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

(10) **DE 699 34 530 T2** 2007.07.26

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 932 298 B1**
(21) Deutsches Aktenzeichen: **699 34 530.8**
(96) Europäisches Aktenzeichen: **99 300 538.8**
(96) Europäischer Anmeldetag: **26.01.1999**
(97) Erstveröffentlichung durch das EPA: **28.07.1999**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **27.12.2006**
(47) Veröffentlichungstag im Patentblatt: **26.07.2007**

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

(30) Unionspriorität:

1393598	**27.01.1998**	**JP**
1395498	**27.01.1998**	**JP**
1395598	**27.01.1998**	**JP**

(74) Vertreter:
TBK-Patent, 80336 München

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Canon K.K., Tokio/Tokyo, JP

(72) Erfinder:
Iwamura, Keiichi, Ohta-ku, Tokyo, JP

(54) Bezeichnung: **Elektronisches Wasserzeichenverfahren und elektronisches Informationsverteilungssystem**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf ein elektronisches Wasserzeichenverfahren, ein elektronisches Informationsverteilungssystem und ein Speichermedium, auf dem die Schritte zum Ausführen des elektronischen Wasserzeichenverfahrens gespeichert werden, so daß diese von einem Computer gelesen werden können. Insbesondere bezieht sich die vorliegende Erfindung auf ein elektronisches Wasserzeichenverfahren zum Copyrightschutz für Digitalinformation, wie bewegte Bilddaten, statische Bilddaten, Audiodaten, Computerdaten und Computerprogramme, ein elektronisches Informationsverteilungssystem, wie ein Multimedianetzwerksystem zum Verteilen von Digitalinformation unter Verwendung des elektronischen Wasserzeichenverfahrens und auf ein Speichermedium, auf dem die Schritte zum Ausführen des elektronischen Wasserzeichenverfahrens so gespeichert werden, daß sie ein Computer lesen kann.

[0002] Als Folge neuerlicher Entwicklungen bezüglich Computernetzwerken und der Verfügbarkeit von preisgünstigen Hochleistungscomputern sind elektronische Transaktionen beim Handel mit Produkten über ein Netzwerk populär geworden.

[0003] Produkte für solche Transaktionen können Digitaldaten sein, die beispielsweise Bilder enthalten.

[0004] Da jedoch eine große Anzahl von vollständigen Kopien an Digitaldaten leicht aufbereitet werden kann, wäre auch ein Nutzer, der Digitaldaten verkauft, in der Lage, Kopien rechtswidrig aufzubereiten, die dieselbe Qualität wie das Original haben, und könnte diese als Kopierdaten verteilen. Im Ergebnis wird dem Inhaber des Copyrights für die Digitaldaten sein rechtmäßiger Preis nicht bezahlt oder einer Person (wird nachstehend mit "Verkäufer" bezeichnet), der dem Verkaufserlös aus den Digitaldaten die Berechtigung durch Copyrightbesitz zusteht, und es kommt zu einer Copyrightverletzung.

[0005] Wenn einmal ein Copyrightinhaber oder ein Verkäufer (nachstehend wird eine Person, die in legaler Weise Digitaldaten vertreibt, allgemein als "Server" bezeichnet) Digitaldaten an einen Nutzer gesendet hat, ist der Schutz gegenüber rechtswidrigen Kopierens der Daten nicht mehr möglich.

[0006] Eine elektronische Wasserzeichentechnik ist folglich anstelle eines Verfahrens zum direkten Schutz rechtswidrigen Kopierens vorgeschlagen worden. Gemäß der elektronischen Wasserzeichentechnik wird ein spezieller Prozeß für die Digitaldaten und Copyrightinformation bezüglich der Digitaldaten ausgeführt, oder für Nutzerinformation, die in die Digitaldaten eingebettet ist. Wenn somit eine rechtswidrige Kopie der Digitaldaten entdeckt wird, kann die Person, die die kopierten Daten verteilt hat, identifiziert werden.

[0007] In einem herkömmlichen elektronischen Wasserzeichensystem wird ein Server als voll vertrauenswürdig angesehen. Wenn ein Server in einem herkömmlichen System nicht vertrauenswürdig ist und einige Arten von rechtswidriger Verteilungsaktivitäten durchführt, kann ein Nutzer, der kein Vergehen begangen hat, fälschlicherweise dem rechtswidrigen Datenkopieren angeklagt werden.

[0008] Dies tritt auf, weil in einem herkömmlichen elektronischen Wasserzeichensystem, wie es in Fig. 1 gezeigt ist, wenn ein Nutzer Information d1 zum Identifizieren eines Nutzer in Digitaldaten g einbettet (in der folgenden Erläuterung werden Bilddaten als Digitaldaten verwendet), die an den Nutzer verteilt werden, und danach eine Weiterverteilung der Daten ohne Erlaubnis des Nutzers erfolgt, die die Identifikationsdaten des Nutzers enthalten, dann gibt es keinen Weg für den Nutzer, sich gegen die Beschuldigung vom Server zu wehren, obwohl in dieser Instanz es der Server ist, der die rechtswidrige Tat ausgeführt hat.

[0009] Als Gegenmaßnahme ist ein System (Fig. 2) unter Verwendung eines öffentlichen Verschlüsselungsverfahrens vorgeschlagen worden.

[0010] Gemäß dem öffentlichen Verschlüsselungsverfahren unterscheiden sich Verschlüsselung und Entschlüsselung, wobei zur Verschlüsselung ein öffentlicher Schlüssel verwendet wird, während die Entschlüsselung einen Geheimschlüssel erfordert. RSA-Verschlüsselung und E1Gamal-Verschlüsselung sind typische, allgemein bekannte Beispiele für ein Verschlüsselungssystem.

[0011] Nachstehend erläutert sind ein (a) Merkmale eines öffentlichen Verschlüsselungssystems und (b) Protokolle für Geheimübertragungen und berechtigte Übertragungen.

(a) Merkmale öffentlicher Verschlüsselung

(1) Da sich Verschlüsselungscode und Entschlüsselungscode voneinander unterscheiden und weil der Verschlüsselungscode veröffentlicht werden kann, ist ein geheimer Auslieferungsprozeß für den Verschlüsselungscode nicht erforderlich, und die Verteilung ist einfach.
(2) Da die Verschlüsselungscodes von Nutzern veröffentlicht werden, müssen die Nutzer nur ihre Entschlüsselungscodes für die geheime Speicherung angeben.
(3) Eine Berechtigungsfunktion kann bereitgestellt werden, mit der ein Lieferungsempfänger nachweisen kann, daß der Absender keinen Betrug verübt und daß die empfangene Mitteilung unver-

ändert ist.

(b) Protokolle für öffentliche Verschlüsselung

[0012] Wenn beispielsweise E(kp, M) eine Verschlüsselungsoperation für eine Mitteilung M bedeutet, die einen öffentlichen Schlüssel kp verwendet, und D(ks, M) eine Verschlüsselungsoperation für die Mitteilung M bedeutet, die einen Geheimschlüssel ks verwendet, genügt der öffentliche Verschlüsselungsalgorithmus den folgenden Bedingungen.

(1) Die Berechnungen für den Schlüssel E(kp, M) können leicht unter Verwendung der Verschlüsselung kp erfolgen, die bereitsteht, und die Berechnungen für die Entschlüsselung D(ks, M) kann ebenfalls leicht unter Verwendung des bereitstehenden Entschlüsselungscodes ks erfolgen.

(2) Sofern ein Nutzer den Entschlüsselungscode ks nicht kennt, selbst wenn der Nutzer den Verschlüsselungscode kp und die Rechenprozeduren zum Entschlüsseln von E(kp, M), und auch die verschlüsselte Mitteilung C = E(kp, M) kennt, kann der Nutzer nicht ermitteln, was die Mitteilung M beinhaltet, weil eine große Anzahl von Berechnungen erforderlich ist.

[0013] Wenn zusätzlich zu den Bedingungen (1) und (2) die folgende Bedingung (3) hinzukommt, kann die Geheimübertragungsfunktion realisiert werden.

(3) Die Verschlüsselung E(kp, M) kann festgelegt werden für alle Mitteilungen (Volltext) M und

D(ks, E(kp, M)) = M

wird eingerichtet. Das heißt, irgendeiner kann die Berechnungen für die Verschlüsselung E(kp, M) unter Verwendung der öffentlichen Verschlüsselung kp ausführen, aber nur ein Nutzer, der den Geheimschlüssel ks kennt, kann die Berechnungen für den Entschlüsselungsprozeß D(ks, E(kp, M)) zum Erzielen der Inhalte der Mitteilung M ausführen.

[0014] Wenn zusätzlich zu den obigen Bedingungen (1) und (2) die folgende Bedingung (4) hinzukommt, kann die berechtigte Übertragung realisiert werden.

(4) Der Verschlüsselungsprozeß D(ks, M) kann festgelegt werden für alle (Volltext-) Mitteilungen M, und

E(kp, D(ks, M)) = M

wird eingerichtet. Das heißt, nur ein Nutzer, der den Geheimschlüssel ks hat, kann die Berechnungen für den Entschlüsselungsprozeß D(ks, M) ausführen. Selbst wenn ein anderer Nutzer versucht, D(ks', M) zu berechnen, unter Verwendung eines Bogus-Geheimschlüsselscodes ks' [Bogus: kriminelle Gruppe im Internet] und die Berechnungen wie ein Nutzer ausführt, der den Geheimschlüsselscode ks besitzt, wäre das Ergebnis

E(kp, D(ks', M) ≠ M

und ein Lieferungsempfänger würde verstehen, daß die empfangene Information rechtswidrig aufbereitet ist.

[0015] sWenn der Wert D(ks, M) geändert wird, kommt das Ergebnis

E(kp, D(ks, M)') ≠ M

zustande, und ein Lieferungsempfänger würde verstehen, daß die Empfangsinformation rechtswidrig aufbereitet wurde.

[0016] Im oben beschriebenen Verschlüsselungsverfahren wird eine Operation E(), für die der öffentliche Verschlüsselungscode (nachstehend als öffentlicher Schlüssel bezeichnet) kp verwendet wird, "Verschlüsselung" genannt, und die Operation D() für die der Geheimverschlüsselungscode (wird nachstehend ebenfalls als Geheimschlüssel bezeichnet) ks verwendet und "Entschlüsselung" genannt.

[0017] Für eine Geheimübertragung führt ein Sender eine Verschlüsselung aus, und ein Lieferungsempfänger führt die Entschlüsselung aus, während für eine berechtigte Übertragung ein Sender die Entschlüsselung und ein Lieferungsempfänger die Verschlüsselung ausführt.

[0018] Die nachstehend gezeigten Protokolle dienen der Geheimübertragung, einer berechtigten Übertragung und einer Geheimübertragung für einen Lieferungsempfänger B, der eine Signatur trägt, die durch einen Sender A aufgetragen wird, unter Verwendung des öffentlichen Verschlüsselungssystems.

[0019] Der Geheimschlüssel vom Sender A ist ksA, und der öffentliche Schlüssel ist kpA, und der Geheimschlüssel vom Lieferungsempfänger B ist ksB, und der öffentliche Schlüssel ist kpB.

[Geheimübertragung]

[0020] Die folgenden Prozeduren werden ausgeführt für die Geheimübertragung einer (Volltext-) Mitteilung M vom Sender A zum Lieferungsempfänger B.

[0021] Schritt 1: Der Sender A sendet dem Lieferungsempfänger B eine Mitteilung C, die durch Anwenden des öffentlichen Schlüssels kpB vom Lieferungsempfänger B zum Verschlüsseln der Mitteilung M folgendes enthält:

C = E(kpB, M).

[0022] Schritt 2: Zum Erzielen der Originalvolltextmitteilung M verwendet der Lieferungsempfänger den Geheimschlüssel ksB an, um die Empfangsmitteilung C folgendermaßen zu entschlüsseln:

M = D(ksB, C).

[0023] Da dieser öffentliche Schlüssel kpB vom Lieferungsempfänger B offen für viele verfügbar ist, können unspezifizierte Personen, andere Nutzer als der Sender A, ebenfalls Geheimmitteilungen an den Lieferungsempfänger B senden.

[Berechtigte Übertragung]

[0024] Für die berechtigte Übertragung einer (Volltext-) Mitteilung M vom Sender A zum Lieferungsempfänger B werden die folgenden Prozeduren ausgeführt.

[0025] Schritt 1: Der Sender A sendet eine Mitteilung S an den Lieferungsempfänger B, die er erstellt hat durch Anwenden des eigenen Geheimschlüssels, und zwar auf folgende Weise:

S = D(ksA, M).

[0026] Diese Mitteilung S wird signierte Mitteilung genannt und die angewendete Operation zum Aufbereiten der signierten Mitteilung S wird "Signieren" genannt.

[0027] Schritt 2: Zum Erzielen der Originalvolltextmitteilung M wendet der Lieferungsempfänger B den öffentlichen Schlüssel kpA des Senders A an, um die signierte Mitteilung S folgendermaßen umzusetzen:

M = E(kpA, S).

[0028] Wenn der Lieferungsempfänger B sicherstellt, daß die Mitteilung M Sinn macht, weist er nach, daß die Mitteilung M vom Sender A gesendet wurde. Und von daher ist der öffentliche Schlüssel kpA vom Sender A für viele unspezifizierte Personen verfügbar; andere Nutzer als der Lieferungsempfänger B können ebenfalls die signierte Mitteilung S berechtigen, die der Sender A gesendet hat. Dieses Autorisieren wird "Digitalsignieren" genannt.

[Geheimübertragung mit Signatur]

[0029] Die folgenden Prozeduren werden ausgeführt für die Geheimsendung an den Lieferungsempfänger B vom Sender A einer (Volltext-) Mitteilung M, für die eine Signatur bereitgestellt ist.

[0030] Schritt 1: Der Sender A bereitet die signierte Mitteilung S auf durch Anwenden des Geheimschlüssels ksA zum Signieren der Mitteilung M wie folgt:

S = D(ksA, M).

[0031] Danach wird zum Aufbereiten einer verschlüsselten Meldung C, die danach an den Lieferungsempfänger B gesandt wird, der Sender A den öffentlichen Schlüssel kpB vom Lieferungsempfänger B anwenden zum Verschlüsseln der signierten Mitteilung S wie folgt:

C = E(kpB, S).

[0032] Schritt 2: Zum Erzielen der signierten Mitteilung S wendet der Lieferungsempfänger B seinen Geheimschlüssel ksB an, um die verschlüsselte Mitteilung C folgendermaßen zu entschlüsseln:

S = D(ksB, C).

[0033] Zum Erzielen der Originalvolltextmitteilung M wendet der Lieferungsempfänger B den öffentlichen Schlüssel kpA vom Sender A an, um die signierte Mitteilung S folgendermaßen umzusetzen:

M = E(kpA, S).

[0034] Wenn der Lieferungsempfänger sichergestellt hat, daß die Mitteilung M Sinn macht, wird nachgewiesen, daß die Mitteilung M vom Sender A kommt.

[0035] Für die Geheimübertragung, für die eine Signatur bereitsteht, kann die Reihenfolge, in der die Berechnungsfunktionen ausgeführt werden, in individuellen Schritten umgekehrt werden. Mit anderen Worten, bei den obigen Prozeduren wird
Schritt 1:

C = E(kpB, D(ksA, M))

Schritt 2:

M = E(kpA, D(ksB, C))

in dieser Reihenfolge ausgeführt. Für eine derartige Geheimübertragung kann die folgende Reihenfolge angewandt werden:
Schritt 1:

C = D(ksA, E(kpB, M))

Schritt 2:

M = D(ksB, E(kpA, C)).

[0036] Nachstehend erläutert sind die Operationsprozeduren für ein herkömmliches elektronisches Wasserzeichensystem unter Verwendung des oben beschriebenen öffentlichen Verschlüsselungsverfah-

rens.

1) Zuerst wird ein Kontrakt d2 bezüglich des Austauschs der Bilddaten g vom Server und vom Nutzer vorbereitet.

2) Als nächstes erzeugt der Nutzer eine Zufallszahl ID zur Eigenidentifizierung und wendet diese ID an zum Erzeugen einer Unidirektionalfunktion f.

[0037] Die Unidirektionalfunktion ist eine, die verwendet wird, wenn für eine Funktion y = f(x) das Berechnen von y aus x leicht ist, aber das Berechnen von x aus y schwierig ist. Beispielsweise eine einzige Faktorenzerlegung oder ein diskreter Logarithmus für eine Ganzzahl mit einer Anzahl von Ziffern wird häufig verwendet als Unidirektionalfunktion.

3) Dann bereitet der Nutzer die Signaturinformation d3 vor unter Verwendung des eigenen Geheimschlüssels ksU und sendet diesen mit dem Kontrakt d2 und der Unidirektionalfunktion f an den Server.

4) Dem folgend weist der Server die Signaturinformation d3 und den Kontrakt d2 unter Verwendung des öffentlichen Schlüssels kpU vom Nutzer nach.

5) Nach abgeschlossenem Nachweis bettet der Server in die Bilddaten g eine aktuelle Datenverteilungsaufzeichnung d4 und die Zufallszahl ID, die der Nutzer vorbereitet hat, und erzeugt Bilddaten, die ein elektronisches Wasserzeichen (g + d4 + ID) enthalten.

6) Letztlich sendet der Server die Bilddaten an den Nutzer, die das elektronische Wasserzeichen (g + d4 + ID) enthalten.

[0038] Wird eine rechtswidrige Kopie der Daten gefunden, dann erfolgt das Auslesen der eingebetteten Information aus den rechtswidrigen Bilddaten, und ein spezieller Nutzer wird unter Verwendung der ID identifiziert, die dort drin enthalten ist. Zu dieser Zeit basiert ein Anspruch vom Server, der die rechtswidrige Kopie nicht ohne Erlaubnis verteilt hat, auf folgender Grundlage.

[0039] Da die verwendetet ID zum Spezifizieren eines Nutzers vom Nutzer erzeugt wird und da die durch Verwenden diese ID die Signatur des Nutzers bereitgestellt ist für die Unidirektionalfunktion f, kann der Server eine derartige ID für einen beliebigen Nutzer nicht erzeugen.

[0040] Da jedoch ein Nutzer, der offiziell einen Kontrakt mit dem Server hat, die eigene ID an den Server senden muß, können nur Nutzer, die keine Kontrakte mit dem Server haben, nicht des Begehens einer Rechtswidrigkeit angeklagt werden, wohingegen ein Nutzer, der offiziell einen Kontrakt hat, angeklagt werden kann.

[0041] Folglich ist ein System (Fig. 3) vorgeschlagen worden, um die Beschuldigung zu neutralisieren, daß ein Vergehen von einem Nutzer begangen wurde, der offiziell einen Kontrakt besitzt.

[0042] Dieses System wird realisiert durch Unterteilen des Servers in einen Originalbildserver und in einen Einbettungsserver. Gemäß diesem System wird das eingebettete elektronische Wasserzeichen während der Verschlüsselung und während der Entschlüsselung nicht zerstört.

[0043] Die Operationsprozeduren für das System in Fig. 3 sind nachstehend beschrieben.

1) Zuerst gibt zum Erzielen gewünschter Bilddaten ein Nutzer eine Anforderung ab, die die eigene Signatur d5 trägt, an einen Originalbildserver.

2) Der Originalbildserver wendet die Nutzersignatur d5 zum Nachweis der Inhalte der Anforderung an und verschlüsselt danach die angeforderten Bilddaten g und sendet die verschlüsselten Daten an einen Einbettungsserver.

[0044] Zu dieser Zeit sendet der Originalbildserver an den Einbettungsserver die Bilddaten g, begleitet von der Signatur für einen Nutzernamen u und für Mitsignierung von Inhalten d6. Der Originalbildserver sendet auch eine Verschlüsselungsfunktion f' an den Nutzer, die sich auf die Verschlüsselung bezieht.

3) Der Einbettungsserver weist die empfangenen verschlüsselten Bilddaten g' und die Signatur (u + d6) nach, verwendet den Nutzernamen u und die Mitsignierinhalte d6 zum Vorbereiten und Einbetten der Nutzerinformation d7 zum speziellen Identifizieren eines Nutzers, und dadurch werden Verschlüsselungsdaten
(g' + d7) mit einem elektronischen Wasserzeichen erstellt. Dann sendet der Einbettungsserver an den Nutzer die verschlüsselten Bilddaten (g' + d7), die das elektronische Wasserzeichen enthalten.

4) Der Nutzer nutzt die Verschlüsselungsfunktion f', die er vom Originalbildserver bekommen hat, um die verschlüsselten Bilddaten zu entschlüsseln, die ein elektronisches Wasserzeichen (g' + d7) enthalten, und um die Bilddaten zu bekommen, die das elektronische Wasserzeichen (g + d7) bereitstellt.

[0045] Wenn später eine Rechtswidrigkopie gefunden wird, verschlüsselt der Originalbildserver die rechtswidrigen Bilddaten und liest die eingebettete Funktion aus und sendet diese an den Einbettungsserver. Der Einbettungsserver identifiziert insbesondere einen Nutzer aus der eingebetteten Information.

[0046] Da in diesem System ein Originalbildserver nicht in die Bilddaten g eingebettet ist, spezifiziert die Nutzerinformation d7 insbesondere einen Nutzer, und von daher kennt der Einbettungsserver die Entschlüsselungsfunktion f nicht (und kann das Originalbild nicht empfangen), der individuelle Server kann

keine rechtswidrige Verteilung offizieller Serverbilddaten im Kontrakt verteilen, in denen die Nutzerinformation d7 eingebettet ist.

[0047] Weder die Kollusion [geheime Absprache] des Originalbildservers mit dem Einbettungsserver noch die Kollusion des Einbettungsservers mit dem Nutzer werden im System gemäß Fig. 3 berücksichtigt. Da der Einbettungsserver die verschlüsselten Bilddaten g' für die Bilddaten g speichert, die die Originalbilddaten sind, und da der Nutzer die Verschlüsselungsfunktion f' hält, wenn der Originalbildserver in Kollusion mit dem Einbettungsserver ist, können die Server wie im System gemäß Fig. 2 eine rechtswidrige Tat ausführen. Und wenn der Einbettungsserver in Kollusion mit dem Nutzer ist, kann das Originalbild (Bilddaten g) rechtswidrig gewonnen werden.

[0048] Der Originalbildserver sendet die Verschlüsselungsfunktion f' an den Nutzer; wenn jedoch der Nutzer keine adäquate Verwaltungssteuerung für die Entschlüsselungsfunktion f' bereitstellt, wird die Unachtsamkeit des Nutzers im Einbettungsserver dazu führen, Kenntnis von der Verschlüsselungsfunktion f' zu erlangen, obwohl der Einbettungsserver nicht in Kollusion mit dem Nutzer ist.

[0049] Im System in Fig. 3 enthält der Originalbildserver weiterhin kein Einbettungsmittel noch kann er das Einbetten korrekt durchführen. Da jedoch die eingebettete Information vom Originalbildserver ausgelesen wird, kann der Originalbildserver in korrekter Weise das Einbetten durch Analysieren der eingebetteten Information ausführen.

[0050] Daß aus diesem Grund der Einbettungsserver die eigene Signatur nicht eingebettet hat, bildet die Entsprechung zwischen der eingebetteten Information und der Nutzerinformation das einzige Einbettungsservergeheimnis. Die Entsprechung zwischen der eingebetteten Funktion und der Nutzerfunktion ist jedoch keine Zufallsentsprechung, die die Verwendung einer Datenbank einschließt. Wenn eine eingebettete Information von der Nutzerinformation zu speziellen Regeln aufbereitet wird, gibt es eine hohe Wahrscheinlichkeit, daß das Analysieren der eingebetteten Information möglich wird. In diesem Falle, wie im System in Fig. 2, ist das Ausführen einer rechtswidrigen Tat möglich.

[0051] In diesem Falle, wie auch im System in Fig. 2, ist das Ausführen einer rechtswidrigen Tat möglich.

[0052] Während ein System mit Nutzer und Server vorgeschlagen wurde, obwohl nicht vollständig, ist die vorhandene Sicherheit mit einem System, bei dem Server in hierarchischer Struktur vorgesehen sind, nicht garantiert.

[0053] Der Grund hierfür ist folgender. Für ein System (hierarchisches Netzwerk 1), das in Fig. 4 gezeigt ist, bei dem eine Vielzahl von Handelsagenturen 1 bis m sich unter einem Server befinden und Nutzer 11 bis 1n und Nutzer m1 bis mn sich unter individuellen Handelagenturen befinden, oder für ein System (hierarchisches Netzwerk 2), das in Fig. 5 gezeigt ist, bei dem einer aus einer Vielzahl von Autoren 1 bis m anfragt, ob eine Handelsagentur, die ihn repräsentiert, Bilddaten verkauft, und dann die Handelsagentur Bilddaten verkauft, die vom relevanten Autor für viele Nutzer 1 bis n berechtigt wurden, wobei die Teilnehmer an einen Server (oder Autor), eine Agentur und einen Nutzer angeschlossen sind, so daß die im System möglicherweise auftretende Kollusion, in dem es drei Teilnehmer gibt, komplexer ist als im System, bei dem es zwei Teilnehmer gibt.

[0054] Das in Fig. 3 gezeigte System könnte als ein solches angesehen werden, das über einen Server, eine Agentur und einen Nutzer verfügt. Das herkömmliche System hat jedoch kein hierarchisches System durchlaufen und Server sind getrennt vorgesehen, um eine rechtswidrige Tat zu verhindern, der von einem einzelnen Server ausgeführt werden könnte. Wie oben beschrieben, kann diese Kollusion, die auftreten könnte, nicht berücksichtigt werden.

[0055] Die Patentbeschreibung US-A-5.613.004 offenbart die Kombination von Verschlüsselung und Steganographie (Wasserzeichenmarkierung) in Verbindung mit drei getrennten Einheiten. Die Information wird unter Verwendung eines speziellen Schlüssels codiert und ist in Abtastwerten enthalten und weder vorangesetzt noch dem Abtaststrom nachgesetzt. Im Hauptausführungsbeispiel des US-Patents mit der Nummer US-A-5.613.004 umfaßt die Zusatzinformation die Verwendung von Spektraltransformationen unter Benutzung zweier separater Schlüssel.

[0056] Die US-Patentbeschreibung US-A-5.687.236 arbeitet im wesentlichen in derselben Weise wie dies in US-Patentbeschreibung mit der Nummer US-A-5.613.004 offenbart ist und hat somit zu tun mit dem Informationseinfügen in einen Strom von digitalisierten Abtastwerten unter Spektraltransformationsverwendung.

[0057] Nach einem Aspekt der vorliegenden Erfindung vorgesehen ist ein elektronisches Wasserzeichenverfahren, wie es im Patentanspruch 1 angegeben ist.

[0058] Nach einem anderen Aspekt der vorliegenden Erfindung vorgesehen ist ein elektronisches Informationsverteilungssystem, wie es im Patentanspruch 12 angegeben ist.

[0059] Diese Mittel oder Einheiten können wenigstens aus drei Arten oder Einheiten bestehen.

[0060] Ausführungsbeispiele der vorliegenden Erfindung sind nachstehend anhand der beiliegenden Zeichnung beschrieben.

[0061] Fig. 1 ist ein Diagramm zur Erläuterung eines herkömmlichen elektronischen Wasserzeichensystems;

[0062] Fig. 2 ist ein Diagramm zur Erläuterung eines herkömmlichen elektronischen Wasserzeichensystems, das durch Verbesserung des Systems gemäß Fig. 1 entstanden ist;

[0063] Fig. 3 ist ein Diagramm zur Erläuterung eines herkömmlichen elektronischen Wasserzeichensystems (2), das durch Verbessern des Systems gemäß Fig. 1 entstanden ist;

[0064] Fig. 4 ist ein Diagramm zur Erläuterung eines hierarchischen Systems (enthält einen Server, Agenturen und Nutzer), das ein herkömmliches elektronisches Wasserzeichenverfahren anwendet;

[0065] Fig. 5 ist ein Diagramm zur Erläuterung eines hierarchischen Systems (enthält Autoren, Agenturen und Nutzer), das ein herkömmliches elektronisches Wasserzeichenverfahren anwendet;

[0066] Fig. 6 ist ein Blockdiagramm, das die Anordnung eines Systems nach einem ersten Ausführungsbeispiel der vorliegenden Erfindung darstellt;

[0067] Fig. 7 ist ein Ablaufdiagramm zur Erläuterung einer Nachweisverarbeitung, die das System ausführt;

[0068] Fig. 8 ist ein Blockdiagramm, das ein Beispiel eines elektronischen Wasserzeichensystems darstellt;

[0069] Fig. 9 ist ein Blockdiagramm, das die Anordnung eines Systems nach einem zweiten Ausführungsbeispiel der vorliegenden Erfindung darstellt;

[0070] Fig. 10 ist ein Diagramm zur Erläuterung eines allgemeinen Bildformats;

[0071] Fig. 11 ist ein Diagramm zur Erläuterung einer Bilddateistruktur (I);

[0072] Fig. 12 ist ein Diagramm zur Erläuterung einer Bilddateistruktur (II);

[0073] Fig. 13 ist ein Diagramm zur Erläuterung von Eigenschaften, die ein Verfahren zur Datenspeicherung beschreiben;

[0074] Fig. 14 ist ein Diagramm zur Erläuterung eines Bilddateibeispiels, das aus einer Vielzahl von Bildern mit unterschiedlicher Auflösung aufgebaut ist;

[0075] Fig. 15 ist ein Diagramm zur Erläuterung von Bildern auf Ebenen mit unterschiedlichen Auflösungen;

[0076] Fig. 16 ist ein Diagramm zur Erläuterung einer Kacheldatei für individuelle Bilddaten;

[0077] Fig. 17 ist ein Diagramm zur Erläuterung eines Beispiels von einem elektronischen Wasserzeichensystem;

[0078] Fig. 18 ist ein Diagramm zur Erläuterung eines elektronischen Wasserzeichensystems nach einem dritten Ausführungsbeispiel der vorliegenden Erfindung;

[0079] Fig. 19 ist ein Diagramm zur Erläuterung eines weiteren Beispiels von einem elektronischen Wasserzeichensystem;

[0080] Fig. 20 ist ein Diagramm zur Erläuterung eines weiteren Beispiels eines elektronischen Wasserzeichensystems;

[0081] Fig. 21 ist ein Diagramm zur Erläuterung eines elektronischen Wasserzeichensystems nach einem vierten Ausführungsbeispiel der vorliegenden Erfindung;

[0082] Fig. 22 ist ein Diagramm, das eine Systemkonfiguration erläutert;

[0083] Fig. 23 ist ein Blockdiagramm zur Erläuterung eines Beispiels von einem elektronischen Wasserzeichensystem;

[0084] Fig. 24 ist ein Blockdiagramm zur Erläuterung eines fünften Ausführungsbeispiels der vorliegenden Erfindung;

[0085] Fig. 25 ist ein Blockdiagramm zur Erläuterung eines weiteren Beispiels eines elektronischen Wasserzeichensystems;

[0086] Fig. 26 ist ein Blockdiagramm zur Erläuterung eines sechsten Ausführungsbeispiels der vorliegenden Erfindung.

[Erstes Ausführungsbeispiel]

[0087] Das vorliegende Ausführungsbeispiel wird beispielsweise angewandt für ein hierarchisches System (ein System mit mehreren Agenturen), wie in Fig. 4 gezeigt.

[0088] Fig. 6 ist ein schematisches Diagramm, das die Anordnung für das System in Fig. 4 von einem Server, einer Vielzahl von Agenturen und einem der Nutzer zeigt, der zur Agentur gehört.

[0089] Ein System **100** ist nachstehend anhand Fig. 6 erläutert.

[0090] Das System **100** ist ein Netzwerksystem, das aufgebaut ist aus Mehrfacheinheiten (nicht dargestellt), die ein Endgerät **10** auf der Serverseite (Serverendgerät), ein Endgerät **40** auf der Agenturseite (Agenturendgerät) und ein Endgerät **20** auf der Nutzerseite (Nutzerendgerät). Die individuellen Einheiten tauschen über das Netzwerk Digitaldaten aus.

[0091] Das Serverendgerät verfügt über: eine elektronische Wasserzeicheneinbettungseinheit **12** zum Aufnehmen beispielsweise von Bilddaten (Digitaldaten) G und Agenturinformation M; eine erste Verschlüsselungseinheit **13** zum Aufnehmen und Abgeben von der elektronischen Wasserzeicheneinbettungseinheit **12**; eine erste Verschlüsselungseinheit **14** zum Aufnehmen von Daten aus dem Agenturendgerät **40**; eine Identifikationseinheit **15** zum Aufnehmen von Daten aus dem Agenturendgerät **40**; und über einen Tabelleneintragssuchgenerator **16** zum Aufnehmen des Ausgangssignals von der ersten Verschlüsselungseinheit **14**.

[0092] Die Ausgangssignale der ersten Verschlüsselungseinheit **13** und vom Tabelleneintragssuchgenerator **16** werden an das Agenturendgerät **40** gesandt, und das Ausgangssignal der ersten Verschlüsselungseinheit **14** wird über das Agenturendgerät **40** gesendet, sowohl zum Tabelleneintragssuchgenerator **16** als auch zum Nutzerendgerät **20**.

[0093] Das Agenturendgerät **40** verfügt über: einen Kontraktgenerator **41** zum Aufnehmen von Daten aus dem Nutzerendgerät **20**; eine elektronische Wasserzeicheneinbettungseinheit **42** zum Aufnehmen der Ausgangssignale vom Kontraktgenerator **41** und der ersten Verschlüsselungseinheit **13** vom Serverendgerät **10**; eine dritte Verschlüsselungseinheit **43** zum Aufnehmen des Ausgangssignals von der elektronischen Wasserzeicheneinbettungseinheit **42**; einen Tabelleneintragssuchgenerator **44** zum Aufnehmen des Ausgangssignals aus der dritten Verschlüsselungseinheit **43**; eine Identifikationseinheit **45** zum Aufnehmen des Ausgangssignals vom Tabelleneintragssuchgenerator **44**, eine dritte Verschlüsselungseinheit **46** und über eine Identifikationseinheit **47** zum Aufnehmen von Daten aus dem Nutzerendgerät **20**; sowie über eine elektronische Wasserzeicheneinbettungseinheit **48** zum Aufnehmen des Ausgangssignals von der dritten Verschlüsselungseinheit **46**.

[0094] Die Daten aus der dritten Verschlüsselungseinheit **43** werden an den Tabelleneintragssuchgenerator **44** und auch an die erste Verschlüsselungseinheit **14** und die Identifikationseinheit **15** des Serverendgeräts **11** gesandt. Die Daten aus dem Tabelleneintragssuchgenerator **16** und dem Serverendgerät **10** werden auch der Identifikationseinheit **45** zugesandt, und die Daten aus der Identifikationseinheit **45** werden auch dem Nutzerendgerät **20** zugesandt. Daten aus dem Nutzerendgerät **20** werden an die elektronische Wasserzeicheneinbettungseinheit **48** gesandt, und die Daten aus der elektronischen Wasserzeicheneinbettungseinheit **48** werden an das Nutzerendgerät **20** gesandt.

[0095] Das Nutzerendgerät **20** verfügt über: einen Kontraktgenerator **21** zum Senden von Daten an die Kontraktidentifikationseinheit **41** vom Agenturendgerät **40**; eine zweite Verschlüsselungseinheit **24** und über eine Identifikations-/Signaturerzeugungseinheit **28** zur Aufnahme von Daten über das Agenturendgerät **40** aus der ersten Verschlüsselungseinheit **14** des Serverendgeräts **10**; und über einen Tabelleneintragssuchgenerator **26** zum Aufnehmen von Daten aus der zweiten Verschlüsselungseinheit **24**; und über eine zweite Verschlüsselungseinheit **27** zum Aufnehmen des Ausgangssignals aus der elektronischen Wasserzeicheneinbettungseinheit **48** des Agenturendgeräts **40**.

[0096] Die von der zweiten Verschlüsselungseinheit **24** erzeugten Daten werden an den Tabelleneintragssuchgenerator **26** und auch an die dritte Verschlüsselungseinheit **46** und die Identifikationseinheit **47** vom Agenturendgerät **40** gesandt. Die Daten, die der Tabelleneintragssuchgenerator **26** erzeugt hat, werden auch an die Identifikationseinheit **47** vom Agenturendgerät abgegeben. Die Daten, die die Identifikationseinheit **45** vom Agenturendgerät **40** erzeugt hat, werden an die Identifikations-/Signaturerzeugungseinheit **28** gesandt.

[0097] Im obigen System **100** ist die Information bezüglich des ersten Verschlüsselungsprozesses, wie dem angewandten Verfahren und einem Geheimschlüssel nur dasjenige, welches für den Server verfügbar ist; die Information bezüglich des zweiten Verschlüsselungsprozesses ist nur die, die für den Nutzer verfügbar ist; und die Information bezüglich dem dritten Verschlüsselungsprozeß ist nur die, die der Agentur verfügbar ist.

[0098] Angemerkt sei jedoch, daß ein Eigentum dieser Verschlüsselungsprozesse ungeachtet der Tatsache, welcher Verschlüsselungsprozeß als erster ausgeführt wird, eine Mitteilung unter Verwendung des Entschlüsselungsprozesses dechiffriert werden kann.

[0099] Der Entschlüsselungsprozeß wird hiernach wiederholt durch "Ei()", der Entschlüsselungsprozeß wird wiederholt durch "Di()", und der Einbettungsprozeß bezüglich eines elektronischen Wasserzeichens wird wiederholt mit "+". Die elektronische Wasserzeicheneinbettungsverarbeitung, die das System **100** somit ausführt, ist nachstehend als erstes erläutert.

[Einbettungsverarbeitung]

1) Zur Erzielung gewünschter Bilddaten gibt das Anwenderendgerät zunächst eine Anforderung an die Agentur ab, die die Nutzersignatur trägt. Die angeforderten Daten sind die Information (Nutzersignaturinformation), die der Kontraktgenerator **21** erzeugt und die nachstehend als Kontraktinformation bezeichnet ist.

[0100] Das Agenturendgerät **40** empfängt Kontraktinformation vom Nutzer, identifiziert diese und fordert an, daß der Server die Bilddaten bereitstellt.

2) Die elektronische Wasserzeicheneinbettungseinheit **12** vom Serverendgerät **10** bettet die Agenturinformation M in die Bilddaten G ein, die von der Agentur angefordert wurden.

[0101] Die erste Verschlüsselungseinheit **13** führt einen ersten Entschlüsselungsprozeß E() für Bilddaten (G + M) durch, bei denen die Agenturinformation M von der elektronischen Wasserzeicheneinbettungseinheit **12** eingebettet wurde, und sendet die sich ergebenden Daten an die Agentur.

[0102] Auf diese Weise empfängt das Agenturendgerät **40** die ersten verschlüsselten Bilddaten E1(G + M).

3) Der Kontraktgenerator **41** des Agenturendgeräts **40** erzeugt Anwenderinformation U unter Verwendung der Kontraktinformation für den Nutzer.

[0103] Die elektronische Wasserzeicheneinbettungseinheit **42** bettet die Nutzerinformation ein, die der Kontraktgenerator **41** in den ersten verschlüsselten Bilddaten E1(G + M) vom Server empfangen hat.

[0104] Die dritte Verschlüsselungseinheit **42** führt einen dritten Verschlüsselungsprozeß E3() für die ersten verschlüsselten Bilddaten E1(G + M) + U aus, in denen die Nutzerinformation U von der elektronischen Wasserzeicheneinbettungseinheit **42** eingebettet wurde, und sendet die erzielten Bilddaten (dritte verschlüsselte Bilddaten) E3(E1(G + M) + U) an den Server.

[0105] Gleichzeitig erzeugt der Tabelleneintragssuchgenerator **44** einen Tabelleneintragssuchwert H1 für die Sendedaten (dritte verschlüsselte Bilddaten) E3(E1(G + M) + U), signiert sie und sendet den erzielten Tabelleneintragssuchwert H1 an das Serverendgerät **10**.

[0106] Im Ergebnis empfängt das Serverendgerät **10** die dritten verschlüsselten Bilddaten E3(E1(G + M) + U) und den Tabelleneintragssuchwert H1 mit dessen Signatur.

[0107] Der Tabelleneintragssuchwert ist ein Wert, der erzielt werden wird durch Berechnen der Eintragssuchfunktion h(), und die Tabelleneintragssuchfunktion ist eine Kompressionsfunktion, die selten eine Kollision verursacht. Mit Kollision ist ein Fall gemeint, daß für unterschiedliche Werte x1 und x2, dann h(x1) = h(x2). Die Kompressionsfunktion ist eine solche zum Umsetzen einer Bitkette mit einer spezifischen Bitlänge in eine Bitkette mit anderer Bitlänge. Die Tabelleneintragssuchfunktion ist eine solche h(), durch die folglich eine Bitkette mit einer spezifischen Bitlänge umgesetzt wird in eine Bitkette mit anderer Bitlänge, und für die Werte x1 und x2, die der Beziehung h(x1) = h(x2) genügen, nicht leicht gefunden werden. Da der Wert x, der der Beziehung y = h(x) genügt, nicht leicht aus einem beliebigen Wert y gewonnen werden kann, wird folglich die Tabelleneintragssuchfunktion eine Unidirektionalfunktion. Spezifische Beispiele für die Tabelleneintragssuchfunktion sind ein MD (Message Digest) 5 oder ein SHA (Secure Hash Algorithm).

4) Die Identifikationseinheit **15** vom Serverendgerät **10** identifiziert die Signatur für den Tabelleneintragssuchwert H1, den das Agenturendgerät **40** empfangen hat, und bestätigt, daß der Tabelleneintragssuchwert H1 zum Tabelleneintragssuchwert paßt, der unter Verwendung der Sendedaten erzeugt wurde (dritte verschlüsselte Bilddaten E3(E1(G + M) + U). Nach Abschluß des Bestätigungsprozesses speichert die Identifikationseinheit **15** die Empfangsdaten.

[0108] Die erste Entschlüsselungseinheit **14** entschlüsselt den ersten verschlüsselten Abschnitt der dritten verschlüsselten Bilddaten E3(E1(G + M) + U) aus dem Agenturendgerät **40** und sendet die gewonnenen Bilddaten an das Nutzerendgerät **20**.

[0109] Gleichzeitig erzeugt der Tabelleneintragssuchgenerator **16** einen Tabelleneintragssuchwert H2 für die Sendedaten E3(G + M + D1(U)), setzt ein Vorzeichen und sendet die Daten an das Agenturgerät **40**.

[0110] Das Agenturendgerät **40** empfängt somit Daten E3(G + M + D1(U)) und den Tabelleneintragssuchwert H2 mit der Signatur.

5) Die Identifikationseinheit **45** vom Agenturendgerät **40** identifiziert die Signatur für jeden Tabelleneintragssuchwert H2, der vom Serverendgerät **10** kommt, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten E3(G + M + D1(U)) paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, speichert die Identifikationseinheit **45** die empfangenen Daten.

[0111] Darüber hinaus sendet die Identifikationseinheit **45** die vom Server empfangenen Daten in unveränderter Form an den Nutzer.

[0112] Das Nutzerendgerät **20** empfängt die Daten

E3(G + M + D1(U)) und den Tabelleneintragssuchwert H2 mit der Signatur.

6) Die Identifikations-/Signaturerzeugungseinheit **28** identifiziert die Signatur für jeden Tabelleneintragssuchwert H2, der vom Agenturendgerät **40** kommt, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten E3(G + M + D1(U)) paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, werden die empfangenen Daten gespeichert.

