URSPRÜNGLICHER 64-BIT-SCHLÜSSEL
174
166
324
GEHEIMER GEN-SCHLÜSSEL
GEO-VERRIEGELUNGSSCHLÜSSEL

FIG. 12

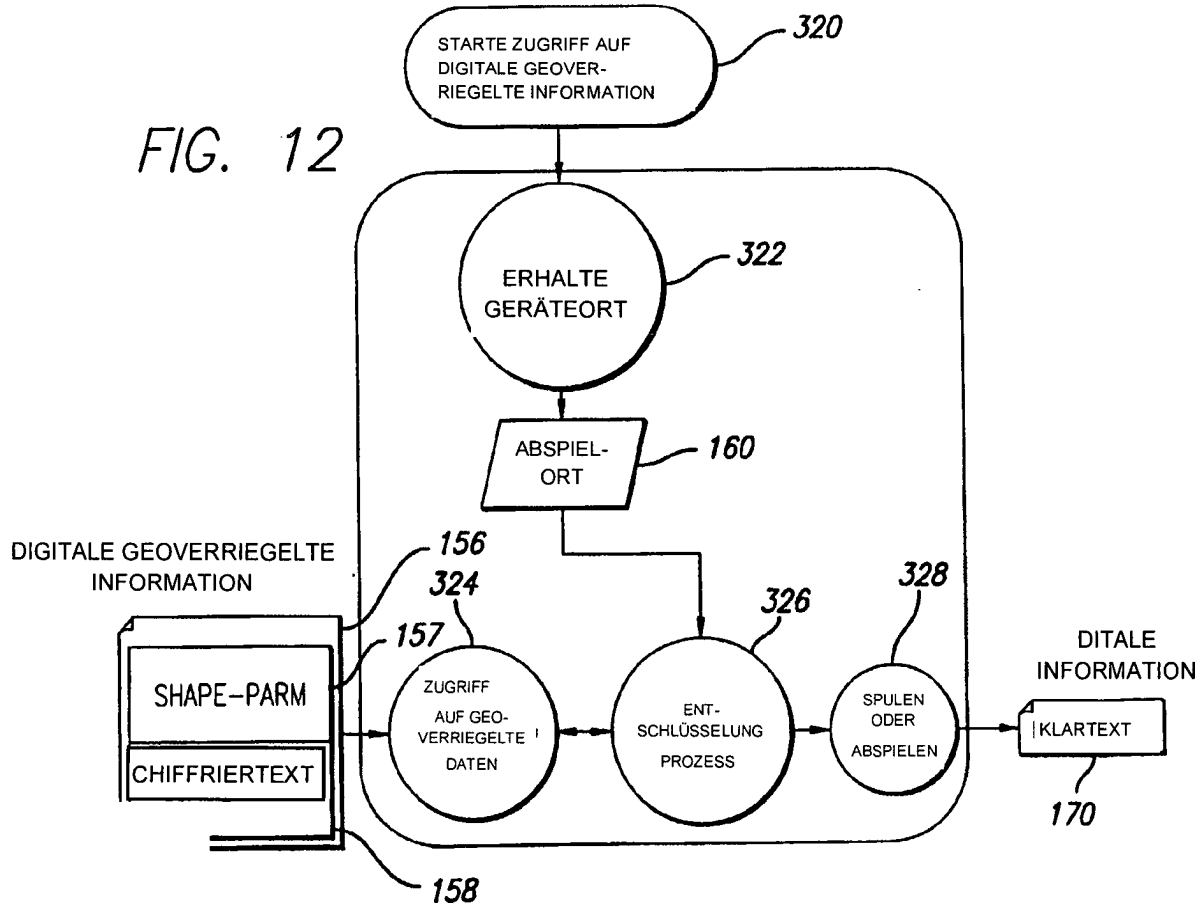
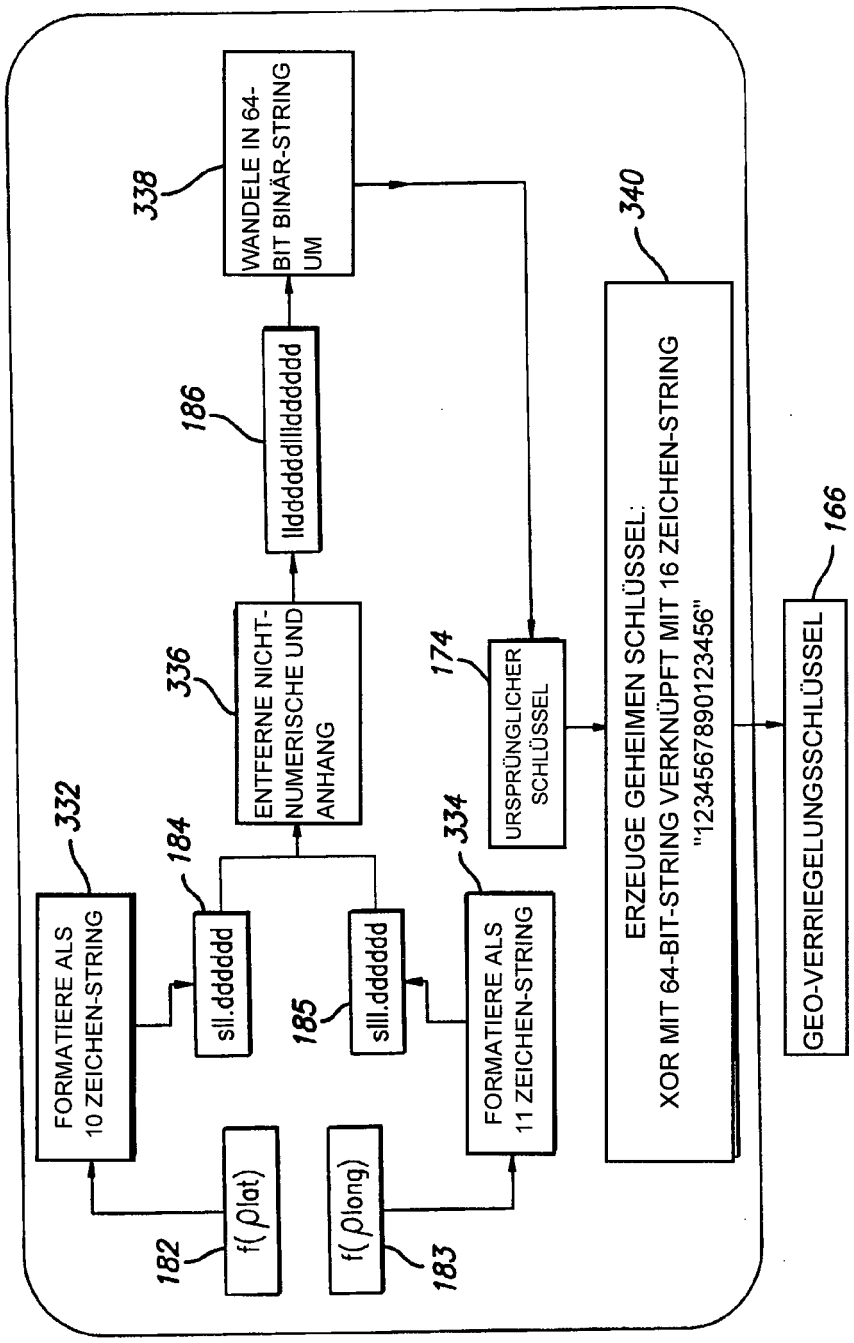

