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

(10) **DE 600 12 515 T2** 2005.08.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 181 810 B1**
(21) Deutsches Aktenzeichen: **600 12 515.7**
(86) PCT-Aktenzeichen: **PCT/EP00/04053**
(96) Europäisches Aktenzeichen: **00 929 504.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 00/74371**
(86) PCT-Anmeldetag: **05.05.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **07.12.2000**
(97) Erstveröffentlichung durch das EPA: **27.02.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **28.07.2004**
(47) Veröffentlichungstag im Patentblatt: **04.08.2005**

(51) Int Cl.[7]: **H04N 1/32**

(30) Unionspriorität:
9907139 01.06.1999 FR

(84) Benannte Vertragsstaaten:
DE, ES, FR, GB, IT

(73) Patentinhaber:
Thomson Licensing S.A., Boulogne-Billancourt, FR

(72) Erfinder:
FURON, Teddy, 92648 Boulogne, FR; DUHAMEL, Pierre, 92648 Boulogne, FR

(74) Vertreter:
Wördemann, H., Dipl.-Ing., Pat.-Anw., 31787 Hameln

(54) Bezeichnung: **SYSTEM ZUM WASSERZEICHNEN VON DIGITALEN DATEN MIT GEBRAUCH VON VERFAHREN ZUM EINFÜGEN UND AUFFINDEN VON WASSERZEICHEN**

Beschreibung

[0001] Die vorliegende Erfindung betrifft das Gebiet der Markierung (watermarking oder mit einem "Wasserzeichen" versehen) von digitalen Daten. Sie betrifft insbesondere ein System zur Markierung von Daten unter Anwendung neuer Verfahren zum Einfügen und Auffinden von Markierungen sowie Geräte zur Durchführung dieser Verfahren.

[0002] Neuste Verfahren zum Schutz gegen das verbotene Kopieren von digitalen Daten verwenden das Prinzip der Markierung von Daten, die in der Einfügung einer Markierung besteht, allgemein bezeichnet als ein "watermark" in einen Multimedia-Inhalt (Standbild, Video, Ton, usw.) in einer nicht wahrnehmbaren Weise. Die Markierung kann zum Beispiel ein Signal sein, das anzeigt, dass der Inhalt nicht kopiert werden darf, oder ein anderes Datenwort, das es dem Anwender des Multimedia-Inhalts ermöglicht, illegale Kopien zu ermitteln.

[0003] Um ihre Rolle einwandfrei zu erfüllen, muss die Markierung robust sein gegenüber Umsetzungen des Markierungsinhalts, unabhängig davon, ob diese Umsetzungen unbeabsichtigt durch einen Piraten oder Hacker erfolgen, der die Markierung löschen möchte, oder aus Verzerrungen resultiert, die während der Übertragung des die Markierungsdaten enthaltenden Signals erfolgt ist.

[0004] Aus dem Stand der Technik sind verschiedene Lösungen für Markierungsdaten bekannt. Verwiesen wird insbesondere auf die Dokumente EP-A-0 828 372, EP-A-0 840 513, WO-A-98/03014 oder WO-A-98/54897, die Verfahren zum Einfügen von Markierungen in zu schützende Daten und Verfahren zur Ermittlung der Anwesenheit derartiger Markierungen in den Daten beschreiben.

[0005] Ein Schema, das allgemein zur Beschreibung des Prinzips der Markierung von Daten benutzt wird, ist dasjenige von **Fig. 1**. Ein erster Teil 1 betrifft die Einfügung eines verborgenen Datenworts W (die Markierung) in einen zu schützenden Inhalt C. Das resultiert in einen mit einer Markierung versehenen Inhalt CT. Der Teil 2 betrifft die Ermittlung der Anwesenheit eines Datenworts W in dem empfangenen Inhalt CT. Ein zusätzliches Datenwort K wird außerdem in dem Vorgang zur Einfügung und Ermittlung der Markierung benötigt. Dieses Datenwort, das in einer geheimen Weise sowohl von dem Gerät zur Einfügung und Ermittlung der Markierung benutzt wird, wird als der Schlüssel bezeichnet, in Analogie zu den so genannten symmetrischen oder Verschlüsselungssystemen mit einem privaten Schlüssel.