[0113] Zusätzlich erzeugt die Identifikations-/Signaturerzeugungseinheit **28** ihre eigene Signatur A für den Tabelleneintragssuchwert H2 und sendet den Tabelleneintragssuchwert H2 mit der Signatur über die Agentur zum Server.

[0114] Die Identifikationseinheit **45** vom Agenturendgerät **40** und vom Tabelleneintragssuchgenerator **16** vom Serverendgerät **10** identifiziert die Signatur A, die der Nutzer gesendet hat, und speichert diese.

7) Die zweite Verschlüsselungseinheit **24** vom Nutzerendgerät **20** führt einen zweiten Verschlüsselungsprozeß E() für die Daten E3(G + M + D1(U)) aus, die von der Agentur kommen, und sendet die erhaltenen Daten an die Agentur.

[0115] Gleichzeitig erzeugt der Tabelleneintragssuchgenerator **26** einen Tabelleneintragssuchwert H3 für die Sendedaten E2(E3(G + M + D1(U))), signiert sie und sendet den Tabelleneintragswert H3 mit der Signatur an die Agentur. Zusätzlich erzeugt der Tabelleneintragssuchgenerator **26** eigene Bescheinigungsdaten S und sendet diese an die Agentur.

[0116] Im Ergebnis empfängt das Agenturendgerät **40** die Daten E2(E3(G + M + D1(U))), den Tabellereintragssuchwert H3 mit der Signatur und die Bescheinigungsinformation S.

8) Die Identifikationseinheit **47** vom Agenturendgerät **40** identifiziert die Signatur für den Tabelleneintragssuchwert H3 vom Nutzer und bestätigt, daß der Tabelleneintragssuchwert zum Tabelleneintragssuchwert für die Sendedaten E2(E3(G + M + D1(U))) paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, werden die empfangenen Daten gespeichert.

[0117] Die dritte Entschlüsselungseinheit **46** entschlüsselt den dritten verschlüsselten Abschnitt der Daten E2(E3(G + M + D1(U))), die vom Nutzer kommen.

[0118] Die elektronische Wasserzeicheneinbettungseinheit **48** bettet die Bescheinigungsinformation S in die Daten E2(G + M + D1(U)) ein, die die dritte Entschlüsselungseinheit **46** empfangen hat, und sendet die sich ergebenden Daten E2(G + M + D1(U)) + S an den Nutzer.

[0119] Die zweite Entschlüsselungseinheit **27** entschlüsselt den zweiten verschlüsselten Abschnitt der Daten E2(G + M + D1(U)) + S und liest Bilddaten aus und gibt sie ab mit einem elektronischen Wasserzeichen die Bilddaten G_W.

[0120] Die Bilddaten G_W werden dargestellt mit

$G_W = G + M + D1(U) + D2(S)$.

[0121] Dies zeigt auf, daß die Agenturinformation M, die erste verschlüsselte Nutzerinformation (elektronische Wasserzeicheninformation) U und die zweite verschlüsselte Signaturinformation S in die Originalbilddaten eingebettet sind.

[0122] Da die Agentur mit dem Einbetten der Signaturinformation S für den Nutzer belastet ist, wie zuvor beschrieben, kann der Nutzer grundsätzlich keine rechtswidrige Tat ausführen. Wenn die Agentur die Nutzerinformation U und die Signaturinformation S für den Nutzer einbettet, wird die Nutzerinformation U durch das erste Verschlüsseln beeinflußt, die nur der Server kennt, und die Signaturinformation wird von der zweiten Verschlüsselung beeinflußt, die nur der Nutzer kennt. Folglich kann die Agentur D1(U + D2(S)) nicht direkt in die Originalbilddaten G einbetten.

[0123] Wird eine rechtswidrige Kopie (ein rechtswidriges Bild) gefunden, wird ein rechtswidriger Nutzer spezifiziert durch Ausführen der in Fig. 7 gezeigten Verarbeitung (nachstehend wird dieser Prozeß als Nachweisprozeß bezeichnet). In diesem Ausführungsbeispiel jedoch sei angemerkt, daß Bilddaten nicht durch Abwandeln oder Löschen der elektronischen Wasserzeicheninformation berührt werden.

[Nachweisverarbeitung]

1) Zuerst liest das Serverendgerät **10** die Agenturinformation M' aus dem rechtswidrigen Bild G_W' aus, das gefunden wurde (Schritt S101).

[0124] Wird die Agenturinformation M' nicht ausgelesen, ist sichergestellt, daß der Server (oder der Autor) eine rechtswidrige Tat begangen hat (Schritt S102). Dies ist so, weil die Serverseite die Agenturinformation M' in die Bilddaten eingebettet hat.

2) Wenn bei 1) die korrekte Agenturinformation M ausgelesen ist (M' = M), unterbreitet der Server dem Nachweisbüro **30** die rechtswidrigen Bilddaten G_W' und den ersten Verschlüsselungscode und fordert die erste Verschlüsselung der rechtswidrigen Bilddaten G_W' an (Schritt S103) sowie das Auslesen der Nutzerinformation U' (Schritt S104).

[0125] Wird die korrekte Nutzerinformation U' ausgelesen (U' = U), dann schreitet die Programmsteue-

rung fort zu 8), wie später zu beschreiben ist.

3) Wenn unter 2) die korrekte Nutzerinformation nicht ausgelesen wird, fordert das Nachweisbüro **30** die gespeicherten Daten E3(E1(G + M) + U) an sowie den Tabelleneintragssuchwert H1 und die Signatur. Danach entschlüsselt das Nachweisbüro **30** den ersten verschlüsselten Abschnitt der Daten E3(E1(G + M) + U), erzeugt den Tabelleneintragssuchwert und bestätigt, daß der Tabelleneintragssuchwert zum Tabelleneintragssuchwert H2 paßt, der in der Agentur gespeichert ist. Zur selben Zeit überprüft das Nachweisbüro **30** die Signatur, die für den Tabelleneintragssuchwert H2 bereitgestellt ist (Schritt S105).

4) Wenn unter 3) der vom Nachweisbüro **30** erzeugte Tabelleneintragssuchwert nicht mit dem Tabelleneintragssuchwert H2 übereinstimmt, den die Agentur gespeichert hat, dann ermittelt das Nachweisbüro **30**, daß der Server eine rechtswidrige Tat begangen hat (Schritt S106).

[0126] Das bedeutet, daß der erste Verschlüsselungscode, den der Server durchgemacht hat, nicht korrekt ist.

5) Wenn der vom Nachweisbüro **30** erzeugte Tabelleneintragssuchwert zu dem Tabelleneintragssuchwert H2 paßt, den die Agentur gespeichert hat, fordert das Nachweisbüro **30** an, daß die Agentur den dritten Verschlüsselungscode anwendet, entschlüsselt den dritten Verschlüsselungsabschnitt der Daten E3(E1(G + M) + U), gespeichert im Server und liest aus den gewonnenen Daten die Nutzerinformation U' aus (Schritt S107).

6) Wenn die korrekte Nutzerinformation U' unter 5) mit (U' = U) ausgelesen ist, ermittelt das Nachweisbüro **30**, daß der Server eine rechtswidrige Tat begangen hat (Schritt S108).

[0127] Dies zeigt auf, daß die Nutzerinformation U' korrekt in die Bilddaten eingebettet worden ist. Da darüber hinaus durch den Nachweisvorgang, wie er bis 5) ausgeführt wurde, bestimmt ist, daß der erste Verschlüsselungsabschnitt für die rechtswidrigen Bilddaten G_W' Korrektheit besteht und die Nutzerinformation U' rechtswidrig ist, ist es offensichtlich, daß nur der Server, der den ersten Verschlüsselungscode kennt, die rechtswidrigen Bilddaten G_W' erzeugen konnte.

7) Wenn unter 5) die korrekte Nutzerinformation U' nicht ausgelesen wird, ermittelt das Nachweisbüro **30** die Nachweisinformation, daß die Agentur eine rechtswidrige Tat begangen hat (Schritt S109).

[0128] Die zeigt auf, daß die korrekte Nutzerinformation U' in die Bilddaten während des Einbettungsprozesses eingebettet wurde, und die Agentur war mit der Einbettung der Nutzerinformation beschäftigt.

8) Wenn unter 2) die korrekte Nutzerinformation U' mit (U' = U) ausgelesen ist, fordert das Nachweisbüro **30** an, daß der Server und die Agentur den gespeicherten Tabelleneintragssuchwert H2 und eine Signatur A' unterbreiten, bereitgestellt für den Nutzer zum Tabelleneintragssuchwert H2. und die Signatur A' wird nachgewiesen (Schritt S110).

9) Wenn unter 8) die korrekte Signatur nicht identifiziert wird (nicht unterbreitet wird), ermittelt das Nachweisbüro **30**, daß der Server und die Agentur in eine rechtswidrige Tat verwickelt sind (Schritt S111).

[0129] Dies zeigt auf, daß der Server und die Agentur, die in die Fälschung der Daten G + M + D1(U') verwickelt sind, einen beliebigen Nutzer darstellen (Nutzerinformation U').

10) Wenn unter 8) die korrekte Signatur A' identifiziert ist mit (A' = A), fordert das Nachweisbüro **30** an, daß der Nutzer den zweiten Verschlüsselungscode unterbreitet und führt die zweite Verschlüsselung für die rechtswidrigen Bilddaten G_W' aus (Schritt S112). Dann wird die Signaturinformation S' ausgelesen (Schritt S113).

11) Wenn unter 10) die korrekte Signaturinformation S' ausgelesen ist mit (S' = S), dann ermittelt das Nachweisbüro **30**, daß der Nutzer eine rechtswidrige Tat begangen hat (Schritt S114).

[0130] Dies liegt daran, daß der Prozeß zum Ausführen des zweiten Verschlüsselungsvorgangs und zum Auslesen der Signaturinformation S' nur vom Nutzer ausgeführt werden kann.

12) Wenn unter 10) die korrekte Signaturinformation S' nicht ausgelesen wird, dann fordert das Nachweisbüro **30** an, daß der Nutzer das gespeicherte Bild E3(G + M + D1(U)) unterbreitet, den Tabelleneintragssuchwert H3 mit der Signatur, und identifiziert den Tabelleneintragssuchwert H3 und die Signatur. Dann führt das Nachweisbüro den zweiten Verschlüsselungsvorgang für die Daten E3(G + M + D1(U)) aus und erzeugt einen Tabelleneintragssuchwert für die Daten, um zu ermitteln, ob diese zum Tabelleneintragssuchwert passen. Zur selben Zeit überprüft auch das Nachweisbüro **30** die Signatur für den Tabelleneintragssuchwert H3 (Schritt S115).

13) Wenn unter 12) der vom Nachweisbüro **30** erzeugte Tabelleneintragssuchwert nicht zum Tabelleneintragssuchwert H3 paßt, den der Nutzer gespeichert hat, ermittelt das Nachweisbüro **30**, daß eine rechtswidrige Tat vom Anwender begangen wurde (Schritt S116).

[0131] Das liegt daran, weil der zweite Verschlüsselungscode nicht korrekt ist, den der Nutzer unterbreitet hat.

14) Wenn unter 12) der Tabelleneintragssuchwert, den das Nachweisbüro **30** erzeugt hat, zum Tabelleneintragssuchwert H3 paßt, den der Nutzer ge-

speichert hat, ermittelt das Nachweisbüro **30**, daß die Agentur eine rechtswidrige Tat begangen hat (Schritt S117).

[0132] Dies liegt daran, daß die Agentur die korrekte Signaturinformation S nicht in die Bilddaten während des Einbettungsprozesses eingebettet hat.

[0133] Wie zuvor gemäß dem ersten Ausführungsbeispiel beschrieben, ist das Nachweisbüro nicht erforderlich, so lange bis ein rechtswidriges Bild gefunden wird, und es kann nicht bestimmt werden, ob irgendwelche rechtswidrigen Taten ausgeführt worden sind, bevor ein rechtswidriges Bild gefunden ist. Solange die oben beschriebene Nachweisverarbeitung allgemein bekannt ist, und der Server, die Agentur und die Nutzer die Ergebnisse dieser Verarbeitung überwachen, kann eine rechtswidrige Tat dieser gemäß der Situation spezifiziert werden, auch ohne das Nachweisbüros **30** zu involvieren.

[0134] Fig. 8 ist ein schematisches Diagramm, das die hierarchische Anordnung vom System gemäß Fig. 5 darstellt, von einem einer Vielzahl von Autoren (oder Servern), einer Agentur und einem beliebigen Benutzer, einer aus einer Vielzahl von Nutzern.

[0135] Nachstehend anhand Fig. 8 ist speziell System **200** erläutert.

[0136] Das System **200** hat dieselbe Struktur wie das System **100** in Fig. 6, mit folgender Ausnahme.

1) Eine elektronische Wasserzeicheneinbettungseinheit **12** ist im Serverendgerät **10** nicht vorgesehen, und nur Bilddaten G werden an eine erste Verschlüsselungseinheit **13** gesandt.

2) Ein Tabelleneintragssuchgenerator **49** zum Aufnehmen des Ausgangssignals von einer elektronischen Wasserzeicheneinbettungseinheit **48** ist weiterhin vorgesehen für ein Agenturendgerät **400**. Die vom Tabelleneintragssuchgenerator **49** erzeugten Daten werden an ein Nutzerendgerät **20** gesandt.

3) Eine Identifiziereinheit **29** ist zusätzlich für das Nutzerendgerät **20** vorgesehen und nimmt die Ausgangssignale der elektronischen Wasserzeicheneinbettungseinheit **48** und vom Tabelleneintragssuchgenerator im Agenturendgerät **40** auf.

[0137] Wie zuvor beschrieben ist das System **200** so ausgelegt, daß das Einbetten der Agenturinformation M eine fortgelassene Agentur darstellt.

[0138] Zunächst erläutert wird die elektronische Wasserzeicheneinbettungsverarbeitung, die das System **200** ausführt.

[0139] Dieselben Bezugszeichen werden für das System in Fig. 6 verwandt und bedeuten entsprechende Komponenten im System **200** gemäß Fig. 8, und eine erneute detaillierte Erläuterung dieser ist hier fortgelassen.

[Einbettungsverarbeitung]

1) Zum Erzielen von Bilddaten (Kontraktinformation) gibt das Nutzerendgerät **20** zunächst an die Agentur eine Anforderung ab, die die Signatur vom Nutzer trägt.

[0140] Das Agenturendgerät **40** empfängt Kontraktinformation vom Nutzer, identifiziert sie und fordert an, daß ein Server Bilddaten bereitstellt.

2) Im Serverendgerät führt die erste Verschlüsselungseinheit **13** einen ersten Verschlüsselungsprozeß E1 für Bilddaten G aus und sendet die sich ergebenden Bilddaten an die Agentur.

[0141] Auf diese Weise empfängt das Agenturendgerät **40** die ersten verschlüsselten Bilddaten E1(G).

3) Der Kontraktgenerator **41** vom Agenturendgerät **40** erzeugt Nutzerinformation U unter Verwendung der Kontraktinformation für den Nutzer.

[0142] Die elektronische Wasserzeicheneinbettungseinheit **42** bettet die Nutzerinformation U ein, die der Kontraktgenerator **41** in den ersten verschlüsselten Bilddaten E1(G) erzeugt hat, die der Server empfangen hat.

[0143] Die dritte Verschlüsselungseinheit **43** führt einen dritten Verschlüsselungsprozeß E3 für die ersten verschlüsselten Bilddaten E1(G) + U aus, wobei die Nutzerinformation von der elektronischen Wasserzeicheneinbettungseinheit **42** eingebettet wurde, und sendet die erzielten Bilddaten (dritte verschlüsselte Bilddaten) E3(E1(G) + U) an den Server.

[0144] Gleichzeitig erzeugt der Tabelleneintragssuchgenerator **44** einen Tabelleneintragssuchwert H1 für die Sendedaten (dritte verschlüsselte Bilddaten E3(E1(G) + U)), signiert sie und sendet den gewonnenen Tabelleneintragssuchwert H1 zum Serverendgerät **10**.

[0145] Im Ergebnis empfängt das Serverendgerät **10** die dritten verschlüsselten Bilddaten E3(E1(G) + U) und den Tabelleneintragssuchwert H1 mit der Signatur.

4) Die Identifizierungseinheit **15** vom Serverendgerät **10** identifiziert die Signatur für den Tabelleneintragssuchwert H1, der vom Agenturendgerät **40** kommt, und bestätigt, daß der Tabelleneintragssuchwert H1 zum Tabelleneintragssuchwert paßt, der unter Verwendung der Sendedaten (dritte verschlüsselte Bilddaten E3(E1(G) + U)) erzeugt wurde. Nach Abschluß des Bestätigungsprozesses speichert die Identifiziereinheit **15** die empfangenen Daten.

[0146] Die erste Verschlüsselungseinheit **14** verschlüsselt den ersten Verschlüsselungsabschnitt der dritten Verschlüsselungsbilddaten E3(E1(G) + U), die das Agenturendgerät **40** empfangen hat, und sendet die gewonnenen Bilddaten an das Nutzerendgerät **20**.

[0147] Zur selben Zeit erzeugt der Tabelleneintragssuchgenerator **16** einen Tabelleneintragssuchwert H2 für die Sendedaten (E3(G + D1(U)), signiert sie und sendet die Daten an das Agenturendgerät **40**.

[0148] Das Agenturendgerät **40** empfängt somit die Daten E3(G + D1(U)) und den Tabelleneintragssuchwert H2 mit der Signatur.

5) Die Identifizierungseinheit **45** und das Agenturendgerät **40** identifizieren die Signatur für den Tabelleneintragssuchwert H2, der aus dem Serverendgerät **10** empfangen wurde, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten E3(G + D1(U) paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, speichert die Identifizierungseinheit **45** die empfangenen Daten.

[0149] Darüber hinaus sendet die Identifizierungseinheit **45** die vom Server empfangenen Daten in unveränderter Form an den Nutzer.

[0150] Folglich empfängt das Nutzerendgerät **20** die Daten E3(G + D1(U)) und den Tabelleneintragssuchwert H2, der vom Agenturendgerät **40** kommt, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten E3(G + D1(U)) paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, werden die empfangenen Daten gespeichert.

6) Die Identifizierungs-/Signaturerzeugungseinheit **28** erzeugt die eigene Signatur A für den Tabelleneintragssuchwert H2 und sendet den Tabelleneintagssuchwert H2 mit der Signatur über die Agentur an den Server.

[0151] Die Identifizierungseinheit **45** vom Agenturendgerät **40** und dem Tabelleneintragssuchgenerator **16** vom Serverendgerät **10** identifizieren die Signatur A, die der Nutzer gesendet hat, und sie wird gespeichert.

7) Die zweite Verschlüsselungseinheit **24** vom Nutzerendgerät **20** führt einen zweiten Verschlüsselungsprozeß E() für die Daten E3(G + D1(U)) aus, empfangen von der Agentur, und sendet die gewonnenen Daten an die Agentur.

[0152] Gleichzeitig erzeugt der Tabelleneintragssuchgenerator **26** einen Tabelleneintragssuchwert H3 für die Sendedaten E2(E3(G + D1(U))), signiert diese und sendet den Tabelleneintragssuchwert H3 mit der Signatur an die Agentur. Darüber hinaus erzeugt der Tabelleneintragssuchgenerator **26** eigene Bescheinigungsdaten S und sendet sie an die Agentur.

[0153] Im Ergebnis empfängt das Agenturendgerät **40** die Daten E2(E3(G + D1(U))), den Tabelleneintragssuchwert H3 mit der Signatur und die Bescheinigungsinformation S.

8) Die Identifizierungseinheit **47** des Agenturendgeräts **40** identifiziert die Signatur für den Tabelleneintragssuchwert H3 vom Nutzer und bestätigt, daß der Tabelleneintragssuchwert H3 zum Tabelleneintragssuchwert für die Sendedaten E2(E3(G + D1(U))) paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, werden die empfangenen Daten gespeichert.

[0154] Die dritte Entschlüsselungseinheit **46** verschlüsselt den dritten Verschlüsselungsabschnitt der Daten E2(E3(G + D1(U))) vom Nutzer.

[0155] Die elektronische Wasserzeicheneinbettungseinheit **48** bettet die Bescheinigungsinformation S in die Daten E2(G + D1(U)) ein, die von der dritten Entschlüsselungseinheit **46** kommen, und sendet die sich ergebenden Daten E2(G + D1(U)) + S an den Nutzer.

[0156] Auf diese Weise empfängt das Nutzerendgerät die Daten E2(G + D1(U)) + S.

9) Im Nutzerendgerät **20** entschlüsselt die zweite Entschlüsselungseinheit **27** den zweiten Verschlüsselungsabschnitt der Daten E2(G + D1(U)) + S und liest die Bilddaten G_W aus und gibt sie mit einem elektronischen Wasserzeichen ab.

[0157] Die Bilddaten G_W werden folgendermaßen dargestellt $G_W = G + D1(U) + D2(S)$.

[0158] Dies zeigt auf, daß die erste verschlüsselte Nutzerinformation (elektronische Wasserzeicheninformation) U und die zweite Verschlüsselungssignaturinformation S in die Originalbilddaten eingebettet sind.

[0159] Da die Agentur verantwortlich ist für das Einbetten der Signaturinformation S für den Nutzer, wie zuvor beschrieben, kann der Nutzer grundsätzlich eine rechtswidrige Tat begehen. Während die Agentur die Nutzerinformation U und die Signaturinformation S für den Nutzer einbettet, wird die Nutzerinformation von der ersten Verschlüsselung beeinflußt, die nur der Server kennt, und die Signaturinformation wird von der zweiten Verschlüsselung berührt, die nur der Nutzer kennt. Folglich kann die Agentur nicht direkt D1(U + D2(S)) in die Originalbilddaten G einbetten.

[0160] Wenn eine rechtswidrige Kopie (ein rechtswidriges Bild) gefunden wird, kann eine Agentur, die eine rechtswidrige Tat begangen hat, durch Ausfüh-

ren der folgenden Nachweisverarbeitung spezifiziert werden, ohne die oben beschriebene Agenturinformation M zu verwenden. Angemerkt sei, daß die Bilddaten nicht von der Modifizierung und dem Löschen eines elektronischen Wasserzeichens berührt werden.

[Nachweisprozeß]

1) Zuerst unterbreitet der Server dem Nachweisbüro **30** einen ersten Verschlüsselungscode, der aus rechtswidrigen Bilddaten G_W' gewonnen wird, die entdeckt worden sind, und fordert eine erste Verschlüsselung der rechtswidrigen Bilddaten G_W' und das Auslesen der Nutzerinformation U' an.

[0161] Wenn die korrekte Nutzerinformation U' mit (U' = U) ausgelesen wird, schreitet das Programm fort zu 7), was später zu beschreiben ist.

2) Wenn unter 1) die korrekte Nutzerinformation nicht ausgelesen wird, fordert das Nachweisbüro **30** aus dem Server die gespeicherten Daten E3(E1(G) + U) an sowie den Tabelleneintragssuchwert H1 mit der Signatur. Das Nachweisbüro **30** identifiziert dann den Tabelleneintragssuchwert H1 und die Signatur. Danach entschlüsselt das Nachweisbüro **30** den ersten verschlüsselten Abschnitt der Daten E3(E1(G) + U), erzeugt den zugehörigen Tabelleneintragssuchwert und bestätigt, daß der Tabelleneintragssuchwert zum Tabelleneintragssuchwert H2 paßt, der in der Agentur gespeichert ist. Gleichzeitig überprüft das Nachweisbüro **30** die für den Tabelleneintragssuchwert H2 bereitgestellt Signatur.

3) Wenn der vom Nachweisbüro **30** unter 2) erzeugte Tabelleneintragssuchwert nicht zum Tabelleneintragssuchwert H2 paßt, der in der Agentur gespeichert ist, ermittelt das Nachweisbüro **30**, daß der Server eine rechtswidrige Tat begangen hat.

[0162] Das bedeutet, daß der erste Verschlüsselungscode, den der Server unterbreitet hat, nicht korrekt ist.

4) Wenn unter 2) der vom Nachweisbüro **30** erzeugte Tabelleneintragssuchwert zum Tabelleneintragssuchwert H2 paßt, der in von der Agentur gespeichert ist, dann fordert das Nachweisbüro **30** an, daß die Agentur den dritten Verschlüsselungscode unterbreitet, verschlüsselt den dritten Verschlüsselungsabschnitt der Daten E3(E1(G) + U), die im Server gespeichert sind, und liest aus den gewonnenen Daten die Nutzerinformation U' aus.

5) Wenn die korrekte Nutzerinformation U' unter 4) ausgelesen ist, ermittelt das Nachweisbüro **30**, daß der Server eine rechtswidrige Tat begangen hat.

[0163] Dies zeigt auf, daß die Nutzerinformation korrekt in die Bilddaten eingebettet worden ist. Da darüber hinaus durch den Nachweisprozeß, wie er unter 4) ausgeführt wurde, bestimmt ist, daß der erste Verschlüsselungsabschnitt für die rechtswidrigen Bilddaten G_W' korrekt ist und die Nutzerinformation U' rechtswidrig ist, wird offensichtlich, daß nur der Server, der den ersten Verschlüsselungscode kennt, die rechtswidrigen Daten G_W' erzeugt haben kann.

6) Wird unter 4) keine korrekte Nutzerinformation U' ausgelesen, dann ermittelt das Nachweisbüro **30**, daß die Agentur eine rechtswidrige Tat begangen hat.

[0164] Dies zeigt auf, daß die korrekte Nutzerinformation U' nicht in die Bilddaten während des Einbettungsprozesses eingebettet worden ist, und die Agentur ist verantwortlich für das Einbetten der Nutzerinformation.

7) Wenn die korrekte Nutzerinformation U' unter 1) ausgelesen wird (U' = U), fordert das Nachweisbüro **30** an, daß der Server und die Agentur den gespeicherten Tabelleneintragssuchwert H2 und eine Signatur A' unterbreiten, bereitgestellt vom Nutzer für den Tabelleneintragssuchwert H2, und die Signatur A' wird identifiziert.

8) Wenn die korrekte Signatur A' unter 7) nicht identifiziert wird (nicht unterbreitet), ermittelt das Nachweisbüro **30**, daß der Server und die Agentur in eine rechtswidrige Tat verwickelt sind.

[0165] Dies zeigt auf, daß der Server und die Agentur in die Fälschung der Daten G + D1(U') verwickelt sind, die einen beliebigen Anwender (Nutzerinformation U') darstellen.

9) Wenn die korrekte Signatur A' unter 7) identifiziert ist (A' = A), dann fordert das Nachweisbüro **30** an, daß der Nutzer den zweiten Verschlüsselungscode unterbreitet und die zweite Verschlüsselung für die rechtswidrigen Bilddaten G_W' ausführt. Dann wird die Signaturinformation S' ausgelesen.

10) Wenn die korrekte Signaturinformation S' unter 9) ausgelesen ist mit (S' = S), dann ermittelt das Nachweisbüro **30**, daß eine rechtswidrige Tat vom Nutzer begangen wurde.

[0166] Dies liegt daran, weil der Prozeß zum Ausführen des zweiten Verschlüsselungsvorgangs und zum Auslesen der Signaturinformation S' nur vom Nutzer ausgeführt werden kann.

11) Wenn unter 9) nicht die korrekte Signaturinformation S' ausgelesen wird, fordert das Nachweisbüro **30** an, daß der Nutzer das gespeicherte Bild E3(G + D1(U)) unterbreitet, den Tabelleneintragssuchwert H3 mit Signatur und den Tabelleneintragssuchwert H3 und die Signatur identifiziert. Dann führt das Nachweisbüro **30** den zweiten Verschlüsselungsvorgang für die Daten D3(G + D1(U)) aus und erzeugt einen Tabelleneintragssuchwert für die Daten, um zu ermitteln, ob diese

zum Tabelleneintragssuchwert H3 passen. Gleichzeitig überprüft auch das Nachweisbüro **30** die Signatur für den Tabelleneintragssuchwert H3.
12) Wenn der Tabelleneintragssuchwert, den das Nachweisbüro **30** unter 11) erzeugt hat, zum Tabelleneintragssuchwert H3 paßt, den der Nutzer gespeichert hat, ermittelt das Nachweisbüro **30** eine rechtswidrige Tat, die die Agentur begangen hat.

[0167] Dies liegt daran, daß der vom Nutzer unterbreitete zweite Verschlüsselungscode nicht korrekt ist.

13) Wenn der unter 11) erzeugte Tabelleneintragssuchwert, den das Nachweisbüro **30** unter 11) erzeugt hat, zum Tabelleneintragssuchwert H3 paßt, den der Nutzer gespeichert hat, ermittelt das Nachweisbüro **30**, daß die Agentur eine rechtswidrige Tat begangen hat.

[0168] Dies liegt daran, daß die Agentur die korrekte Signaturinformation S während des Einbettungsprozesses nicht in die Bilddaten eingebettet hat.

[0169] Wie zuvor beschrieben ist das Nachweisbüro nicht erforderlich, bis daß ein rechtswidriges Bild gefunden wird, und eine beliebige rechtswidrige Tat kann nicht als ausgeführt bestimmt werden, bevor ein rechtswidriges Bild gefunden ist. Sofern die oben beschriebene Nachweisverarbeitung allgemein bekannt ist und der Server, die Agentur und der Nutzer die Ergebnisse dieser Verarbeitung überwachen, kann zusätzlich eine rechtswidrige Tat dieser gemäß der Situation selbst ohne Einbeziehen des Nachweisbüros **30** spezifiziert werden.

(Zweites Ausführungsbeispiel)

[0170] Kürzlich ist der Geldtransfer über Netzwerke, eine Wertpapierübertragungsprozedur, die man elektronische Barzahlung nennt, in Verwendung gekommen. Da wie bei der regulären Barzahlung der Name vom Eigentümer der elektronischen Barzahlungsübertragung nicht identifiziert wird, bleibt die Anonymität beibehalten. Wäre die Anonymität nicht möglich, könnte ein Verkäufer eines Produkts aus der elektronischen Bargeldübertragung Informationen bezüglich des Käufers und die Nutzung des Produkts gewinnen, und die Privatsphäre eines Nutzers wäre nicht geschützt. Folglich ist der Schutz der Privatsphäre eines Nutzers genauso wichtig wie der Schutz, der für ein einem Urheber gewährtes Copyright vorgesehen ist, der ein elektronisches Wasserzeichen verwendet.

[0171] Folglich ist im zweiten Ausführungsbeispiel für den Käufer die Anonymität gewahrt, und wenn eine rechtswidrige Tat, wie rechtswidriges Verteilen von Bildern, entdeckt wird, ist es möglich, einen nicht autorisierten Verteiler zu identifizieren, womit der ursprüngliche Zweck eines elektronischen Wasserzeichens erfüllt ist. Dies wird erreicht durch Anwenden beispielsweise eines in Fig. 9 gezeigten Systems **300**.

[0172] Das System **300** hat dieselbe Struktur wie das System **200** in Fig. 8, wobei ein anonymes öffentliches Schlüsselbescheinigung für ein Nutzerendgerät **20** vorgesehen ist, das von einem Bescheinigungsbüro **50** ausgegeben wird.

[0173] Um die Signaturinformation zu berechtigen, wird im allgemeinen eine Bescheinigung von der Organisation ausgegeben, die sich Bescheinigungsbüro nennt, und dem öffentlichen Schlüssel hinzugefügt, der verwendet wird, wenn die Signaturinformation überprüft wird.

[0174] Ein Bescheinigungsbüro ist eine Organisation, die Bescheinigungen für öffentliche Schlüssel ausgibt, die für die Nutzer vorgesehen sind, um die öffentliche Schlüsselberechtigung bereitzustellen, die mit den Erfordernissen des öffentlichen Verschlüsselungssystems in Übereinstimmung ist. Das heißt, ein Bescheinigungsbüro verwendet den eigenen Geheimschlüssel zum Bereitstellen einer Signatur für den öffentlichen Schlüssel des Nutzers oder für Daten, die den Benutzer betreffen, und zu diesem Zweck wird eine Bescheinigung vorbereitet und ausgegeben. Wenn ein Nutzer von einem anderen Nutzer einer Signatur empfängt, die von einer Bescheinigung begleitet ist, überprüft der Nutzer die Bescheinigung unter Verwendung des öffentlichen Schlüssels des Bescheinigungsbüros, um die Berechtigung nachzuweisen, die der Nutzer bereitstellt, der den öffentlichen Schlüssel gesendet hat (oder zumindest die Tatsache, daß die Berechtigung dem Nutzer vom Bescheinigungsbüro bereitgestellt ist). Sowohl VeriSign als auch CyberTrust sind allgemein bekannte Organisationen, die derartige Bescheinigungsbüros betreiben.

[0175] Wenn bei Prozedur 1) vom Einbettungsprozeß im Beispiel von Fig. 8 eine Agentur eine Signatur zum Nachweis der Kontraktinformation überprüft, die für einen Nutzer unterbreitet wurde, kann die Agentur den öffentlichen Schlüssel mit einer Signatur verwenden, die das Bescheinigungsbüro ausgegeben hat.

[0176] Da jedoch der Name des Besitzers vom öffentlichen Schlüssel generell in die Bescheinigung geschrieben wird, ist die Nutzeranonymität zum Zeitpunkt des Verkaufs der Daten nicht gewahrt.

[0177] Wenn andererseits das Bescheinigungsbüro die Entsprechung des öffentlichen Schlüssels und deren Besitzern geheim hält, kann der Name des Besitzers nicht in eine Bescheinigung geschrieben werden, die für einen öffentlichen Schlüssel ausgegeben wird. Ein öffentlicher Schlüssel, für den eine Bescheinigung bereitsteht, wird als "anonymer öffentlicher

Schlüssel mit Bescheinigung" bezeichnet.

[0178] Wenn ein Anwender in der Prozedur 1) des oben beschriebenen Einbettungsprozesses an einen Server nicht nur Kontraktinformationen sondern auch eine Signatur für die Kontraktinformation und einen anonymen öffentlichen Schlüssel sendet, begleitet mit einer Bescheinigung, um die Überprüfung der Signaturinformation S zu ermöglichen, dann kann der Nutzer anonym bleiben, wenn Digitaldaten gekauft werden. Der anonyme öffentliche Schlüssel, der von einer Bescheinigung begleitet wird, wird folglich an die Agentur als Information gesandt, die zum Nutzernachweis verwendet wird. Und wenn eine rechtswidrige Transaktion aufgedeckt wird und der Nutzer identifiziert werden muß, dann wird der anonyme öffentliche Schlüssel, begleitet mit der Bescheinigung, an das Bescheinigungsbüro **50** mit der Aufforderung gesandt, den Nutzernamen zu nennen, der demjenigen des Besitzers vom öffentlichen Schlüssel entspricht.

[0179] Wenn die Prozedur 1) im Einbettungsprozeß und die Prozedur 7) im Nachweisprozeß gemäß dem Beispiel in Fig. 8 wie im Folgenden ausgeführt werden, dann kann die Anonymität eines Nutzers, der Digitaldaten kauft, beibehalten werden, aber wenn eine rechtswidrige Transaktion entdeckt wird, dann kann der für die Ausführung dieser Transaktion verantwortliche Nutzer identifiziert werden.

[0180] Der Einbettungsprozeß und der Nachweisprozeß, den das System **300** in Fig. 9 ausführt, ist nachstehend speziell beschrieben.

[0181] Dieselben Bezugszeichen, die im System **200** gemäß Fig. 8 verwendet wurden, werden hier ebenfalls verwendet, um entsprechende Komponenten im System **300** gemäß Fig. 9 zu bezeichnen, und eine erneute detaillierte Erläuterung dieser wird nicht gegeben. Nur die unterschiedlichen Abschnitte werden speziell erläutert.

[0182] Da die Prozeduren, anders als Prozedur 1) im Einbettungsprozeß und die Prozedur 1) im Nachweisprozeß dieselben wie jene des Beispiels gemäß Fig. 8 sind, gibt es hier keine detaillierte Erläuterung.

[Einbettungsprozeß]

1') Im Nutzerendgerät stellt zunächst ein Kontraktgenerator **21** für Kontraktinformation zum Anfragen gewünschter Bilddaten eine Signatur bereit, die einem anonymen öffentlichen Schlüssel entspricht, begleitet von einer Bescheinigung, die das Bescheinigungsbüro **50** ausgestellt hat. Gemeinsam mit dem von der Bescheinigung begleiteten anonymen öffentlichen Schlüssel wird die Kontraktinformation vom Nutzer an die Agentur gesandt.

[0183] Das Agenturendgerät **40** identifiziert die empfangene Kontraktinformation unter Verwendung des anonymen öffentlichen Schlüssels, begleitet von der Bescheinigung, und gibt eine Anforderung nach den Bilddaten an den Server ab. **57** Hiernach werden Prozeduren 2) bis 9) des Einbettungsprozesses im zweiten Ausführungsbeispiel durchgeführt.

[0184] Der Nutzer kann in diesem Falle grundsätzlich keine rechtswidrige Tat begehen, und die Agentur kann D1(U + D2(5)) nicht direkt in die Originalbilddaten einbetten.

[0185] Wenn eine rechtswidrige Kopie (rechtswidriges Bild) gefunden wird, wird der folgende Nachweisprozeß durchgeführt.

[Nachweisprozeß]

1) bis 6) Zuerst werden die Prozeduren 1) bis 6) des Nachweisprozesses im zweiten Ausführungsbeispiel durchgeführt.
7') Wenn in Prozedur 1) eine korrekte Nutzerinformation U' mit (U' = U) ausgelesen wird, unterbreitet ein Nachweisbüro **30** dem Bescheinigungsbüro **50** die Nutzerinformation U' und den anonymen öffentlichen Schlüssel, begleitet von der Bescheinigung, die aus der Kontraktinformation ausgelesen ist. Das Nachweisbüro **30** fordert vom Bescheinigungsbüro **50** die Identität des Nutzers an, dessen Name demjenigen des Besitzers vom anonymen öffentlichen Schlüssel entspricht. Das Nachweisbüro **30** fordert auch an, daß der Server und die Agentur einen gespeicherten Tabelleneintragssuchwert H2 und eine Signatur A' unterbreiten, für den Tabelleneintragssuchwert H2, der für den Nutzer vorgesehen ist, und identifiziert die Signatur A'.

[0186] Danach werden die Prozeduren 8) bis 13) im Nachweisprozeß vom zweiten Ausführungsbeispiel durchgeführt.

[0187] Wie zuvor gemäß dem zweiten Ausführungsbeispiel beschrieben, besteht für das Nachweisbüro kein Bedarf, bis ein rechtswidriges Bild entdeckt worden ist, und keine rechtswidrige Tat kann ausgeführt werden, bis ein rechtswidriges Bild entdeckt ist. Solange die oben beschriebene Nachweisverarbeitung allgemein bekannt ist und der Server, die Agentur und der Nutzer darüber hinaus die Ergebnisse der Verarbeitung überwachen, kann eine rechtswidrige Tat, die von irgendeinem dieser begangen wurde, entsprechend der Situation identifiziert werden, selbst ohne die Fürsprache des Nachweisbüros **30**.

[0188] Im zweiten Ausführungsbeispiel ist zusätzlich ein Bescheinigungsbüro **50** für das System **200** im Beispiel von Fig. 8 vorgesehen. Die Modifizierung der Systemanordnung ist jedoch nicht hierauf be-

schränkt, und ein Bescheinigungsbüro **50** kann für das System **100** im ersten Ausführungsbeispiel vorgesehen sein. In diesem Falle entspricht die Prozedur 1) im Einbettungsprozeß im ersten Ausführungsbeispiel der Prozedur 1') für das zweite Ausführungsbeispiel, und Prozedur 8) im Nachweisprozeß im ersten Ausführungsbeispiel entspricht der Prozedur 7) für das zweite Ausführungsbeispiel.

[0189] Verschiedene Daten können unter Verwendung des nachstehenden Bildformats gespeichert werden, um Bilddaten im ersten bis dritten Ausführungsbeispiel sowie Tabelleneintragssuchwerte zu enthalten, die während des Einbettungsprozesses für die elektronische Wasserzeicheninformation gewonnen werden.

[0190] Gemäß dem folgenden allgemeinen Bildformat können beispielsweise Bilddaten, die in individuellen Schritten gesendet werden, in einem Bilddatenabschnitt gespeichert werden, und ein zugehöriger Tabelleneintragssuchwert und dessen Signatur können in einem Bildkopfabschnitt gespeichert werden. Ein Tabelleneintragssuchwert und die begleitende Signatur, die der Nutzer zurückhalten muß, und der zweite Verschlüsselungscode können des weiteren im Bildkopfabschnitt gespeichert werden, während Bilddaten mit einem elektronischen Wasserzeichen im Bilddatenabschnitt gespeichert werden können.

[0191] Gemäß dem folgenden FlashPixTM-Dateiformat kann das allgemeine Bildformat, das den Tabelleneintragssuchwert und die Signatur enthält, als Daten in jeder Ebene gespeichert werden. Auch der Tabelleneintragssuchwert und die Signatur können als Eigenschaftsinformation in einem Eigentumssatz gespeichert werden.

[Erläuterung zum generellen Bildformat]

[0192] Gemäß dem generellen Bildformat ist eine Bilddaten unterteilt in einen Bildkopfabschnitt und in einen Bilddatenabschnitt, wie in Fig. 10 gezeigt.

[0193] Im Bildkopfabschnitt gespeicherte Informationen sind im allgemeinen solche, die zum Lesen von Bilddaten aus einer Bilddatei erforderlich sind, sowie zusätzliche Informationen zur Erläuterung der Inhalte eines Bildes. Im Beispiel gemäß Fig. 10 gespeichert sind ein Bildformatidentifizierer, der den Namen eines Bildformats beschreibt, eine Dateigröße, die Breite, Höhe und Tiefe eines Bildes, Informationen, ob Daten komprimiert sind, eine Auflösung, der Versatz für einen Bilddatenspeicherort, die Größe einer Farbpalette und so weiter. Bilddaten werden sequentiell im Bilddatenabschnitt gespeichert.

[0194] Typische Beispiele derartiger Bildformate sind das BMP-Format von Microsoft und das GIF-Format von CompuServe.

[Erläuterung des Dateiformats]

[0195] Gemäß dem folgenden Dateiformat werden Eigenschaftsinformationen, gespeichert im Bildkopfabschnitt, und die Bilddaten, gespeichert im Bilddatenabschnitt, neu angeordnet, um einer Struktur besser zu entsprechen, und werden dann in der Datei gespeichert. Eine strukturierte Bilddatei ist in den Fig. 11 und Fig. 12 gezeigt.

[0196] Auf die individuellen Eigenschaften und die Daten in der Datei wird als Speicherbereiche und Ströme zugegriffen, die den Dateiverzeichnissen und den Dateien von MS-DOS entsprechen.

[0197] In den Fig. 11 und Fig. 12 sind die schattierten Abschnitte Speicherbereiche, und nicht schattierte Bereiche sind Ströme. Bilddaten und Bildeigenschaftsinformationen werden in den Strömen gespeichert.

[0198] In Fig. 11 sind die Bilddaten hierarchisch entsprechend deren unterschiedlicher Auflösung angeordnet, mit einem Bild für jede Auflösung, das Unterbild genannt wird und durch eine Auflösung 0, 1,... oder n dargestellt wird. Für ein Bild für jede Auflösung ist die Information, die zum Lesen der Bilddaten erforderlich ist, im Unterbildkopfbereich gespeichert, und die Bilddaten sind in einem Unterbilddatenbereich gespeichert.