STARTE ZUGRIFF AUF DIGITALE GEOVER-RIEGELTE INFORMATION
320
ERHALTE GERÄTEORT
322
ABSPIEL-ORT
160
DIGITALE GEOVERRIEGELTE INFORMATION
156
324
157
326
328
SHAPE-PARM
CHIFFRIERTEXT
ZUGRIFF AUF GEO-VERRIEGELTE DATEN
ENT-SCHLÜSSELUNG PROZESS
SPULEN ODER ABSPIELEN
DITALE INFORMATION
KLARTEXT
170
158

FIG. 13


182
f(ρlat)
183
f(ρlong)
FORMATIERE ALS 10 ZEICHEN-STRING
332
FORMATIERE ALS 11 ZEICHEN-STRING
334
sll.ddddd
184
slll.ddddd
185
ENTFERNE NICHT-NUMERISCHE UND ANHANG
336
lldddddlllddddd
186
WANDELE IN 64-BIT BINÄR-STRING UM
338
URSPRÜNGLICHER SCHLÜSSEL
174
ERZEUGE GEHEIMEN SCHLÜSSEL:
XOR MIT 64-BIT-STRING VERKNÜPFT MIT 16 ZEICHEN-STRING
"1234567890123456"
340
GEO-VERRIEGELUNGSSCHLÜSSEL
166