[0006] Zum Beispiel besteht eine bekannte Lösung zur Markierung, die in den Dokumenten EP-A-0 828 372 und EP-A-0 840 513 beschrieben wird, in dem Zusatz eines Pseudo-Zufallsrauschens zu den Daten, die markiert werden sollen. Der Ermittlungsvorgang wird in diesem Fall durch Bildung einer Korrelationsberechnung durchgeführt: die empfangenen Daten werden als mit einer Markierung versehen erklärt, wenn die Korrelation mit der Referenz-Pseudrauschfolge (benutzt für die Einfügung der Markierung) größer ist als ein bestimmter Schwellwert. In diesem Beispiel bildet die Referenz-Pseudorauschfolge den Schlüssel K des Schemas für die Daten für das Markierungs-Schema von **Fig. 1**.

[0007] Das Problem bei diesem Schema besteht darin, dass jede Einheit, die die Markierung ermitteln kann, denselben Schlüssel K benutzten muss, wie die Einheit, die die Markierung eingefügt hat. In diesem Fall kann die Einheit, die die Markierung ermitteln kann, dieses außerdem löschen oder es ändern. Dadurch entfällt der gesamte Nutzen der ursprünglichen Markierung der Daten. Infolgedessen sollte ein Anbieter des durch die Markierung geschützten Inhalts seinen Schlüssel K nicht kommunizieren, der für die Einfügung der Markierung diente, anders als in einer geheimen Weise zu bewährten Objekten. Das beschränkt nennenswert die Möglichkeiten der Daten-Markierung auf zahlreichen Gebieten.

[0008] Insbesondere auf dem Gebiet der elektronischen Consumer-Geräte ist es hinreichend bekannt, dass es nahezu unmöglich ist, in jedem Fall bei vernünftigen Kosten geheime Parameter in einer Einrichtung oder in einer eine derartigen Einrichtung enthaltenen Software zu speichern. Smart Cards. die als die einzigen Teile der Einrichtung angesehen werden, die die Speicherung eines Geheimpara-meters ermöglichen, sind selbst nicht leistungsfähig genug, die Berechnungen mit einem Vorgang mit Markierungserkennung durchzuführen.

[0009] In dem oben beschriebenen Beispiel, wo die Markierung durch Hinzufügung einer Pseudo-Zufallsrauschfolge zu den Daten erfolgt, die mit einer Markierung versehen werden, selbst wenn die Referenz-Pseudorauschfolge geheim in dem Markierungs-Ermittlungsgerät gespeichert wird, wurde gezeigt, dass ein Pirat theoretisch die Referenzfolge entdecken und dadurch die Markierung aus den Daten durch Beobachtung des Ausgangs von dem Detektor als eine Funktion einer großen Zahl von verschiedenen Eingangssignalen beseitigen kann.

[0010] Der Erfindung liegt die Aufgabe zugrunde, die oben genannten Probleme zu lösen.

[0011] Zu diesem Zweck betrifft die Erfindung ein Verfahren zur Einfügung einer Markierung in Daten, die einen zu schützenden Inhalt darstellen, wie im Anspruch 1 angegeben.

[0012] Gemäß einem bevorzugten Aspekt der Erfindung enthält das Verfahren außerdem die folgenden Schritte:

e) Durchführung einer Pseudozufalls-Verschachtelung der Modulationsfolge vor dem Schritt c),

f) Durchführung derselben Pseudozufalls-Verschachtelung der Daten Modulationsfolge vor dem Schritt d) und

g) Durchführung einer inversen Verschachtelung nach dem Schritt d}, um so die markierten Daten zu bilden.

[0013] Die Erfindung betrifft außerdem ein Verfahren zur Ermittlung einer Markierung in einen empfangenen Inhalt darstellende Daten, wie im Anspruch 3 angegeben.