[0199] Die Eigentumssätze, die aus den Eigenschaftsinformationen aufgebaut sind, die festgelegt sind durch deren Sortierung in Übereinstimmung mit dem Nutzungszweck und ihren Inhalten, umfassen Summary Info. Property Sets, Image Info. Property Sets, Image Content Property Sets und Extension List Property Sets.

[Erläuterung für jeden Eigentumssatz]

[0200] Ein Summary Info. Property Set ist kein inhärenter Teil dieses Dateiformats, sondern ist erforderlich zum Speichern des Titels, des Namens und des Autors einer Datei und eines Thumb-Nail-Bildes.

[0201] Eine allgemeine Information bezüglich einer Speichereinheit (Speicherung) ist im Com Obj. Stream gespeichert.

[0202] Image Content Property Set ist eine Eigenschaft zum Beschreiben eines Speicherverfahrens, das für Bilddaten verwendet wird (siehe Fig. 13). Für diese Eigenschaft vorgesehen ist die Zählung der Ebenen von Bilddaten, die Breite und Höhe eines Bildes bei maximaler Auflösung, die Breite, die Höhe und die Farbe eines Bildes bei jeder Auflösung, und die Festlegung der Quantisierungstabelle einer Huffman-Tabelle, die für die JPEG-Kompression verwendet wird.

[0203] Extension List Property Set ist ein Bereich, der verwendet wird zum Hinzufügen einer Information, die in der Grundspezifikation des obigen Dateiformats nicht enthalten ist.

[0204] In einem ICC Profile-Bereich ist ein spezielles ICC-Umsetzprofil (International Color Consortium) für die räumliche Farbumsetzung beschrieben.

[0205] Im Image Info. Property Set gespeichert sind verschiedene Arten von Informationen, die für Bilddaten verwendet werden können. Beispielsweise können die folgenden Informationsarten beschreiben, wie ein Bild aufgenommen und verwendet werden kann:

– Information bezüglich eines Aufnahmeverfahrens oder eines allgemeinen Verfahrens für Digitaldaten;
– Information bezüglich Copyright;
– Information bezüglich der Inhalte eines Bildes (eine Person oder eine Szene in einem Bild)
– Information bezüglich einer Kamera, die zum Aufnehmen eines Fotos verwendet wird;
– Information bezüglich Einstellungen, die für eine Kamera verwendet werden (Belichtung, Belichtungszeit, Entfernung, Blitzverwendung und so weiter);
– Information bezüglich einer Auflösung für eine Digitalkamera oder einen Mosaikfilter;
– Information bezüglich Namen des Filmherstellers und Namen und Art des Films (negativ/positiv, Farbe/monochrom); Information bezüglich Art und Größe, wenn das Original ein Buch oder eine andere Drucksache ist; und
– Information bezüglich Scanner und Softwareanwendung, die zum Abtasten eines Bildes verwendet werden, und Bedienperson.

[0206] In Fig. 12 gezeigt ist eine Bilddatei, in der ein Sehparameter, der verwendet wird zur Anzeige eines Bildes, und Bilddaten gemeinsam gespeichert sind. Der Sehparameter ist ein Satz von Koeffizienten, die zur Verwendung gespeichert sind, wenn eine Drehung, Vergrößerung/Verkleinerung, Verschiebung, Bildumsetzung und Filterverarbeitung für ein angezeigtes Bild eingestellt werden.

[0207] In Fig. 12 ist in einen Global Info. Property Set-Bereich eine Liste verschlossener Eigenschaften geschrieben, beispielsweise ein Index für ein Maximalbild, ein Index für den am meisten geänderten Punkt und Informationen bezüglich der Person, die die letzte Korrektur ausgeführt hat.

[0208] Source/Result FlashPix Image Object bildet des weiteren die Grundlage der Bilddaten, aber ist hingegen Source FlashPix Image Object erforderlich, dann ist Result FlashPix Image Object optimal. Originalbilddaten werden im Bereich Source FlashPix Image Object gespeichert, und Bilddaten, gewonnen durch Bildverarbeitung unter Verwendung des Sehparameters, werden im Result FlashPix Image Object-Bereich gespeichert.

[0209] Source/Result Desc. Property Set ist ein Eigentumssatz, der verwendet wird zum Identifizieren der obigen Bilddaten. Eine Bild-ID, ein Eigentumssatz, für den Änderungen gesperrt sind, und die Daten und die Zeit der letzten Aktualisierung werden in diesem Bereich gespeichert.

[0210] In einem Bereich Transform Property Set werden ein affiner Umsetzkoeffizient zur Verwendung von Drehung, Vergrößerung/Verkleinerung und zum Verschieben eines Bildes, eine Farbumsetzmatrix, ein Kontrasteinstellwert und ein Filterkoeffizient gespeichert.

[Erläuterung, wie Bilddaten zu handhaben sind]

[0211] Für die Erläuterung verwendet wird ein Bildformat, das eine Vielzahl von Bildern mit unterschiedlichen Auflösung enthält, die erzielt werden durch Unterteilung der Bilddaten in eine Vielzahl von Kacheln.

[0212] In Fig. 14 gezeigt ist ein Beispiel von Bilddaten, das aufgebaut ist aus einer Vielzahl von Bildern mit unterschiedlichen Auflösungen. In Fig. 14 besteht ein Bild mit der höchsten Auflösung aus X0 Spalten × Y0 Zeilen, und ein Bild mit nächst höherer Auflösung besteht aus X0/2 Spalten × Y0/2 Zeilen. Die Anzahl von Spalten und die Anzahl von Zeilen wird sequentiell um 1/2 verringert, bis die Spalten und Zeilen gleich oder kleiner als 64 Pixel sind, oder bis die Spalten und Zeilen einander gleichen.

[0213] Als Ergebnis der Schichtung von Bilddaten ist die Anzahl von Ebenen in einer Bilddatei die Bildeigenschaftsinformation erforderlich, und die Kopfteilinformation und die Bilddaten, die für das allgemeine Bildformat erläutert worden sind, sind für ein Bild in jeder Ebene erforderlich (siehe Fig. 10). Die Anzahl von Ebenen in einer Bilddatei, die Breite und Höhe des Bildes bei dessen maximaler Auflösung, die Breite, die Höhe und die Farbe des Bildes mit einer individuellen Auflösung, und ein Kompressionsverfahren werden im Bereich Image Content Property Set gespeichert (siehe Fig. 13).

[0214] Das Bild an der Ebene bei jeder Auflösung wird unterteilt in Kacheln, die jeweils 64 × 64 Pixel haben, wie in Fig. 15 gezeigt. Wenn ein Bild beginnend mit dem linken oberen Abschnitt unterteilt wird in Kacheln von 64 × 64 Pixeln, dann kann ein Leerraum in einem Teil einer Kachel an der rechten Kante oder an der unteren Kante auftreten. In diesem Falle wird das rechteste Bild oder das unterste Bild wiederholt eingefügt, um eine Kachel von 64 × 64 Pixel zu bilden.

[0215] In diesem FlashPixTM-Format werden Bild-

daten für individuelle Kacheln unter Verwendung entweder der JPEG-Kompression oder des Einzelfarb- oder eines Nichtkompressionsverfahrens gespeichert. Die JPEG-Kompression ist eine Bildkompressionstechnik, die international standardisiert ist durch ISO/IEC JTC1/SC29, und somit wird eine Erläuterung dieser Technik hier nicht gegeben. Das Einzelfarbverfahren ist eine Technik, bei der im Falle, daß eine Kachel vollständig von Pixeln mit derselben Farbe aufgebaut ist, die Kachel als Einzelfarbe ohne individuell aufgezeichnete Pixelwerte ausgedrückt wird. Dieses Verfahren ist insbesondere effektiv für Bilder, die nicht unter Verwendung von Computergraphiken erzeugt werden.

[0216] Die Bilddaten, die solchermaßen in Kacheln unterteilt sind, werden beispielsweise im Unterbilddatenstrom in Fig. 11 gespeichert, und die Gesamtzahl der Kacheln, die Größe der individuellen Kacheln, der Ort, an dem die Daten beginnen, und das Datenkompressionsverfahren werden im Bereich Subimage Header gespeichert (siehe Fig. 16).

[0217] Im ersten und zweiten Ausführungsbeispiel kann die elektronische Wasserzeicheninformation unter Verwendung verschiedener Verfahren eingebettet werden.

[0218] Die erste bis dritte Verschlüsselung können ebenfalls realisiert werden unter Verwendung verschiedener Verfahren, wie ein Verschlüsselungssystem zum Ändern der Bitanordnung in Übereinstimmung mit dem Verschlüsselungscode.

[0219] Darüber hinaus können ein Tabelleneintragssuchwert und die Signatur vorgesehen werden für alle Daten, die zu senden sind.

[0220] In diesen Ausführungsbeispielen werden die ersten Verschlüsselung bis zur dritten Verschlüsselung während des elektronischen Wasserzeicheninformations-Einbettungsprozesses ausgeführt, um eine dritte Partei daran zu hindern, die beim Server, beim Nutzer und bei der Agentur gespeicherte Information erlangen.

[0221] DES-Verschlüsselung (Data Encryption Standard Verschlüsselung) oder eine Tabelleneintragssuchfunktion können jedoch verwendet werden, um Anzapfungen und Änderungen der Daten über einen Übertragungsweg von einer dritten Partei zu vermeiden.

[0222] Im ersten und im zweiten Ausführungsbeispiel wird des weiteren der Server (oder der Autor) mit der Feststellung der rechtswidrigen Datenverteilung beauftragt. Sofern jedoch ein elektronisches Wasserzeichenauslesemittel vorgesehen ist, kann ein Nutzer eine rechtswidrige Datenverteilung und die Nutzerinformation feststellen, die rechtswidrige verteilt wurde, obwohl der Nutzer den Geheimschlüssel für die erste Verschlüsselung oder für die zweite Verschlüsselung nicht kennt. wenn der Fall rechtswidriger Datenverteilung festgestellt ist, muß der Nutzer nur dem Server den begonnenen Nachweisvorgang mitteilen. Der Prozeß des Feststellens rechtswidriger Verteilungen ist folglich nicht auf den Server beschränkt.

[0223] Der Server kann in die Bilddaten nicht nur die Nutzerinformation U, sondern auch andere notwendige Informationen einbetten, wie beispielsweise Copyright-Informationen und Informationen bezüglich der Bilddatenverteilungsumstände. Um die Geheiminformation einzubetten, müssen der Server oder die Agentur darüber hinaus nur den Einbettungsprozeß aus, der der ersten Verschlüsselung folgt, so dass zusätzlich zur Signaturinformation die Information in den Bilddaten eingebettet werden kann, die durch die erste Verschlüsselung betroffen ist. Die Nutzerinformation U wird nicht immer vor der ersten Verschlüsselung eingebettet, sondern kann auch nach der erste Verschlüsselung eingebettet werden (in diesem Falle kann die Feststellung der Nutzerinformation U nur vom Server, der Agentur oder von einer Person ausgeführt werden, die den Geheimschlüssel kennt, der für die erste Verschlüsselung verwendet wird).

[0224] Wenn der Nutzer eine zweite Dateneinheit ist, die einen Drucker oder ein Endgerät gemeinsam verwendet, können die Signaturinformation des Nutzers und die zweite Verschlüsselung die Signaturinformation und das Verschlüsselungssystem für den Drucker oder das Endgerät enthalten, die gemeinsam benutzt werden.

[0225] Die erste Verschlüsselungsinformation des Servers (oder des Autors) kann weitestgehend über das Netzwerk oder unter Verwendung einer CD-ROM verteilt werden, selbst ohne eine vom Nutzer angeforderte Verteilung auf der Grundlage der Kontraktinformation.

[0226] Die Signaturinformation S für den Nutzer wird nicht notwendigerweise vom öffentlichen Verschlüsselungsverfahren erzeugt, sondern kann auch eine Information sein (beispielsweise eine Codenummer), die der Nutzer auf der Grundlage der Kontraktinformation festlegt.

[0227] Zum Verwenden der Verschlüsselung für 40 Bits oder mehr ist in den Vereinigten Staaten ein Schlüsselverwaltungsbüro zum Verwalten eines Verschlüsselungscodes erforderlich, um die nicht autorisierte Verwendung der Verschlüsselung zu vermeiden. Das Nachweisbüro **30** kann folglich auch als Schlüsselverwaltungsbüro dienen. Und wenn das Nachweisbüro **30** Vorausverwaltung des zweiten Verschlüsselungscodes vorsieht, kann das Nachweisbüro **30** selbst die Nachweisprozesse 1) bis 3)

durch Überwachen eines rechtswidrigen Bildes ausführen. Der erste Verschlüsselungscode des Servers kann entweder von demselben Nachweisbüro oder von einem anderen Codeverwaltungsbüro verwaltet werden. Und die Schlüssel des Servers und des Nutzers können von dem Schlüsselverwaltungsbüro erzeugt und verteilt werden.

[0228] Anstelle einer Einzelagentur kann darüber hinaus eine Vielzahl von Agenturen hierarchisch strukturiert vorgesehen sein. In diesem Falle kann eine spezielle Agentur der hierarchischen Struktur die Verarbeitung der beauftragten Agentur ausführen, oder die individuellen Agenturen können das Protokoll zum Spezifizieren einer beauftragten Agentur aus.

[0229] Nach Empfang einer Anforderung in diesen Ausführungsbeispielen ist der Server (oder der Autor) verantwortlich für das Senden der ersten Verschlüsselungsdaten E1(G) oder E1(G + M) der Originaldaten an die Agentur. Der Server kann jedoch die Daten E1(G) oder E1(G + M) im voraus an die Agentur senden.

[0230] Das dritte Verschlüsselungsverfahren der Agentur berührt die Bilddaten G_W nicht, die letztlich erzielt werden. Die Bilddaten G_W können jedoch von der dritten Verschlüsselung durch den Vorgang beeinflußt werden, wodurch die Nutzerinformation U nach der dritten Verschlüsselung eingebettet wird oder wodurch die Signaturinformation S nach der dritten Verschlüsselung eingebettet wird.

[0231] Das Ziel der vorliegenden Erfindung kann erreicht werden, wenn ein Speichermedium, auf dem als Softwareprogrammcode die Schritte zum Realisieren der Funktionen vom Host und der Endgeräte im ersten und zweiten Ausführungsbeispiel gespeichert sind, an ein System oder an die Vorrichtung des Servers, der Agentur oder des Nutzers geliefert wird, und wenn der Computer (oder eine CPU oder eine MPU) im System oder in der Vorrichtung die Schritte durch Lesen des Programmcodes ausführen kann, der auf dem Speichermedium gespeichert ist.

[0232] In diesem Falle wird der aus dem Speichermedium gelesene Programmcode verwendet zum Realisieren der Funktionen der oben beschriebenen Ausführungsbeispiele. Das Speichermedium, auf dem der Programmcode gespeichert ist, bildet die vorliegende Erfindung.

[0233] Ein Speichermedium zum Liefern eines solchen Programmcodes kann beispielsweise ein ROM, eine Diskette, eine Festplatte, eine optische Platte, eine magnetooptische Platte, eine CD-ROM, eine CD-R, ein Magnetband oder eine nichtflüchtige Speicherkarte sein.

[0234] Darüber hinaus enthält der Umfang der vorliegenden Erfindung nicht nur einen Fall, bei dem die Funktionen des ersten und zweiten Ausführungsbeispiels realisiert werden, wenn der Programmcode gelesen und von einem Computer ausgeführt wird, sondern auch einen Fall, bei dem entsprechend einem Befehl, der im Programmcode enthalten ist, die Funktionen der obigen Ausführungsbeispiele realisiert werden, wenn ein Betriebssystem, das auf dem Computer läuft, einen Teil oder die gesamte aktuelle Verarbeitung ausführt.

[0235] Des weiteren umfaßt die vorliegende Erfindung einen Fall, bei dem Programmcodes, gelesen aus einem Speichermedium, in einen Speicher geschrieben werden, der auf eine Funktionserweiterungskarte gesteckt ist, die in den Computer eingeführt wird, oder auf einer Funktionserweiterungseinheit, die mit einem Computer verbunden ist, und in Übereinstimmung mit den Programmcodebefehlen führt eine CPU, montiert auf die Funktionserweiterungskarte oder auf die Funktionserweiterungseinheit, einen Teil oder die gesamte aktuelle Verarbeitung aus, um die Funktionen zu realisieren, die im ersten bis dritten Ausführungsbeispiel enthalten sind.

[0236] Wie zuvor gemäß dem ersten und zweiten Ausführungsbeispiel beschrieben, kann die Information bezüglich der dritten Dateneinheit (der Nutzer) von der zweiten Dateneinheit (Agentur) eingebettet werden. In diesem Falle kann die dritte Dateneinheit keine rechtswidrige Tat begehen. Die zweite Dateneinheit kann des weiteren nicht direkt in die Originaldateninformation (Nutzerinformation U oder Signaturinformation S) bezüglich der dritten Dateneinheit eingebettet werden, weil diese Information von einem Verschlüsselungsgerät berührt wird (die erste Verschlüsselung und die Verschlüsselung, die das erste Verschlüsselungsmittel verwendet), die nur die erste Dateneinheit (der Server oder der Autor) kennt, oder von einem Verschlüsselungsgerät (die zweite Verschlüsselung und die Verschlüsselung, die die zweite Verschlüsselung anwendet), die nur die dritte Dateneinheit kennt.

[0237] Eine rechtswidrige Datenverteilung kann in einem hierarchisch strukturierten Netzwerk folglich verhindert werden, und ein sicheres System kann bereitgestellt werden. Des weiteren kann die Anonymität des Nutzers leicht realisiert werden.

[0238] Nachstehend anhand Fig. 17 beschrieben ist ein weiteres Beispiel.

[0239] Ein elektronisches Wasserzeichenverfahren wird beispielsweise in einem in Fig. 17 gezeigten System **100** ausgeführt.

[0240] Genauer gesagt, das System **100** ist ein Netzwerksystem, das aus mehreren Dateneinheiten

(nicht dargestellt) aufgebaut ist, die ein Endgerät **10** auf der Seite einer ersten Dateneinheit (nachstehend als erstes Endgerät bezeichnet), ein Endgerät **20** auf der Seite der zweiten Dateneinheit (nachstehend als zweites Endgerät bezeichnet) und ein Endgerät **30** auf der Seite eines Nachweisbüros (nachstehend als Nachweisendgerät bezeichnet) beinhalten. Die individuellen Dateneinheiten tauschen über das Netzwerk Digitaldaten aus.

[0241] Das erste Endgerät **10** ist aufgebaut mit: einer Kontraktidentifizierungseinheit **11** zum Aufnehmen von Daten aus dem zweiten Endgerät **20**; einer elektronischen Wasserzeicheneinbettungseinheit **12** zum Aufnehmen beispielsweise des Ausgangssignals von der Kontraktidentifizierungseinheit **11** und von Bilddaten (Digitaldaten); einer ersten Verschlüsselungseinheit **13** zum Aufnehmen des Ausgangssignals aus der elektronischen Wasserzeicheneinbettungseinheit **12**; und mit einer ersten Entschlüsselungseinheit **14** zum Aufnehmen von Daten aus dem zweiten Endgerät **20**. Die Daten für die erste Verschlüsselungseinheit **13** und die erste Entschlüsselungseinheit **14** werden an das zweite Endgerät **20** gesandt.

[0242] Das zweite Endgerät **20** verfügt über: einen Kontraktgenerator **21** zum Senden von Daten an die Kontraktidentifizierungseinheit **11** vom ersten Endgerät **10**; einen Signaturgenerator **22**; eine elektronische Wasserzeicheneinbettungseinheit **23** zum Aufnehmen von Daten aus dem Signaturgenerator **22** und aus der ersten Verschlüsselungseinheit **13** des ersten Endgeräts **10**; eine zweite Verschlüsselungseinheit **24** zum Aufnehmen von Daten aus der elektronischen Wasserzeicheneinbettungseinheit **23**; und über eine zweite Entschlüsselungseinheit **25** zum Aufnehmen der Daten aus der ersten Entschlüsselungseinheit **14** des ersten Endgeräts **10**. Die Daten aus der zweiten Entschlüsselungseinheit **25** werden als Bilddaten mit einem elektronischen Wasserzeichen abgegeben. Die Daten aus der zweiten Verschlüsselungseinheit **24** werden an die erste Entschlüsselungseinheit **14** vom ersten Endgerät **10** und zum Nachweisendgerät **30** gesandt.

[0243] Das Nachweisendgerät **30** verfügt über: eine zweite Entschlüsselungseinheit **31** zum Aufnehmen von Daten aus der zweiten Verschlüsselungseinheit **24** vom zweiten Endgerät **20**; und über eine elektronische Wasserzeichenidentifizierungseinheit **32** zum Aufnehmen von Daten aus der zweiten Entschlüsselungseinheit **31**. Die Daten aus der elektronischen Wasserzeichenidentifizierungseinheit **32** werden an das erste Endgerät **10** und an das zweite Endgerät **20** gesandt, und die Daten aus der zweiten Entschlüsselungseinheit **31** werden an die erste Entschlüsselungseinheit **14** vom ersten Endgerät **10** gesandt.

[0244] Im solchermaßen eingerichteten elektronischen Informationsverteilungssystem nach diesem Beispiel wird die Einbettungsverarbeitung sortiert in einen ersten Einbettungsprozeß zum Senden von Digitaldaten aus den Servern oder den Autoren an die in Fig. 4 oder in Fig. 5 gezeigte Agentur, und in einen zweiten Einbettungsprozeß zum Senden von Digitaldaten der Agentur an die Nutzer. In diesem Beispiel ist das folgende Protokoll dasselbe wie dasjenige, das im ersten und im zweiten Einbettungsprozeß verwendet wird. Ingesamt wird der erste Einbettungsprozeß zuerst ausgeführt, und dann folgt der zweite Einbettungsprozeß.

[0245] In der folgenden Erläuterung für den ersten Einbettungsprozeß bedeutet die erste Dateneinheit einen Server oder einen Autor, und die zweite Dateneinheit bedeutet eine Agentur. Für den zweiten Einbettungsprozeß bedeutet die erste Dateneinheit die Agentur, und die zweite Dateneinheit bedeutet einen Nutzer. Zumindest das Endgerät, das die Agentur verwendet, enthält folglich alle Prozessoren, die für das erste Endgerät **10** und für das zweite Endgerät **20** in Fig. 17 vorgesehen sind.

[0246] Ein spezielles Protokoll z um Ausführen des ersten und des zweiten Einbettungsprozesses ist nachstehend anhand Fig. 17 beschrieben. Gemäß diesem Protokoll ist eine Information bezüglich der ersten Verschlüsselung, wie das Verfahren und ein Geheimschlüssel, nur für die erste Dateneinheit verfügbar, und eine Information bezüglich der zweiten Verschlüsselung ist nur für die zweite Dateneinheit verfügbar. Angemerkt sei jedoch, dass für diese Verschlüsselungsprozesse ein Eigentumsrecht besteht, das, ungeachtet wessen Verschlüsselungsprozeß zuerst ausgeführt wird, die verschlüsselten Daten entschlüsseln kann. Angemerkt sei jedoch, daß für diese Verschlüsselungsprozesse ein Eigentum darin besteht, daß ungeachtet der Tatsache, welcher Verschlüsselungsvorgang als erstes ausgeführt wird, die verschlüsselten Daten entschlüsselt werden können. Hiernach wird der Verschlüsselungsprozeß dargestellt durch "Ei()", der Entschlüsselungsprozeß wird dargestellt durch "Di()", und der Einbettungsprozeß bezüglich des elektronischen Wasserzeichens wird dargestellt durch "+".

[0247] Die von einem solchermaßen eingerichteten System **100** ausgeführte Verarbeitung ist nachstehend beschrieben. Eine Erläuterung wird zunächst für die elektronische Wasserzeicheneinbettungsbearbeitung gegeben.

[Einbettungsprozeß]

1) Zuerst fordert die zweite Dateneinheit vom zweiten Endgerät **20** aus dem ersten Endgerät **10** (erste Dateneinheit) gewünschte Bilddaten an, die die Signatur tragen. Die angeforderten Daten sind

eine Signaturinformation, die der Kontraktgenerator **21** erzeugt und die nachstehend Kontraktinformation genannt wird.

2) In der ersten Dateneinheit vom ersten Endgerät **10** verwendet die Kontraktidentifizierungseinheit **11** die Signatur der zweiten Dateneinheit zum Identifizieren der empfangenen Kontraktinformation und bereitet dann die Nutzerinformation U unter Verwendung der Kontraktinformation auf. Die elektronische Wasserzeicheneinbettungseinheit **12** bettet die angeforderten Bilddaten G der Nutzerinformation U ein, die die Kontraktidentifizierungseinheit **11** aufbereitet hat. Die erste Verschlüsselungseinheit **13** führt die erste Verschlüsselung E1() für die Daten (G + U) aus, wobei die Nutzerinformation U von der elektronischen Wasserzeicheneinbettungseinheit **12** eingebettet worden ist, und sendet die gewonnenen Daten an das zweite Endgerät **20**. Das zweite Endgerät **20** empfängt folglich die ersten verschlüsselten Bilddaten E1(G + U).

3) Im zweiten Endgerät **20** erzeugt der Signaturgenerator **22** eine Signaturinformation S unter Verwendung des Geheimschlüssels der zweiten Dateneinheit. Die elektronische Wasserzeicheneinbettungseinheit bettet die Signaturinformation S ein, die der Signaturgenerator **22** erzeugt hat, und zwar in die ersten verschlüsselten Bilddaten E1(G + U), die gesendet (verteilt) wurden vom ersten Endgerät **10**. Die zweite Verschlüsselungseinheit **24** führt die zweite Verschlüsselung für die ersten verschlüsselten Bilddaten E1(G + U) + S aus, wobei die Signaturinformation S von der elektronischen Wasserzeicheneinbettungseinheit **23** eingebettet worden ist. Die gewonnenen Bilddaten werden dann an das Nachweisendgerät **30** gesandt. Das Nachweisendgerät **30** empfängt folglich die zweiten verschlüsselten Bilddaten E2(E1(G + U) + S).

[0248] Die zweite Verschlüsselungseinheit **24** erzeugt einen Tabellennachtragssuchwert H2 für die zweiten verschlüsselten Bilddaten E2(E1(G + U) + S), die das Nachweisbüro **30** gesendet hat. Die zweite Verschlüsselungseinheit **24** stellt dann eine Signatur für den Tabelleneintragssuchwert H2 bereit und akzeptiert die Signaturinformation S und den zweiten Verschlüsselungsgeheimcode, sendet diesen an das Nachweisbüro **30**, begleitet von einer Geheiminformation bezüglich des elektronischen Wasserzeichens. Die Geheiminformation bildet die Information, die sich auf die Einbettungsposition und die Stärke bezieht, die erforderlich ist zum Feststellen eines elektronischen Wasserzeichens, und verschlüsselt ist unter Verwendung eines anderen Verschlüsselungsverfahrens, das mit dem Nachweisendgerät **30** gemeinsam genutzt wird.

[0249] Der Tabelleneintragssuchwert ist ein solcher, der gewonnen wird durch Berechnen der Tabelleneintragssuchfunktion h(), und die Tabelleneintragssuchfunktion ist eine Kompressionsfunktion, die selten zu einer Kollision führt. Eine Kollision in diesem Falle würde bedeuten, daß für die unterschiedlichen Werte x1 und x2 dann h(x1) = h(x2) ist. Die Kompressionsfunktion ist eine solche zum Umsetzen einer Bitkette mit einer spezifischen Bitlänge in eine Bitkette mit veränderter Bitlänge. Folglich ist die Tabelleneintragssuchfunktion h() eine solche, durch die eine Bitkette mit spezifischer Bitlänge umgesetzt wird in eine Bitkette veränderter Bitlänge, und für die Werte x1 und x2 nicht gefunden werden, die der Beziehung h(x1) = h(x2) genügen. Da Wert x, der der Beziehung y = h(x) genügt, nicht leicht für einen beliebigen Wert y gefunden wird, ist die Tabelleneintragssuchfunktion eine Unidirektionalfunktion. Spezielle Beispiele der Tabelleneintragssuchfunktion sind ein MD (Message Digest) 5 oder ein SHA (Secure Hash Algorithm).

4) Das Nachweisendgerät **30** identifiziert die Signatur, die begleitet ist vom Tabelleneintragssuchwert H2, der vom zweiten Endgerät **20** kommt, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten paßt. Nach Bestätigung der Anpassung verschlüsselt die zweite Verschlüsselungseinheit **31** die zweiten Verschlüsselungsbilddaten E2(E1(G + U) + S), die vom zweiten Endgerät **20** kommen, und liest die Signaturinformation S daraus aus. Die elektronische Wasserzeichenidentifizierungseinheit **32** überprüft die Signaturinformation S, und wenn die Signaturinformation S korrekt ist, wird die Nachweisinformation aufbereitet unter Verwendung der Signatur für das Nachweisbüro **30**. Letztlich sendet das Nachweisbüro **30** die zweiten verschlüsselten Bilddaten E2(E1(G + U) + S) und den Tabelleneintragssuchwert H2 und dessen begleitende Signatur an das erste Endgerät **10**, wobei alles vom zweiten Endgerät **20** empfangen wird, und die Nachweisinformation für diese und deren Signatur.

5) Die erste Dateneinheit im ersten Endgerät **10** identifiziert die Nachweisinformation und die begleitende Signatur, empfangen aus dem Nachweisendgerät **30**, und auch die zweiten verschlüsselten Bilddaten E2(E1(G + U) + S) sowie den Tabelleneintragssuchwert H2 und die begleitende Signatur. Nach Abschluß dieses Bestätigungsprozesses entschlüsselt die erste Entschlüsselungseinheit **14** den ersten verschlüsselten Abschnitt der zweiten verschlüsselten Bilddaten E2(E1(G + U) + S), um die Bilddaten E2(G + U) + D1(E2(S)) zu erhalten, die wiederum an das zweite Endgerät **20** gesandt werden.

6) Die zweite Entschlüsselungseinheit **25** im zweiten Endgerät **20** entschlüsselt den zweiten verschlüsselten Abschnitt der Bilddaten E2(G + U + D1(E2(S)) aus dem ersten Endgerät **10** und liest Bilddaten G_W aus, in die das elektronische Wasserzeichen eingebettet ist. Die Bilddaten G_W, die das elektronische Wasserzeichen enthalten, wer-

den folglich dargestellt mit $G_W = G + U + D1(S)$. Das bedeutet, daß die Nutzerinformation U und die Signaturinformation S für die zweite Dateneinheit, die von der ersten Entschlüsselung betroffen sind, als elektronische Information in die Originalbilddaten eingebettet sind.

[0250] Wenn das Nachweisendgerät **30** in Prozedur 4) die elektronische Wasserzeicheninformation nicht nachweist, weil entweder die erste oder die zweite Dateneinheit eine rechtswidrige Tat begangen hat, werden die Meldungen auf diese Wirkung an das erste und das zweite Endgerät **10** beziehungsweise 20 gesandt. Wenn der Handel zu dieser Zeit angehalten wird, obwohl die erste Dateneinheit den Preis der Daten nicht erhalten kann, kann vermieden werden, daß zur selben Zeit die Bilddaten von einer zweiten Dateneinheit rechtswidrig gewonnen werden; oder obwohl die zweite Dateneinheit die Bilddaten nicht bekommen kann, ist zur selben Zeit der Preis der Daten für die erste Dateneinheit nicht zu zahlen. Da weder die erste noch die zweite Dateneinheit einen Gewinn oder Verlust erfährt, ist das Begehen einer rechtswidrigen Tat sinnlos.

[0251] Wenn insbesondere der elektronische Wasserzeicheneinbettungsprozeß ausgeführt wird, wird im ersten Einbettungsprozeß die Agentur, die die zweite Dateneinheit bildet, Bilddaten G_W bekommen, die ein elektronisches Wasserzeichen enthalten, das aufbereitet ist durch Einbetten der eigenen Signaturinformation S in die Originaldaten G aus dem Server oder durch den Autor, der die erste Dateneinheit bildet. Angemerkt sei, daß wenn die Nutzerinformation und die Signaturinformation für den ersten Einbettungsprozeß U1 beziehungsweise S1 sind, die Bilddaten G_W, die das elektronische Wasserzeichen enthalten, das die Agentur erhält, gleich $G_W = G + U1 + D1(S1)$ ist.

[0252] Diesem folgend wird der zweite Einbettungsprozeß in derselben Weise ausgeführt (die Agentur ist die erste Dateneinheit), während die Bilddaten G_W, die ein elektronisches Wasserzeichen enthalten, das gewonnen wird von der Agentur, als Originalbild verwendet werden. Der Nutzer, der als zweite Dateneinheit dient, kann dann die Bilddaten erhalten, die ein elektronisches Wasserzeichen enthalten, $G_{WW} = G + U1 + D1(S1) + U2 + D3(S2)$. Die Nutzerinformation und die Signaturinformation im zweiten Einbettungsprozeß sind U2 beziehungsweise S2, und die von der Agentur ausgeführte Verschlüsselung wird dargestellt mit E3(), während die Entschlüsselung mit D3() dargestellt wird.

[0253] Wenn eine rechtswidrige Kopie (rechtswidrige Bilder) entdeckt wird, kann die Partei, die die rechtswidrige Tat begangen hat, leicht identifiziert werden durch Ausführen folgenden einfachen Nachweisprozesses. Dieser Nachweisprozeß wird unterteilt in einen ersten Nachweisprozeß, der dem ersten Einbettungsprozeß entspricht und den der Server oder der Autor der Agentur ausführt, und ein zweiter Nachweisprozeß, der dem zweiten Einbettungsprozeß entspricht und den die Agentur und der Nutzer ausführen. Der erste Nachweisprozeß wird zuerst ausgeführt, und dann wird der zweite Nachweisprozeß ausgeführt.

[0254] Im ersten Nachweisprozeß werden die Nutzerinformation und die Signaturinformation U1 und S1 sowie die Verschlüsselung und Entschlüsselung von der Agentur ausgeführt mit E3() beziehungsweise D3(). Die Nutzerinformation und die Signaturinformation sind im zweiten Nachweisprozeß U2 beziehungsweise S2. Die Bilddaten werden von der Modifizierung und dem Löschen der elektronischen Wasserzeicheninformation nicht berührt.

[Nachweisprozeß]

1) Im ersten Nachweisprozeß liest die erste Dateneinheit vom ersten Endgerät **10** die Nutzerinformation U' aus den rechtswidrigen Bilddaten $G_W' = G + U' + D1(S')$, die entdeckt worden sind. Die erste Dateneinheit führt die erste Verschlüsselung für die rechtswidrigen Bilddaten G_W' aus und liest die Signaturinformation S' aus. Wird die Nutzerinformation U' nicht ausgelesen, dann wird ermittelt, daß die erste Dateneinheit die rechtswidrige Tat begangen hat.
2) wenn im ersten Nachweisprozeß (S' = S) die korrekte Signaturinformation S' aus dem ersten Nachweisprozeß ausgelesen ist, wird der zweite Nachweisprozeß initialisiert. Dieselbe Prozedur erfolgt im zweiten Nachweisprozeß. Wenn die korrekte Signaturinformation gefunden ist, wird ermittelt, daß die zweite Dateneinheit die rechtswidrige Tat begangen hat. Dies liegt daran, daß nur die zweite Dateneinheit die korrekte Signaturinformation wie die erste Dateneinheit aufbereiten konnte, die keine Kenntnis über die korrekte Signaturinformation hat.
3) Wird die korrekte Signaturinformation nicht ausgelesen ($S' \neq S$), dann wird ermittelt, daß die erste Dateneinheit die rechtswidrige Tat begangen hat.

[0255] Nach dem elektronischen Wasserzeichenverfahren gemäß dem vierten Ausführungsbeispiel werden Verschlüsselung von Digitaldaten und der Einbettungsprozeß für ein elektronisches Wasserzeichen vom ersten und vom zweiten Endgerät **10** beziehungsweise **20** ausgeführt, und die Verschlüsselung und die Identifizierung der korrekten elektronischen Wasserzeicheninformation werden vom Nachweisendgerät **30** ausgeführt. Selbst wenn die erste Dateneinheit oder die zweite Dateneinheit individuell eine rechtswidrige Kopie vorbereiten, kann die rechtswidrige Tat leicht festgestellt werden, und zu-

sätzlich kann das Verüben der rechtswidrigen Tat leicht identifiziert werden.

[0256] Da nach diesem Verfahren des weiteren das Nachweisbüro die Ergebnisse vom ersten Einbettungsprozeß überprüft, ist eine Kollusion nicht effektiv, so daß die Kollusion vom Server oder dem Autor mit der Agentur und dem Nutzer nicht auftreten würde. Selbst wenn eine solche Kollusion auftreten sollte, kann eine rechtswidrige Tat leicht festgestellt werden. Die Sicherheit des Prozesses ist auf der Grundlage der Voraussetzung eingerichtet, daß das Nachweisbüro vertrauenswürdig ist.

(Drittes Ausführungsbeispiel)

[0257] In der letzten Zeit wird die Übertragung von Geld über Netzwerke, eine Wertpapierübertragungsprozedur, die elektronischer Geldverkehr genannt wird, in Benutzung gekommen. Da mit der regulären Barzahlung der Name vom Eigentümer einer elektronischen Bargeldübertragung nicht identifiziert wird, ist die Anonymität gewahrt. Wenn die Wahrung der Anonymität nicht möglich wäre, könnte ein Verkäufer eines Produkts aus einer elektronischen Bargeldübertragungsinformation bezüglich einem Käufer die Produktnutzung erhalten, und die Privatsphäre vom Nutzer wäre nicht mehr geschützt. Der Schutz der Privatsphäre des Nutzers ist wichtig wie auch der Schutz für ein gewährtes Copyright für einen Schöpfer, der ein elektronisches Wasserzeichen verwendet.

[0258] Im dritten Ausführungsbeispiel ist folglich die Anonymität eines Nutzers für einen Käufer vorgesehen, und wenn eine rechtswidrige Tat, wie rechtswidriges Verteilen von Bildern, entdeckt wird, ist es möglich, einen unberechtigten Verteiler zu identifizieren, was der ursprüngliche Zweck eines elektronischen Wasserzeichens ist. Dies wird erreicht durch Anwenden beispielsweise eines Systems, wie es in Fig. 18 gezeigt ist.

[0259] Das System **200** hat dieselbe Struktur wie das System **100** für das Beispiel in Fig. 17, während eine anonyme öffentliche Schlüsselbescheinigung, die ausgegeben wird von einem Bescheinigungsbüro **40**, für ein zweites Endgerät vorgesehen ist.

[0260] Um die Signaturinformation zu berechtigen, wird eine Bescheinigung von einer Organisation ausgegeben, die sich Bescheinigungsbüro nennt, und einem öffentlichen Schlüssel hinzugefügt, der verwendet wird, wenn die Signaturinformation überprüft wird.

[0261] Ein Bescheinigungsbüro ist eine Organisation, die Bescheinigungen für öffentliche Schlüssel ausgibt, die für die Nutzer bestimmt sind, um die öffentliche Schlüsselberechtigung bereitzustellen, die in Übereinstimmung mit den Erfordernissen des öffentlichen Codeverschlüsselungssystems ist. Das heißt, ein Bescheinigungsbüro verwendet den eigenen Geheimschlüssel, um eine Signatur für den öffentlichen Schlüssel des Nutzers bereitzustellen, oder für Daten bezüglich dem Nutzer, und zu diesem Zweck wird eine Bescheinigung vorbereitet und ausgegeben. Wenn ein Nutzer von einem anderen Nutzer eine Signatur erhält, die mit einer Bescheinigung versehen ist, überprüft der Nutzer die Bescheinigung unter Verwendung des öffentlichen Schlüssels des Bescheinigungsbüros, um die Berechtigung nachzuweisen, die der Nutzer bereitstellt, der den öffentlichen Schlüssel gesendet hat (oder wenigstens die Tatsache, daß die Berechtigung dem Nutzer vom Bescheinigungsbüro bereitgestellt wurde). Sowohl VeriSign als auch CyberTrust sind allgemein bekannte Organisationen, die solche Bescheinigungsbüros bedienen.

[0262] Wenn die Prozedur 2) vom zweiten Einbettungsprozeß in Fig. 17 als Beispiel eine Signatur zum Nachweisen der Kontraktinformation überprüft, die für einen Nutzer unterbreitet wurde, kann die Agentur den öffentlichen Schlüssel mit einer Signatur verwenden, die vom Bescheinigungsbüro **40** in Fig. 18 ausgegeben wurde. Da jedoch der Name vom Besitzer des öffentlichen Schlüssels im allgemeinen in die Bescheinigung geschrieben wird, ist die Nutzeranonymität zu den gekauften Zeitdaten nicht gegeben.

[0263] Wenn andererseits das Bescheinigungsbüro **40** die Korrespondenz der öffentlichen Schlüssel und ihrer Eigentümer geheimhält, kann der Name eines Besitzers nicht in eine Bescheinigung geschrieben werden, die als öffentlicher Schlüssel ausgegeben werden soll. Ein anonymes Zertifikat für einen öffentlichen Schlüssel wird nachstehend als "Bescheinigung über einen anonymen öffentlichen Schlüssel" bezeichnet, und ein öffentlicher Schlüssel, für den eine Bescheinigung bereitgestellt ist, wird ein "anonymer öffentlicher Schlüssel mit Bescheinigung" genannt. Wenn in der Prozedur 1) der oben beschriebenen zweiten Einbettungsverarbeitung ein Nutzer an einen Server nicht nur Kontraktinformation sondern auch eine Signatur für die Kontraktinformation und einen anonymen öffentlichen Schlüssel sendet, der von einer Bescheinigung begleitet ist, um die Überprüfung der Signaturinformation S zu ermöglichen, kann der Nutzer anonym bleiben, wenn Digitaldaten verkauft werden.

[0264] Der anonyme öffentliche Schlüssel, der von der Bescheinigung begleitet ist, wird an die Agentur als Information gesendet, die für den Nutzernachweis verwendet wird. Und wenn eine rechtswidrige Transaktion festgestellt wird und der Nutzer identifiziert werden muß, wird der anonyme öffentliche Schlüssel in Begleitung mit der Bescheinigung an das Bescheinigungsbüro **40** mit einer Anfrage nach dem Nutzer-

namen gesendet, der demjenigen des Besitzers vom öffentlichen Schlüssel entspricht. Wenn folglich die Prozeduren 1) und 2) im zweiten Einbettungsprozeß und Prozedur 1) im zweiten Nachweisprozeß in Fig. 8 als Beispiel folgendermaßen ausgeführt werden, kann die Anonymität eines Nutzers beim Kaufen digitaler Daten erhalten bleiben, wenn aber eine rechtswidrige Transaktion entdeckt wird, kann der Nutzer identifiziert werden, der für das Verüben der Transaktion verantwortlich ist.

[0265] Der Einbettungsprozeß und der Nachweisprozeß, den das System **200** in Fig. 18 ausübt, wird speziell beschrieben.