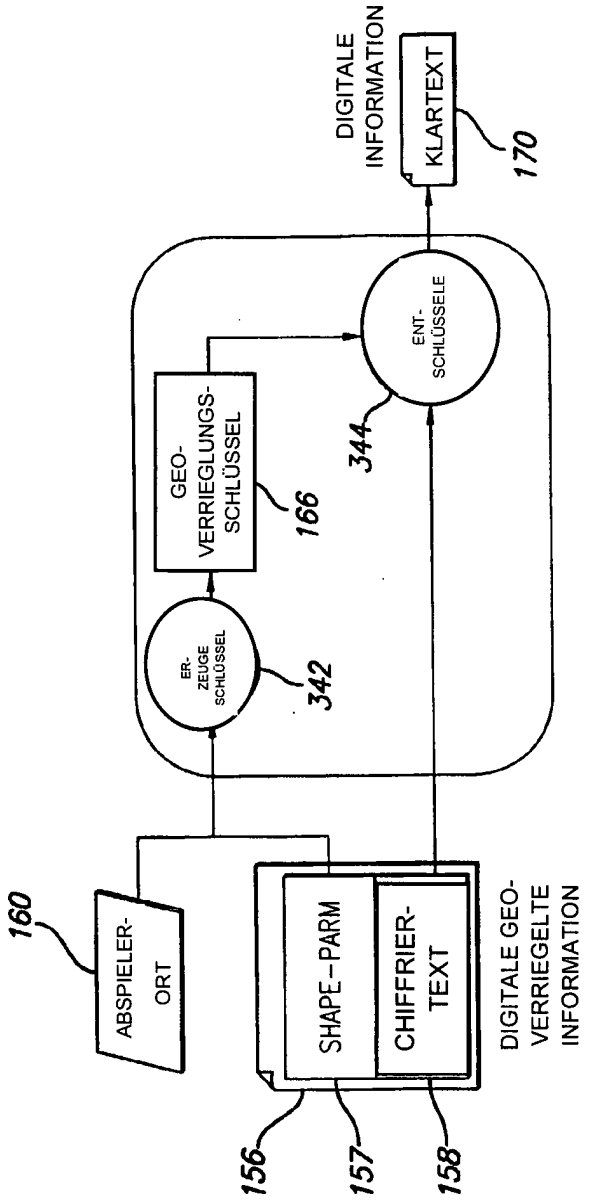

DIGITALE INFORMATION
KLARTEXT
170
ENT-SCHLÜSSELE
344
GEO-VERRIEGLUNGS-SCHLÜSSEL
166
ER-ZEUGE SCHLÜSSEL
342
160
ABSPIELER-ORT
SHAPE-PARM
CHIFFRIER-TEXT
DIGITALE GEO-VERRIEGELTE INFORMATION
156
157
158