[0014] Gemäß einem anderen bevorzugten Aspekt der Erfindung erfolgt eine Pseudozufalls-Verschachtelung der empfangenen Daten, die identisch ist zu der im Schritt f) erfolgenden Verschachtelung, vor dem Schritt i).

[0015] Die Erfindung betrifft außerdem ein Gerät zur Einfügung einer Markierung in einen zu schützenden Inhalt darstellende Daten, wie im Anspruch 5 angegeben.

[0016] Gemäß einer bevorzugten Ausführungsform der Erfindung enthält das Gerät außerdem:

– erste Mittel zur Pseudozufalls-Verschachtelung der Daten, die den zu schützenden Inhalt darstellen, zur Lieferung verschachtelter Daten,

– zweite Mittel zur Pseudozufalls-Verschachtelung, die identisch sind zu den ersten Mitteln für den Empfang der Modulationsfolge, und so eine verschachtelte Modulationsfolge zuzuführen, wobei die verschachtelte Modulationsfolge den Mutiplikationsmitteln zur Multiplikation mit der gefilterten Pseudozufallsrauschfolge zugeführt wird,

– wobei die verschachtelten Daten den Additionsmitteln zugeführt werden, um so zu der gefilterten Pseudozufallsrauschfolge addiert zu werden, multipliziert mit der verschachtelten Modulationsfolge, und

– Mittel zur inversen Verschachtelung der ersten Verschachtelungsmittel, verbunden mit dem Ausgang der Addiermittel, um so die mit einer Markierung versehenen Daten zuzuführen.

[0017] Gemäß einer besonderen Ausführungsform der Erfindung enthält das Gerät:

– Mittel zur Umsetzung des zu schützenden Inhalts in den Inhalt darstellende Daten, und

– Mittel zur inversen Umsetzung der markierten Daten in einen markierten Inhalt.

[0018] Die Erfindung betrifft außerdem ein Gerät zur Ermittlung einer Markierung in Daten, die einen empfangenen Inhalt darstellen, wie im Anspruch 8 angegeben.

[0019] Gemäß einer besonderen Ausführungsform enthält das Gerät außerdem:

– Mittel zur Pseudozufalls-Verschachtelung der Daten, die den empfangenen Inhalt darstellen, zur Durchführung derselben Verschachtelung wie die ersten Verschachtelungsmittel des Einfügegeräts, wobei die verschachtelten Daten den Mitteln für die Gewinnung der Leistungsspektraldichte zugeführt werden.

[0020] Gemäß einer anderen bevorzugten Ausführungsform enthält das Gerät außerdem:

– Mittel zur Umsetzung des empfangenen Inhalts in den Inhalt darstellende Daten, wobei die Umsetzmittel dieselbe Umsetzung bewirken wie die Umsetzmittel des Einfügegeräts.

[0021] Weitere Merkmale und Vorteile der Erfindung ergeben sind aus der folgenden Beschreibung einer nicht-einschränkenden besonderen Ausführungsform der Erfindung anhand der beigefügten Figuren:

[0022] Die vorher beschriebene Fig. 1 zeigt ein bekanntes Schema für die Markierung von digitalen Daten,

[0023] Fig. 2 zeigt schematisch ein Gerät zur Einfügung einer Markierung gemäß der Erfindung,

[0024] Fig. 3 zeigt schematisch ein Gerät zur Markierungsermittlung gemäß der Erfindung,

[0025] Fig. 4 zeigt ein neues Schema für die Markierung von digitalen Daten gemäß der Erfindung.

[0026] In Fig. 2 ist ein Gerät gemäß der Erfindung für die Einfügung einer Markierung in ein Signal schematisch dargestellt, das einen zu schützenden Inhalt darstellt. Dieses Signal kann insbesondere ein digitales Video- oder Audiosignal oder irgendein anderes Signal sein, das Standbilder wie eine Fotographie oder ein Computer-berechnetes synthetisches Bild darstellt, oder allgemeiner ein einen Multimediainhalt darstellendes Signal.