[Einbettungsprozeß]

1) Zunächst stellt im zweiten Endgerät **20** ein Kontraktgenerator **21** gewünschte Bilddaten für Kontraktinformation bereit, eine Signatur, die dem anonymen öffentlichen Schlüssel entspricht, begleitet von einer Bescheinigung, die das Bescheinigungsbüro **40** ausgegeben hat. Gemeinsam mit dem anonymen öffentlichen Schlüssel, der von der Bescheinigung begleitet ist, sendet das zweite Endgerät **20** die Kontraktinformation an das erste Endgerät **10**.
2) Im ersten Endgerät **10** überprüft eine Kontraktidentifizierungseinheit **11** den öffentlichen Schlüssel der zweiten Dateneinheit unter Verwendung des öffentlichen Schlüssels des Bescheinigungsbüros **40**. Die Kontraktidentifizierungseinheit **11** identifiziert die Signatur für die Kontraktinformation unter Verwendung des anonymen öffentlichen Schlüssels der zweiten Dateneinheit, und nachdem der Bestätigungsprozeß abgeschlossen ist, wird die Nutzerinformation unter Verwendung wenigstens entweder der Kontraktinformation oder vom anonymen Schlüssel aufbereitet. Eine elektronische Wasserzeicheneinbettungseinheit **12** bettet die Nutzerinformation U in die Bilddaten G ein, die die Kontraktidentifizierungseinheit **11** aufbereitet hat. Eine erste Verschlüsselungseinheit **13** führt die erste Verschlüsselung E1() für die Bilddaten G aus und sendet die gewonnenen Daten an das zweite Endgerät **20**. Das zweite Endgerät empfängt somit die ersten verschlüsselten Bilddaten E1(G + U).

[0266] Da die Prozeduren 3) bis 6) dieselben wie jene im Beispiel von Fig. 17 sind, wird hier keine weitere Erläuterung gegeben.

[Nachweisprozeß]

1) Im zweiten Nachweisprozeß liest das erste Endgerät **10** Nutzerinformationen aus den entdeckten rechtswidrigen Bilddaten G_{WW}' aus. Das erste Endgerät **10** führt des weiteren die erste Verschlüsselung für die rechtswidrigen Bilddaten G_{WW}' aus und liest daraus die Signaturinformation. Das erste Endgerät **10** liefert dann die ausgelesene Nutzerinformation und den anonymen öffentlichen Schlüssel, der aus der Kontraktinformation gewonnen wurde, an das Bescheinigungsbüro **40** und fordert den Namen der zweiten Dateneinheit an, der dem anonymen öffentlichen Schlüssel entspricht. Wird die Nutzerinformation nicht ermittelt, dann ist es sicher, daß die erste Dateneinheit eine rechtswidrige Tat begangen hat.

[0267] Die Prozeduren 2) und 3) sind dieselben wie im Beispiel von Fig. 17.

[0268] Wenn Digitaldaten gekauft werden, wie zuvor gemäß dem dritten Ausführungsbeispiel beschrieben, kann der Nutzer seine Anonymität bezüglich des Nachweisbüros aufrecht erhalten.

[0269] In einem in Fig. 19 gezeigten Beispiel wird eine Erläuterung für die Gesamtverarbeitung gegeben, wobei der Server oder der Autor in Fig. 4 oder in Fig. 5 Digitaldaten über die Agentur an den Nutzer verteilt.

[0270] Genauer gesagt, ein elektronisches Wasserzeichenverfahren wird vom System **300** ausgeführt, das in Fig. 19 gezeigt ist.

[0271] Das System **300** in Fig. 19 ist ein Netzwerksystem, das aus Mehrfachdateneinheiten (nicht dargestellt), die ein Endgerät **50** auf der Seite des Servers enthalten (nachstehend als Serverendgerät bezeichnet), einem Endgerät **60** auf der Seite der Agentur (wird nachstehend als Agenturendgerät bezeichnet), einem Endgerät **70** auf der Nutzerseite (wird nachstehend als Nutzerendgerät bezeichnet) und aus einem Endgerät **30** auf der Seite des Nachweisbüros (wird nachstehend als Nachweisendgerät bezeichnet) aufgebaut ist. Die individuellen Dateneinheiten tauschen Digitaldaten über das Netzwerk aus.

[0272] Das Serverendgerät **50** verfügt über: Eine erste Verschlüsselungseinheit **51** zum Aufnehmen beispielsweise von Bilddaten (Digitaldaten); und über eine erste Entschlüsselungseinheit **52** zum Aufnehmen von Daten aus dem Nutzerendgerät **70** und dem Nachweisendgerät **30**. Die Daten aus der ersten Verschlüsselungseinheit **51** werden an das Agenturendgerät **60** gesendet, und die Daten aus der ersten Entschlüsselungseinheit **52** werden an das Nutzerendgerät **70** gesendet.

[0273] Das Agenturendgerät **60** verfügt über: eine Kontraktidentifizierungseinheit **61** zum Aufnehmen von Daten aus dem Nutzerendgerät **70**; und über eine elektronische Wasserzeicheneinbettungseinheit **62** zum Aufnehmen des Ausgangssignals der ersten Verschlüsselungseinheit **51** des Serverendgeräts **50**. Die Daten aus der elektronischen Wasserzeicheneinbettungseinheit **62** werden an das Nutzerendgerät **70** gesendet.

heit **61** werden zum Nutzerendgerät **70** und zum Nachweisendgerät **30** gesandt.

[0274] Das Nutzerendgerät **70** verfügt über: einen Kontraktgenerator **71** zum Senden von Daten an die Kontraktidentifizierungseinheit **61** des Agenturendgeräts **60**; einen Signaturgenerator **72**; eine elektronische Wasserzeicheneinbettungseinheit **73** zum Aufnehmen von Daten aus dem Signaturgenerator **72** und der elektronischen Wasserzeicheneinbettungseinheit **62** des Agenturendgeräts **60**; eine zweite Verschlüsselungseinheit **74** zum Aufnehmen von Daten aus der elektronischen Wasserzeicheneinbettungseinheit **73**; und über eine zweite Entschlüsselungseinheit **75** zum Aufnehmen von Daten aus der ersten Entschlüsselungseinheit **52** vom Serverendgerät **50**. Die Daten aus der zweiten Entschlüsselungseinheit **75** werden als Bilddaten gesendet, die ein elektronisches Wasserzeichen enthalten. Die Daten aus der zweiten Verschlüsselungseinheit **74** werden zur ersten Entschlüsselungseinheit **52** des Serverendgeräts **50** und des Nachweisendgeräts **30** gesendet.

[0275] Das Nachweisendgerät **30** verfügt über: eine zweite Entschlüsselungseinheit **31** zum Aufnehmen von Daten aus der elektronischen Wasserzeicheneinbettungseinheit **62** vom Agenturendgerät **60** und von der zweiten Verschlüsselungseinheit **74** des Nutzerendgeräts **70**; und über eine elektronische Wasserzeichenidentifizierungseinheit **32** zum Aufnehmen von Daten aus der zweiten Entschlüsselungseinheit **31**. Die Daten aus der elektronischen Wasserzeicheneinheit **32** werden an die erste Entschlüsselungseinheit **52** vom Serverendgerät **50** geliefert.

[0276] Die mit dem solchermaßen eingerichteten System **300** ausgeführte Verarbeitung wird nun erläutert. Für das in Fig. 19 gezeigte Protokoll ist die Information bezüglich der ersten Verschlüsselung, wie das Verfahren und dessen Geheimschlüssel, nur für den Server oder für den Autor verfügbar, und die Information bezüglich der zweiten Verschlüsselung ist nur für den Nutzer verfügbar. Angemerkt sei jedoch, daß für diese Verschlüsselungsprozesse ein Eigentum besteht, wobei die verschlüsselten Daten entschlüsselt werden können, ungeachtet der Tatsache, welcher Verschlüsselungsprozeß als erster ausgeführt wurde. Während das hierarchische System gemäß Fig. 5 in der folgenden Erläuterung verwendet wird, kann diese Erläuterung für das in Fig. 4 gezeigte System angewandt werden, indem der Autor mit dem Server vertauscht wird.

[Einbettungsprozeß]

1) Zuerst fordert das Nutzerendgerät **70** an, daß das Agenturendgerät **60** gewünschte Bilddaten mit Signatur bereitstellt. Die angeforderten Daten sind Informationen (Nutzersignaturinformationen), die der Kontraktgenerator **71** erzeugt und die nachstehend als Kontraktinformationen bezeichnet werden. Im Agenturendgerät **60** verwendet die Kontraktidentifizierungseinheit **61** die Signatur vom Nutzer, um die empfangene Kontraktinformation zu identifizieren, und reicht dann eine Anforderung für Bilddaten an das Serverendgerät (Autor) **50** weiter. Nach Empfang dieser Anforderung führt die erste Verschlüsselungseinheit **51** vom Serverendgerät **50** die erste Verschlüsselung E1() von Bilddaten G aus und sendet die gewonnenen Daten an das Agenturendgerät **60**.

2) Im Agenturendgerät **60** bereitet die Kontraktidentifizierungseinheit **61** die Nutzerinformation U unter Verwendung der Kontraktinformation vor, die das Nutzerendgerät **70** geliefert hat. Die elektronische Wasserzeicheneinbettungseinheit **62** bettet die Nutzerinformation U, die die Kontraktidentifizierungseinheit **61** erzeugt hat, in die ersten verschlüsselten Bilddaten E1(G) ein, die das Serverendgerät **50** gesandt hat. Das Nutzerendgerät **70** empfängt folglich die ersten verschlüsselten Bilddaten E1(G) + U mit der darin enthaltenen Nutzerinformation U.

[0277] Die elektronische Wasserzeicheneinbettungseinheit **62** des Agenturendgeräts **60** sendet an das Nachweisendgerät **30** eine Geheiminformation bezüglich eines elektronischen Wasserzeichens. Die Geheiminformation ist die Information, die den Einbettungsabschnitt und die Stärke der Feststellung eines elektronischen Wasserzeichens betrifft, und diese wird nach einem anderen Verschlüsselungsverfahren verschlüsselt, das mit dem Nachweisendgerät **30** gemeinsam verwendet wird.

3) Im Nutzerendgerät **70** erzeugt der Signaturgenerator **22** Signaturinformationen S unter Verwendung des Geheimschlüssels des Nutzers. Die elektronische Wasserzeicheneinbettungseinheit **73** bettet in die ersten verschlüsselten Bilddaten E1(G) + U, die vom Agenturendgerät **60** gesendet (verteilt) wurden, die Signaturinformation S ein, die der Signaturgenerator **72** erzeugt hat. Die zweite Verschlüsselungseinheit **74** führt eine zweite Verschlüsselung für die ersten verschlüsselten Bilddaten E1(G) + U + S aus, wobei die Signaturinformation S von der elektronische Wasserzeicheneinbettungseinheit **73** eingebettet worden ist, und die gewonnen Bilddaten werden dann an das Nachweisendgerät **30** gesandt. Das Nachweisendgerät **30** empfängt folglich die zweiten verschlüsselten Bilddaten E2(E1(G) + U + S).

[0278] Die zweite Verschlüsselungseinheit **74** des Nutzerendgeräts **70** erzeugt zu dieser Zeit einen Tabelleneintragssuchwert H2 für die zweiten verschlüsselten Bilddaten E2(E1(G) + U + S), die an das Nachweisendgerät **30** zu senden sind. Die zweite Verschlüsselungseinheit **74** stellt dann eine Signatur für den Tabelleneintragssuchwert H2 bereit und sendet

diese gemeinsam mit der Geheiminformation bezüglich des elektronischen Wasserzeichens und dem zweiten Verschlüsselungsgeheimcode an das Nachweisendgerät **30**.

4) Das Nachweisendgerät **30** identifiziert die Signatur, die vom Tabelleneintragssuchwert H2 begleitet ist, empfangen aus dem Nutzerendgerät **70**, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, entschlüsselt die zweite Entschlüsselungseinheit **31** die zweiten verschlüsselten Bilddaten E2(E1(G) + U + S), die vom Nutzerendgerät **70** kommen, und liest daraus die Nutzerinformation U und die Signaturinformation S aus. Die elektronische Wasserzeichenidentifizierungseinheit **32** überprüft dann die Nutzerinformation U und die Signaturinformation S, und wenn die Information U und die Information S korrekt sind, dann wird die Nachweisinformation unter Verwendung der Signatur vom Nachweisendgerät **30** aufbereitet. Letztlich sendet das Nachweisendgerät **30** die zweiten verschlüsselten Bilddaten E2(E1(G) + U + S) gemeinsam mit dem Tabelleneintragssuchwert H2 und mit der begleitenden Signatur, die alle vom Nutzerendgerät **70** kommen, sowie die Nachweisinformationen dafür und deren begleitende Signatur an das Serverendgerät **50**.

5) Im Serverendgerät **50** identifiziert der Autor die Nachweisinformation und deren begleitende Signatur, empfangen vom Nachweisendgerät **30**, sowie die zweiten verschlüsselten Bilddaten E2(E1(G) + U + S) und den Tabelleneintragssuchwert H2 und dessen begleitende Signatur. Nachdem dieser Bestätigungsprozeß abgeschlossen ist, entschlüsselt die erste Entschlüsselungseinheit **52** den ersten verschlüsselten Abschnitt der zweiten verschlüsselten Bilddaten E2(E1(G) + U + S), um die Bilddaten E2(G) + D1(E2(U + S)) zu gewinnen, die wiederum an das Nutzerendgerät **70** gesandt werden.

6) Im Nutzerendgerät **70** entschlüsselt die zweite Entschlüsselungseinheit **75** den zweiten verschlüsselten Abschnitt der Bilddaten E2(G) + D1(E2(U + S)) aus dem Nutzerendgerät **50** und liest die Bilddaten G_W aus, in die ein elektronisches Wasserzeichen eingebettet ist. Die Bilddaten G_W und das enthaltene elektronische Wasserzeichen werden dargestellt mit $G_W = G + D1(U + S)$. Das bedeutet, daß die Nutzerinformation U und die Signaturinformation S des Nutzers, die von der ersten Entschlüsselung betroffen sind, als elektronische Information in die Originalbilddaten eingebettet werden.

[0279] Wenn in Prozedur 4) das Nachweisendgerät **30** nicht nachweist, daß die elektronische Wasserzeicheninformation korrekt ist, und zwar weil entweder der Autor oder der Nutzer eine rechtswidrige Tat begangen hat, werden diesbezügliche Meldungen an das Serverendgerät **50**, das Agenturendgerät **60** und das Nutzerendgerät **70** gesandt. Da selbst bei zu dieser Zeit beendetem Handel keiner dieser Beteiligten weder einen Gewinn noch einen Verlust erleidet, ist das Begehen einer rechtswidrigen Tat sinnlos.

[0280] Wenn eine rechtswidrige Kopie (rechtswidriges Bild) G_W' entdeckt wird, kann die Partei, die die rechtswidrige Tat begangen hat, durch Ausführen einer einfachen Nachweisverarbeitung leicht identifiziert werden. Angemerkt sei, daß die Bilddaten von der Abwandlung und dem Löschen der elektronischen Wasserzeicheninformation nicht berührt werden.

[Nachweisprozeß]

1) Im Serverendgerät **50** führt der Autor als erstes die erste Verschlüsselung der rechtswidrigen Bilddaten G_W' aus und liest die Nutzerinformation U aus. Wenn die Nutzerinformation U nicht ausgelesen wird, ist sichergestellt, daß der Autor die rechtswidrige Tat begangen hat.

2) Wird die korrekte Nutzerinformation U ausgelesen, dann wird die Signaturinformation aus den Daten ausgelesen, die durch die erste Verschlüsselung der rechtswidrigen Bilddaten G_W' gewonnen wurden.

3) Ist die korrekte Signaturinformation ausgelesen, dann ist sichergestellt, daß der Nutzer eine rechtswidrige Tat begangen hat. Dies liegt daran, daß die korrekte Signaturinformation nur vom Nutzer und dem Autor aufbereitet werden kann, da die Agentur keinerlei Kenntnis der Signaturinformation besitzt.

4) Wird die korrekte Signaturinformation nicht ausgelesen, dann ist sichergestellt, daß der Autor eine rechtswidrige Tat begangen hat.

[0281] Gemäß dem elektronischen Wasserzeichenverfahren nach dem Beispiel von Fig. 19 werden die Verschlüsselung der Digitaldaten und der Einbettungsprozeß für ein elektronisches Wasserzeichen vom Serverendgerät **50**, dem Agenturendgerät **60** und dem Nutzerendgerät **70** ausgeführt, und die Verschlüsselung und die Identifizierung der korrekten elektronischen Wasserzeicheninformation erfolgen durch das Nachweisendgerät **30**. Wenn der Autor, die Agentur oder der Nutzer individuell eine rechtswidrige Kopie aufbereitet hat, kann die rechtswidrige Tat folglich leicht festgestellt werden und die rechtswidrige Partei kann leicht identifiziert werden. Da nach diesem Verfahren das Nachweisbüro die Ergebnisse des ersten Einbettungsprozesses und des zweiten Einbettungsprozesses überprüft, ist eine Kollision folglich nicht wirksam, so daß die Kollision vom Server oder vom Autor mit der Agentur und dem Nutzer nicht auftreten kann. Selbst wenn eine derartige Kollision auftreten sollte, kann die rechtswidrige Tat

leicht festgestellt werden. Die Sicherheit dieses Prozesses basiert auf der Voraussetzung, daß das Nachweisbüro vertrauenswürdig ist.

[0282] In einem anderen Beispiel, das dem Beispiel von Fig. 19 gleicht, wird die Gesamtverarbeitung erläutert, wobei der Server oder der Autor in Fig. 4 oder in Fig. 5 Digitaldaten über die Agentur an den Nutzer verteilt. Dieses Beispiel ist nachstehend anhand Fig. 20 beschrieben. Genauer gesagt, es wird ein elektronisches Wasserzeichenverfahren gemäß Fig. 20 durch ein System **400** durchgeführt.

[0283] In Fig. 20 ist das System **400** ein Netzwerksystem, das aufgebaut ist aus Mehrfachdateneinheiten (nicht dargestellt), die ein Serverendgerät **50**, ein Agenturendgerät **60**, ein Nutzerendgerät **70** und ein Nachweisendgerät **30** enthalten. Die individuellen Dateneinheiten tauschen Digitaldaten über das Netzwerk aus.

[0284] Das Serverendgerät **50** verfügt über: eine erste Verschlüsselungseinheit **51** zum Aufnehmen beispielsweise von Bilddaten (Digitaldaten); und über eine erste Entschlüsselungseinheit **52** zum Aufnehmen von Daten aus dem Nutzerendgerät **70** und dem Nachweisendgerät **30**. Die Daten aus der ersten Verschlüsselungseinheit **51** werden an das Agenturendgerät **60** gesandt, und die Daten aus der ersten Entschlüsselungseinheit **52** werden an das Nutzerendgerät **70** gesandt.

[0285] Das Agenturendgerät **60** verfügt über: eine Kontraktidentifizierungseinheit **61** zum Aufnehmen von Daten aus dem Nutzerendgerät **70**; eine elektronische Wasserzeicheneinbettungseinheit **62** zum Aufnehmen des Ausgangssignal von der Kontraktidentifizierungseinheit **61** und von der ersten Verschlüsselungseinheit **51** des Serverendgeräts **50**; und über eine elektronische Wasserzeicheneinbettungseinheit **63** zum Aufnehmen von Daten aus dem Nutzerendgerät **70**. Die Daten aus der elektronischen Wasserzeicheneinbettungseinheit **62** werden an das Nutzerendgerät **70** und das Nachweisendgerät **30** gesandt. Das Ausgangssignal aus der elektronischen Wasserzeicheneinbettungseinheit **63** wird auch an das Serverendgerät **50** und an das Nachweisendgerät **30** gesandt.

[0286] Das Nutzerendgerät **70** verfügt über: einen Kontraktgenerator **71** zum Senden von Daten an die Kontraktidentifizierungseinheit **61** des Agenturendgeräts **60**; einen Signaturgenerator **72**; eine zweite Verschlüsselungseinheit **74** zum Aufnehmen von Daten aus der elektronischen Wasserzeicheneinbettungseinheit **62** vom Agenturendgerät **60**; und über eine zweite Entschlüsselungseinheit **75** zum Aufnehmen von Daten aus der ersten Entschlüsselungseinheit **52** vom Serverendgerät **50**. Die Daten aus der zweiten Entschlüsselungseinheit **75** werden als Bilddaten gesandt, die ein elektronisches Wasserzeichen enthalten. Die Daten aus der zweiten Verschlüsselungseinheit **74** werden an die elektronische Wasserzeicheneinbettungseinheit **63** des Agenturendgeräts **60** und an das Nachweisendgerät **30** gesandt.

[0287] Das Nachweisendgerät **30** verfügt über: eine zweite Entschlüsselungseinheit **31** zum Aufnehmen von Daten aus der elektronischen Wasserzeicheneinbettungseinheit **63** des Agenturendgeräts **60** und der zweiten Verschlüsselungseinheit **74** des Nutzerendgeräts **70**; und über eine elektronische Wasserzeichenidentifizierungseinheit **32** zum Aufnehmen von Daten aus der zweiten Entschlüsselungseinheit **31** und aus der elektronischen Wasserzeicheneinbettungseinheit **63** des Agenturendgeräts **60**. Die Daten der elektronischen Wasserzeicheneinheit **32** werden an die erste Entschlüsselungseinheit **52** des Serverendgeräts **50** geliefert.

[0288] Die vom solchermaßen eingerichteten System **400** ausgeführte Verarbeitung ist nachstehend erläutert. Für das in Fig. 20 gezeigte Protokoll ist die Information bezüglich der ersten Verschlüsselung, wie das Verfahren und dessen Geheimschlüssel, nur für den Server oder den Autor verfügbar, und Informationen bezüglich der zweiten Verschlüsselung ist nur für den Nutzer verfügbar. Angemerkt sei jedoch, daß für diese Verschlüsselungsprozesse ein Eigentum vorhanden ist, durch das die verschlüsselten Daten entschlüsselt werden können, ungeachtet der Tatsache, welcher Verschlüsselungsprozeß als erstes ausgeführt wird. Während das hierarchische System, wie es in Fig. 5 gezeigt ist, für die folgende Erläuterung verwendet wird, kann diese Erläuterung auch auf ein System gemäß Fig. 4 angewandt werden, indem der Autor mit dem Server ausgetauscht wird.

[Einbettungsprozeß]

1) Das Nutzerendgerät **70** fordert zunächst an, daß das Agenturendgerät **60** gewünschte Bilddaten bereitstellt, die eine Signatur tragen. Die angeforderten Daten sind Informationen (Signaturinformationen des Nutzers), die vom Kontraktgenerator **72** erzeugt werden und die hiernach als Kontraktinformationen bezeichnet werden. Im Agenturendgerät **60** verwendet die Kontaktidentifizierungseinheit **61** die Signatur vom Nutzer zum Identifizieren der empfangenen Kontraktinformation und reicht dann eine Anforderung für Bilddaten an das Serverendgerät (Autor) **50** weiter. Nach Empfang dieser Anforderung führt die erste Verschlüsselungseinheit **51** vom Serverendgerät **50** die erste Verschlüsselung E1() der Bilddaten G aus und sendet die gewonnenen Daten E1(G) an das Agenturendgerät **60**.

2) Im Agenturendgerät **60** bereitet die Kontraktidentifizierungseinheit **61** Nutzerinformationen U

unter Verwendung der Kontraktinformation aus dem Nutzerendgerät **70** vor. Die elektronische Wasserzeicheneinbettungseinheit **62** bettet die Nutzerinformation U, die die Kontraktidentifizierungseinheit **61** erzeugt hat, in die ersten verschlüsselten Bilddaten E1(G) ein, die das Serverendgerät **50** gesendet hat. Das Nutzerendgerät **70** empfängt folglich die ersten verschlüsselten Bilddaten E1(G) + U mit der darin enthaltenen Nutzerinformation U.

3) Im Nutzerendgerät **70** führt die zweite Verschlüsselungseinheit **74** die zweite Verschlüsselung der ersten verschlüsselten Bilddaten E1(G) + U aus, die das Agenturendgerät **60** geliefert hat, und sendet die erzielten Bilddaten E2(E1(G) + U) an das Agenturendgerät **60**. Der Signaturgenerator **72** erzeugt eine Signaturinformation S, die nur der Nutzer vorbereiten kann, und sendet diese gemeinsam mit den zweiten verschlüsselten Bilddaten E2(E1(G) + U) an das Agenturendgerät **60**. Die zweite Verschlüsselungseinheit **74** sendet des weiteren den zweiten Verschlüsselungsgeheimcode an das Nachweisendgerät **30**.

4) Im Agenturendgerät **60** bettet die elektronische Wasserzeicheneinbettungseinheit **63** eine Signaturinformation S in die zweiten verschlüsselten Bilddaten E2(E1(G) + U) ein, wobei die Informationen in beiden Fällen vom Nutzerendgerät **70** empfangen werden, und sendet die gewonnenen Bilddaten an das Nachweisendgerät **30**. Das Nachweisendgerät **30** empfängt somit die zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S und deren begleitende Signaturinformation.

[0289] Zu dieser Zeit erzeugt das Agenturendgerät **60** einen Tabelleneintragssuchwert H2 für die zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S, die an das Nachweisbüro **30** zu senden sind. Das Agenturendgerät **60** stellt dann eine Signatur für den Tabelleneintragssuchwert H2 bereit und sendet diese gemeinsam mit der Geheiminformation bezüglich des elektronischen Wasserzeichens und dem zweiten Verschlüsselungsgeheimcode an das Nachweisendgerät **30**. Die Geheiminformation ist eine solche, die den Einbettungsabschnitt und die zum Feststellen eines elektronischen Wasserzeichens erforderliche Stärke betrifft und die nach einem anderen Verschlüsselungsverfahren verschlüsselt wird, das gemeinsam mit dem Nachweisendgerät **30** verwendet wird.

5) Das Nachweisendgerät **30** identifiziert die Signatur, die den Tabelleneintragssuchwert H2 begleitet, empfangen aus dem Agenturendgerät **60**, und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert für die Sendedaten paßt. Nachdem der Bestätigungsprozeß abgeschlossen ist, liest die elektronische Wasserzeichenidentifizierungseinheit **32** die Signaturinformation S aus den zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S aus, die das Agenturendgerät **60** geliefert hat. Die zweite Entschlüsselungseinheit **31** entschlüsselt die zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S aus dem Nutzerendgerät **70**, und liest daraus die Nutzerinformation U aus.

[0290] Die elektronische Wasserzeichenidentifizierungseinheit **32** überprüft die Nutzerinformation U und die Signaturinformation S. Wenn die Informationen U und S korrekt sind, wird die Nachweisinformation unter Verwendung der Signatur vom Nachweisendgerät **30** aufbereitet. Letztlich sendet das Nachweisendgerät **30** die zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S und den Tabelleneintragssuchwert H2 und dessen begleitende Signatur, die alle aus dem Agenturendgerät **60** empfangen wurde, sowie deren Nachweisinformation und deren Signatur an das Serverendgerät **50**.

6) Im Serverendgerät **50** identifiziert der Autor die Nachweisinformation und deren begleitende Signatur, empfangen vom Nachweisendgerät **30**, sowie auch die zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S und den Tabelleneintragssuchwert H2 und dessen begleitende Signatur. Nachdem dieser Bestätigungsprozeß abgeschlossen ist, entschlüsselt die erste Entschlüsselungseinheit **52** den ersten verschlüsselten Abschnitt der zweiten verschlüsselten Bilddaten E2(E1(G) + U) + S, um die Bilddaten E2(G) + D1(E2(U) + S) zu erhalten, die wiederum an das Nutzerendgerät **70** gesandt werden.

7) Im Nutzerendgerät **70** entschlüsselt die zweite Entschlüsselungseinheit **75** den zweiten verschlüsselten Abschnitt der Bilddaten E2(G) + D1(E2(U) + S), die vom Serverendgerät **50** kommen, und liest die Bilddaten G_W aus, in die ein elektronisches Wasserzeichen eingebettet ist. Die Bilddaten G_W, die das elektronische Wasserzeichen enthalten, werden folglich dargestellt durch $G_W = G + D1(U + D2(S))$. Dies bedeutet, daß die Nutzerinformation U, die von der ersten Verschlüsselung berührt wurde, und die Signaturinformation S des Nutzers, die sowohl in der ersten als auch in der zweiten Verschlüsselung berührt wurden, als elektronische Information in die Originalbilddaten eingebettet sind.

[0291] Wenn in Prozedur 5) das Nachweisendgerät **30** die elektronische Wasserzeicheninformation nicht nachweist, weil entweder der Autor oder der Nutzer eine rechtswidrige Tat begangen haben, werden diesbezügliche Meldungen an das Serverendgerät **50**, das Agenturendgerät **60** und an das Nutzerendgerät **70** gesandt. Da selbst bei zu dieser Zeit beendetem Handel keiner dieser Beteiligten weder einen Gewinn noch einen Verlust erleidet, ist das Begehen einer rechtswidrigen Tat sinnlos. Wenn eine rechtswidrige Kopie (rechtswidriges Bild) G_W' entdeckt wird, kann die Partei, die die rechtswidrige Tat begangen hat, leicht durch Ausführen des folgenden einfachen

Nachweisprozesses identifiziert werden. Angemerkt sei, daß die Bilddaten durch Modifizieren und Löschen der elektronischen Wasserzeicheninformation nicht beeinträchtigt werden.

[Nachweisprozeß]

1) Im Serverendgerät **50** führt der Autor als erstes die erste Verschlüsselung für rechtswidrige Bilddaten G_W' aus und liest die Nutzerinformation U aus. Wenn die Nutzerinformation U nicht ausgelesen ist, wird ermittelt, daß der Autor eine rechtswidrige Tat begangen hat.
2) Wenn die korrekte Nutzerinformation ausgelesen ist, ermittelt das Serverendgerät **50** für das Nachweisendgerät **30** die ersten verschlüsselten Bilddaten G_W' und die Nutzerinformation U' und fordert die Überprüfung dieser an. Das Nachweisendgerät **30** führt die zweite Verschlüsselung für die ersten verschlüsselten Bilddaten G_W' aus (deren Verschlüsselungsfunktion ist nicht dargestellt) und liest die Signaturinformation aus.
3) wenn die korrekte Signaturinformation ausgelesen ist, wird ermittelt, daß der Nutzer eine rechtswidrige Tat begangen hat.
4) Wird die korrekte Signaturinformation nicht ausgelesen, ist zu ermitteln, daß der Autor eine rechtswidrige Tat begangen hat.

[0292] Nach dem anhand Fig. 20 beschriebenen elektronischen Wasserzeichenverfahren werden die Verschlüsselung von Digitaldaten und der Einbettungsprozeß für ein elektronisches Wasserzeichen vom Serverendgerät **50** ausgeführt, dem Agenturendgerät **60** und dem Nutzerendgerät **70**, und die Verschlüsselung und die Identifizierung der korrekten elektronischen Wasserzeicheninformation erfolgen mit dem Nachweisendgerät **30**. Selbst wenn der Autor, die Agentur oder der Nutzer individuell eine rechtswidrige Kopie vorbereiten, kann folglich die rechtswidrige Tat leicht festgestellt werden. Darüber hinaus kann die rechtswidrige Partei leicht identifiziert werden. Da nach diesem Verfahren das Nachweisbüro des weiteren die Ergebnisse des ersten Einbettungsprozesses und des zweiten Einbettungsprozesses überprüft, ist eine Kollusion nicht wirksam, so daß die Kollusion vom Server oder dem Autor mit der Agentur und dem Nutzer nicht auftreten wird. Selbst bei Auftreten einer Kollusion kann eine rechtswidrige Tat leicht festgestellt werden. Die Sicherheit dieses Prozesses basiert auf der Voraussetzung, daß das Nachweisbüro vertrauenswürdig ist.

(Viertes Ausführungsbeispiel)

[0293] Wenn in der Anordnung gemäß Fig. 19 nach dem vierten Ausführungsbeispiel ein Nutzer Digitaldaten einkauft, kann die Anonymität des Nutzers gewahrt werden, und wenn eine rechtswidrige Tat, wie die Verteilung eines rechtswidrigen Bildes, entdeckt wird, läßt sich die Partei entdecken, die die rechtswidrige Tat begangen hat. Dies wird realisiert unter Verwendung beispielsweise eines in Fig. 21 gezeigten Systems **500**. Das System **500** hat dieselbe Anordnung wie das vom System **300** in Fig. 19, mit der Ausnahme, daß ein Nutzerendgerät **70** eine anonyme öffentliche Schlüsselbescheinigung aus einem Bescheinigungsbüro **40** erhält.

[0294] Wenn in diesem Ausführungsbeispiel, wie auch im dritten Ausführungsbeispiel, das Bescheinigungsbüro **40** das Geheimnis der Korrespondenz von öffentlichen Schlüsseln und die Namen deren Besitzer wahrt, wird ein Besitzername nicht in eine Bescheinigung für den öffentlichen Schlüssel eingegeben. Wenn in Prozedur 1) des Einbettungsprozesses gemäß dem Beispiel in

[0295] Fig. 19 ein Nutzer nicht nur eine Kontraktinformation, sondern auch eine Signatur für die Kontraktinformation sendet, und ein anonymer öffentlicher Schlüssel, begleitet mit einer Bescheinigung, die zum Überprüfen der Signaturinformation S verwendet wird, kann der Nutzer anonym bleiben, wenn Digitaldaten eingekauft werden.

[0296] Der anonyme öffentliche Schlüssel, der mit einer Bescheinigung begleitet ist, wird folglich an die Agentur als Identifizierungsinformation für den Nutzer gesandt. Wenn eine rechtswidrige Tat entdeckt wird, wird dann der anonyme öffentliche Schlüssel, begleitet mit der Bescheinigung, an das Bescheinigungsbüro **40** gesandt mit dem Namen des Nutzers, der dem öffentlichen Schlüssel entspricht, der angefordert wird, um den Nutzer identifizieren zu können. Wenn die Prozedur 1) im Einbettungsprozeß und die Prozedur 1) im Nachweisprozeß gemäß Beispiel in Fig. 19 folgendermaßen geändert werden, kann die Anonymität eines Nutzers aufrechterhalten werden, wenn Digitaldaten gekauft werden, während bei Aufdecken einer rechtswidrigen Tat die Partei, die diese rechtswidrige Tat begangen hat, identifiziert werden kann.

[0297] Angemerkt sei, daß ein Nutzer anonym bleiben kann, wenn er Digitaldaten kauft, und daß im Falle einer erkannten rechtswidrigen Tat die Partei, die diese rechtswidrige Tat begangen hat, durch Ändern der Prozedur 1) im Einbettungsprozeß und der Prozedur 1) im Nachweisprozeß im Beispiel gemäß Fig. 20 identifiziert werden kann, und zwar folgendermaßen.

[0298] Der Einbettungsprozeß und der Nachweisprozeß, die das System **500** in Fig. 21 ausführt, ist nachstehend speziell erläutert.

[Einbettungsprozeß]

1) Im Nutzerendgerät **70** stellt ein Kontraktgenera-

tor **71** zunächst für eine Kontraktinformation, die verwendet wird zum Anfragen gewünschter Daten, eine Signatur bereit, die einem anonymen öffentlichen Schlüssel entspricht, der mit einer Bescheinigung begleitet ist, die das Bescheinigungsbüro **40** ausgibt. Der Kontraktgenerator **71** sendet dann an ein Agenturendgerät **60** den anonymen öffentlichen Schlüssel und die Kontraktinformation, die mit Signatur begleitet ist. In Agenturendgerät **60** identifiziert eine Kontraktidentifizierungseinheit **61** die empfangene Kontraktinformation unter Verwendung des anonymen öffentlichen Schlüssels und fordert dann die Bilddaten vom Autor an. Nach Empfang der Anforderung führt eine erste Verschlüsselungseinheit **51** in einem Serverendgerät **50** die erste Verschlüsselung E1() der Bilddaten G an und sendet die gewonnenen Bilddaten E1(G) an das Agenturendgerät **60**.

[0299] Da die Prozeduren 2) bis 6) dieselben wie jene im Beispiel von Fig. 19 sind, wird hier keine erneute Erläuterung gegeben.

[Nachweisprozeß]

1) Im Serverendgerät **50** führt die erste Verschlüsselungseinheit **51** die erste Verschlüsselung der rechtswidrigen Bilddaten G_W' aus, die entdeckt worden sind, und liest daraus die Nutzerinformation aus. Das Serverendgerät **50** unterbreitet dem Bescheinigungsbüro **40** die ausgelesene Nutzerinformation und den anonymen öffentlichen Schlüssel, der unter Verwendung der Kontraktinformation identifiziert wurde, und fordert den Nutzernamen an, der dem anonymen öffentlichen Schlüssel entspricht. Wenn die Nutzerinformation nicht ausgelesen wird, ist sichergestellt, daß der Autor die rechtswidrige Tat begangen hat.

[0300] Die Prozeduren 2) bis 4) sind dieselben wie jene im Beispiel von Fig. 19.

[0301] Wenn Digitaldaten gekauft werden, kann ein Nutzer bezüglich dem Nachweisbüro anonym bleiben, wie zuvor gemäß dem vierten Ausführungsbeispiel beschrieben.

[0302] Um Bilddaten im dritten und vierten Ausführungsbeispiel sowie Tabelleneintragssuchwerte zu erhalten, gewonnen während des Einbettungsprozesses für die elektronische Wasserzeicheninformation, kann dies unter Verwendung des oben beschriebenen Bildformates gespeichert werden. Gemäß dem allgemeinen Bildformat werden beispielsweise Bilddaten zu individuellen Schritten gesendet und können in einem Bilddatenabschnitt gespeichert werden, und ein zugehöriger Tabelleneintragssuchwert und dessen Signatur kann in einem Bildkopfabschnitt gespeichert werden. Ein Tabelleneintragssuchwert und dessen begleitende Signatur, die der Nutzer zurückhalten muß, und der zweite Verschlüsselungscode kann des weiteren im Bildkopfabschnitt gespeichert werden, während die Daten mit einem elektronischen Wasserzeichen im Bilddatenabschnitt gespeichert werden können.

[0303] Im dritten und vierten Ausführungsbeispiel kann die elektronische Wasserzeicheninformation unter Verwendung verschiedener Verfahren eingebettet werden.

[0304] Die erste Verschlüsselung und die zweite Verschlüsselung kann ebenfalls realisiert werden durch Anwenden verschiedener Verfahren, beispielsweise eines Verschlüsselungssystems zum Ändern der Bitanordnung in Übereinstimmung mit einem Verschlüsselungscode. Darüber hinaus kann ein Tabelleneintragssuchwert und dessen Signatur bereitgestellt werden für alle Daten, die zu senden sind. In diesen Ausführungsbeispielen werden die erste Verschlüsselung und die zweite Verschlüsselung während des elektronischen Wasserzeicheninformationseinbettungsprozesses ausgeführt, um den Server, den Nutzer und die Agentur davor zu schützen, einander die dort gespeicherte Information anzufordern. DES-Kryptographie oder DES-Verschlüsselung (Data Encryption Standard Verschlüsselung) oder eine Tabelleneintragssuchfunktion können verwendet werden, um das Abhören und Ändern von Daten über den Übertragungsweg durch eine dritte Partei zu vermeiden.

[0305] Im dritten und vierten Ausführungsbeispiel ist die erste Dateneinheit (der Server oder der Autor) beschäftigt mit der Feststellung rechtswidriger Datenverteilung. Sofern ein elektronisches Wasserzeichenauslesemittel bereitsteht, kann jedoch jeder Nutzer eine rechtswidrige Datenverteilung und eine Nutzerinformation erkennen, die rechtswidrig verteilt worden ist, obwohl man nicht den Geheimschlüssel für die erste Verschlüsselung oder die zweite Verschlüsselung kennt. Wenn der Fall einer rechtswidrigen Datenverteilung festgestellt ist, muß der Nutzer nur die erste Dateneinheit für den Nachweisprozeß für den zu beginnenden Nachweisprozeß melden. Der Prozeß des Feststellens rechtswidriger Verteilungen ist folglich nicht auf die erste Dateneinheit beschränkt.

[0306] Die erste Dateneinheit oder die Agentur kann in die Bilddaten nicht nur die Nutzerinformation U, sondern auch andere erforderliche Information, wie eine Copyrightinformation und eine Information bezüglich Bilddatenverteilungsbedingung einbetten. Zum Einbetten einer Geheiminformation muß die erste Dateneinheit nur den Einbettungsprozeß zusätzlich ausführen, der der ersten Verschlüsselung folgt, so daß zusätzlich zur Signaturinformation die Information, die von der ersten Verschlüsselung betroffen ist, in die Bilddaten eingebettet wird. Die Nutzerinformation wird nicht immer vor der ersten Verschlüsse-

lung eingebettet, sondern kann nach der ersten Verschlüsselung eingebettet werden (in diesem Falle kann das Feststellen der Nutzerinformation U nur von der ersten Einheit erfolgen oder von einer Person, die den Geheimschlüssel kennt, der für die erste Verschlüsselung verwendet wurde).

[0307] Wenn die zweite Dateneinheit ein Nutzer ist, der einen Drucker oder ein Endgerät gemeinsam verwendet, kann die Signaturinformation für die zweite Dateneinheit und die zweite Verschlüsselung die Signaturinformation und das Verschlüsselungssystem für den Drucker oder für das Endgerät enthalten, die in gemeinsamer Verwendung sind. Die erste verschlüsselte Information aus der ersten Dateneinheit kann weitestgehend über eine Netzwerk verteilt werden oder durch eine CD-ROM, selbst ohne Anforderung der Verteilung durch eine zweite Dateneinheit auf der Grundlage der Kontraktinformation. Die Signaturinformation S für die zweite Dateneinheit wird nicht notwendigerweise mit dem Verschlüsselungsverfahren des öffentlichen Schlüssels erzeugt, sondern kann eine Information sein (beispielsweise eine Codezahl), die der Nutzer auf Grundlage der Kontraktinformation festlegt.

[0308] Zur Anwendung der Verschlüsselung für 40 Bits oder mehr ist in den Vereinigten Staaten ein Schlüsselverwaltungsbüro erforderlich, um einen Verschlüsselungscode anzufordern, damit die nicht berechtigte Verwendung der Verschlüsselung vermieden wird. Das Nachweisbüro **30** kann folglich als Schlüsselverwaltungsbüro dienen. Und wenn das Nachweisbüro eine verbesserte Verwaltung des zweiten Verschlüsselungscodes bereitstellt, kann das Nachweisbüro selbst die Nachweisprozesse 1) bis 3) durch Überwachen eines rechtswidrigen Bildes ausführen. Der erste Verschlüsselungscode von der ersten Dateneinheit kann verwaltet werden entweder durch dasselbe Nachweisbüro oder durch ein anderes Codeverwaltungsbüro. Die Schlüssel der ersten Dateneinheit und der zweiten Dateneinheit können vom Codeverwaltungsbüro erzeugt und verteilt werden.

[0309] Anstelle einer Einzelagentur kann darüber hinaus eine Vielzahl von Agenturen hierarchisch strukturiert vorgesehen sein. In diesem Falle kann eine speziell beauftragte Agentur in der hierarchischen Struktur die Verarbeitung ausführen, die die beauftragte Agentur ausführt, oder die individuellen Agenturen können das Protokoll zum Spezifizieren der Agentur ausführen, die zu beauftragen ist. Wenn nur eine Agentur vorgesehen ist, wie in Fig. 5 gezeigt, kann das Einbetten der Nutzerinformation U1 bezüglich der Agentur entfallen.

[0310] Nach Empfang einer Anforderung ist der Autor verantwortlich für das Senden an die Agentur von den ersten verschlüsselten Daten E1(G) von den Originaldaten G. Der Autor kann jedoch die Daten E1(G) schon im voraus senden.