FIG. 14

FIG. 15

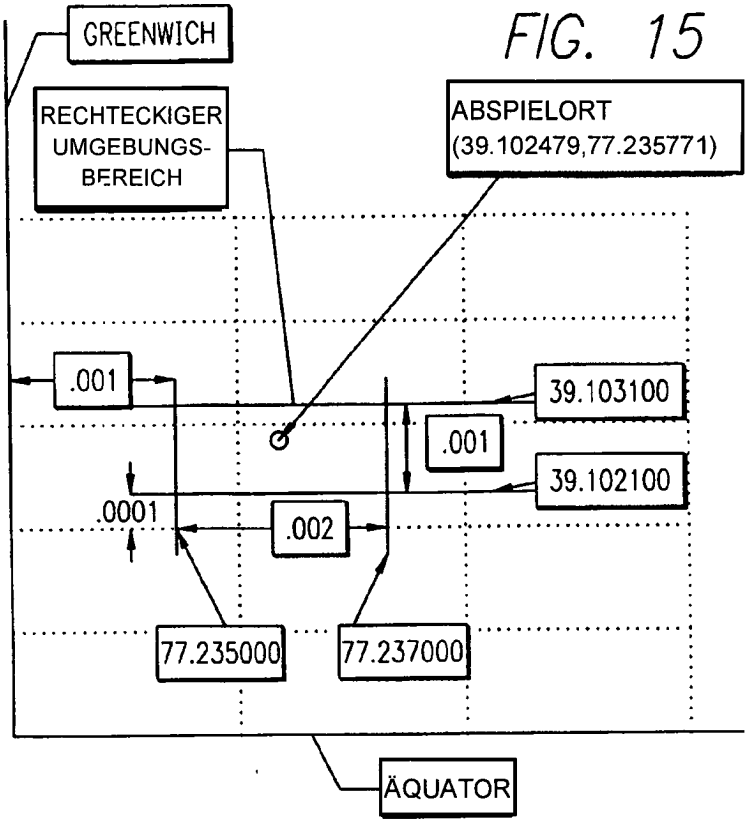

GREENWICH
RECHTECKIGER UMGEBUNGS-BEREICH
ABSPIELORT (39.102479,77.235771)
.001
39.103100
.001
39.102100
.0001
.002
77.235000
77.237000
ÄQUATOR

FIG. 16

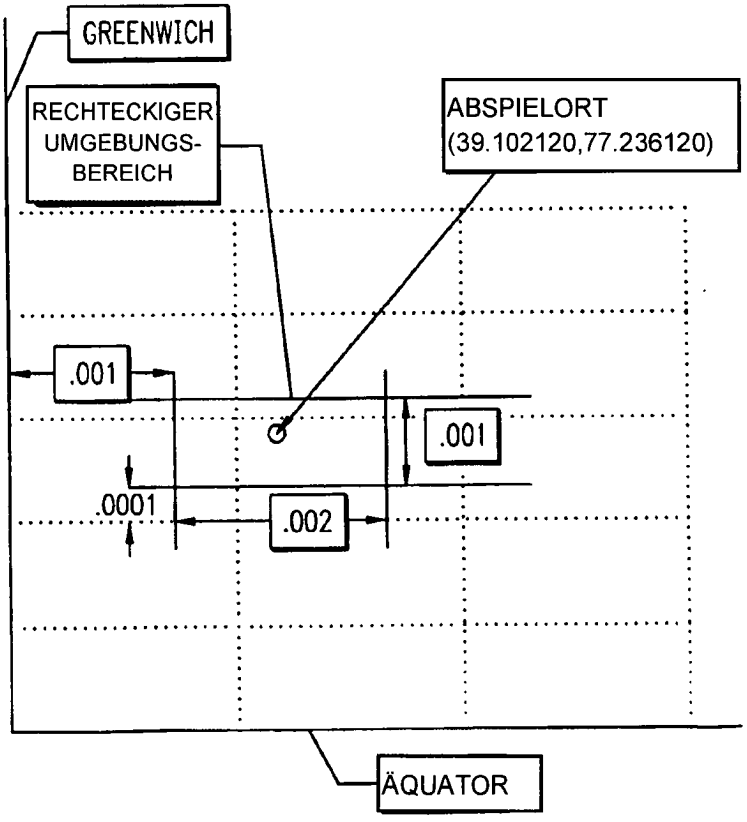
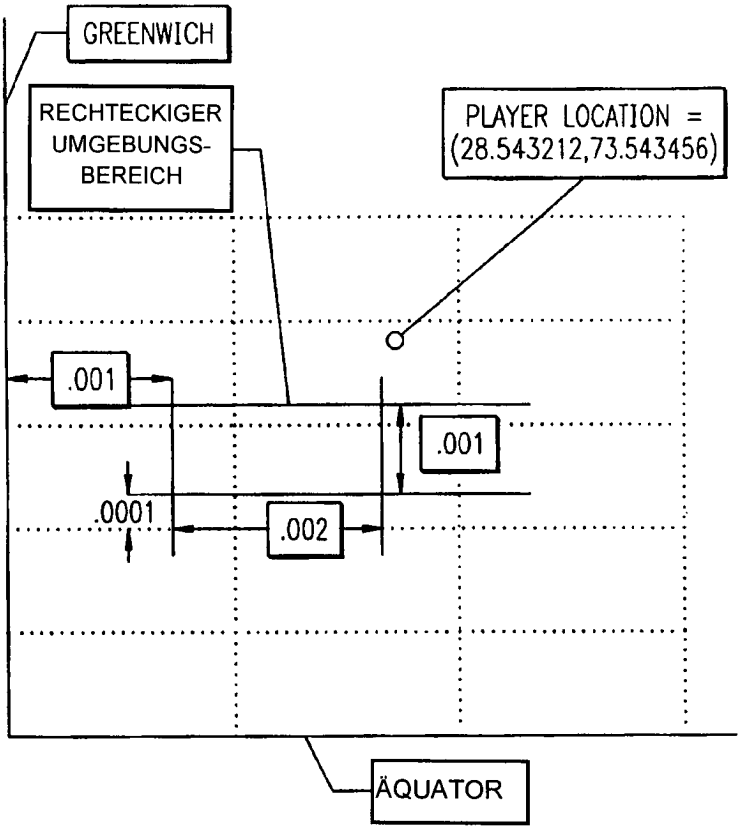