[0027] Zunächst wird der zu schützende Inhalt durch eine Umsetzung Modulo **10** in eine Folge von digitalen Daten $x = \{x_n\}$ umgesetzt, wobei n zwischen 1 und N liegt. Wenn zum Beispiel der zu schützende Inhalt ein Bild mit n Pixeln ist, können die Koeffizienten x_n der Luminanz jedes Pixels des Bildes entsprechen. Diese können auch Koeffizienten einer diskreten Fourier-Transformation sein, die den Inhalt des zu schützenden Signals darstellen, oder andere Koeffizienten einer Fourier-Mellin-Transformation oder Koeffizienten einer Wellenform-Zerlegung sein, wenn der zu schützende Inhalt ein Standbild ist.

[0028] Die Datenfolge x, die den zu schützenden Inhalt darstellt, wird einerseits zu einem Modul HPM **12** übertragen, das eine Modulationsfolge $m = \{m_n\}$, $\forall n \in [1..N]$ ausgibt. Das Modul HPM berechnet diese Modulationsfolge als eine Funktion von Algorithmen aufgrund der menschlichen Wahrnehmungsmodelle wie das Modell von Sarnoff des Auges. Die Folge $m = \{m_n\}$ stellt den maximalen Rauschbetrag dar, der zu jedem Koeffizienten x_n ohne wahrnehmbaren Qualitätsverlust addiert werden kann.

[0029] Gemäß einem Aspekt der Erfindung wird die Datenfolge x außerdem zu einem Verschachteler **20** übertragen, der eine Zufallspermutation p der Koeffizienten x_n durchführt und so eine Folge von verschachtelten Koeffizienten $\tilde{x} = \{x_{p(n)}\}$ liefert. Der Zweck dieser Verschachtelung der Datenfolge x wird im Folgenden erläutert.

[0030] Die Modulationsfolge m wird außerdem zu einem Verschachteler **14** übertragen, der dieselbe Permutation p der Koeffizienten m_n durchführt wie diejenige durch den Verschachteler **20**, um so eine verschachtelte Modulationsfolge $\tilde{m} = \{m_{p(n)}\}$ auszugeben.

[0031] Um die Markierung zu bilden, die in die Datenfolge x, die den zu schützenden Inhalt darstellt, eingefügt wird, liefert ein (nicht dargestellter) Pseudozufalls-Rauschgenerator zunächst eine Pseudo-Rauschfolge $v = \{v_n\}$, $\forall n \in [1..N]$ mit einer Gaußverteilung. Diese Pseudorauschfolge v wird dem Eingang eines Filters 16 vom Typ der so genannten Linear Time Invarianz (LTI) zugeführt, dessen Impulsantwort ist: $h = \{h_n\}$, $\forall n \in [1..L]$, wobei L eine ganze Zahl entsprechend der Länge des Filters ist, und dessen Spektralantwort H(f) ist, wobei H(f) die Fourier-Transformation von h ist.

[0032] Am Ausgang des Filters **16** erhält man eine gefilterte Pseudozufallsfolge $w = \{w_n\}$, $\forall n \in [1..N]$, die die folgende Gleichung (1) erfüllt:

$$w_n = \sum_{k=1}^{L} v_{n-k} * h_k = h_n \otimes v_n \quad \forall n \in [1..N] \qquad (1)$$

[0033] Darin stellt $\otimes$ das Konvulotionsprodukt dar. Aus diesem können nach dem Interferenz-Theorem die folgenden zwei Gleichungen (2) und (3) abgeleitet werden:

$$\varphi_{ww}(\tau) = (h \otimes h) \otimes \varphi_{vv}(\tau) \qquad (2)$$

[0034] Darin bezeichnen $\varphi_{ww}(\tau)$ und $\varphi_{vv}(\tau)$ die Autokorrelations-Funktionen von w beziehungsweise von v, und

$$\Phi_{ww}(f) = |H(f)|^2 \cdot \Phi_{vv}(f) \qquad (3)$$

[0035] Darin bezeichnen $\Phi_{ww}(f)$ und $\Phi_{vv}(f)$ die Leistungsspektraldichten von $\varphi_{ww}(\tau)$ beziehungsweise $\varphi_{vv}(\tau)$, das heißt ihre Fourier-Transformationen.