[0311] Die in den Fig. 19 und Fig. 20 beschriebene Agentur ist ein Beispiel, und das vierte Ausführungsbeispiel führt keine Verschlüsselung E3() und keine Entschlüsselung D3() aus. Die Daten können jedoch unter Verwendung des Verschlüsselungsprozesses E3() verschlüsselt werden, nachdem die Daten zunächst vom Autor empfangen worden sind, oder die Daten können entschlüsselt werden unter Verwendung des Entschlüsselungsprozesses D3(), bevor die Daten an den Autor gesandt werden.

[0312] Gemäß dem oben beschriebenen elektronischen Wasserzeicheneinbettungsverfahren und dem System werden der Datenverschlüsselungsprozeß und der elektronische Wasserzeicheneinbettungsprozeß von einer Vielzahl von Mitteln oder Dateneinheiten bewerkstelligt. Ein Auftreten einer Rechtswidrigität wenigstens eines Verschlüsselungsprozesses und des elektronischen Wasserzeicheneinbettungsprozesses, die ausgeführt werden durch die Mittel oder durch die Dateneinheiten, wird nachgewiesen durch ein Mittel oder durch eine Dateneinheit, die sich von dem obigen Mittel und der obigen Dateneinheit unterscheidet. Wenn Daten rechtswidrig kopiert und über ein hierarchisch strukturiertes Netzwerk verteilt werden, kann folglich die rechtswidrige Tat und die Partei präzise identifiziert werden, die die rechtswidrige Tat begangen hat. Im Ergebnis kann das Begehen einer rechtswidrigen Tat verhindert werden, und ein sicheres System, das gegenüber rechtswidriger Verteilung von Daten schützt, kann bereitgestellt werden. Darüber hinaus kann dieses System leicht angewandt werden für ein Codeverwaltungsbüro, das die Anonymität eines Nutzers aufrechterhält und die rechtswidrige Verschlüsselung von Daten verhindert.

[0313] Fig. 22 ist ein schematisches Diagramm, das in der Gesamtheit die Anordnung eines Beispiels von einem elektronischen Informationsverteilungssystem darstellt.

[0314] Der Server S hält als Inhalte elektronische Information, und Agenturen A1 bis Am, die den Kontrakt mit dem Server S zur Verteilung der elektronischen Information machen. Die Agenturen A1 bis Am erhalten durch Ausgabe von Anforderungen vom Server S als elektronische Information die Daten, die sie wünschen, und sie speichern die empfangenen Daten.

[0315] Nutzer U11 bis U1n machen einen Kontrakt mit der Agentur A1, um elektronische Informationsdienste zu erhalten. Nutzer ermitteln Anforderungen an die Agentur A1 für die Verteilung der gespeicherten Inhalte, und nach Empfang dieser speichern sie sie als elektronische Information. Die Beziehungen

zwischen den Agenturen A1 bis Am und den Nutzern U21 bis U2n und Um1 bis Umn sind dieselben wie diejenigen, die zwischen der Agentur A1 und den Nutzern U11 bis U1n bestehen.

[0316] Das folgende elektronische Wasserzeichenüberlagerungsverfahren wird in diesem Beispiel angewandt auf ein in Fig. 22 gezeigtes System. Die speziellen Ausführungsbeispiele für das elektronische Wasserzeichenüberlagerungsverfahren werden nun anhand der Fig. 23 bis Fig. 26 beschrieben.

[0317] Die Verarbeitung ist in einen Prozeß 1 abgebrochen, wobei der Server S in Fig. 22 Bilddaten als elektronische Information an die Agenturen A1 bis Am sendet, und in Prozeß 2, bei dem Agenturen A1 bis Am Bilddaten an die Nutzer U11 bis Umn senden. In den folgenden Ausführungsbeispielen, die das elektronische Wasserzeichenüberlagerungsverfahren anwenden, wird im wesentlichen dasselbe Protokoll für die Prozesse 1 und 2 verwendet. Zunächst wird Prozeß 1 ausgeführt, und dann folgt Prozeß 2. Ein spezielles Protokoll für die Prozesse 1 und 2 wird erläutert.

[0318] Das Netzwerksystem in Fig. 23 enthält eine erste Dateneinheit, ein Endgerät **10**, eine zweite Dateneinheit, eine Endgerät **20** und ein Nachweisbüro **30**. Die erste Dateneinheit, Endgerät **10**, verfügt über: eine Kontraktidentifizierungseinheit **11** zum Aufnehmen von Daten aus dem Endgerät **20**; eine erste elektronische Wasserzeicheneinbettungseinheit **12** zum Aufnehmen beispielsweise von Bilddaten (Digitaldaten); eine erste Verschlüsselungseinheit **13** zum Aufnehmen des Ausgangssignals von der ersten elektronischen Wasserzeicheneinbettungseinheit **12**; eine erste Entschlüsselungseinheit **14** zum Aufnehmen von Daten aus dem Endgerät **20**; eine zweite elektronische Wasserzeicheneinbettungseinheit **15** zum Aufnehmen von Daten aus dem Endgerät **20** und aus der ersten Entschlüsselungseinheit **14**; und über einen Tabelleneintragessuchgenerator **16** zum Aufnehmen des Ausgangssignals von der zweiten elektronischen Wasserzeicheneinbettungseinheit **15**. Die Ausgangssignale der ersten Verschlüsselungseinheit **13** und des Tabelleneintragssuchgenerators **16** werden dem Endgerät **20** zugesandt. Und das Ausgangssignal der zweiten elektronischen Wasserzeicheneinbettungseinheit **15** wird sowohl an den Tabelleneintragssuchgenerator **16** als auch an das Endgerät **20** gesandt.

[0319] Das zweite Dateneinheitsendgerät **20** verfügt über: einen Kontraktgenerator **21** zum Aufnehmen von Daten an die Kontraktidentifizierungseinheit **11** vom Endgerät **10**; einen Signaturgenerator **22**; eine zweite Verschlüsselungseinheit **24** zum Aufnehmen von Daten aus der ersten Verschlüsselungseinheit **13** vom Endgerät **10**; eine zweite Entschlüsselungseinheit **25** zum Aufnehmen von Daten aus der zweiten elektronischen Wasserzeicheneinbettungseinheit **15** und aus der ersten Verschlüsselungseinheit **13** im Endgerät **10**; und über eine Tabelleneintragssuchidentifizierungseinheit **27** zum Aufnehmen von Daten aus der zweiten elektronischen Wasserzeicheneinbettungseinheit **15** und aus dem Tabelleneintragssuchgenerator **16** des Endgeräts **10**. Die von der zweiten Entschlüsselungseinheit **25** erzeugten Daten werden als Daten abgegeben, die mit einem elektronischen Wasserzeichen begleitet sind. Die von der zweiten Verschlüsselungseinheit **25** erzeugten Daten werden an die erste Entschlüsselungseinheit **14** des Endgeräts **10** gesandt. Die vom Signaturgenerator **22** erzeugten Daten werden an die zweite elektronische Wasserzeicheneinheit **15** vom Endgerät **10** gesandt.

[0320] Im obigen System ist nur die Information bezüglich des ersten Verschlüsselungsprozesses für den Server verfügbar, sowie das verwendete Verfahren und ein Geheimschlüssel; Information bezüglich des zweiten Verschlüsselungsprozesses ist nur diejenige, die für zweite Dateneinheit verfügbar ist. Angemerkt sei jedoch, daß ein Eigentum dieser Verschlüsselungsprozesse ungeachtet des zuerst ausgeführten Verschlüsselungsprozesses darin besteht, daß eine Mitteilung unter Verwendung des Entschlüsselungsprozesses entschlüsselt werden kann.

[0321] Nachstehend wird der Verschlüsselungsprozeß mit "Ei()" dargestellt, der Entschlüsselungsprozeß wird mit "Di()" dargestellt, und der Einbettungsprozeß bezüglich eines elektronischen Wasserzeichens wird mit "+" dargestellt.

[0322] Nachstehend wird das Verarbeiten erläutert, das das System in Fig. 23 ausführt. Der elektronische Wasserzeicheneinbettungsprozeß wird als erstes beschrieben.

[Einbettungsprozeß]

1) Zuerst fordert die zweite Dateneinheit, das Endgerät **20**, gewünschte Bilddaten an, die die Nutzersignatur tragen, aus dem Endgerät **10**. Die angeforderten Daten sind eine Information (Signaturinformation für die zweite Dateneinheit), die der Kontraktgenerator **21** erzeugt und die nachstehend Kontraktinformation genannt wird.
2) Im Endgerät **10** identifiziert die Kontraktidentifizierungseinheit **11** die empfangene Kontraktinformation unter Verwendung der Signatur für die zweite Dateneinheit und bereitet danach die Nutzerinformation U auf unter Verwendung der Kontraktinformation. Die erste elektronische Wasserzeicheneinbettungseinheit **12** bettet in die angeforderten Bilddaten G die Nutzerinformation U ein, die die Kontraktidentifizierungseinheit **11** aufbereitet hat. Die erste Verschlüsselungseinheit **13** führt einen ersten Verschlüsselungsprozeß E() für

die Bilddaten (G + U) aus, wobei die Nutzerinformation U von der ersten elektronischen Wasserzeicheneinbettungseinheit **12** eingebettet wurde, und die sich ergebenden Bilddaten werden an das Endgerät **20** gesandt. Das Endgerät **20** empfängt somit die ersten verschlüsselten Bilddaten E1(G + U).

3) Im Endgerät **20** führt die zweite Verschlüsselungseinheit **24** einen zweiten Verschlüsselungsprozeß für die ersten verschlüsselten Bilddaten E1(G + U) aus, die vom Endgerät **10** kommen, und sendet die erhaltenen zweiten Verschlüsselungsbilddaten E2(E1(G + U)) an das Endgerät **10**. Gleichzeitig verwendet der Signaturgenerator **22** in der zweiten Dateneinheit den eigenen Geheimschlüssel zum Erzeugen einer Signaturinformation S und sendet diese zum Endgerät **10**.

4) Die erste Entschlüsselungseinheit **14** im Endgerät **10** entschlüsselt den ersten verschlüsselten Abschnitt der zweiten verschlüsselten Bilddaten E2(E1(G + U)), die vom Endgerät **20** kommen. Die zweite elektronische Wasserzeicheneinbettungseinheit **15** identifiziert die Signaturinformation S vom Endgerät **20**. Die zweite elektronische Wasserzeicheneinbettungseinheit **15** bettet die Signaturinformation S in die Bilddaten E2(G + U) ein, die die erste Entschlüsselungseinheit **14** erzeugt hat, und sendet die gewonnenen Bilddaten an das Endgerät **20**. Der Tabelleneintragssuchgenerator **16** erzeugt einen Tabelleneintragssuchwert H1 für die Sendedaten E2(G + U) + S, signiert sie und sendet sie gemeinsam mit den Bilddaten E2(G + U) + S den gewonnenen Tabelleneintragssuchwert H1 an das Endgerät **20**. Im Ergebnis empfängt das Endgerät **20** die Bilddaten E2(G + U) + S sowie den Tabelleneintragssuchwert H1 mit der begleitenden Signatur.

[0323] Der Tabelleneintragssuchwert ist ein solcher, den man durch Berechnen der Tabelleneintragssuchfunktion h() gewinnt, und die Tabelleneintragssuchfunktion ist eine Kompressionsfunktion, die selten eine Kollision verursacht. Eine Kollision in diesem Falle würde bedeuten, daß für unterschiedliche Werte x1 und x2 dann H(x1) = h(x2) ist. Die Kompressionsfunktion ist eine solche zum Umsetzen einer Bitkette mit einer speziellen Bitlänge in eine Bitkette mit veränderter Bitlänge. Die Tabelleneintragssuchfunktion ist eine solche h(x1), durch die eine Bitkette mit spezieller Bitlänge umgesetzt wird in eine Bitkette mit unterschiedlicher Bitlänge, wofür Werte x1 und x2, die der Beziehung h(x1) = h(x2) genügen, nicht gefunden werden. Da Wert x, der der Beziehung y = h(x) genügt, nicht leicht aus einem beliebigen Wert y gewonnen werden kann, ist folglich die Tabelleneintragssuchfunktion eine Unidirektionalfunktion. Spezielle Beispiele für die Tabelleneintragssuchfunktion sind ein MD (Message Digest) 5 oder ein SHA (Secure Hash Algorithm).

[0324] 5) Die Tabelleneintragssuchidentifizierungseinheit **27** des Endgeräts **20** identifiziert den Tabelleneintragssuchwert H1 und dessen begleitende Signatur, die vom Endgerät **10** empfangen werden, und bestätigt, daß der Tabelleneintragssuchwert H1 zum Tabelleneintragssuchwert paßt, der unter Verwendung der Daten E2(G + U) + S erzeugt wird. Nachdem der Bestätigungsprozeß abgeschlossen ist, werden die Daten E2(G + U) + S und der Tabelleneintragssuchwert H1 und dessen begleitende Signatur gespeichert.

[0325] Die zweite Entschlüsselungseinheit **25** entschlüsselt den zweiten verschlüsselten Abschnitt der Daten E2(G + U) + S und liest Bilddaten G_W aus, in die ein elektronisches Wasserzeichen eingebettet ist. Dies zeigt auf, daß die Nutzerinformation U und die zweite verschlüsselte Signaturinformation S als elektronische Wasserzeicheninformation in die Originalbilddaten eingebettet sind.

[0326] Gemäß dem elektronischen Wasserzeicheneinbettungsverfahren dieses Beispiels, wie es zuvor beschrieben wurde, kann grundsätzlich die zweite Dateneinheit keine rechtswidrige Tat begehen, weil die erste Dateneinheit voll verantwortlich für das Einbetten der elektronischen Wasserzeicheninformation ist. Die erste Dateneinheit empfängt die Signaturinformation S direkt von der zweiten Dateneinheit und bettet sie als elektronisches Wasserzeichen ein. Da durch die Prozedur 5) jedoch die Einbettungsprozeßsignaturinformation D2(S), gewonnen vom Endgerät **20**, von der zweiten Verschlüsselung beeinflußt wird, die nur die zweite Dateneinheit ausführen kann, kann die erste Dateneinheit die zweite Dateneinheit nicht veranlassen, wegen einer Straftat durch direktes Einbetten der Signaturinformation D2(S) in die Originalbilddaten beschuldigt zu werden.

[0327] Ist der oben beschriebene Einbettungsvorgang ausgeführt, dann kann die Agentur im Prozeß 1 Bilddaten G_W mit einem elektronischen Wasserzeichen gewinnen, wobei die Signaturinformation in das Originalbild G vom Server oder dem Autor eingebettet ist. Unter der Annahme, daß die Nutzerinformation und die Signaturinformation beim Fortschreiten U1 und S1 sind und daß die Verschlüsselung und die Entschlüsselung von der Agentur ausgeführt werden, dargestellt ist mit Ea() beziehungsweise Da2(), wird das Bild mit dem elektronischen Wasserzeichen, gewonnen von der Agentur, dargestellt mit G_W = G + U1 + Da2(S1). Wenn im Prozeß 2 derselbe Einbettungsvorgang ausgeführt wird, während die Bilddaten G_W der Agentur als Originalbilddaten verwendet werden, dann kann der Nutzer Bilddaten annehmen, die ein elektronisches Wasserzeichen haben, G_{WW} = G + U1 + Da2(S1) + U2 + Du2(S2). In diesem Falle wird angenommen, daß die Nutzerinformation und die Signaturinformation im Prozeß 2 U2 beziehungsweise S2 sind, und die Verschlüsselung und die Entschlüs-

selung, die der Nutzer ausführt, werden zu Eu2() beziehungsweise Ddu2().

[0328] Wenn eine rechtswidrige Kopie G_{ww}' entdeckt ist, dann wird eine Partei, die die rechtswidrige Tat begangen hat, durch den folgenden Nachweisprozeß identifiziert. Dieser Nachweisprozeß wird unterteilt in den Nachweis 1, der dem Prozeß 1 zum Nachweisen des Servers oder des Autors und der Agentur dient, und Nachweis 2 zum Nachweisen der Agentur und des Nutzers. Der Nachweisprozeß 1 erfolgt als erstes, und dann wird der Nachweisprozeß 2 ausgeführt. Beim Nachweis 1 werden die Nutzerinformation und die Signaturinformation festgelegt mit U1 beziehungsweise S1 und die Verschlüsselung und die Entschlüsselung, die die Agentur ausführt, werden zu Ea2() beziehungsweise Da2(). Beim Nachweis 2 werden die Nutzerinformation und die Signaturinformation festgelegt mit U2 beziehungsweise S2, und die Verschlüsselung und die Entschlüsselung, die der Nutzer ausführt, werden festgelegt mit Eu2() beziehungsweise Du2().

[0329] Angemerkt sei, daß Bilddaten nicht durch das Modifizieren oder das Löschen der elektronischen Wasserzeicheninformation beeinflußt werden.

[Nachweisprozeß]

1) Beim Nachweis 1 für den Server S und die Agentur A liest zuerst das Endgerät **10** auf der Serverseite (erste Dateneinheit) die Nutzerinformation U1' aus den rechtswidrigen Bilddaten G_{ww}' = G + U' + U2' + Da(S1') + Du2(S2') aus. Wenn dann die Nutzerinformation U' nicht ausgelesen werden kann, wird ermittelt, daß der Server S die rechtswidrige Tat begangen hat.
2) Der Server S, der die erste Dateneinheit ist, unterbreitet das rechtswidrige Bild G_{ww}' und die ausgelesene Nutzerinformation U1' dem Nachweisbüro und fordert an, daß das Nachweisbüro **30** die Agentur A überprüft, die die zweite Dateneinheit ist.
3) Das Nachweisbüro **30** fordert an, daß die zweite Dateneinheit den zweiten Verschlüsselungscode unterbreitet, der dort gespeichert ist. Das Nachweisbüro **30** führt die zweite Verschlüsselung für das rechtswidrige Bild G_{ww}' aus, um die Signaturinformation S1' auszulesen.
4) Wenn die korrekte Signaturinformation S1' ausgelesen ist, das heißt, wenn S1' = S1 ist, wird ermittelt, daß der Server S, der die erste Dateneinheit ist, die rechtswidrige Tat nicht begangen hat, und die Programmsteuerung schreitet fort zum Nachweis 2.
5) Wird in der Prozedur 4) die korrekte Signaturinformation nicht ausgelesen, das heißt, wenn S1' nicht gleich S1 ist, dann überprüft das Nachweisbüro **30** die Daten Ea2(G + U1) + S1, den Tabelleneintragssuchwert H1 und dessen begleitende Signatur S1, die alle der Server S sendet, der die erste Dateneinheit ist, an die Agentur A, die die zweite Dateneinheit ist. Das Nachweisbüro **30** bestätigt, daß der Tabelleneintragssuchwert H1 zum Tabelleneintragssuchwert paßt, der aus Ea2(G + U1) + S1 gewonnen wurde. Dann entschlüsselt das Nachweisbüro **30** die Daten Ea2(G + U1) + S1 unter Verwendung des zweiten Verschlüsselungscodes, der von der Agentur A in Prozedur 3) unterbreitet wurde, und liest die Bilddaten G_W aus, in die ein elektronisches Wasserzeichen eingebettet wird.
6) Wenn die korrekten Bilddaten, in die das elektronische Wasserzeichen eingebettet ist, nicht ausgelesen werden können, wird ermittelt, daß die Agentur A die rechtswidrige Tat begangen hat. Das bedeutet, daß der zweite Verschlüsselungscode in Prozedur 3) nicht korrekt ist.
7) Wenn die korrekten Bilddaten, in die ein elektronisches Wasserzeichen eingebettet ist, ausgelesen werden können, wird ermittelt, daß der Server die rechtswidrige Tat begangen hat.

[0330] Nachstehend erläutert ist der Nachweis 2, der durchgeführt wird, wenn in Prozedur 4) ermittelt ist, daß der Server die rechtswidrige Tat nicht begangen hat. Beim Nachweis 2 wird die Nutzerinformation U' aus den rechtswidrigen Bilddaten G_{ww}' = G + U1' + U2' + Da2(S1') + Du2(S2') ausgelesen. Wird die Nutzerinformation U2' nicht ausgelesen, dann wird ermittelt, daß die Agentur A, die die erste Dateneinheit ist, die rechtswidrige Tat begangen hat.

[0331] Wie in der obigen Prozedur **2**) unterbreitet die Agentur A, die als erste Dateneinheit beim Nachweis **2** dient, die rechtswidrigen Bilddaten G_{ww}' und die ausgelesene Nutzerinformation U2' dem Nachweisbüro **30** und fordert an, daß das Nachweisbüro **30** den Nutzer U überprüft, der die zweite Dateneinheit ist. Wie in der Prozedur **3**) fordert das Nachweisbüro **30** an, daß die zweite Dateneinheit den dort gespeicherten zweiten Verschlüsselungscode unterbreitet, und liest die Signaturinformation S2' aus, indem die zweite Verschlüsselung für die rechtswidrigen Bilddaten G_{ww}' ausgeführt wird. Ist die korrekte Signaturinformation S' ausgelesen, das heißt, wenn S2' = S2 ist, dann wird ermittelt, daß der Nutzer, der die zweite Dateneinheit ist, die rechtswidrige Tat begangen hat.

[0332] Wenn die korrekte Signaturinformation S2' nicht ausgelesen werden kann, das heißt, wenn die Signaturinformation S2' nicht zu S2 wie in Prozedur 5) paßt, dann überprüft das Nachweisbüro **30** die Daten Eu2(G_W + U2) + S2 und den Tabelleneintragssuchwert H1' und dessen begleitende Signatur S2, die alle von der Agentur A, die die erste Dateneinheit ist, ein den Nutzer U gesendet werden, der die zweite Dateneinheit ist. Das Nachweisbüro **30** bestätigt dann, daß der Tabelleneintragssuchwert H1' zum Ta-

belleneintragssuchwert paßt, der aus den Daten $Eu2(G_W + U2) + S2$ gewonnen wird, und danach entschlüsselt das Nachweisbüro **30** die Daten $Eu2(G_W + U2) + S2$ unter Verwendung des zweiten Verschlüsselungscodes, der vom Nutzer U unterbreitet wurde, und liest die Bilddaten G_{WW} aus, in die ein elektronisches Wasserzeichen eingebettet ist.

[0333] Wenn die korrekten Bilddaten, in die das elektronische Wasserzeichen eingebettet ist, nicht ausgelesen werden können, wird wie in Prozedur 6) ermittelt, daß der Nutzer U, der die zweite Dateneinheit ist, die rechtswidrige Tat begangen hat.

[0334] Dies bedeutet, daß der zweite Verschlüsselungscode, den der Nutzer unterbreitet hat, nicht korrekt ist. Wenn die korrekten Bilddaten, in die das elektronische Wasserzeichen eingebettet ist, ausgelesen werden können, dann wird wie in Prozedur 7) ermittelt, daß die Agentur A, die die erste Dateneinheit ist, die rechtswidrige Tat begangen hat.

[0335] Für den Nachweis 1 und für den Nachweis 2 wird im wesentlichen dieselbe Prozedur wie oben beschrieben ausgeführt, und nur die Definitionen für die erste und die zweite Dateneinheit müssen geändert werden. Auch die Partei, die die rechtswidrige Tat begangen hat, kann in derselben Weise identifiziert werden.

[0336] Wie aus dem Nachweisprozeß hervorgeht, beinhaltet das Endgerät des Nachweisbüros **30** dieselben Funktionen wie die zweite Verschlüsselungseinheit **24**, die zweite Entschlüsselungseinheit **25** und die Tabelleneintragssucheinheit **27** vom Endgerät **20**.

[0337] Da im obigen Beispiel die Prozesse 1 und 2 unabhängig voneinander ausgeführt werden, ist eine Kollusion sinnlos. Selbst wenn beispielsweise die Agentur mit dem Nutzer kolludiert, kann der Nutzer den Prozeß 1 nicht beeinflussen. Selbst wenn der Server mit der Agentur kolludiert oder wenn der Server mit den Nutzer kolludiert, so könnten weder der Nutzer noch die Agentur die letztlichen Bilddaten erhalten, die ein elektronisches Wasserzeichen enthalten, das durch die Verschlüsselung vom Nutzer oder von der Agentur bewirkt wird.

[0338] Es gibt für das Nachweisbüro **30** keinen Bedarf, bis ein rechtswidriges Bild festgestellt ist, und es kann keine rechtswidrige Tat als ausgeführt bestimmt werden, bis ein rechtswidriges Bild entdeckt worden ist. So lange die oben beschriebene Nachweisverarbeitung allgemein bekannt ist und die erste und zweite Dateneinheit die Ergebnisse dieser Verarbeitung überwachen, kann darüber hinaus von diesen eine rechtswidrige Tat entsprechend der Situation festgestellt werden, selbst ohne Einbeziehen des Nachweisbüros.

(Fünftes Ausführungsbeispiel)

[0339] Der Geldtransfer über Netzwerke, eine Wertpapierübertragungsprozedur, die man elektronische Barzahlung nennt, ist seit kurzem in Verwendung gekommen. Da wie bei regulärer Bargeldzahlung der Name vom Eigentümer der elektronischen Bargeldübertragung nicht identifiziert wird, bleibt die Anonymität erhalten. Wenn das Erzielen von Anonymität nicht möglich wäre, könnte ein Verkäufer eines Produkts aus dem elektronischen Bargeldtransfer Informationen bezüglich eines Käufers und die Nutzung des Produkts beziehen, womit die Privatsphäre des Nutzers nicht geschützt wäre. Der Schutz der Privatsphäre eines Nutzers ist genauso wichtig wie der Schutz, den man für ein dem Schöpfer gewährtes Copyright bereitstellt, der ein elektronisches Wasserzeichen verwendet.

[0340] Im einem fünften Ausführungsbeispiel ist folglich die Anonymität des Nutzers für einen Käufer vorgesehen, und wenn eine rechtswidrige Tat entdeckt wird, wie das rechtswidrige Verteilen von Bildern, dann ist es möglich, den nichtberechtigten Verteiler zu identifizieren, was die Ursprungsabsicht eines elektronischen Wasserzeichens bedeutet. Dies wird erzielt durch Verwenden beispielsweise eines in Fig. 24 gezeigten Systems.

[0341] Das System hat dieselbe Struktur wie das in Fig. 23 gezeigte System **100**, wobei eine Bescheinigung mit anonymem öffentlichem Schlüssel, die ein Bescheinigungsbüro **40** ausgibt, für ein Nutzerendgerät **20** vorgesehen ist.

[0342] Um die Signaturinformation zu berechtigen, wird im allgemeinen eine Bescheinigung von einer Organisation ausgestellt, die Bescheinigungsbüro genannt wird, und diese wird dem öffentlichen Schlüssel hinzugefügt, der Verwendung findet, wenn die Signaturinformation überprüft wird.

[0343] Ein Bescheinigungsbüro ist eine Organisation, die Bescheinigungen für öffentliche Schlüssel ausgibt, die für Nutzer ausgestellt werden, um die öffentliche Schlüsselberechtigung bereitzustellen, die in Übereinstimmung mit den Erfordernissen des öffentlichen Codeverschlüsselungssystems ist. Das heißt, ein Bescheinigungsbüro verwendet den eigenen Geheimschlüssel zum Bereitstellen einer Signatur für den öffentlichen Schlüssel des Nutzers oder für Daten, die den Nutzer betreffen, und zu diesem Zweck wird eine Bescheinigung vorbereitet und ausgestellt. Wenn ein Nutzer von einem anderen Nutzer eine Signatur erhält, die mit einer Bescheinigung versehen ist, dann überprüft der Nutzer die Bescheinigung unter Verwendung des öffentlichen Schlüssels des Bescheinigungsbüros, um die Berechtigung nachzuweisen, die vom Nutzer bereitgestellt wird, der den öffentlichen Schlüssel gesandt hat (oder we-

nigstens die Tatsache, daß die Berechtigung dem Nutzer vom Bescheinigungsbüro gegeben wurde). Sowohl VeriSign als auch CyberTrust sind allgemein bekannte Organisationen, die derartige Bescheinigungsbüros betreiben.

[0344] Wenn bei Prozedur 2) des Einbettungsprozesses im Beispiel von Fig. 23 eine erste Dateneinheit eine Signatur überprüft, um die Kontraktinformation nachzuweisen, die für einen Nutzer (zweite Dateneinheit) unterbreitet wurde, dann kann die erste Dateneinheit den öffentlichen Schlüssel mit einer Signatur verwenden, die vom Bescheinigungsbüro **40** in Fig. 24 ausgestellt wurde. Da der Name des Besitzers vom öffentlichen Schlüssel im allgemeinen in die Bescheinigung geschrieben ist, wird die Nutzeranonymität nicht zu der Zeit gewahrt, zu der die Daten gekauft werden.

[0345] Wenn das Bescheinigungsbüro **40** die Verbindung der öffentlichen Schlüssel und deren Besitzern andererseits geheim hält, dann kann der Name des Besitzers nicht in eine Bescheinigung geschrieben werden, die für einen öffentlichen Schlüssel ausgegeben wird. Eine anonyme Bescheinigung für einen öffentlichen Schlüssel wird hiernach als "anonyme öffentliche Schlüsselbescheinigung" bezeichnet, und ein öffentlicher Schlüssel, für den eine derartige Bescheinigung vorgesehen ist, wird "anonymer öffentlicher Schlüssel mit Bescheinigung" genannt. wenn in der Prozedur 1) des oben beschriebenen Einbettungsprozesses ein Nutzer U nicht nur die Kontraktinformation, sondern auch eine Signatur für die Kontraktinformation und einen anonymen öffentlichen Schlüssel in Begleitung einer Bescheinigung an einen Server sendet, um die Überprüfung der Signaturinformation S zu ermöglichen, dann kann der Nutzer beim Verkauf digitaler Daten anonym bleiben.

[0346] Der anonyme öffentliche Schlüssel, der von der Bescheinigung begleitet ist, wird folglich an die Agentur A als Information gesendet, die zum Nachweis des Nutzers U zu verwenden ist. Und wenn eine rechtswidrige Transaktion entdeckt wird und der Nutzer identifiziert werden muß, dann wird der anonyme öffentliche Schlüssel gemeinsam mit der Bescheinigung an das Bescheinigungsbüro **40** mit einer Anfrage nach dem Nutzernamen gesandt, der demjenigen des Besitzers vom öffentlichen Schlüssel entspricht. Wenn die Prozeduren 1) und 2) im Einbettungsprozeß und die Prozeduren 1) und 2) im Nachweisprozeß im Beispiel von Fig. 23 folgendermaßen ausgeführt werden, dann kann folglich die Anonymität des Nutzers U beim Kauf digitaler Daten aufrecht erhalten werden, aber wenn eine rechtswidrige Transaktion entdeckt wird, dann kann der für das Begehen der Transaktion verantwortliche Nutzer identifiziert werden.

[0347] Der Einbettungsprozeß und der Nachweisprozeß, den das System gemäß Fig. 24 ausführt, werden speziell beschrieben.

[0348] Im in Fig. 24 gezeigten System bedeuten dieselben wie im System von Fig. 23 verwendeten Bezugszeichen die entsprechenden Komponenten, und eine spezielle Erläuterung wird nur für die Abschnitte gegeben, die sich unterscheiden. Da die Verarbeitung dieselbe ist wie im Beispiel von Fig. 23, mit Ausnahme der Prozeduren 1) und 2) im Einbettungsprozeß und der Prozeduren 1) und 2) im Nachweisprozeß, werden diese nicht erneut erläutert.

[Einbettungsprozeß]

1) Im zweiten Dateneinheitsendgerät (Nutzerendgerät) **20** stellt als erstes ein Kontraktgenerator **21** als Kontraktinformation für die Nachfrage nach gewünschten Bilddaten eine Signatur bereit, die einem anonymen öffentlichen Schlüssel entspricht, der von einer Bescheinigung begleitet wird, die ein Bescheinigungsbüro **40** ausgibt. Gemeinsam mit dem anonymen öffentlichen Schlüssel und der begleitenden Bescheinigung sendet das zweite Endgerät **20** die Kontraktinformation an das Endgerät **10** der ersten Dateneinheit (Agentur).

[0349] In der ersten Dateneinheit, im Endgerät **10**, überprüft eine Kontraktidentifizierungseinheit **11** den öffentlichen Schlüssel, der zur z weiten Dateneinheit (Nutzer) gehört, unter Verwendung des öffentlichen Schlüssels vom Bescheinigungsbüro **40**. Die Kontraktidentifizierungseinheit **11** identifiziert die Signatur für die Kontraktinformation unter Verwendung des anonymen öffentlichen Schlüssels der zweiten Dateneinheit, und nachdem die Bestätigungsverarbeitung abgeschlossen ist, wird eine Nutzerinformation U unter Verwendung wenigstens entweder der Kontraktinformation oder des anonymen öffentlichen Schlüssels aufbereitet. Eine erste elektronische Wasserzeicheneinbettungseinheit **12** bettet in Bilddaten G die Nutzerinformation U ein, die die Kontraktidentifizierungseinheit **11** vorbereitet hat. Eine erste Verschlüsselungseinheit **13** führt die erste Verschlüsselung E1() für die Bilddaten G aus und sendet die gewonnenen Daten an die zweite Dateneinheit, Endgerät **20**. Die zweite Dateneinheit, Endgerät **20**, empfängt somit die ersten verschlüsselten Bilddaten E1(G + U).

[0350] Danach werden die Prozeduren 3) bis 5) im Einbettungsprozeß gemäß dem Beispiel in Fig. 23 ausgeführt.

[0351] Die Prozeduren 1) und 2) im Einbettungsprozeß gemäß dem fünften Ausführungsbeispiel können entweder für eine oder für beide vorherig erwähnten Prozesse 1 und 2 angewandt werden. Während die Anonymität im allgemeinen für die Agentur nicht be-

sonders wichtig ist, um die Privatsphäre beizubehalten, ist die Nutzeranonymität sehr wichtig, und sie ist insbesondere in diesem Ausführungsbeispiel wichtig, weil der Einbettungsprozeß verwendet wird, wenn die Agentur ihre Inhalte als elektronische Information an den Nutzer verteilt.

[0352] Als Abwandlung des Ausführungsbeispiels ist folglich ein hierarchisches System effektiver, wenn das in Fig. 23 gezeigte System für die Verteilung der elektronischen Information durch den Server an die Agentur erfolgt, und wenn das System für das fünfte Ausführungsbeispiel gemäß Fig. 24 für die Verteilung der elektronischen Information durch die Agentur an den Nutzer verwendet wird. Das heißt, in einem hierarchischen System kann die Privatsphäre des Nutzers geschützt werden, wenn die Anzahl von Anforderungen, die dem Bescheinigungsbüro **40** unterbreitet werden, möglichst auf ein Minimum beschränkt sind.

[Nachweisprozeß]

[0353] Der Nachweisprozeß ist äußerst effektiv, wenn er auf den Nachweis 2 im Beispiel von Fig. 23 angewandt wird. Erläutert wird dieser Fall folglich unter der Annahme, daß die nachfolgenden Prozeduren 1) und 2) auf den Nachweisprozeß angewandt werden, den die Agentur und der Nutzer ausführen, das heißt Nachweis 2. Zu dieser Zeit wird angenommen, daß in Prozedur 4) von Nachweis 1 ermittelt wurde, daß der Server S keine rechtswidrige Tat begangen hat.

1) In Nachweis 2 für die Agentur A und den Server S liest zunächst das Endgerät **10** auf Seite der Agentur (die erste Dateneinheit) die Nutzerinformation U2' aus den rechtswidrigen Bilddaten G_{WW}' = G + U1' + U2' + Da2(S1') + Du(S2') aus. Kann die Nutzerinformation U2' nicht ausgelesen werden, dann wird ermittelt, daß die Agentur A die rechtswidrige Tat begangen hat. Wenn die Nutzerinformation U2 ausgelesen wurde, werden die ausgelesene Nutzerinformation U2 und der anonyme öffentliche Schlüssel aus der Kontraktinformation dem Bescheinigungsbüro **40** übermittelt, um den Nutzernamen anzufordern, der dem öffentlichen Schlüssel entspricht.

2) Die Agentur A, welches die erste Dateneinheit ist, unterbreitet das rechtswidrige Bild G_{WW}' und die ausgelesene Nutzerinformation U2' dem Nachweisbüro und fordert das Nachweisbüro auf, den Nutzer zu überprüfen, dessen Name dem öffentlichen Schlüssel entspricht.

[0354] Die oben beschriebenen Prozeduren 3) bis 7) im Nachweisprozeß gemäß dem Beispiel in Fig. 23 werden ausgeführt.

[0355] Wenn gemäß dem zuvor beschriebenen fünften Ausführungsbeispiel Digitaldaten gekauft werden, dann kann der Nutzer bezüglich dem Nachweisbüro anonym bleiben.

[0356] Nachstehend anhand Fig. 25 beschrieben ist ein weiteres Beispiel. Dieses Beispiel unterscheidet sich vom Beispiel in Fig. 23 darin, daß die Signaturinformation für die zweite Dateneinheit als elektronisches Wasserzeichen anstelle des ersten Dateneinheitsendgeräts **10** vom zweiten Dateneinheitsendgerät **20** eingebettet ist. Dieselben Bezugszeichen, wie sie in Fig. 23 verwendet werden, werden ebenfalls zum Beschreiben der entsprechenden Komponenten in Fig. 25 verwendet. Für die mit Fig. 23 identische Verarbeitung wird keine erneute Beschreibung gegeben.

[0357] Ein Endgerät **10** ist ausgestattet mit: einer Kontraktidentifizierungseinheit **11** zum Aufnehmen von Daten aus dem Endgerät **20**; einer elektronischen Wasserzeicheneinbettungseinheit **12** zum Aufnehmen von beispielsweise Bilddaten (Digitaldaten); einer ersten Verschlüsselungseinheit **13** zum Aufnehmen des Ausgangssignals von der elektronischen Wasserzeicheneinbettungseinheit **12**; einer ersten Verschlüsselungseinheit **34** zum Aufnehmen von Daten aus dem Endgerät **20**; einer Tabelleneintragssuchidentifizierungseinheit **35** zum Aufnehmen von Daten aus dem Endgerät **20** und aus der ersten Entschlüsselungseinheit **34**; und mit einem Tabelleneintragssuchgenerator **36** zum Aufnehmen des Ausgangssignals aus der ersten Entschlüsselungseinheit **34**. Die Ausgangssignale der ersten Verschlüsselungseinheit **13** und des Tabelleneintragssuchgenerators **36** werden an das Endgerät **20** gesandt. Das Ausgangssignal der ersten Entschlüsselungseinheit **34** wird sowohl an den Tabelleneintragssuchgenerator **36** als auch an das Endgerät **20** gesandt.

[0358] Das zweite Dateneinheitsendgerät **20** ist ausgestattet mit: einem Kontraktgenerator **21** zum Senden von Daten an die Kontraktidentifizierungseinheit **11** vom Endgerät **10**; einem Signaturgenerator **22**; einer elektronischen Wasserzeicheneinbettungseinheit **43** zum Aufnehmen von Daten aus dem Signaturgenerator **22** und aus der ersten Verschlüsselungseinheit **13** des Endgeräts **10**; einer zweiten Verschlüsselungseinheit **44** zum Aufnehmen von Daten aus der elektronischen Wasserzeicheneinbettungseinheit **43**; einem Tabelleneintragssuchgenerator **46** zum Aufnehmen des Ausgangssignal der zweiten Verschlüsselungseinheit **44**; und mit einer zweiten Entschlüsselungseinheit **45** zum Aufnehmen von Daten aus der ersten Entschlüsselungseinheit **34** vom Endgerät **10**; sowie mit einer Tabelleneintragssuchidentifizierungseinheit **47** zum Aufnehmen von Daten aus der ersten Entschlüsselungseinheit **34** und aus dem Tabelleneintragssuchgenerator **36** des Endgeräts **10**. Die von der zweiten Entschlüsselungseinheit **45** erzeugten Daten werden als Daten abgegeben, in die ein elektronisches Wasserzeichen

eingebettet ist.

[0359] Die Daten, die die zweite Verschlüsselungseinheit **44** erzeugt, werden an die erste Entschlüsselungseinheit **34** und an die Tabelleneintragssuchidentifizierungseinheit **34** vom Endgerät **10** gesandt. Die Daten, die der Tabelleneintragssuchgenerator **36** erzeugt hat, werden an die Tabelleneintragssuchidentifizierungseinheit **35** vom Endgerät **10** gesandt.

[0360] Der vom System gemäß Fig. 25 ausgeführte elektronische Wasserzeicheneinbettungsprozeß ist nachstehend beschrieben.

[Einbettungsprozeß]

[0361] Da die Prozeduren 1) und 2) dieselben sind wie jene im Beispiel von Fig. 23, wird keine erneute Erläuterung hierzu gegeben.

3) Im Endgerät **20** erzeugt der Signaturgenerator **22** die Signaturinformation S unter Verwendung des Geheimschlüssels, der zur zweiten Dateneinheit gehört.

[0362] Die elektronische Wasserzeicheneinbettungseinheit **43** bettet die Signaturinformation S, erzeugt vom Signaturgenerator **22**, in die ersten verschlüsselten Bilddaten E1(G + U) ein, die vom Endgerät **10** gesendet (verteilt) wurden.

[0363] Die zweite Verschlüsselungseinheit **44** führt die zweite Verschlüsselung für die ersten verschlüsselten Bilddaten E1(G + U) + S aus, in die die Signaturinformation **5** von der elektronischen Wasserzeicheneinbettungseinheit **43** eingebettet wurde. Die erzielten Bilddaten werden an das erste Dateneinheitsendgerät **10** gesandt.

[0364] Das Endgerät **10** empfängt folglich die zweiten verschlüsselten Bilddaten E2(E1(G + U) + S).

[0365] Der Tabelleneintragssuchgenerator **46** erzeugt einen Tabelleneintragssuchwert H2 für die zweiten verschlüsselten Bilddaten E2(E1(G + U) + S), die an das Endgerät **10** zu senden sind. Der Tabelleneintragssuchgenerator **46** stellt dann eine Signatur für den Tabelleneintragssuchwert H2 bereit und sendet diesen an das Endgerät **10** mit einer Geheiminformation, die sich von der Signaturinformation S unterscheidet, bezüglich des elektronischen Wasserzeichens.

[0366] Die Geheiminformation ist eine solche, die die Einbettungsstelle und die Stärke betrifft, die erforderlich sind zum Feststellen des elektronischen Wasserzeichens, das nach einem anderen Verschlüsselungsverfahren verschlüsselt worden ist, das gemeinsam mit dem Endgerät **10** verwendet wird.

4) Im Endgerät **10** identifiziert die Tabelleneintragssuchidentifizierungseinheit **35** die Signatur für den Tabelleneintragssuchwert H2 aus dem Nutzerendgerät **20** und bestätigt, daß der Tabelleneintragssuchwert H2 zum Tabelleneintragssuchwert der zu sendenden Daten paßt. Nach Abschluß des Bestätigungsprozesses wird der Tabelleneintragssuchwert H2 gespeichert.

[0367] Die erste Entschlüsselungseinheit **34** entschlüsselt den ersten Verschlüsselungsabschnitt der zweiten verschlüsselten Bilddaten E2(E1(G + U) + S) aus dem Endgerät **20** und sendet die gewonnenen Bilddaten an das Endgerät **20**.

[0368] Auf diese Weise empfängt das Nutzerendgerät **20** die Bilddaten E2(G + U) + D1(E2(S)).