GREENWICH
RECHTECKIGER UMGEBUNGS-BEREICH
ABSPIELORT (39.102120,77.236120)
.001
.001
.0001
.002
ÄQUATOR

FIG. 17


GREENWICH
RECHTECKIGER UMGEBUNGS-BEREICH
PLAYER LOCATION = (28.543212,73.543456)
.001
.001
.0001
.002
ÄQUATOR

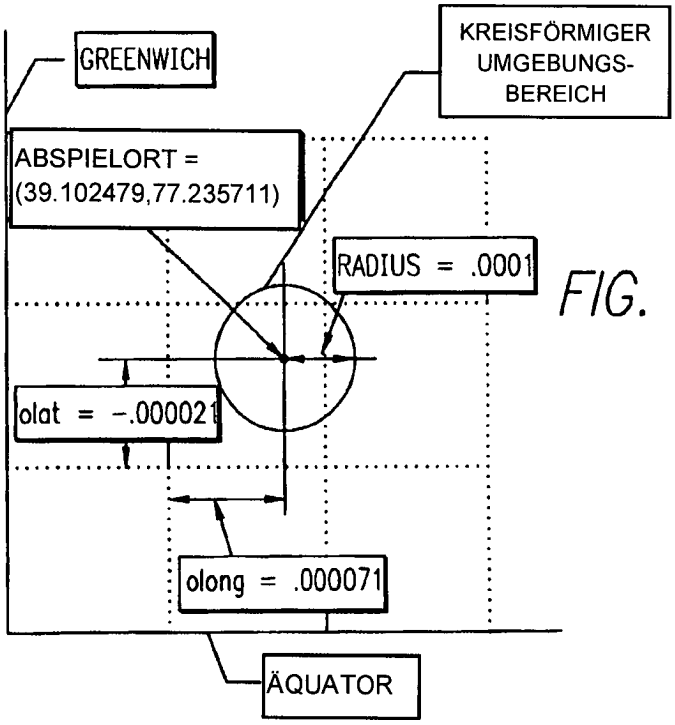

GREENWICH
KREISFÖRMIGER UMGEBUNGS-BEREICH
ABSPIELORT = (39.102479,77.235711)
RADIUS = .0001
olat = -.000021
olong = .000071
ÄQUATOR

FIG. 18

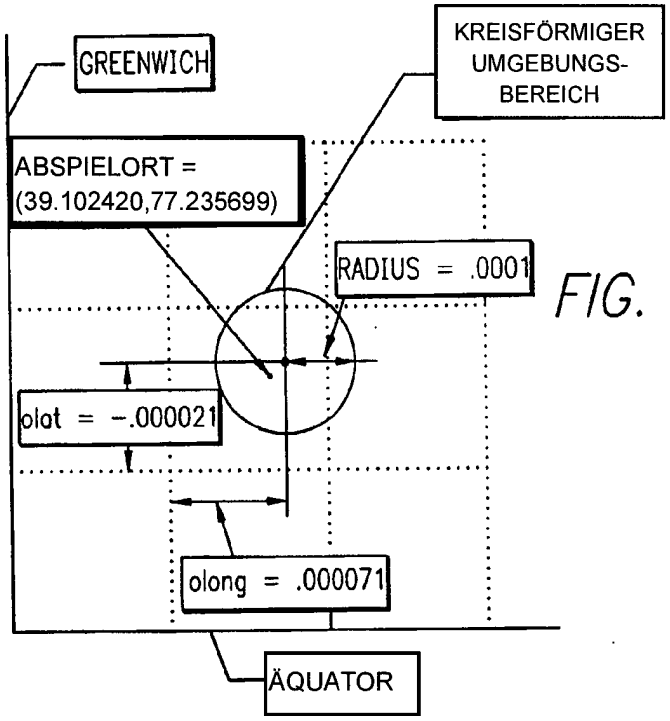

GREENWICH
KREISFÖRMIGER UMGEBUNGS-BEREICH
ABSPIELORT = (39.102420,77.235699)
RADIUS = .0001
olat = -.000021
olong = .000071
ÄQUATOR

FIG. 19