[0369] Der Tabelleneintragssuchgenerator **36** erzeugt einen Tabelleneintragssuchwert H1 für die Bilddaten E2(G + U) + D1(E2(S)), die dem Endgerät **20** zu übermitteln sind. Der Tabelleneintragssuchgenerator **36** stellt dann eine Signatur für den Tabelleneintragssuchwert H1 bereit und sendet diese an das Endgerät **20**.

5) Im Endgerät **20** identifiziert die Tabelleneintragssuchidentifizierungseinheit **47** die Signatur für den Tabelleneintragssuchwert H1 aus dem Serverendgerät **10** und bestätigt, daß der Tabelleneintragssuchwert H1 zum Tabelleneintragssuchwert der zu sendenden Daten paßt. Nachdem die Bestätigung abgeschlossen ist, wird der Tabelleneintragssuchwert H1 gespeichert.

[0370] Die zweite Entschlüsselungseinheit **45** entschlüsselt den zweiten verschlüsselten Abschnitt der Bilddaten E2(G + U) + D1(E2(S)) aus dem Endgerät **10** und liest die Bilddaten G_W aus, in die ein elektronisches Wasserzeichen eingebettet ist.

[0371] Die Bilddaten G_W, in die das elektronische Wasserzeichen eingebettet ist, werden folglich dargestellt mit $G_W = G + U + D1(S)$. Das bedeutet, daß das elektronische Wasserzeichen (Nutzerinformation) U und das elektronische Wasserzeichen (Signaturinformation), die von der ersten Verschlüsselung beeinflußt wird, in die Originalbilddaten G eingebettet sind.

[0372] Die Bilddaten G_W, in die das elektronische Wasserzeichen eingebettet ist, werden gespeichert.

[0373] Wie zuvor beschrieben wird die Nutzerinformation U durch die Verschlüsselung nicht beeinflußt, und die Signaturinformation S wird von der ersten Entschlüsselung beeinflußt.

[0374] Beim Ausführen des oben beschriebenen Einbettungsprozesses kann in Prozeß 1 die Agentur Bilddaten G_W gewinnen, in die ein elektronisches Wasserzeichen eingebettet ist, wobei die Signaturinformation in das Originalbild G vom Server oder vom

Autor eingebettet ist. Unter der Annahme, daß die Nutzerinformation und die Signaturinformation in Prozeß 1 gleich U1 und S1 sind, sind die vom Nutzer ausgeführte Verschlüsselung und Entschlüsselung gleich Es1() und Ds1(), die von der Agentur ausgeführte Verschlüsselung und Entschlüsselung sind gleich Ea() und Da2(), und das Bild, in das das elektronische Wasserzeichen eingebettet ist, gewonnen von der Agentur, wird dargestellt mit G_W = G + U1 + Ds1(S1). Wenn in Prozeß 2 derselbe Einbettungsprozeß ausgeführt wird, während die Bilddaten G_W der Agentur als Originalbilddaten verwendet werden, kann der Nutzer Bilddaten mit einem elektronischen Wasserzeichen G_{WW} = G + U1 + Ds1(S1) + U2 + Da1(S2) gewinnen, wobei die von der Agentur ausgeführte Verschlüsselung und die Entschlüsselung gleich Ea1() und Da1() sind. In diesem Falle wird angenommen, daß die Nutzerinformation und die Signaturinformation im Prozeß 2 gleich U2 beziehungsweise S2 sind.

[0375] Wird eine rechtswidrige Kopie G_{WW}' entdeckt, wie im Beispiel von Fig. 23, erfolgt die Unterteilung der Nachweisverarbeitung in den Nachweis 1, der dem Prozeß 1 entspricht, um den Server oder den Autor und die Agentur nachzuweisen, und in den Nachweis 2, um die Agentur und den Nutzer nachzuweisen. Der Nachweisprozeß 1 wird als erstes ausgeführt, und dann erfolgt der Nachweisprozeß 2. Beim Nachweis 1 werden die Nutzerinformation und die Signaturinformation mit U1 beziehungsweise mit S1 festgelegt, und die Verschlüsselung und die Entschlüsselung, die der Server ausführt, werden festgelegt mit Es1() beziehungsweise mit Ds1(). Im Nachweis 2 werden die Nutzerinformation und die Signaturinformation festgelegt mit U2 beziehungsweise mit S2, und die Verschlüsselung und die Entschlüsselung, die die Agentur ausführt, werden festgelegt mit Ea1() beziehungsweise mit Da().

[0376] Angemerkt sei, daß die Bilddaten durch die Modifizierung oder das Löschen der elektronischen Wasserzeicheninformation nicht beeinflußt werden, wie im fünften Ausführungsbeispiel.

[Nachweisprozeß]

1) Beim Nachweis 1 für den Server S und die Agentur A liest das Endgerät **10** auf der Serverseite (die erste Dateneinheit) zunächst die Nutzerinformation U1' aus den rechtswidrigen Bilddaten G_{WW}' = G + U' + U2' Ds1(S1') + Da1(S2') aus. Das Endgerät **20** führt eine erste Verschlüsselung Es1() für die Bilddaten G_{WW}' aus und liest die Signaturinformation S1' aus. Kann die Nutzerinformation U1' nicht ausgelesen werden, wird ermittelt, daß der Server S die rechtswidrige Tat begangen hat.

2) Ist die korrekte Signaturinformation S1' ausgelesen, das heißt wenn S1' 0 S1 ist, dann übermittelt der Server S die Signaturinformation S1' an das Nachweisbüro **30**, das heißt, es wird ermittelt, daß der Server S, der die erste Dateneinheit ist, die rechtswidrige Tat nicht begangen hat. Die Programmsteuerung schreitet fort zum Nachweis 2.

3) Wenn die korrekte Signaturinformation in Prozedur 2) nicht ausgelesen werden kann, das heißt, wenn S1' nicht zu S1 paßt, wird der Server S zur Anforderung des Nachweises, der die erste Dateneinheit ist, dem Nachweisbüro **30** den gespeicherten Tabelleneintragssuchwert für die zweiten verschlüsselten Bilddaten Ea2(Es1(G + U1) + S1) unterbreiten, und zwar mit der begleitenden Signatur, dem ersten Verschlüsselungscodeschlüssel und der Geheiminformation bezüglich der rechtswidrigen Bilddaten G_{WW}'.

4) Nach Empfang der Anforderung in Prozedur 3) ermittelt das Nachweisbüro **30**, daß die korrekte Signaturinformation S1 nicht aus den rechtswidrigen Bilddaten G_{WW}' ausgelesen werden kann. Dann überprüft das Nachweisbüro **30** den unterbreiteten Tabelleneintragssuchwert H2 und dessen begleitende Signatur, um zu bestätigen, daß der Tabelleneintragssuchwert von den zweiten verschlüsselten Bilddaten Ea2(Es1(G + U1) + S1) zum Tabelleneintragssuchwert H2 paßt, der unterbreitet wurde.

[0377] Nach Abschluß des Bestätigungsprozesses entschlüsselt das Nachweisbüro **30** den ersten verschlüsselten Abschnitt der zweiten verschlüsselten Bilddaten Ea2(Es1(G + U1) + S1), um die Bilddaten Ea2(G + U1) + Ds1(Ea2(S1)) zu gewinnen. Das Nachweisbüro **30** bestätigt, daß der Tabelleneintragssuchwert für die erzielten Daten zu dem Tabelleneintragssuchwert H1 paßt, den die Agentur A hält, die die zweite Dateneinheit ist. Zu dieser Zeit wird auch die Signatur für den Tabelleneintragssuchwert H1 identifiziert.

5) Wenn in Prozedur 4) der Tabelleneintragssuchwert für die Daten Ea2(G + U1) + Ds1(Ea2(S1)) nicht zum Tabelleneintragssuchwert H1 paßt, wird ermittelt, daß der Server S, der die erste Dateneinheit ist, die rechtswidrige Tat begangen hat. Dies bedeutet, daß die Geheimschlüssel für die erste Verschlüsselung in Prozedur 4) vom Einbettungsprozeß und in Prozedur 4) vom Nachprozeß sich unterscheiden.

6) Wenn die beiden Tabelleneintragssuchwerte zueinander passen, dann fordert das Nachweisbüro an, daß die Agentur A, die die zweite Dateneinheit ist, den zweiten verschlüsselten Abschnitt der Daten Ea2(G + U1) + Ds1(Ea2(S1)) entschlüsselt, der in Prozedur 4) des Nachweisprozesses gewonnen wurde. Das Nachweisbüro **30** liest die Signaturinformation S1 aus den sich ergebenden Bilddaten.

7) Wenn die korrekte Signaturinformation S1 nicht ausgelesen wird, das heißt, wenn S1' nicht zu S1 paßt, wird ermittelt, daß die Agentur A die rechts-

widrige Tat begangen hat.
8) Ist die korrekte Signaturinformation ausgelesen, dann wird ermittelt, daß es nicht die Agentur, sondern der Server S war, der die rechtswidrige Tat begangen hat.

[0378] Die nächste Erläuterung gilt dem Nachweis 2, der durchgeführt wird, wenn ermittelt ist, daß der Server S keine rechtswidrige Tat begangen hat. Beim Nachweis 2 wird, wie in Prozedur 1), die Nutzerinformation U2' aus dem rechtswidrigen Bild G_{ww}' = G + U1' + U2' + Ds1(S1') + Da1(S2') ausgelesen. Auch wird die erste Verschlüsselung Ea1() für die Bilddaten G_{ww}' ausgeführt, um die Signaturinformation S2' auszulesen. Wenn die Nutzerinformation U2' nicht ausgelesen werden kann, wird ermittelt, daß die Agentur A die rechtswidrige Tat begangen hat.

[0379] Ist die korrekte Signaturinformation S2' ausgelesen, wie in der obigen Prozedur 2), das heißt, wenn S2' = S2 ist, unterbreitet die Agentur A die Signaturinformation S2' dem Nachweisebüro **30** zum Ermitteln, ob der Nutzer U die rechtswidrige Tat begangen hat.

[0380] Dies geschieht, weil die Signaturinformation S2' nur vom Nutzer U, dem Server S und der Agentur A vorbereitet wird, die keine Kenntnis über die Signaturinformation S2' haben. Angemerkt sei, daß die Rechtmäßigkeit der Signaturinformation S2' nachgewiesen werden kann durch Bestimmen, ob eine vorbestimmte Information, die im voraus von der Kontraktinformation festgelegt ist, unter Verwendung eines öffentlichen Schlüssels ausgegeben werden kann, der dem Geheimschlüssel vom Nutzer entspricht, und beim Erzeugen der Signaturinformation verwendet wird.

[0381] Wird die korrekte Information S2 nicht ausgelesen, wie in Prozedur 3), unterbreitet die Agentur A, die die erste Dateneinheit ist, dem Nachweisbüro **30** den Tabelleneintragssuchwert H2 für gespeicherten zweiten verschlüsselten Bilddaten Eu2(Ea1(G + U1 + U2 + Ds1(S1)) + S2) mit der begleitenden Signatur, dem Geheimschlüssel für die erste Verschlüsselung und mit der Geheiminformation bezüglich des rechtswidrigen Bildes G_{ww}'.

[0382] Wie in Prozedur 4) bestimmt das Nachweisbüro **30**, daß die korrekte Signaturinformation S2 nicht aus dem rechtswidrigen Bild G_{ww}' gelesen werden kann. Das Nachweisbüro **30** überprüft den Tabelleneintragssuchwert H2 und die Signatur, die unterbreitet wurde, und bestätigt, daß der Tabelleneintragssuchwert für die zweiten verschlüsselten Bilddaten Eu2(Ea1(G + U1 + U2 + Ds1(S1)) + S2) zum Tabelleneintragssuchwert H2 paßt, der unterbreitet worden ist. Nach Abschluß des Bestätigungsprozesses entschlüsselt das Nachweisbüro **30** den ersten verschlüsselten Abschnitt der zweiten verschlüsselten Bilddaten Eu2(Ea1(G + U1 + U2 + Ds1(S1)) + S2) und erhält die Daten Eu2(G + U1 + U2 + Ds1(S1)) + Da1(Eu2(S2)). Darüber hinaus bestätigt das Nachweisbüro **30**, daß der Tabelleneintragssuchwert für das gewonnene Bild zum Tabelleneintragssuchwert H1 paßt, den der Nutzer U gespeichert hat, der die zweite Dateneinheit ist. Zu dieser Zeit wird die Signatur für den Tabelleneintragssuchwert H1 identifiziert.

[0383] Wenn der Tabelleneintragssuchwert für die Daten Eu2(G + U1 + U2 + Ds1(s)) + Da1(Eu2(S2)) nicht zum Tabelleneintragssuchwert H1 paßt, wird wie in der obigen Prozedur 5) ermittelt, daß die Agentur A, die die erste Dateneinheit ist, die rechtswidrige Tat begangen hat. Wenn die beiden Tabelleneintragssuchwerte zueinander passen, wie in Prozedur 6), fordert das Nachweisbüro **30** vom Nutzer, der die zweite Dateneinheit ist, den zweiten Verschlüsselungsabschnitt der Daten Eu2(G + U1 + U2 + Ds(S1)) + Da1(Eu2(S2)) zu entschlüsseln. Die Signaturinformation S2 wird aus den entschlüsselten Daten ausgelesen.

[0384] Kann die korrekte Signaturinformation S2 nicht ausgelesen werden, dann wird ermittelt, daß der Nutzer, der die zweite Dateneinheit ist, die rechtswidrige Tat begangen hat. Wird aber die korrekte Signaturinformation S2 ausgelesen, dann wird ermittelt, daß die Agentur, die die erste Dateneinheit ist, die rechtswidrige Tat begangen hat.

[0385] Wie zuvor beschrieben, werden Nachweis 1 und Nachweis 2 im wesentlichen entsprechend derselben Prozedur ausgeführt, und nur die Festlegungen der ersten und der zweiten Dateneinheit müssen geändert werden. Auch die Partei, die die rechtswidrige Tat begangen hat, kann auf dieselbe Weiße identifiziert werden.

[0386] Das Beispiel in Fig. 25 ist dasselbe wie das Beispiel in Fig. 23, sofern der Prozeß 1 und der Prozeß 2 unabhängig voneinander ausgeführt werden; es besteht keine Notwendigkeit für das Nachweisbüro, bis ein rechtswidriges Bild entdeckt worden ist, und keine rechtswidrige Tat kann begangen werden, bis ein rechtswidriges Bild entdeckt worden ist; ein Nachweisbüro ist nicht notwendigerweise erforderlich.

(Sechstes Ausführungsbeispiel)

[0387] Fig. 26 ist ein Diagramm, das ein sechstes Ausführungsbeispiel der vorliegenden Erfindung darstellt. Dieselben Bezugszeichen, wie sie in Fig. 24 und Fig. 25 verwendet sind, werden auch für Komponenten verwendet, die dieselbe Verarbeitung ausführen, und eine erneute Beschreibung dafür entfällt hier. Mit der Anordnung vom Beispiel gemäß

[0388] Fig. 25 nach dem sechsten Ausführungsbei-

spiel sendet der Nutzer die Kontraktinformation an eine Agentur A, um für die Geheimhaltung eines zu schützenden Nutzers S wie im fünften Ausführungsbeispiel zu verfahren, gemeinsam mit einem öffentlichen Schlüssel, begleitet von einer Bescheinigung, die ein Bescheinigungsbüro 4 ausgegeben hat.

[0389] Für den Einbettungsprozeß in diesem Ausführungsbeispiel werden die Prozeduren 1) und 2) in Fig. 25 im Beispiel von Fig. 25 ersetzt durch die Prozeduren 1) und 2) des fünften Ausführungsbeispiels, und die folgenden Prozeduren sind dieselben wie jene im Beispiel von Fig. 25. Dieser Einbettungsprozeß ist in der Weise beeinflussend wie derjenige im fünften Ausführungsbeispiel, wenn die Anwendung zur Verteilung elektronischer Information durch die Agentur an den Nutzer erfolgt.

[0390] Während der Nachweisprozeß in diesem Ausführungsbeispiel auf den Nachweis 2 im Beispiel von Fig. 25 angewandt wird, gibt es einen Unterschied, der nun erläutert wird. Im sechsten Beispiel, wie auch im fünften Ausführungsbeispiel, liest zuerst beim Nachweis 2 für die Agentur A und den Nutzer U das Endgerät **10** auf der Seite der Agentur (erste Dateneinheit) Nutzerinformationen U2' aus den rechtswidrigen Bilddaten G_{WW}' = G + U1' + U2' + Da2(S1') + Du(S2'), die entdeckt worden sind.

[0391] Die Agentur A unterbreitet dem Bescheinigungsbüro **40** die Nutzerinformation U2' und den anonymen öffentlichen Schlüssel aus der Kontraktinformation und fordert den Nutzernamen an, der dem öffentlichen Schlüssel entspricht. Wir die Nutzerinformation U2' nicht ausgelesen, dann wird ermittelt, daß die Agentur A die rechtswidrige Tat begangen hat. Die erste Verschlüsselung erfolgt des weiteren für rechtswidrige Bilddaten G_{WW}' = G + U1' + U2' + Da2(S1') + Du(S2'), und die Signaturinformation S2' wird ausgelesen. Da der nachfolgende Prozeß derselbe wie der Nachweis 2 im Beispiel von Fig. 25 ist, entfällt hier eine erneute Erläuterung.

[0392] Wird die Signaturinformation S2' nicht ausgelesen, dann wird ermittelt, daß der Server S die rechtswidrige Tat begangen hat. Wird die Nutzerinformation U2' ausgelesen, dann unterbreitet die Agentur A die Nutzerinformation U2' und den anonymen Schlüssel, gewonnen aus der Kontraktinformation, an das Bescheinigungsbüro **40** und fordert den Nutzernamen an, der dem öffentlichen Schlüssel entspricht. Die Agentur A, die die erste Dateneinheit ist, unterbreitet dann dem Nachweisbüro die rechtswidrigen Bilddaten G_{WW}' und die ausgelesene Nutzerinformation U2' und fordert eine Überprüfung des Nutzernamens an, der dem öffentlichen Schlüssel entspricht.

[0393] Die elektronische Wasserzeicheninformation in den oben beschriebenen Ausführungsbeispielen läßt sich einbetten unter Verwendung verschiedener Verfahren, beispielsweise allgemein bekannte Verfahren, die als Beispiel beschrieben sind in "Hiding of Static Picture Data Using Pixel Blocks", Shimizu, Numao, Morimoto (IBM, Japan), 53rd Information Processing Institute National Assembly, IN-11, September 1996; oder in "Secure Spread Spectrum Watermarking for Multimedia," I.J. Cox, J. Kilian, T. Leighton and T. Shamoon (NEC), NEC Research Institute Technical Report 95-10.

[0394] Die für die erste Verschlüsselung verwendeten Verfahren und die zweite Verschlüsselung können ebenfalls realisiert werden durch Anwenden verschiedener Verfahren, wie beispielsweise ein Verschlüsselungsverfahren zum Ändern der Bitanordnung in Übereinstimmung mit dem Verschlüsselungscode.

[0395] In Prozedur 2) des Einbettungsprozesses sind darüber hinaus der Tabelleneintragssuchwert und die Signatur nicht in den Bilddaten E1(G + U) enthalten, die an das Nutzerendgerät **20** zu senden sind. Ein Tabelleneintragssuchwert und dessen Signatur kann jedoch für Daten bereitgestellt werden, um zu bestimmen, ob ein Übertragungsweg geändert worden ist.

[0396] Des weiteren werden die erste Verschlüsselung und die zweite Verschlüsselung im elektronischen Wasserzeicheninformationseinbettungsprozeß ausgeführt, um sowohl den Server als auch den Nutzer davor zu schützen, von der Information gemeldet zu werden, die gegenseitig gespeichert ist. DES-Verschlüsselung (Data Encryption Standard Cryptography) oder eine Tabelleneintragssuchfunktion können angewandt werden, um das Abhören und das Ändern der Daten über einen Übertragungsweg durch einen Dritten zu verhindern.

[0397] In den individuellen Ausführungsbeispielen ist die erste Dateneinheit des weiteren mit der Feststellung rechtswidriger Datenverteilung befaßt. Sofern elektronische Wasserzeichenauslesemittel vorgesehen sind, kann jedoch ein beliebiger Nutzer eine rechtswidrige Datenverteilung feststellen und auch die Nutzerinformation, obwohl der Geheimschlüssel für die erste Verschlüsselung oder die zweite Verschlüsselung unbekannt ist. Wird eine rechtswidrige Datenverteilung festgestellt, muß der Nutzer nur dem Server melden, daß der Nachweisprozeß begonnen hat. Die Feststellung rechtswidriger Verteilungen ist folglich nicht auf die erste Dateneinheit beschränkt.

[0398] Das Endgerät **10** der ersten Dateneinheit kann in die Bilddaten nicht nur die Nutzerinformation U, sondern auch andere erforderliche Information einbetten, wie Copyrightinformation und solche, die einen Bilddatenverteilungszustand betrifft. Um Geheiminformation einzubetten, muß das Serverendge-

rät **10** darüber hinaus den Einbettungsprozeß nach der ersten Verschlüsselung ausführen, so daß zusätzlich zur Signaturinformation die Information, die die erste Verschlüsselung beeinflußt, in die Bilddaten eingebettet werden kann. Die Nutzerinformation wird nicht immer vor der ersten Verschlüsselung eingebettet, sondern kann nach der ersten Verschlüsselung eingebettet werden (die Feststellung der Nutzerinformation U kann in diesem Falle nur vom Server ausgeführt werden oder von einer Person, die den Geheimschlüssel kennt, der bei der ersten Verschlüsselung verwendet wird).

[0399] Wenn das Endgerät **20** von der zweiten Dateneinheit ein Gerät ist, das innerhalb der Vielzahl von Nutzern gemeinsam einen Drucker oder ein Endgerät verwendet, kann die Signaturinformation und die zweite Verschlüsselung für die zweite Dateneinheit die Signaturinformation und das Verschlüsselungssystem für den Drucker oder für das Endgerät enthalten, die ja gemeinsam verwendet werden.

[0400] Die erste Verschlüsselungsinformation vom Serverendgerät **10** kann weitestgehend über ein Netzwerk verteilt werden, selbst ohne daß eine Anforderung vom Nutzerendgerät **20** vorliegt, auf der Grundlage der Kontraktinformation.

[0401] Die Signaturinformation S für die zweite Dateneinheit wird nicht notwendigerweise nach dem öffentlichen Verschlüsselungsverfahren erzeugt, sondern kann eine Information sein (beispielsweise eine Codezahl), die der Nutzer auf der Grundlage der Kontraktinformation festlegt.

[0402] Zur Anwendung der Verschlüsselung für 40 Bits oder mehr in den Vereinigten Staaten ist ein Schlüsselverwaltungsbüro zum Verwalten eines Verschlüsselungscodes erforderlich, um die nicht berechtigte Verwendung von der Verschlüsselungseinrichtung zu verhindern. Das Nachweisbüro kann folglich auch als Codeverwaltungsbüro arbeiten. Wenn das Nachweisbüro Vorausverwaltung des zweiten Verschlüsselungscodes bereitstellt, kann das Nachweisbüro selbst die Nachweisprozesse 1) bis 3) ausführen, indem ein rechtswidriges Bild überwacht wird. Der erste Verschlüsselungscode von der ersten Dateneinheit kann entweder vom selben Nachweisbüro verwaltet werden oder von einem anderen Codeverwaltungsbüro. Die Schlüssel vom Server und vom Nutzer können erzeugt und verteilt werden vom Codeverwaltungsbüro.

[0403] Derselbe Verschlüsselungsprozeß oder ein Prozeß, der ein anderes Verschlüsselungsverfahren oder einen anderen Verschlüsselungscode verwendet, kann von der Agentur für die Prozesse 1 und 2 ausgeführt werden.

[0404] Ist die rechtswidrige Tat nicht vom Server begangen, dann kann der Server oder der Autor elektronische Wasserzeicheninformation in Bilddaten einbetten und diese an die Agentur weitergeben, und die Agentur kann andere elektronische Wasserzeicheninformation einbetten und diese dem Nutzer zusenden.

[0405] Anstelle einer Einzelagentur kann darüber hinaus eine Vielzahl von Agenturen hierarchisch gegliedert bereitgestellt werden. In diesem Falle kann eine spezielle beauftragte Agentur mit hierarchischer Struktur die Verarbeitung ausführen, mit der die Agentur beauftragt ist, oder die individuellen Agenturen können das Protokoll zum Spezifizieren der zu beauftragenden Agentur ausführen.

[0406] Ist nur eine Agentur vorgesehen, wie in Fig. 5 gezeigt, dann kann das Einbetten der Nutzerinformation bezüglich der Agentur entfallen.

[0407] Wie im elektronischen Wasserzeichenüberlagerungsverfahren und in der elektronischen Informationsverteilung der obigen Ausführungsbeispielen beschrieben, kann eine rechtswidrige Tat aufgrund Kollusion zwischen zwei Dateneinheiten, und mehreren verfügbaren Kombinationen vermieden werden, wenn es wenigstens unter drei Einheiten zu verteilende abhängige elektronische Informationen gibt.

[0408] Die Ausführungsbeispiele der vorliegenden Erfindung lassen sich per Software realisieren. Somit stellt die vorliegende Erfindung ein Speichermedium bereit, beispielsweise eine Diskette, die eine derartige Software und softwaretragende Signale speichert, beispielsweise wenn diese über ein Netzwerk, wie das Internet, heruntergeladen werden.

Patentansprüche

1. Elektronisches Wasserzeichenverfahren, mit den Verfahrensschritten:
einem ersten Schritt, bei dem eine erste Dateneinheit einen ersten Verschlüsselungsprozeß für Originaldaten ausführt;
einem zweiten Schritt, bei dem eine zweite Dateneinheit wenigstens entweder die von der ersten Verschlüsselung bereitstehenden Daten verwaltet oder verteilt und ein elektronisches Wasserzeichen in die Daten einbettet;
einem dritten Schritt, bei dem eine dritte Dateneinheit einen zweiten Verschlüsselungsprozeß für die Daten ausführt, in die das elektronische Wasserzeichen eingebettet ist; und mit
einem Bescheinigungsbüro, das eine Signatur für die dritte Dateneinheit unter Verwendung eines von einer Bescheinigung begleiteten anonymen öffentlichen Schlüssels überprüft.

2. Verfahren nach Anspruch 1, wobei der erste Schritt wenigstens einen Schritt des Einbettens eines

elektronischen Wasserzeichens umfaßt, bevor oder nachdem der erste Verschlüsselungsprozeß für die Originaldaten ausgeführt ist.

3. Verfahren nach Anspruch 1 oder nach Anspruch 2, bei dem der zweite Schritt über wenigstens einen Schritt des Ausführens eines dritten Verschlüsselungsprozesses verfügt, bevor oder nachdem das elektronische Wasserzeichen eingebettet ist.

4. Verfahren nach einem der Ansprüche 1 bis 3, mit dem weiteren Verfahrensschritt:
Verteilen von Daten, die wenigstens vom das elektronische Wasserzeichen einbettende ersten Verschlüsselungsprozeß oder vom zweiten Verschlüsselungsprozeß beeinflußt werden.

5. Verfahren nach einem der vorstehenden Ansprüche, bei dem die zweite Dateneinheit über eine Vielzahl von Dateneinheiten verfügt.

6. Verfahren nach einem der vorstehenden Ansprüche, bei dem die von der zweiten Dateneinheit einzubettende Information entweder die Information hinsichtlich der dritten Dateneinheit oder die Information hinsichtlich der zu sendenden Daten ist.

7. Verfahren nach einem der vorstehenden Ansprüche, bei dem der erste Schritt einen Verfahrensschritt des Einbettens eines elektronischen Wasserzeichens in Bilddaten wenigstens bevor oder nachdem der erste Verschlüsselungsprozeß für die Originaldaten ausgeführt ist, umfaßt; und wobei von einer n-ten Dateneinheit einzubettende Information entweder eine solche ist, die eine (n+1)-te Dateneinheit oder eine Information bezüglich zu sendender Daten betrifft, wobei n eine Ganzzahl gleich oder größer als 1 ist.

8. Verfahren nach einem der vorstehenden Ansprüche, bei dem der Prozeß zum Einbetten des elektronischen Wasserzeichens ein solcher ist, der Information bezüglich der zweiten Dateneinheit nicht einzubettet.

9. Verfahren nach einem der vorstehenden Ansprüche, bei dem die Originaldaten Bilddaten sind.

10. Speichermedium, das alle Verfahrensschritte eines elektronischen Wasserzeicheneinbettungsverfahren nach einem der Ansprüche 1 bis 9 speichert, so daß diese von einem Computer zu lesen sind.

11. Elektronisches Informationsverteilungssystem, das Daten über ein Netzwerk austauscht, das wenigstens ausgestattet ist mit:
einer ersten Dateneinheit (**10**) mit einem ersten Verschlüsselungsmittel (**13**) zum Ausführen eines ersten Verschlüsselungsprozesses für Originaldaten;
einer zweiten Dateneinheit (**40**) mit einem Verwaltungsverteilungsmittel wenigstens entweder zum Verwalten oder zum Verteilen der Daten, die der Verschlüsselungsprozeß bereitstellt, und mit einem elektronischen Wasserzeicheneinbettungsmittel zum Einbetten eines elektronischen Wasserzeichens in die Daten;
einer dritten Dateneinheit (**20**) mit einem zweiten Verschlüsselungsmittel (**240**) zum Ausführen einer zweiten Verschlüsselung der Daten, wobei ein elektronisches Wasserzeichen eingebettet wird; und mit
einem Nachweismittel (**30**) zum Überprüfen einer Signatur für die dritte Dateneinheit unter Verwendung eines anonymen öffentlichen Schlüssels, der von einer Bescheinigung begleitet ist, die ein Bescheinigungsbüro ausgibt.

12. System nach Anspruch 11, bei dem die erste Dateneinheit wenigstens ein elektronisches Wasserzeicheneinbettungsmittel (**12**) enthält zum Einbetten eines elektronischen Wasserzeichens, bevor oder nachdem der erste Verschlüsselungsprozeß für die Originaldaten ausgeführt ist.

13. System nach Anspruch 11 oder nach Anspruch 12, bei dem die zweite Dateneinheit wenigstens ein drittes Verschlüsselungsmittel (**43**) zum Ausführen eines dritten Verschlüsselungsprozesses enthält, bevor oder nachdem das elektronische Wasserzeichen eingebettet ist.

14. System nach einem der Ansprüche 11 bis 13, das weiterhin ausgestattet ist mit:
einem Verteilungsmittel zum Verteilen von Daten, die wenigstens entweder vom ersten Verschlüsselungsprozeß oder vom zweiten Verschlüsselungsprozeß beeinflußt werden, der das elektronische Wasserzeichen einbettet.

15. System nach einem der Ansprüche 11 bis 14, bei dem die zweite Dateneinheit eine Vielzahl von Dateneinheiten enthält.

16. System nach einem der Ansprüche 11 bis 15, bei dem von der zweiten Dateneinheit einzubettende Information entweder Information bezüglich der dritten Dateneinheit oder Information bezüglich der zu sendenden Daten ist.

17. System nach einem der Ansprüche 11 bis 16, bei dem die erste Dateneinheit über ein elektronisches Wasserzeicheneinbettungsmittel (**12**) verfügt zum Einbetten eines elektronischen Wasserzeichens in Bilddaten wenigstens bevor oder nachdem der erste Verschlüsselungsprozeß für die Originaldaten ausgeführt ist; und wobei das Wasserzeicheneinbettungsmittel von einer n-ten Dateneinheit die Information entweder als Information bezüglich einer (n+1)-ten Dateneinheit oder einer Information einbettet, die sich auf zu sendende Daten bezieht, wobei n eine Ganzzahl gleich oder größer als 1 ist.

18. System nach Anspruch 11 oder 12, dessen elektronisches Wasserzeicheneinbettungsmittel bei der wenigstens einfach vorgesehenen Information bezüglich der zweiten Dateneinheit keine Einbettung vornimmt.

19. System nach einem der Ansprüche 11 bis 18, dessen Originaldaten Bilddaten sind.

20. System nach einem der Ansprüche 11 bis 19, das des weiteren über eine vierte Dateneinheit (**30**) verfügt, um die Länge wenigstens entweder der Verschlüsselungsverarbeitung oder des elektronischen Wasserzeicheneinbettungsprozesses zu überprüfen, den die erste bis dritte Dateneinheit ausführt.

21. System nach einem der Ansprüche 11 bis 20, bei dem die erste Dateneinheit eingerichtet ist zum Einbetten des elektronischen Wasserzeichens nach Nachweisen einer Signatur für die dritte Dateneinheit unter Verwendung des anonymen öffentlichen Schlüssels zusammen mit einer vom Bescheinigungsbüro ausgegebenen Bescheinigung.

22. System nach Anspruch 21, sofern abhängig von einem der Ansprüche 11 bis 20, bei dem die zweite Dateneinheit das elektronische Wasserzeichen einbettet, nachdem eine Signatur für die dritte Dateneinheit unter Verwendung eines anonymen öffentlichen Schlüssels zusammen mit einer vom Bescheinigungsbüro ausgegebenen Bescheinigung nachgewiesen ist.

23. System nach einem der Ansprüche 11 bis 22, bei dem die von der dritten Dateneinheit einzubettende elektronische Wasserzeicheninformation eine Information enthält, daß nur die dritte Dateneinheit zur Aufbereitung bereit ist.

24. System nach Anspruch 20, bei dem die vierte Dateneinheit zum Ausführen des Nachweises in der Lage ist, eine der zweiten Verschlüsselung entsprechende Entschlüsselung auszuführen.

25. System nach Anspruch 21 oder 23, bei dem die von der ersten Dateneinheit einzubettende elektronische Wasserzeicheninformation über Information bezüglich der dritten Dateneinheit verfügt.

26. System nach Anspruch 21 oder 23, bei dem die von der ersten Dateneinheit einzubettende elektronische Wasserzeicheninformation über Information bezüglich zu sendender Digitaldaten verfügt.

27. System nach Anspruch 21 oder 23, bei dem die von der zweiten Dateneinheit einzubettende elektronische Wasserzeicheninformation über Information bezüglich der dritten Dateneinheit verfügt.

Es folgen 24 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

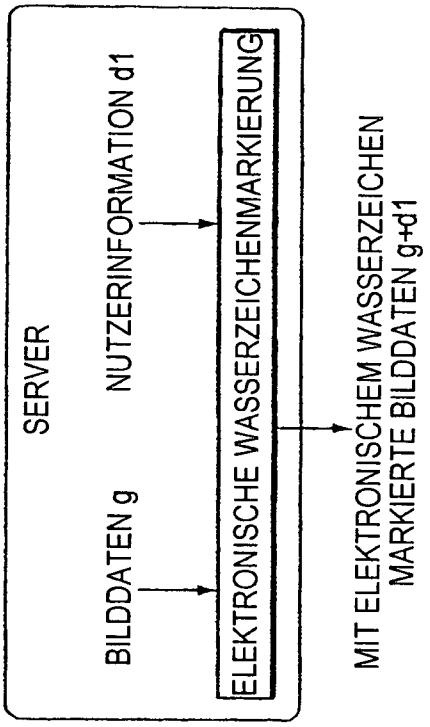


FIG. 2

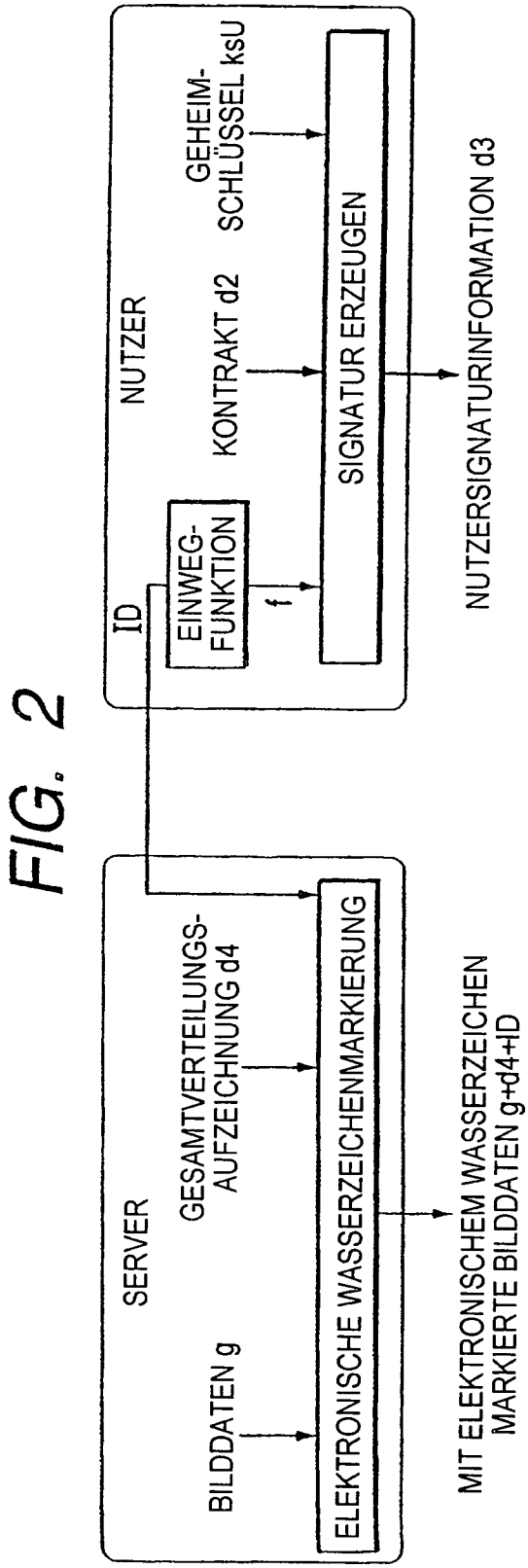


FIG. 3

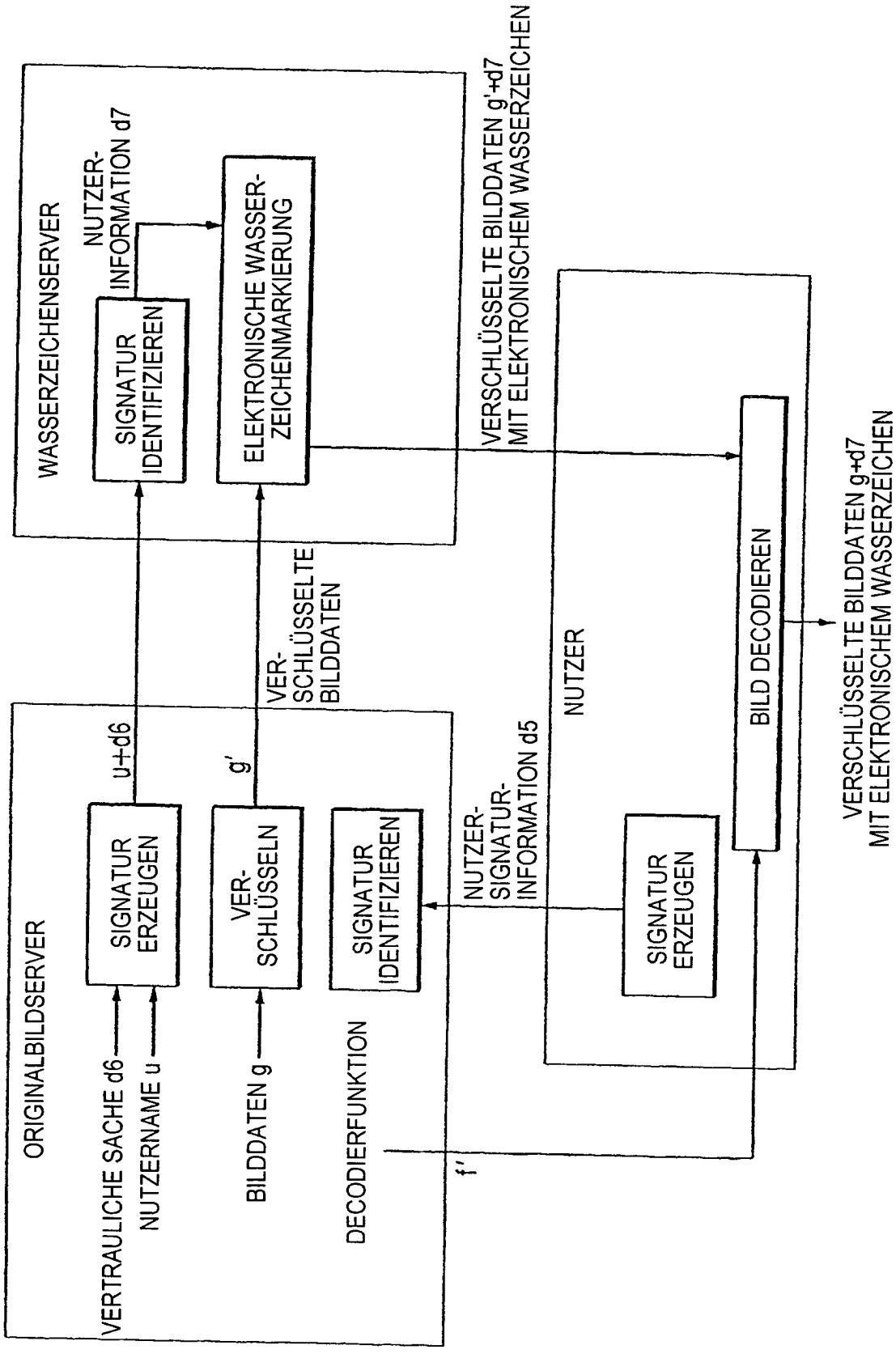

ORIGINALBILDSERVER
VERTRAULICHE SACHE d6
NUTZERNAME u
SIGNATUR ERZEUGEN
u+d6
BILDDATEN g
VER-SCHLÜSSELN
g'
DECODIERFUNKTION
SIGNATUR IDENTIFIZIEREN
VER-SCHLÜSSELTE BILDDATEN
WASSERZEICHENSERVER
NUTZER-INFORMATION d7
SIGNATUR IDENTIFIZIEREN
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
VERSCHLÜSSELTE BILDDATEN g'+d7 MIT ELEKTRONISCHEM WASSERZEICHEN
NUTZER-SIGNATUR-INFORMATION d5
NUTZER
SIGNATUR ERZEUGEN
f'
BILD DECODIEREN
VERSCHLÜSSELTE BILDDATEN g+d7 MIT ELEKTRONISCHEM WASSERZEICHEN

FIG. 4

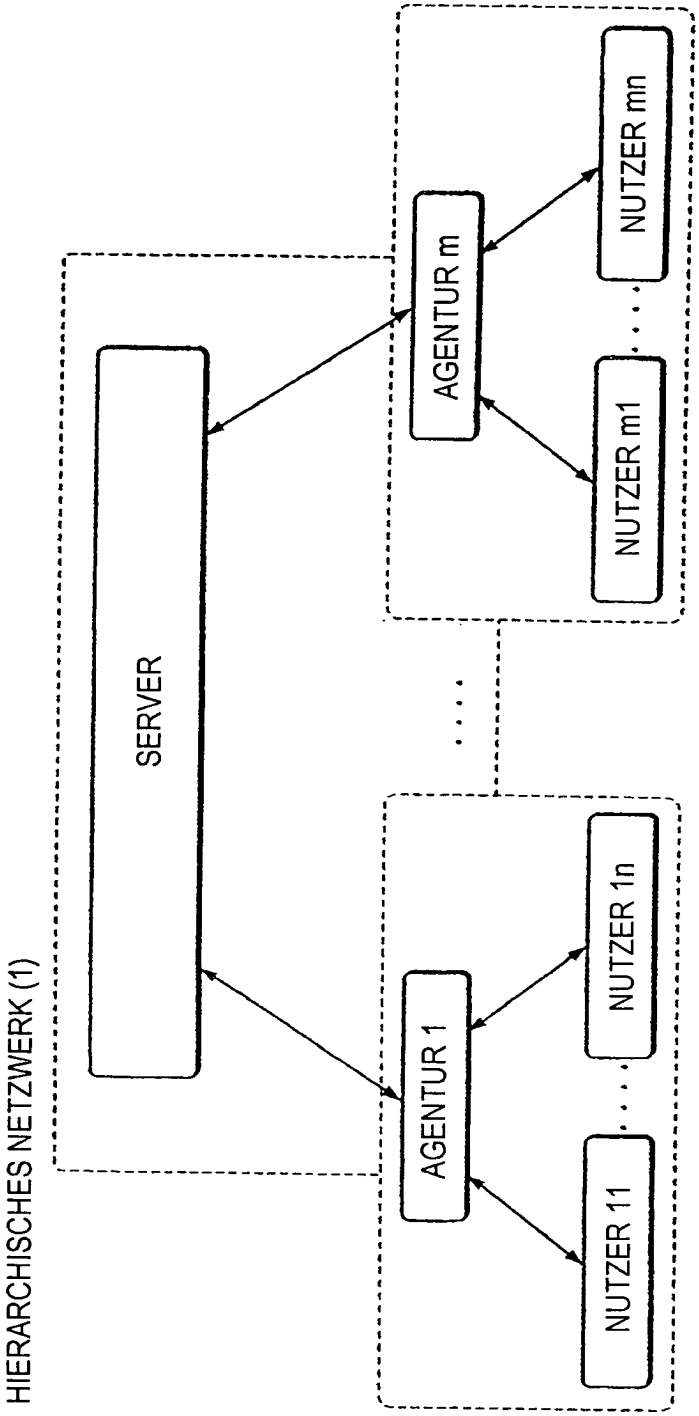
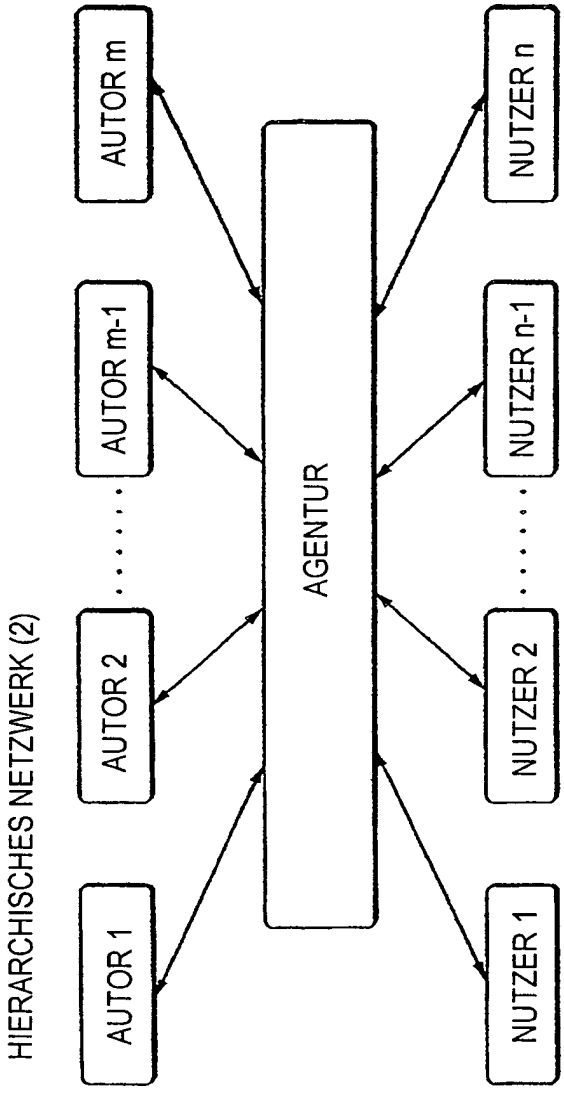

HIERARCHISCHES NETZWERK (1)
SERVER
AGENTUR 1
NUTZER 11
NUTZER 1n
AGENTUR m
NUTZER m1
NUTZER mn

FIG. 5


HIERARCHISCHES NETZWERK (2)
AUTOR 1
AUTOR 2
AUTOR m-1
AUTOR m
AGENTUR
NUTZER 1
NUTZER 2
NUTZER n-1
NUTZER n

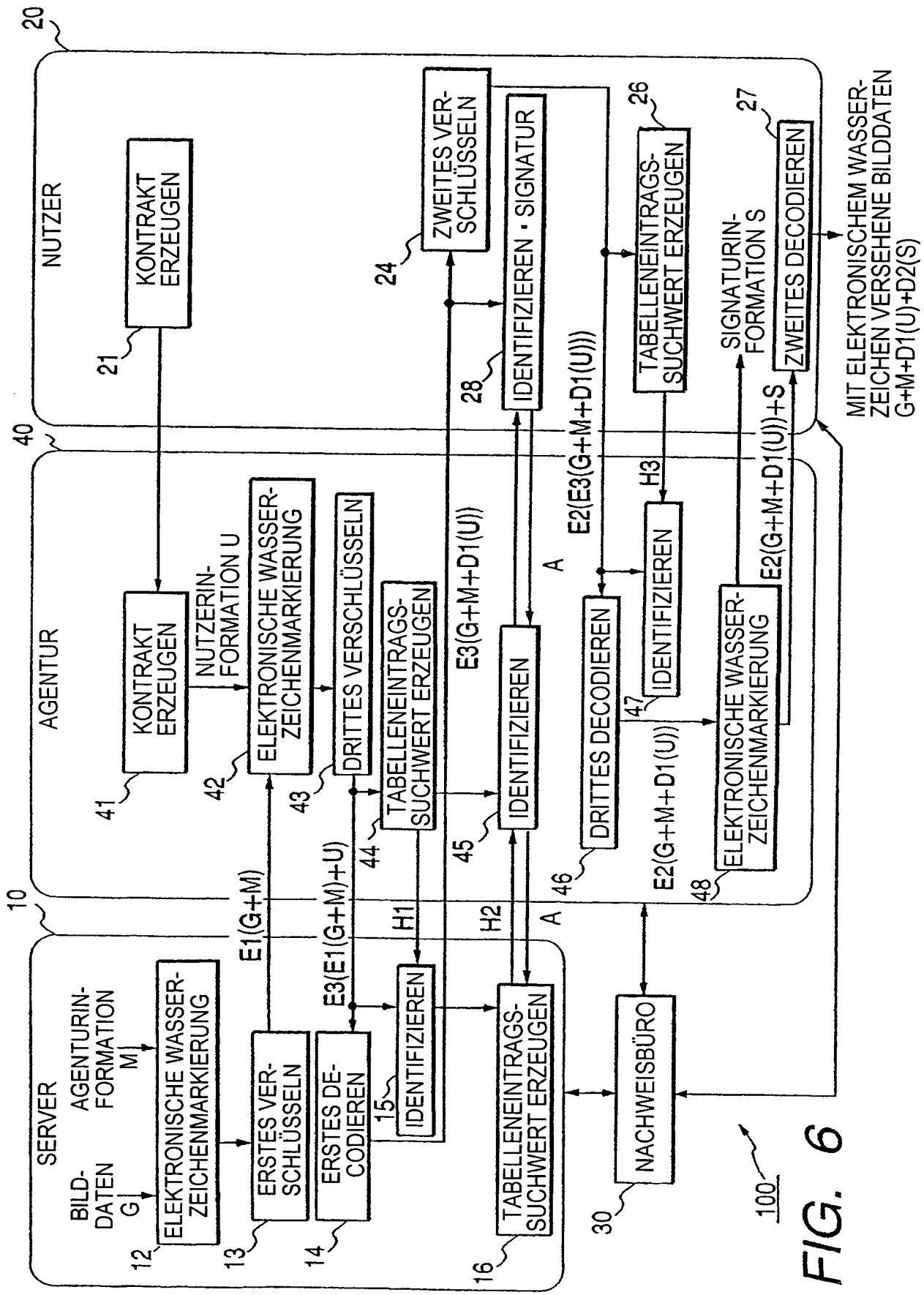
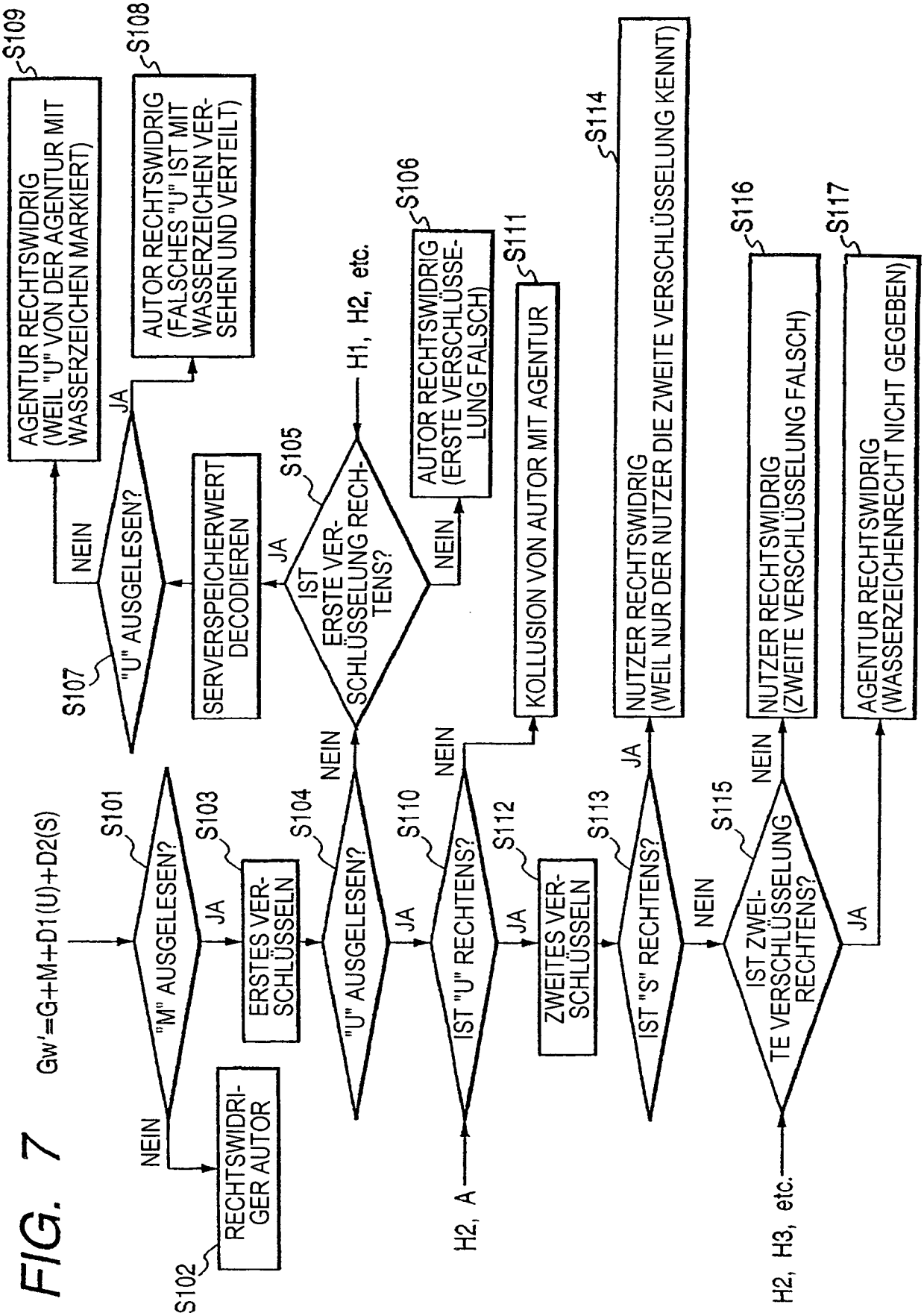

SERVER
BILD-DATEN G
AGENTURIN-FORMATION M
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
ERSTES VER-SCHLÜSSELN
ERSTES DE-CODIEREN
IDENTIFIZIEREN
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
NACHWEISBÜRO
AGENTUR
KONTRAKT ERZEUGEN
NUTZERIN-FORMATION U
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
DRITTES VERSCHLÜSSELN
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
IDENTIFIZIEREN
DRITTES DECODIEREN
IDENTIFIZIEREN
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
NUTZER
KONTRAKT ERZEUGEN
ZWEITES VER-SCHLÜSSELN
IDENTIFIZIEREN • SIGNATUR
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
SIGNATURIN-FORMATION S
ZWEITES DECODIEREN
MIT ELEKTRONISCHEM WASSER-ZEICHEN VERSEHENE BILDDATEN G+M+D1(U)+D2(S)
E1(G+M)
E3(E1(G+M)+U)
E3(G+M+D1(U))
E2(E3(G+M+D1(U)))
E2(G+M+D1(U))
E2(G+M+D1(U))+S
H1
H2
H3
A
A
10
12
13
14
15
16
20
21
24
26
27
28
30
40
41
42
43
44
45
46
47
48
100

FIG. 6

FIG. 7


Gw'=G+M+D1(U)+D2(S)
S101
"M" AUSGELESEN?
NEIN
JA
S102
RECHTSWIDRIGER AUTOR
S103
ERSTES VERSCHLÜSSELN
S104
"U" AUSGELESEN?
NEIN
JA
S105
IST ERSTE VERSCHLÜSSELUNG RECHTENS?
H1, H2, etc.
NEIN
JA
S106
AUTOR RECHTSWIDRIG (ERSTE VERSCHLÜSSELUNG FALSCH)
S107
"U" AUSGELESEN?
NEIN
JA
S108
AUTOR RECHTSWIDRIG (FALSCHES "U" IST MIT WASSERZEICHEN VERSEHEN UND VERTEILT)
S109
AGENTUR RECHTSWIDRIG (WEIL "U" VON DER AGENTUR MIT WASSERZEICHEN MARKIERT)
SERVERSPEICHERWERT DECODIEREN
S110
IST "U" RECHTENS?
NEIN
JA
H2, A
S111
KOLLUSION VON AUTOR MIT AGENTUR
S112
ZWEITES VERSCHLÜSSELN
S113
IST "S" RECHTENS?
NEIN
JA
S114
NUTZER RECHTSWIDRIG (WEIL NUR DER NUTZER DIE ZWEITE VERSCHLÜSSELUNG KENNT)
S115
IST ZWEITE VERSCHLÜSSELUNG RECHTENS?
NEIN
JA
H2, H3, etc.
S116
NUTZER RECHTSWIDRIG (ZWEITE VERSCHLÜSSELUNG FALSCH)
S117
AGENTUR RECHTSWIDRIG (WASSERZEICHENRECHT NICHT GEGEBEN)

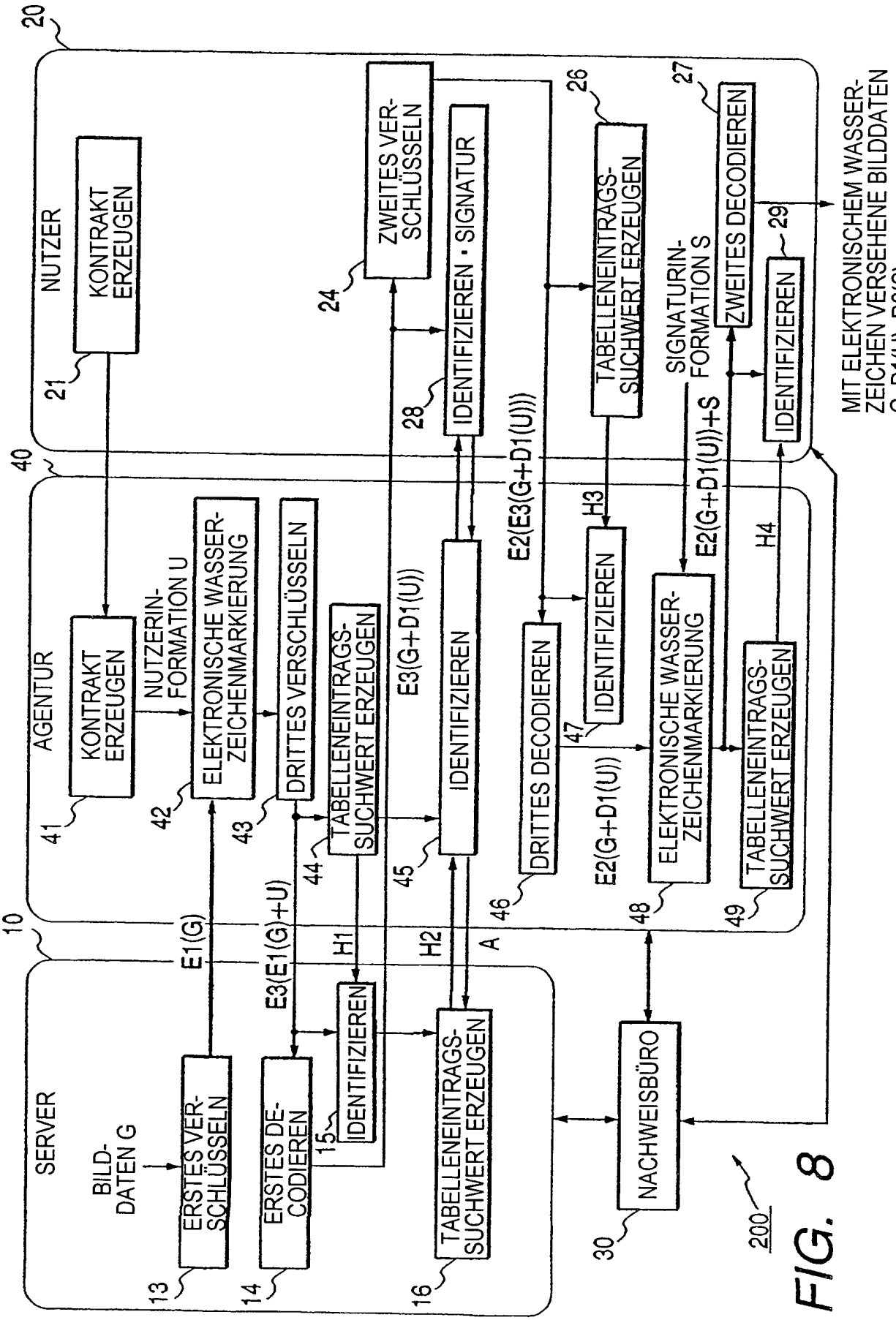

20
NUTZER
KONTRAKT ERZEUGEN
21
ZWEITES VER-SCHLÜSSELN
24
IDENTIFIZIEREN • SIGNATUR
28
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
26
SIGNATURIN-FORMATION S
ZWEITES DECODIEREN
27
IDENTIFIZIEREN
29
MIT ELEKTRONISCHEM WASSER-ZEICHEN VERSEHENE BILDDATEN G+D1(U)+D2(S)
40
AGENTUR
KONTRAKT ERZEUGEN
41
NUTZERIN-FORMATION U
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
42
DRITTES VERSCHLÜSSELN
43
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
44
IDENTIFIZIEREN
45
DRITTES DECODIEREN
46
IDENTIFIZIEREN
47
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
48
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
49
10
SERVER
BILD-DATEN G
ERSTES VER-SCHLÜSSELN
13
ERSTES DE-CODIEREN
14
IDENTIFIZIEREN
15
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
16
NACHWEISBÜRO
30
200
E1(G)
E3(E1(G)+U)
H1
H2
A
E3(G+D1(U))
E2(E3(G+D1(U)))
H3
E2(G+D1(U))
E2(G+D1(U))+S
H4

FIG. 8

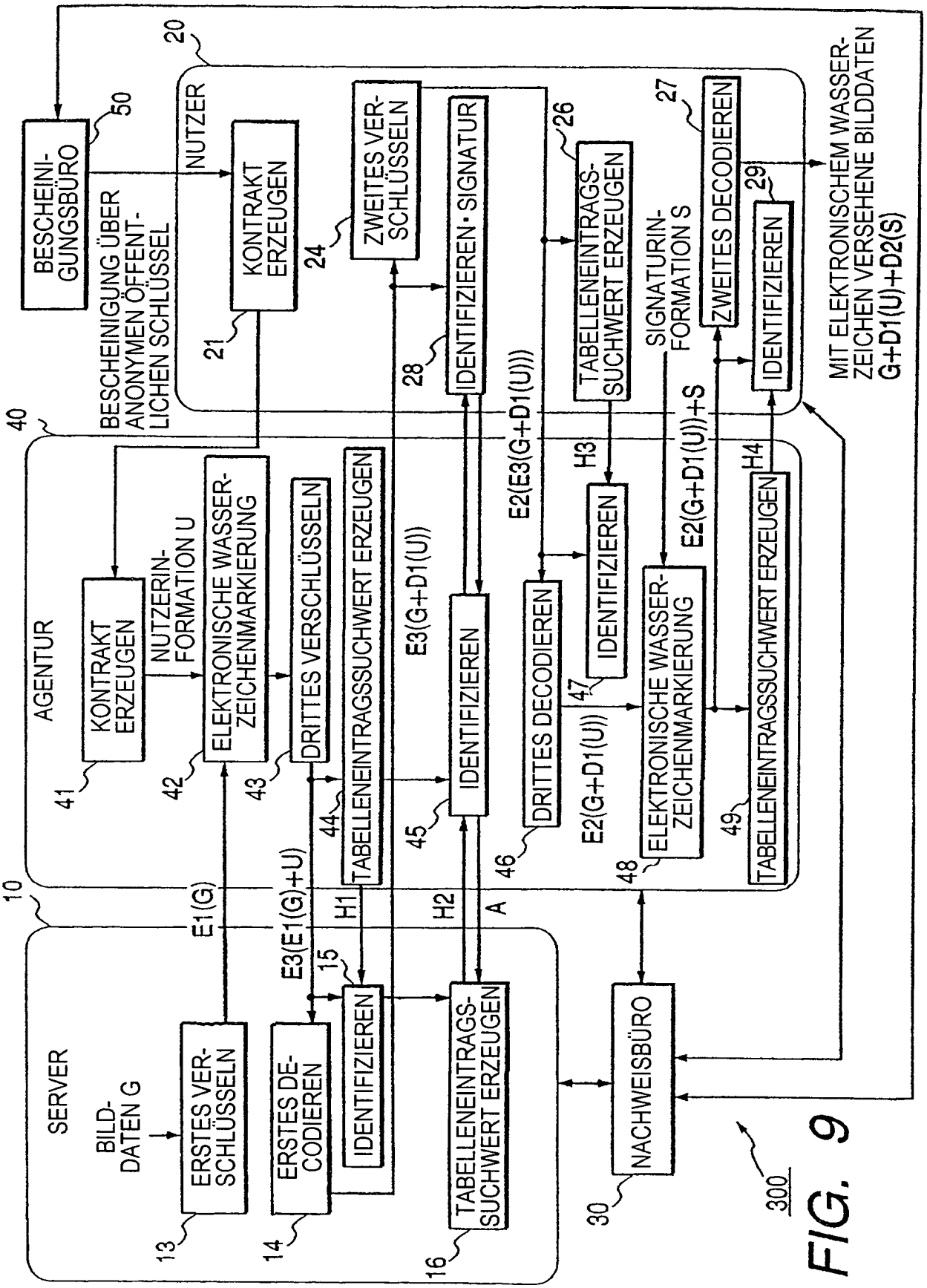

SERVER
BILD-DATEN G
ERSTES VER-SCHLÜSSELN
ERSTES DE-CODIEREN
IDENTIFIZIEREN
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
NACHWEISBÜRO
AGENTUR
KONTRAKT ERZEUGEN
NUTZERIN-FORMATION U
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
DRITTES VERSCHLÜSSELN
TABELLENEINTRAGSSUCHWERT ERZEUGEN
IDENTIFIZIEREN
DRITTES DECODIEREN
IDENTIFIZIEREN
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
TABELLENEINTRAGSSUCHWERT ERZEUGEN
NUTZER
BESCHEINI-GUNGSBÜRO
KONTRAKT ERZEUGEN
ZWEITES VER-SCHLÜSSELN
IDENTIFIZIEREN • SIGNATUR
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
SIGNATURIN-FORMATION S
ZWEITES DECODIEREN
IDENTIFIZIEREN
BESCHEINIGUNG ÜBER ANONYMEN ÖFFENT-LICHEN SCHLÜSSEL
MIT ELEKTRONISCHEM WASSER-ZEICHEN VERSEHENE BILDDATEN G+D1(U)+D2(S)
E1(G)
E3(E1(G)+U)
E3(G+D1(U))
E2(E3(G+D1(U)))
E2(G+D1(U))
E2(G+D1(U))+S
H1
H2
H3
H4
A
10
13
14
15
16
20
21
24
26
27
28
29
30
40
41
42
43
44
45
46
47
48
49
50
300

FIG. 9

FIG. 10

BILDKOPFABSCHNITT	BILDFORMATIDENTIFIZIERER
	DATEIGRÖSSE
	ANZAHL VON PIXELN IN X-RICHTUNG (BREITE)
	ANZAHL VON PIXELN IN Y-RICHTUNG (HÖHE)
	TIEFENGRÖSSERICHTUNG
	MIT ODER OHNE KOMPRESSION
	AUFLÖSUNG
	BIT-MAP-OFFSET
	GRÖSSE DER FARBPALETTE
BILDDATENABSCHNITT	BIT-MAP

FIG. 11

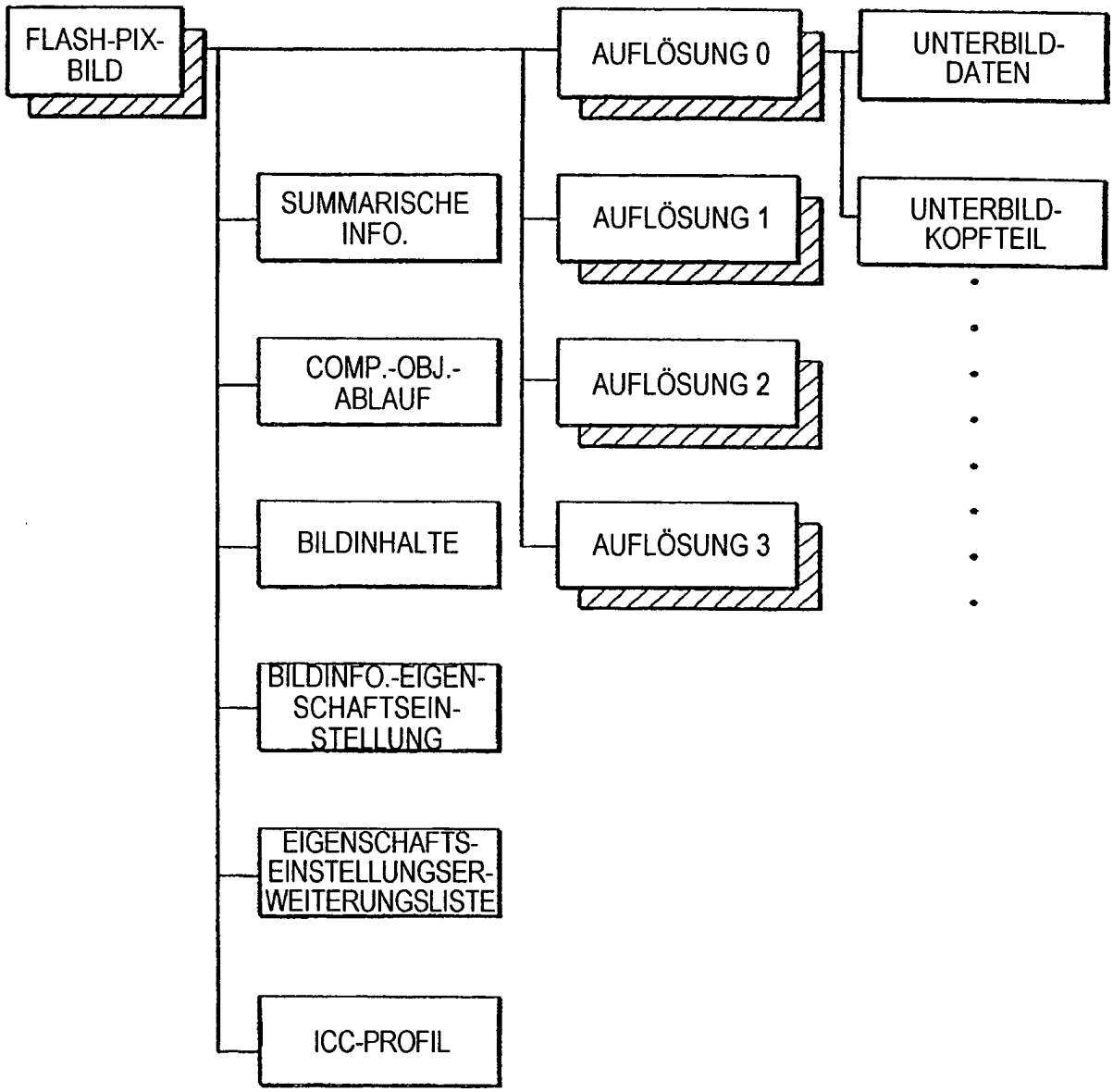

FLASH-PIX-BILD
SUMMARISCHE INFO.
COMP.-OBJ.-ABLAUF
BILDINHALTE
BILDINFO.-EIGEN-SCHAFTSEIN-STELLUNG
EIGENSCHAFTS-EINSTELLUNGSER-WEITERUNGSLISTE
ICC-PROFIL
AUFLÖSUNG 0
AUFLÖSUNG 1
AUFLÖSUNG 2
AUFLÖSUNG 3
UNTERBILD-DATEN
UNTERBILD-KOPFTEIL

FIG. 12

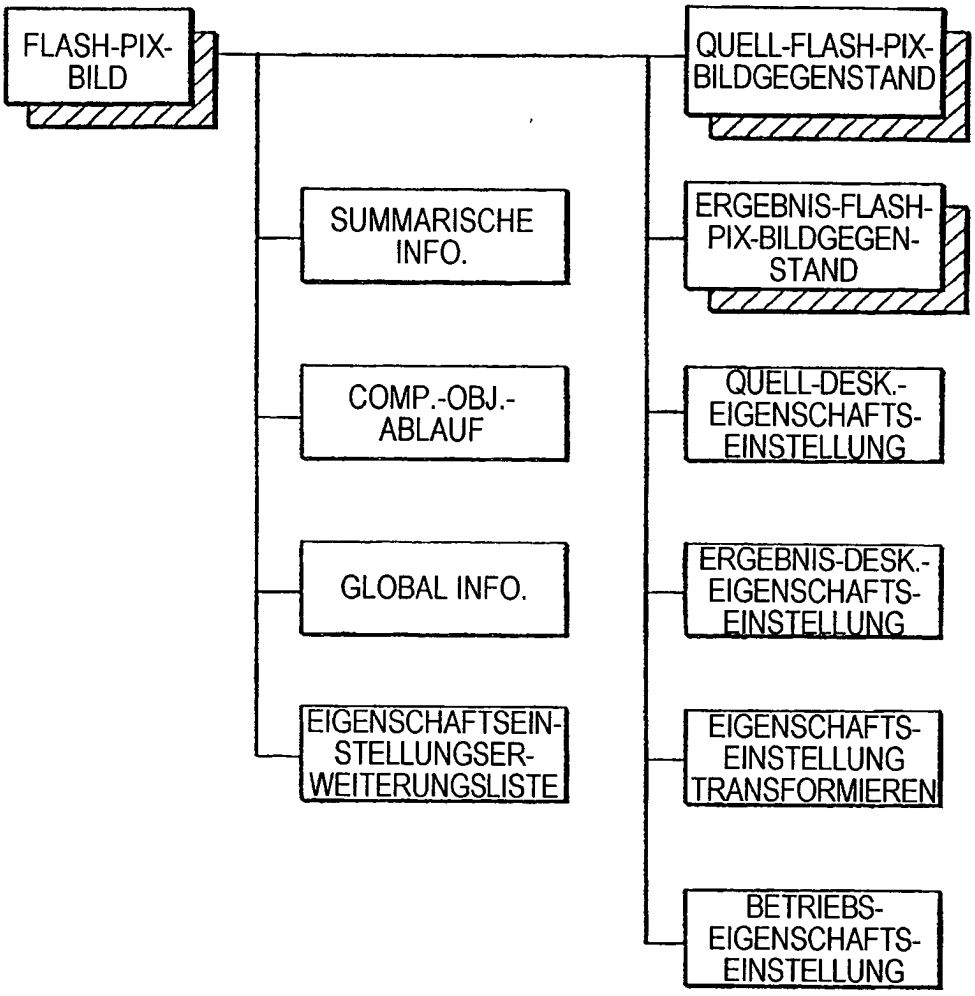

FLASH-PIX-BILD
SUMMARISCHE INFO.
COMP.-OBJ.-ABLAUF
GLOBAL INFO.
EIGENSCHAFTSEIN-STELLUNGSER-WEITERUNGSLISTE
QUELL-FLASH-PIX-BILDGEGENSTAND
ERGEBNIS-FLASH-PIX-BILDGEGEN-STAND
QUELL-DESK.-EIGENSCHAFTS-EINSTELLUNG
ERGEBNIS-DESK.-EIGENSCHAFTS-EINSTELLUNG
EIGENSCHAFTS-EINSTELLUNG TRANSFORMIEREN
BETRIEBS-EIGENSCHAFTS-EINSTELLUNG

FIG. 13

EIGENSCHAFTSNAME	ID CODE	TYP
ANZAHL VON BILDDATEN-SCHICHTEN	0x01000000	VT_UI4
BILDBREITE MIT MAXIMALER AUFLÖSUNG	0x01000002	VT_UI4
BILDHÖHE MIT MAXIMALER AUFLÖSUNG	0x01000003	VT_UI4
HÖHE URSPRUNGSANZEIGE	0x01000004	VT_R4
BREITE URSPRUNGSANZEIGE	0x01000005	VT_R4

EIGENSCHAFTSNAME	ID CODE	TYP
BILDBREITE BEI JEDER AUFLÖSUNG	0x02ii0000	VT_UI4
BILDHÖHE BEI JEDER AUFLÖSUNG	0x02ii0001	VT_UI4
BILDFARBE BEI JEDER AUFLÖSUNG	0x02ii0002	VT_BLOB
FORMATAUSDRUCKSBILD BEI JEDER AUFLÖSUNG, NUMERISCH	0x02ii0003	VT_UI4 | VT_VECTOR

EIGENSCHAFTSNAME	ID CODE	TYP
JPEG-TABELLE	0x03ii0001	VT_BLOB
MAXIMUM INDEX JPEG-TABELLE	0x03000002	VT_UI4

FIG. 14

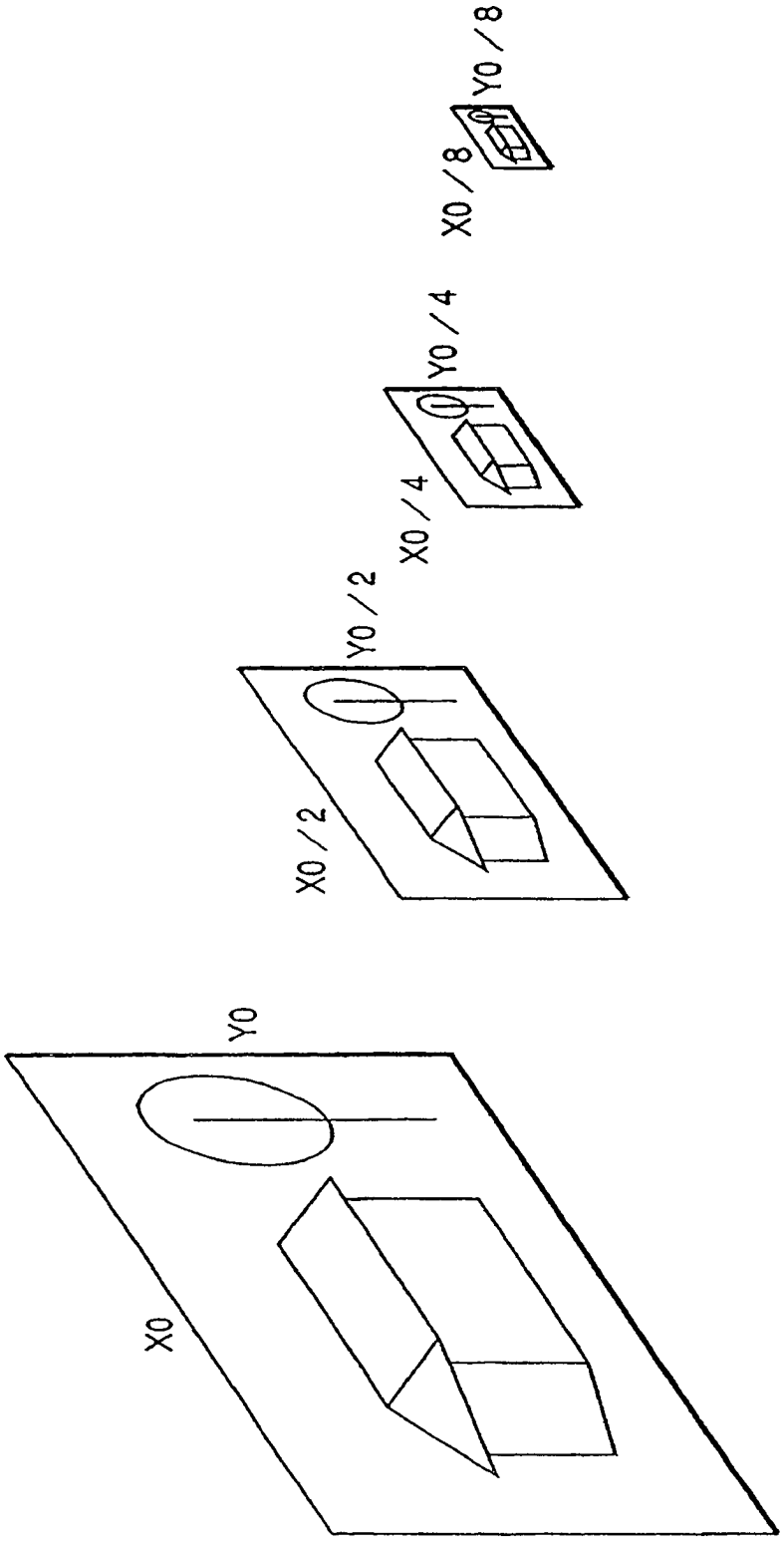


FIG. 15

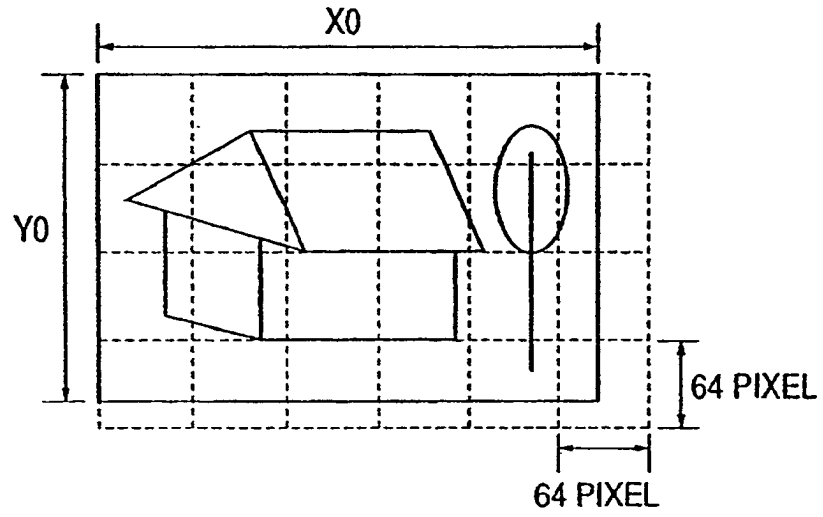


FIG. 16

TEILBILDNAME	LÄNGE	BYTE
BILDBREITE	4	4-7
BILDHÖHE	4	8-11
GESAMTKACHELZAHL	4	12 15
KACHELBREITE	4	16-19
KACHELHÖHE	4	20-23

FIG. 17

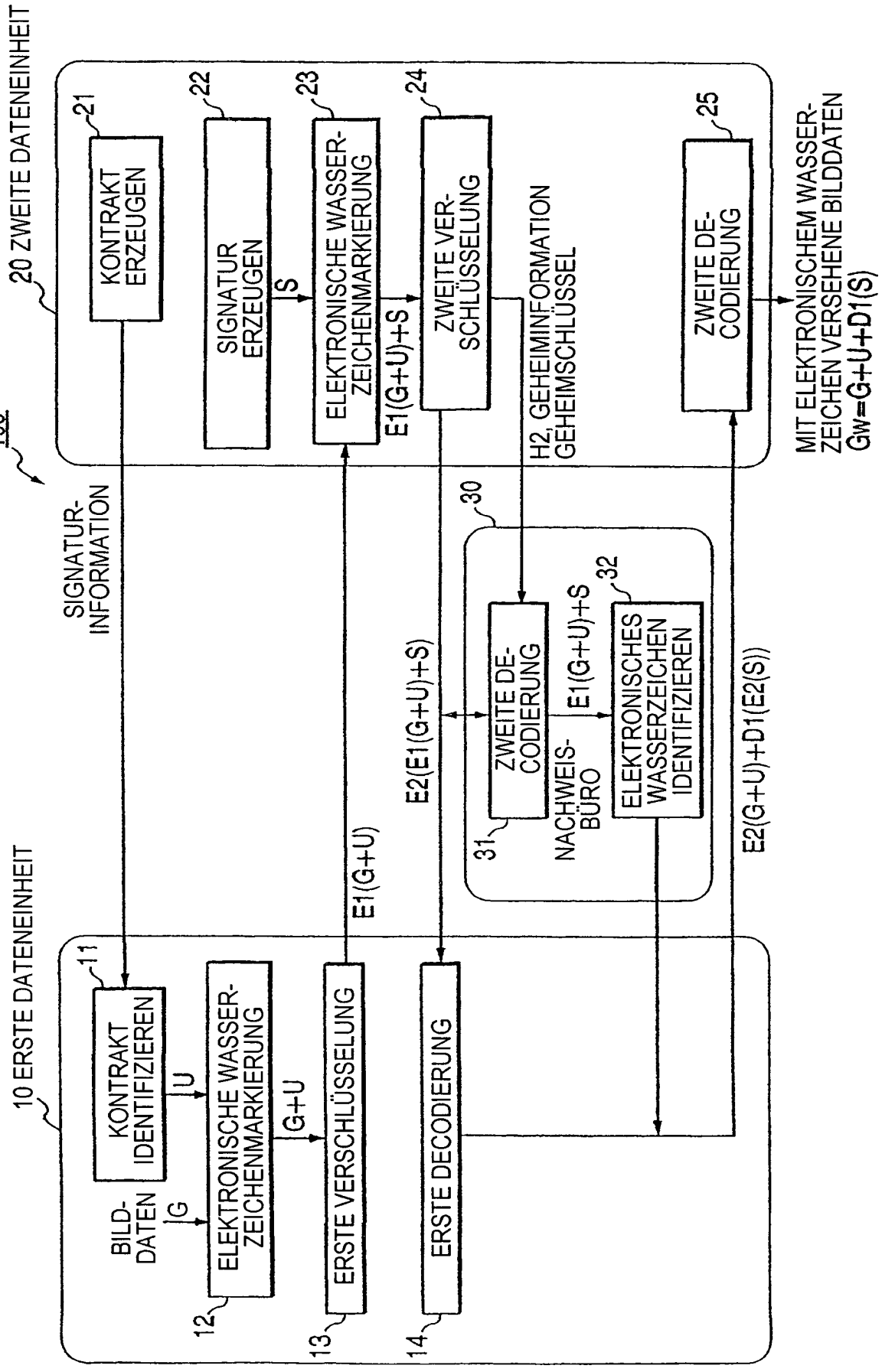

100
10 ERSTE DATENEINHEIT
20 ZWEITE DATENEINHEIT
11
KONTRAKT IDENTIFIZIEREN
U
BILD-DATEN
G
12
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
G+U
13
ERSTE VERSCHLÜSSELUNG
14
ERSTE DECODIERUNG
21
KONTRAKT ERZEUGEN
22
SIGNATUR ERZEUGEN
S
23
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
24
ZWEITE VER-SCHLÜSSELUNG
25
ZWEITE DE-CODIERUNG
SIGNATUR-INFORMATION
E1(G+U)
E1(G+U)+S
H2, GEHEIMINFORMATION GEHEIMSCHLÜSSEL
30
NACHWEIS-BÜRO
31
ZWEITE DE-CODIERUNG
E1(G+U)+S
32
ELEKTRONISCHES WASSERZEICHEN IDENTIFIZIEREN
E2(E1(G+U)+S)
E2(G+U)+D1(E2(S))
MIT ELEKTRONISCHEM WASSER-ZEICHEN VERSEHENE BILDDATEN
Gw=G+U+D1(S)

FIG. 18

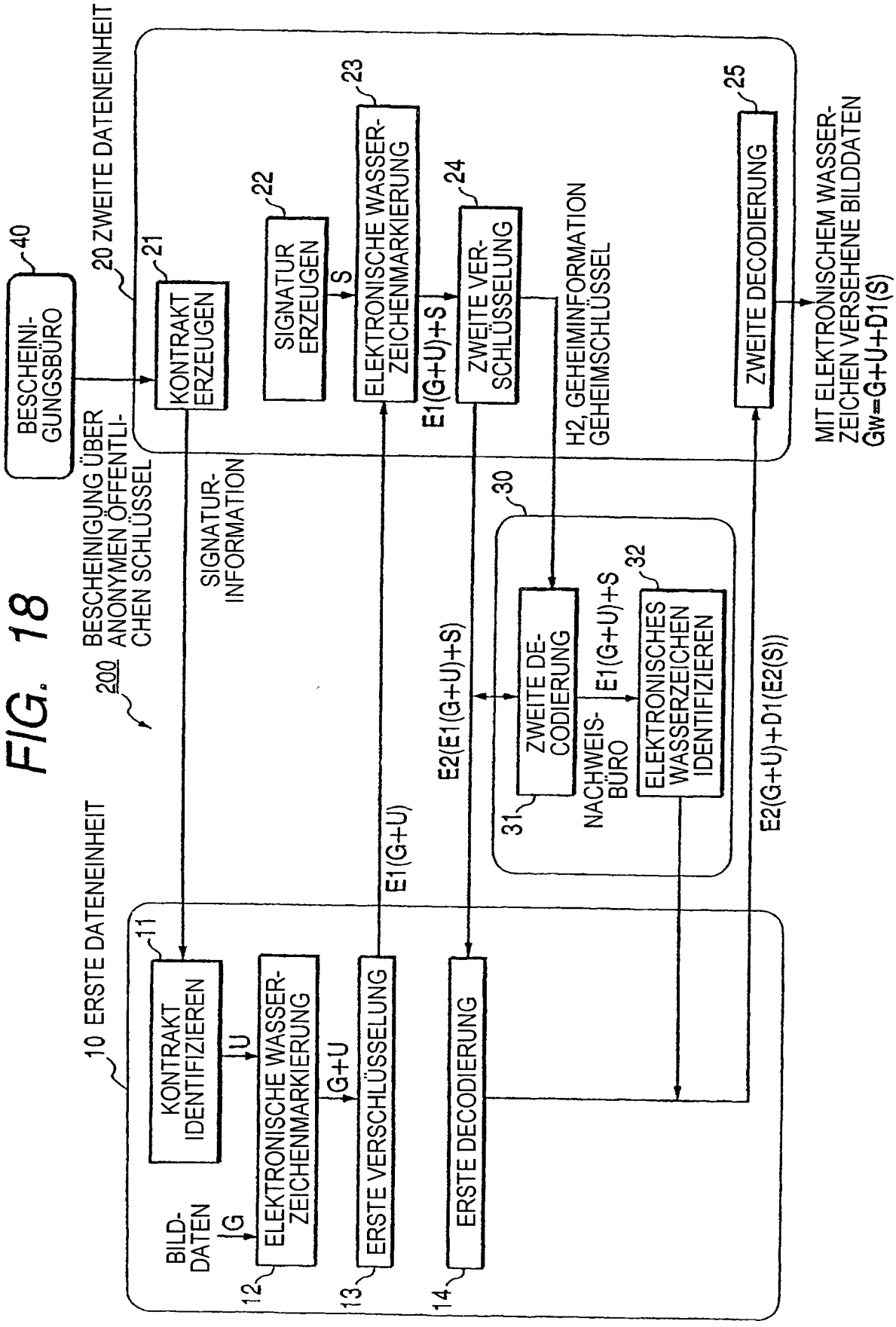

10 ERSTE DATENEINHEIT
20 ZWEITE DATENEINHEIT
200
BESCHEINIGUNG ÜBER ANONYMEN ÖFFENTLICHEN SCHLÜSSEL
BESCHEINIGUNGSBÜRO
40
KONTRAKT ERZEUGEN
21
SIGNATUR ERZEUGEN
22
ELEKTRONISCHE WASSERZEICHENMARKIERUNG
23
ZWEITE VERSCHLÜSSELUNG
24
ZWEITE DECODIERUNG
25
SIGNATURINFORMATION
S
E1(G+U)+S
H2, GEHEIMINFORMATION GEHEIMSCHLÜSSEL
MIT ELEKTRONISCHEM WASSERZEICHEN VERSEHENE BILDDATEN
Gw=G+U+D1(S)
KONTRAKT IDENTIFIZIEREN
11
U
BILDDATEN
G
ELEKTRONISCHE WASSERZEICHENMARKIERUNG
12
G+U
ERSTE VERSCHLÜSSELUNG
13
ERSTE DECODIERUNG
14
E1(G+U)
E2(E1(G+U)+S)
E2(G+U)+D1(E2(S))
NACHWEISBÜRO
30
ZWEITE DECODIERUNG
31
E1(G+U)+S
ELEKTRONISCHES WASSERZEICHEN IDENTIFIZIEREN
32

FIG. 19

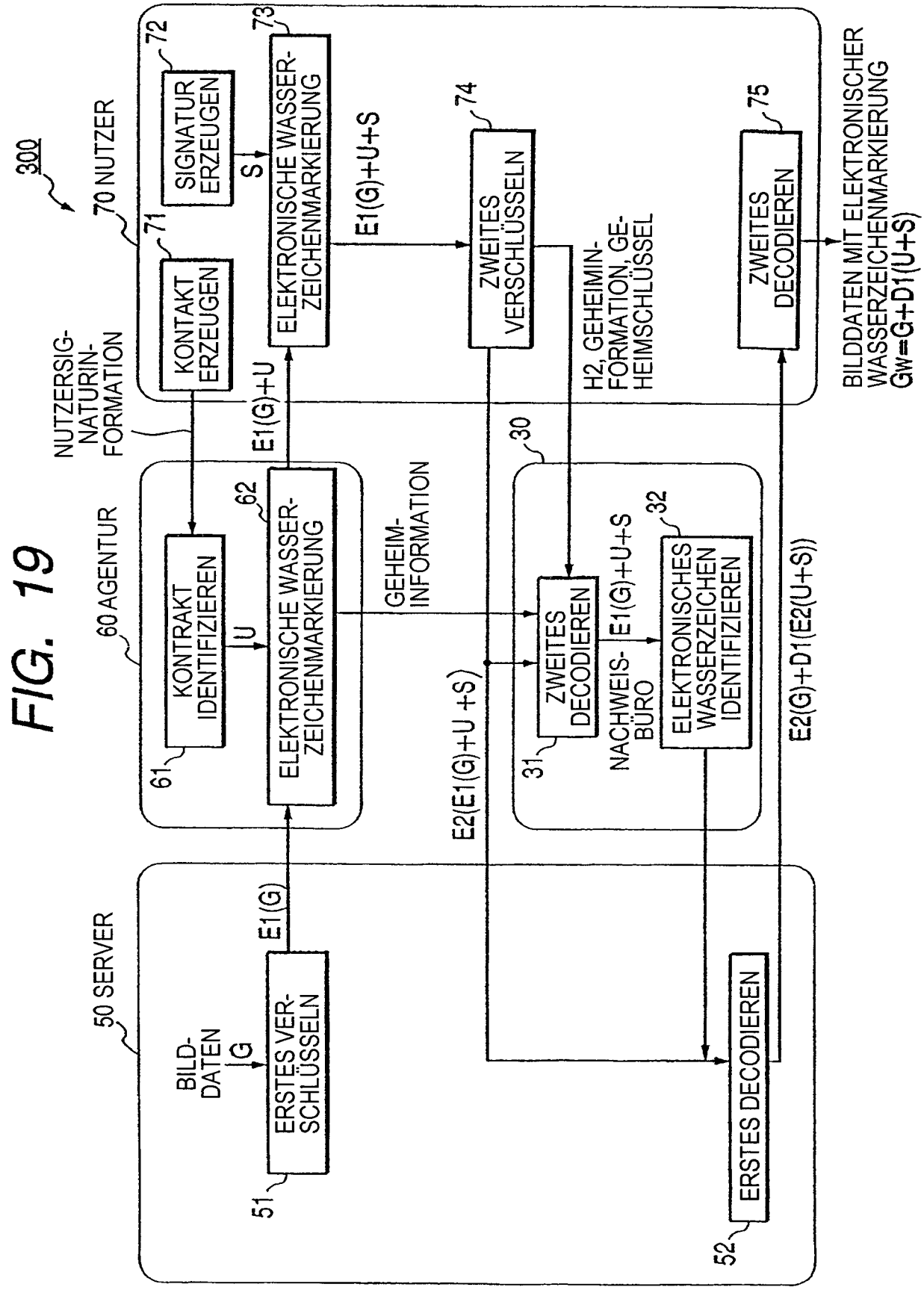

300
70 NUTZER
72
SIGNATUR ERZEUGEN
S
73
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
E1(G)+U+S
74
ZWEITES VERSCHLÜSSELN
75
ZWEITES DECODIEREN
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG Gw=G+D1(U+S)
71
KONTAKT ERZEUGEN
NUTZERSIG-NATURIN-FORMATION
E1(G)+U
H2, GEHEIMIN-FORMATION, GE-HEIMSCHLÜSSEL
60 AGENTUR
62
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
GEHEIM-INFORMATION
30
KONTRAKT IDENTIFIZIEREN
U
61
ZWEITES DECODIEREN
E1(G)+U+S
32
ELEKTRONISCHES WASSERZEICHEN IDENTIFIZIEREN
NACHWEIS-BÜRO
31
E2(E1(G)+U+S)
E2(G)+D1(E2(U+S))
50 SERVER
BILD-DATEN
G
E1(G)
ERSTES VER-SCHLÜSSELN
51
ERSTES DECODIEREN
52

FIG. 20

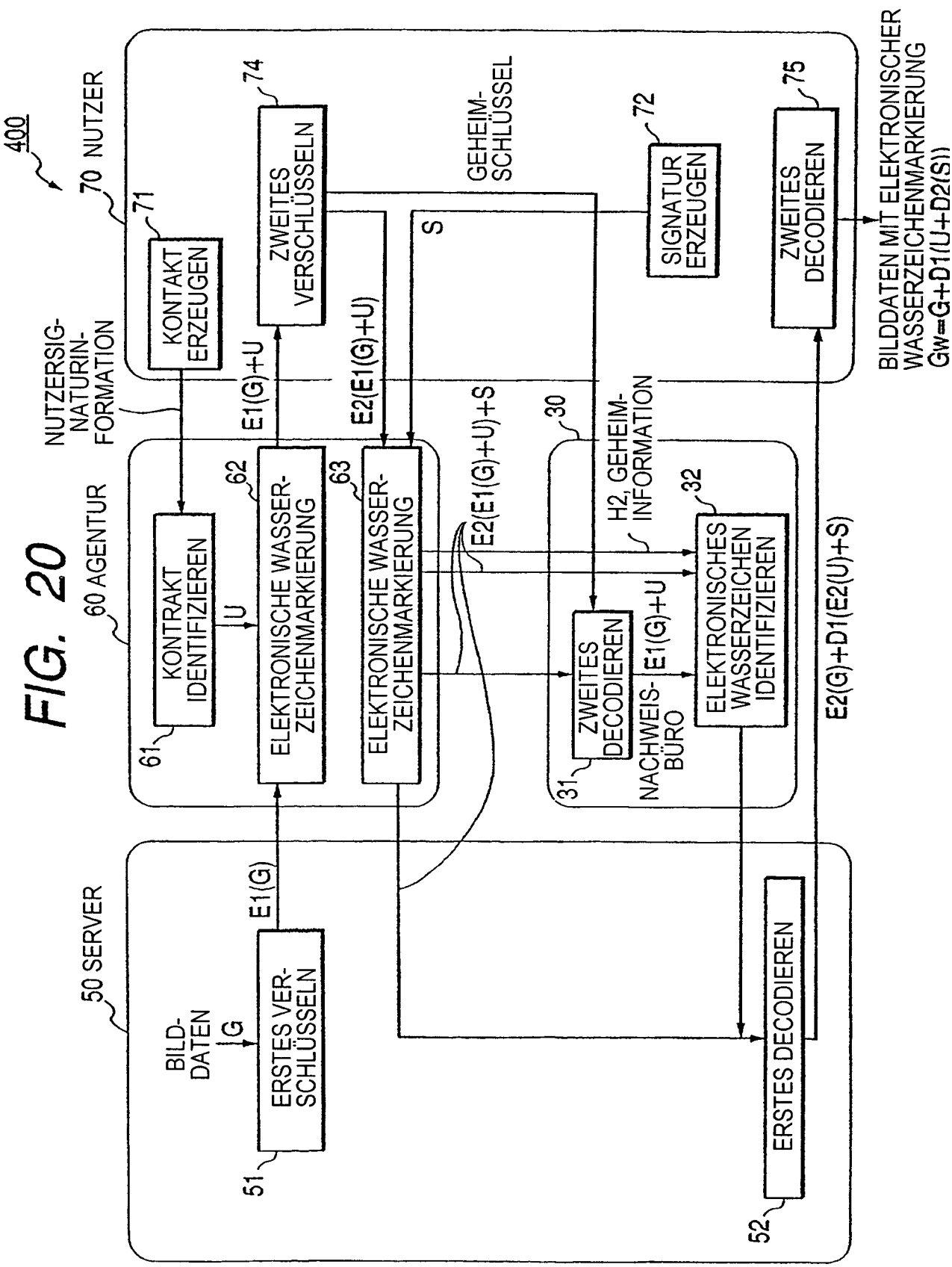

400
70 NUTZER
71
KONTAKT ERZEUGEN
74
ZWEITES VERSCHLÜSSELN
GEHEIM-SCHLÜSSEL
72
SIGNATUR ERZEUGEN
75
ZWEITES DECODIEREN
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG
GW=G+D1(U+D2(S))
NUTZERSIG-NATURIN-FORMATION
E1(G)+U
E2(E1(G)+U)
S
60 AGENTUR
KONTRAKT IDENTIFIZIEREN
U
61
62
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
63
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
E2(E1(G)+U)+S
30
H2, GEHEIM-INFORMATION
32
ELEKTRONISCHES WASSERZEICHEN IDENTIFIZIEREN
ZWEITES DECODIEREN
E1(G)+U
31
NACHWEIS-BÜRO
E2(G)+D1(E2(U)+S)
50 SERVER
BILD-DATEN
G
ERSTES VER-SCHLÜSSELN
E1(G)
51
ERSTES DECODIEREN
52

FIG. 21

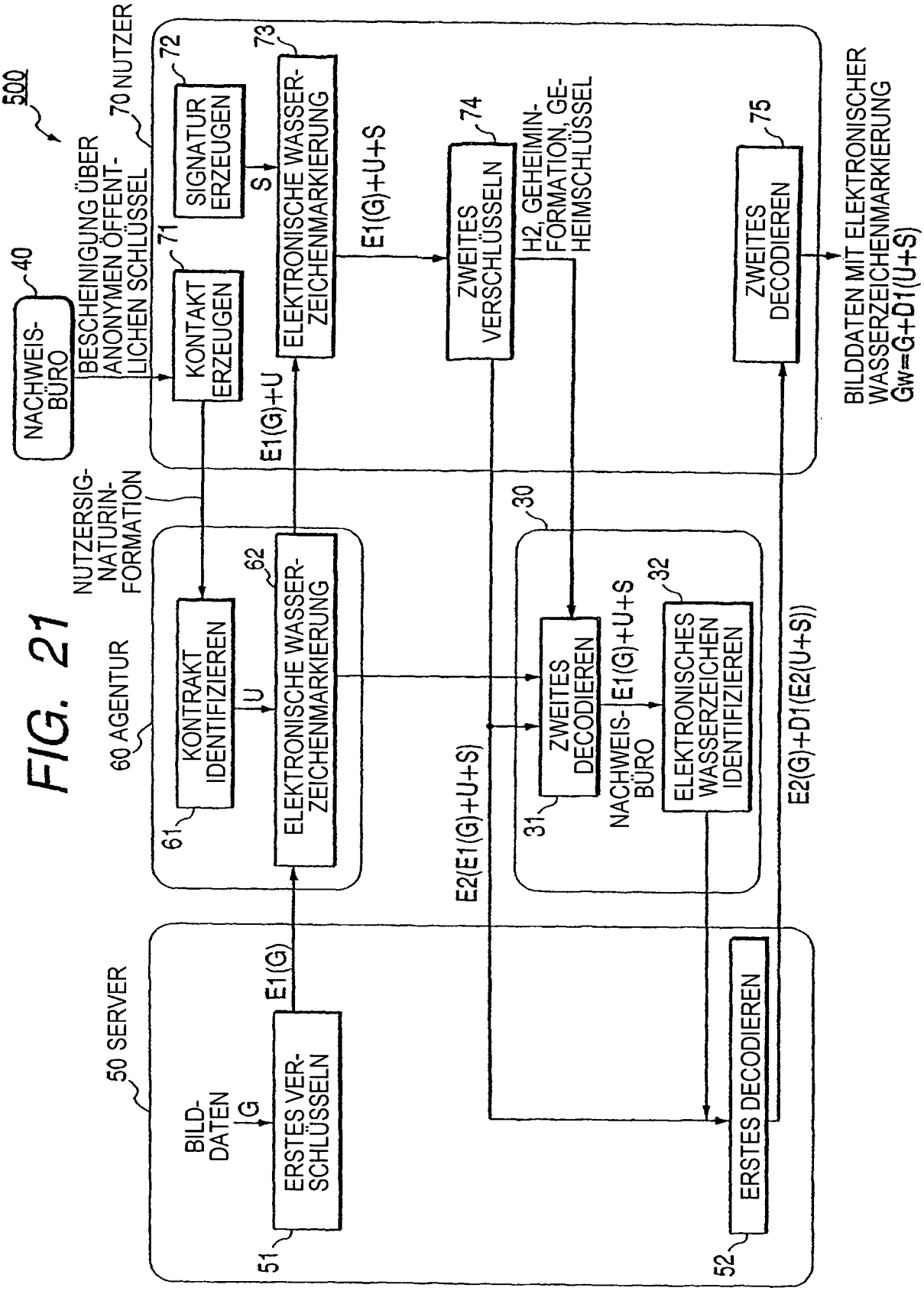

500
70 NUTZER
40
NACHWEIS-BÜRO
BESCHEINIGUNG ÜBER ANONYMEN ÖFFENTLICHEN SCHLÜSSEL
71
KONTAKT ERZEUGEN
72
SIGNATUR ERZEUGEN
S
73
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
E1(G)+U+S
74
ZWEITES VERSCHLÜSSELN
H2, GEHEIMINFORMATION, GEHEIMSCHLÜSSEL
75
ZWEITES DECODIEREN
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG
Gw=G+D1(U+S)
E1(G)+U
NUTZERSIGNATURINFORMATION
60 AGENTUR
61
KONTRAKT IDENTIFIZIEREN
U
62
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
30
31
ZWEITES DECODIEREN
NACHWEIS-BÜRO
E1(G)+U+S
32
ELEKTRONISCHES WASSERZEICHEN IDENTIFIZIEREN
E2(E1(G)+U+S)
E2(G)+D1(E2(U+S))
50 SERVER
BILD-DATEN
G
E1(G)
51
ERSTES VER-SCHLÜSSELN
52
ERSTES DECODIEREN

FIG. 22

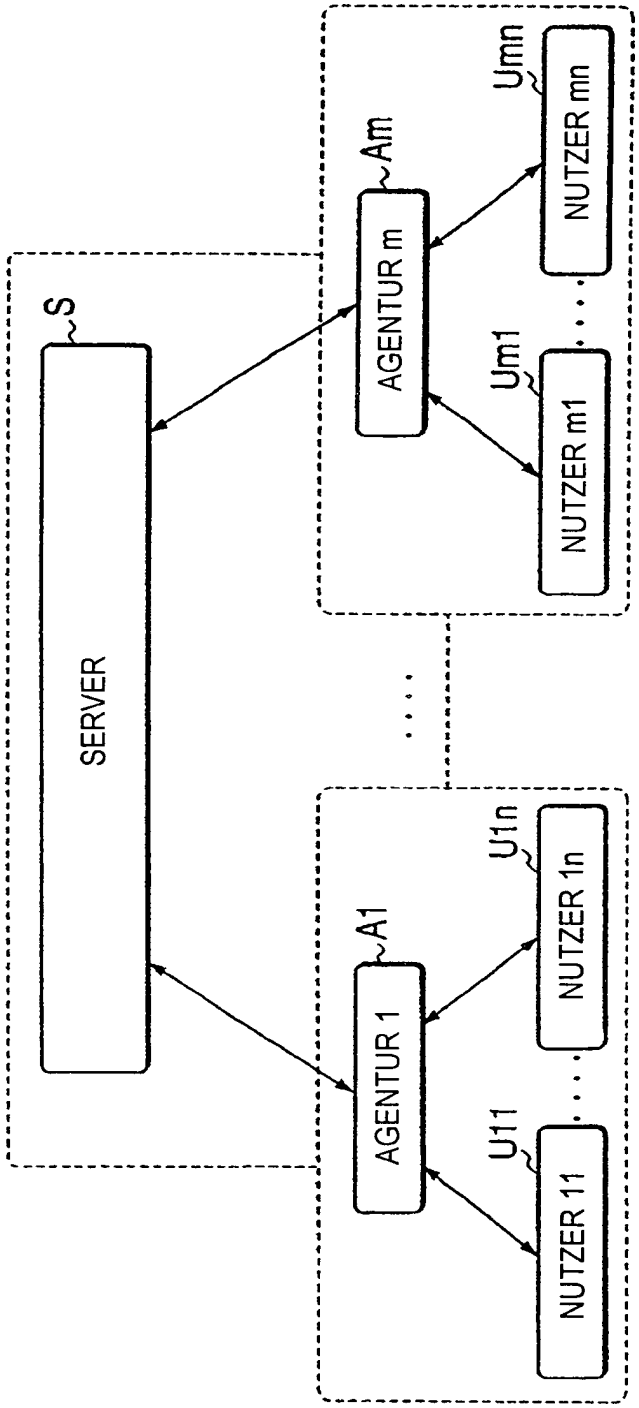

S
SERVER
AGENTUR 1
A1
U11
NUTZER 11
U1n
NUTZER 1n
AGENTUR m
Am
Um1
NUTZER m1
Umn
NUTZER mn

FIG. 23

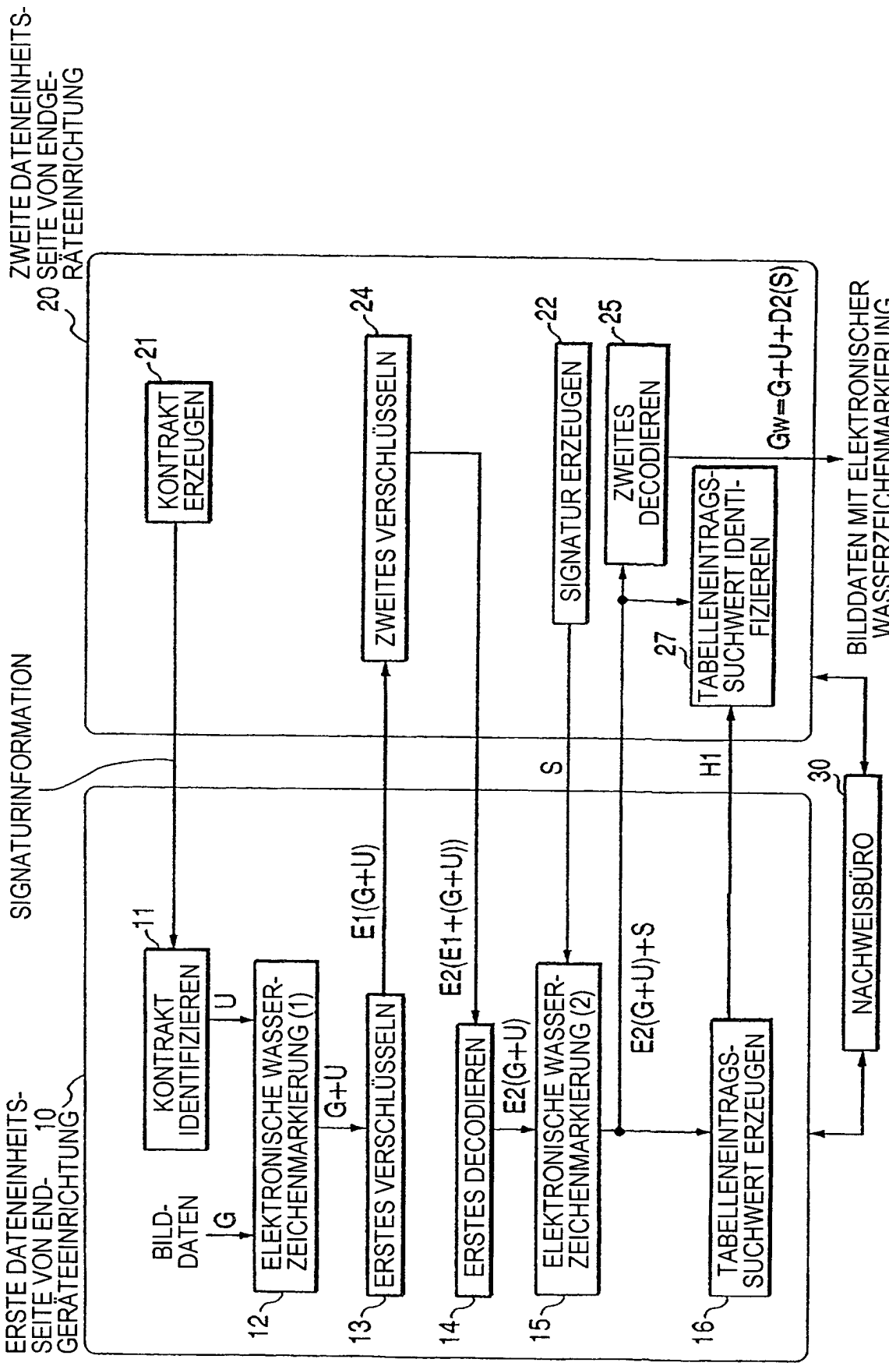

ERSTE DATENEINHEITS-SEITE VON END-GERÄTEEINRICHTUNG
10
ZWEITE DATENEINHEITS-SEITE VON ENDGE-RÄTEEINRICHTUNG
20
SIGNATURINFORMATION
KONTRAKT ERZEUGEN
21
KONTRAKT IDENTIFIZIEREN
11
U
BILD-DATEN
G
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG (1)
12
G+U
ERSTES VERSCHLÜSSELN
13
E1(G+U)
ZWEITES VERSCHLÜSSELN
24
E2(E1+(G+U))
ERSTES DECODIEREN
14
E2(G+U)
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG (2)
15
E2(G+U)+S
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
16
S
SIGNATUR ERZEUGEN
22
H1
ZWEITES DECODIEREN
25
TABELLENEINTRAGS-SUCHWERT IDENTI-FIZIEREN
27
Gw=G+U+D2(S)
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG
NACHWEISBÜRO
30

FIG. 24

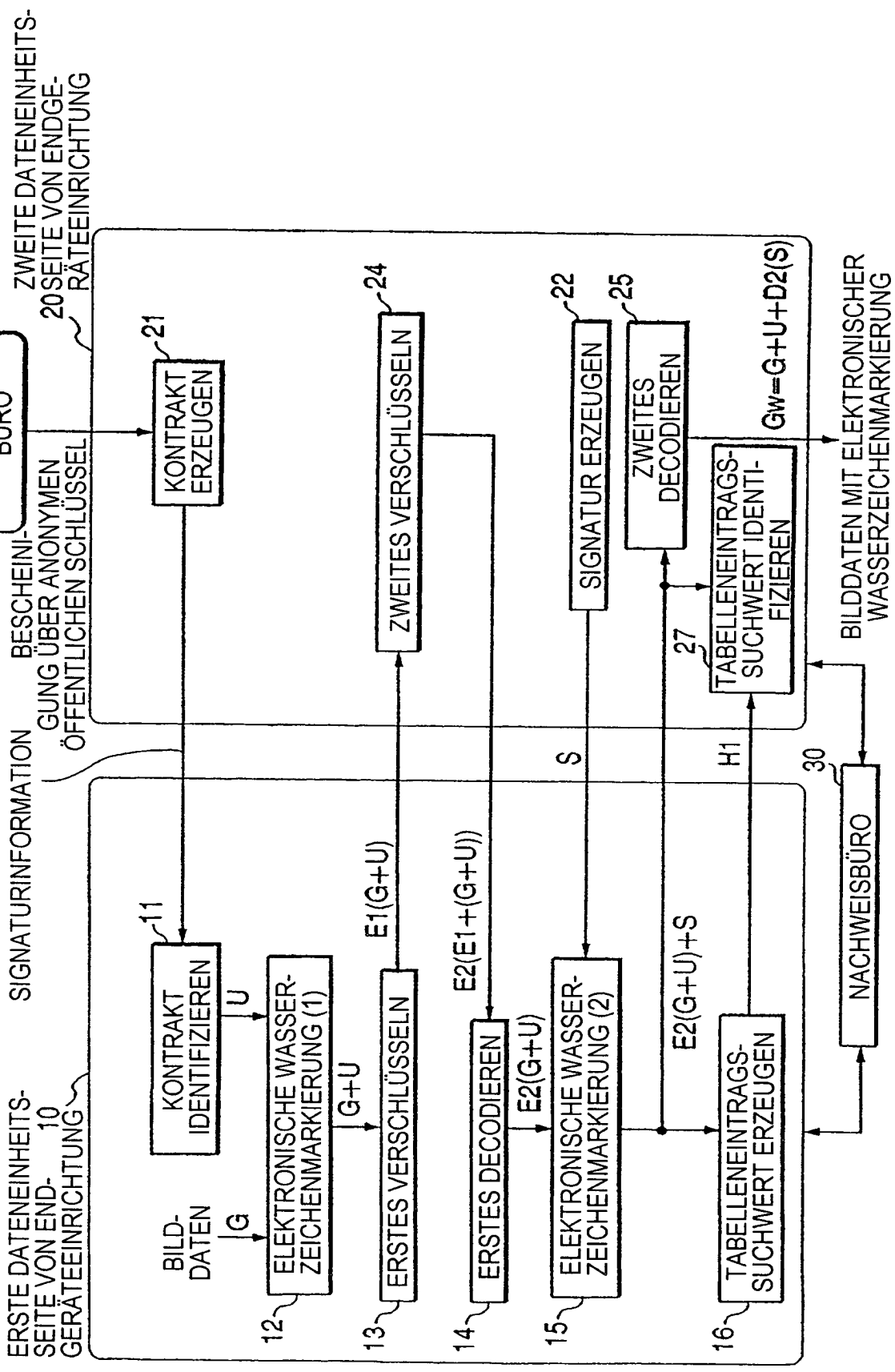

NACHWEIS-BÜRO
40
ZWEITE DATENEINHEITS-SEITE VON ENDGERÄTEEINRICHTUNG
20
BESCHEINIGUNG ÜBER ANONYMEN ÖFFENTLICHEN SCHLÜSSEL
KONTRAKT ERZEUGEN
21
ZWEITES VERSCHLÜSSELN
24
SIGNATURINFORMATION
SIGNATUR ERZEUGEN
22
ZWEITES DECODIEREN
25
Gw=G+U+D2(S)
TABELLENEINTRAGS-SUCHWERT IDENTI-FIZIEREN
27
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG
ERSTE DATENEINHEITS-SEITE VON END-GERÄTEEINRICHTUNG
10
KONTRAKT IDENTIFIZIEREN
11
U
BILD-DATEN
G
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG (1)
12
G+U
ERSTES VERSCHLÜSSELN
13
E1(G+U)
ERSTES DECODIEREN
14
E2(E1+(G+U))
E2(G+U)
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG (2)
15
S
E2(G+U)+S
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
16
H1
NACHWEISBÜRO
30

FIG. 25

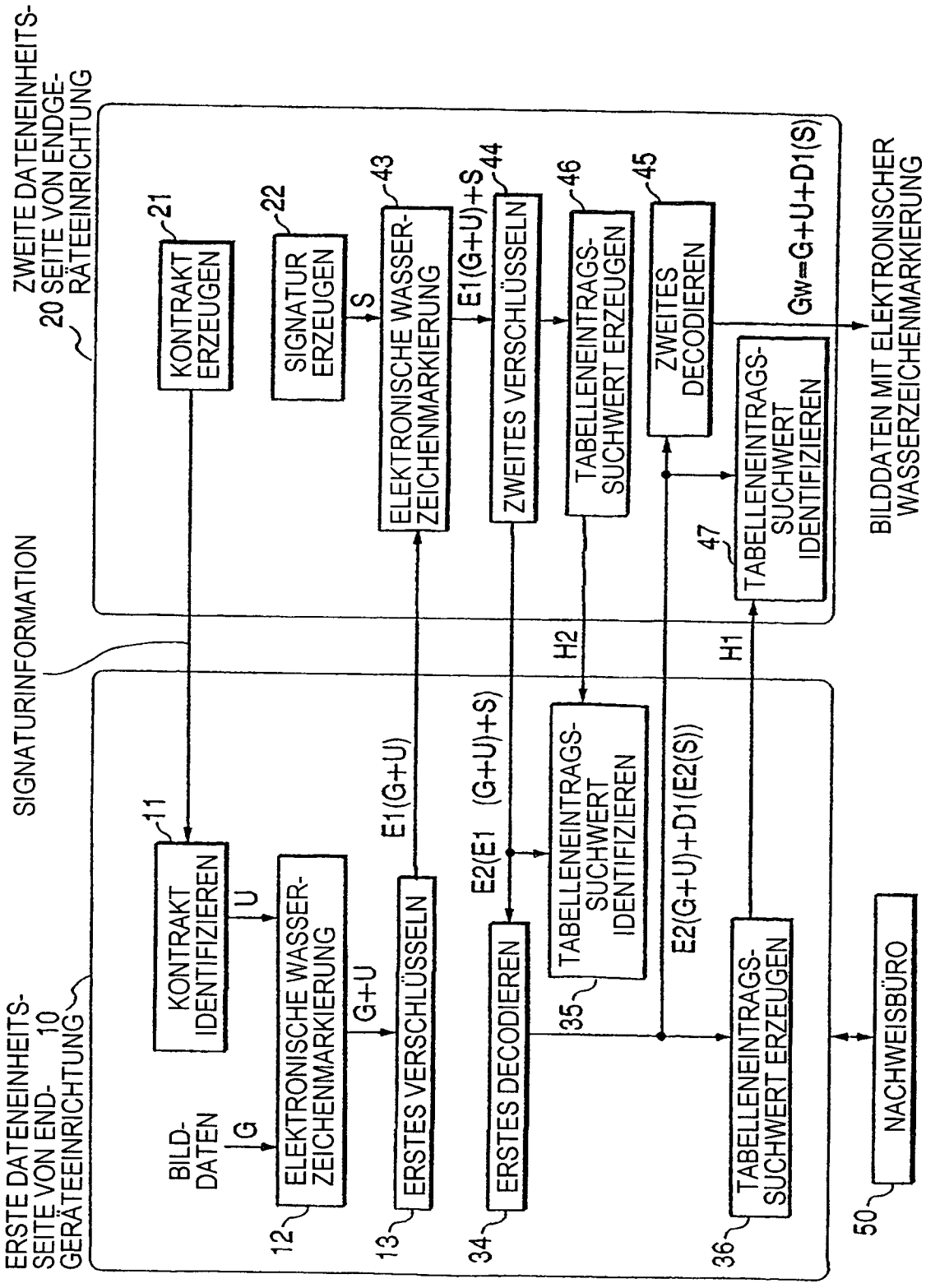
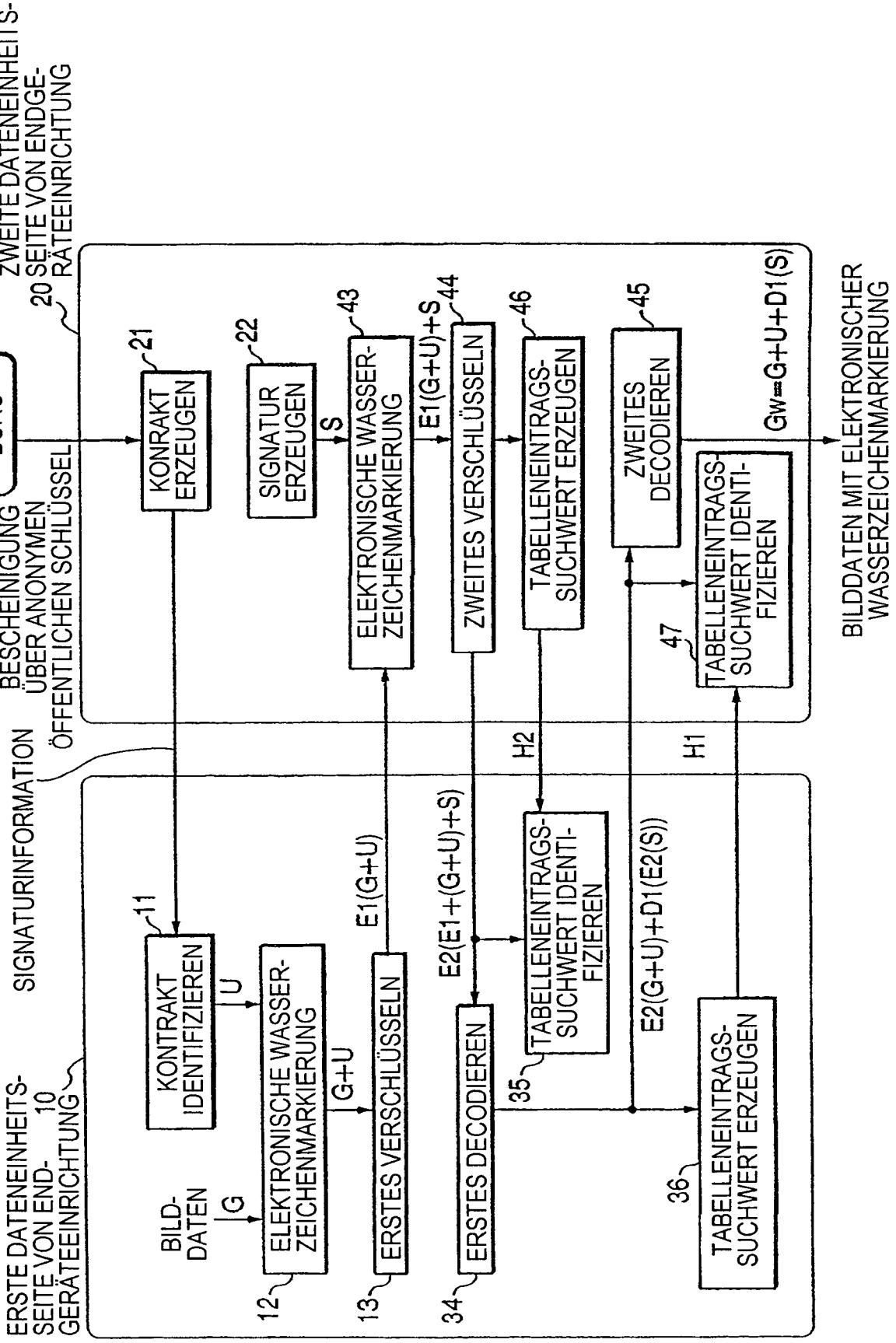

ERSTE DATENEINHEITS-SEITE VON END-GERÄTEEINRICHTUNG
10
SIGNATURINFORMATION
ZWEITE DATENEINHEITS-SEITE VON ENDGE-RÄTEEINRICHTUNG
20
BILD-DATEN
G
KONTRAKT IDENTIFIZIEREN
11
U
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
12
G+U
ERSTES VERSCHLÜSSELN
13
E1(G+U)
KONTRAKT ERZEUGEN
21
SIGNATUR ERZEUGEN
22
S
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
43
E1(G+U)+S
ZWEITES VERSCHLÜSSELN
44
E2(E1 (G+U)+S)
ERSTES DECODIEREN
34
TABELLENEINTRAGS-SUCHWERT IDENTIFIZIEREN
35
H2
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
46
E2(G+U)+D1(E2(S))
ZWEITES DECODIEREN
45
H1
TABELLENEINTRAGS-SUCHWERT IDENTIFIZIEREN
47
Gw=G+U+D1(S)
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
36
NACHWEISBÜRO
50

FIG. 26


ERSTE DATENEINHEITS-SEITE VON END-GERÄTEEINRICHTUNG
10
SIGNATURINFORMATION
ZWEITE DATENEINHEITS-SEITE VON ENDGE-RÄTEEINRICHTUNG
20
BESCHEINIGUNG ÜBER ANONYMEN ÖFFENTLICHEN SCHLÜSSEL
NACHWEIS-BÜRO
40
BILD-DATEN
G
KONTRAKT IDENTIFIZIEREN
11
U
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
12
G+U
ERSTES VERSCHLÜSSELN
13
E1(G+U)
KONRAKT ERZEUGEN
21
SIGNATUR ERZEUGEN
22
S
ELEKTRONISCHE WASSER-ZEICHENMARKIERUNG
43
E1(G+U)+S
ZWEITES VERSCHLÜSSELN
44
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
46
ZWEITES DECODIEREN
45
TABELLENEINTRAGS-SUCHWERT IDENTI-FIZIEREN
47
GW=G+U+D1(S)
BILDDATEN MIT ELEKTRONISCHER WASSERZEICHENMARKIERUNG
E2(E1+(G+U)+S)
ERSTES DECODIEREN
34
TABELLENEINTRAGS-SUCHWERT IDENTI-FIZIEREN
35
H2
E2(G+U)+D1(E2(S))
TABELLENEINTRAGS-SUCHWERT ERZEUGEN
36
H1