[0036] Da v eine Pseudozufalls-Rauschfolge mit Gauß-Verteilung ist, hat ihr Spektrum, das heißt die Funktion $\varphi_{vv}(f)$, einen im Wesentlichen flachen Verlauf. Wenn andererseits diese Folge v durch das Filter **16** gefiltert wird, enthält die resultierende Folge w ein Spektrum $\Phi_{ww}(f)$, das auf Grund des Ausdrucks $|H(f)|^2$ nicht mehr flach ist. Es ist auch wichtig, zu bemerken, um den Rest der Erfindung zu verstehen, dass die Kenntnis von $|H(f)|^2$ (und durch dasselbe Zeichen, Kenntnis des Moduls von H(f): $|H(f)|^2$ es nicht möglich macht, H(f) (und somit h) zurückzugewinnen, da es eine Unsicherheit bezüglich der Phase von H(f) gibt.

[0037] Wieder zu Fig. 2: Die gefilterte Pseudozufallsfolge w wird mit der verschachtelten Modulationsfolge $\tilde{m}$ multipliziert (Multiplizierer **18**), und die resultierende Folge, die die Markierung darstellt, wird zu der Folge der verschachtelten Daten $\tilde{x}$ addiert (Addierstufe **22**).

[0038] Die Ausgangsfolge von der Addierstufe **22** wird mit $\tilde{y} = \{y_{p(n)}\}$ bezeichnet und erfüllt die folgenden Gleichungen (4) und (5):

$$y_{p(n)} = x_{p(n)} + m_{p(n)} \cdot (h_n \otimes v_n) \quad (4)$$

$$\tilde{y} = \tilde{x} + \tilde{m} \cdot (h \otimes v) \quad (5)$$

[0039] Die Leistungsspektraldichte der Folge von mit Markierungen versehenen verschachtelten Daten $\tilde{y}$ ist durch die folgenden Gleichungen (6) und (7) gegeben:

$$\phi_{\overline{yy}}(f) = \left(\mu_x^2 * \delta(f) + \sigma_x^2\right) + \left(\sigma_m^2 * \sigma_v^2 * \sum_w h_w^2\right) + \mu_m^2 * \sigma_v^2 * |H(f)|^2 \quad (7)$$

$$\phi_{\overline{yy}}(f) = \phi_{\overline{ii}}(f) + \phi_{\overline{imm}}(f) * \phi_{h \otimes v}(f) \quad (6)$$

[0040] In der Gleichung (7) bezeichnen μ_j und σ_j die mittlere beziehungsweise die übliche Abweichung der Folge $j = \{j_n\}$ mit $j \in \{x,m,v\}$, $\delta(f)$ entspricht dem Dirac-Impuls, und der Ausdruck

$$\left(\sigma_m^2 * \sigma_v^2 * \sum_w h_w^2\right)$$

ist gleich einer Konstanten.

[0041] Die Folge der mit Markierungen versehenen verschachtelten Daten $\tilde{y}$ wird dann zu einem inversen Verschachteler **24** übertragen, der den Vorgang durchführt, der invers ist zu der Permutation p durch die Verschachteler **20** und **14**, um so eine Folge von mit Markierungen versehenen Daten $y = \{y_n\}$ zu liefern, deren Koeffizienten derselben Ordnung sind wie die anfängliche Ordnung der Daten $x = \{x_n\}$.

[0042] Eine Transformation, die invers ist zu der, die durch das Tranformationsmodul **10** erfolgt, erfolgt dann durch das Modul **26**, um so den markierten Inhalt (oder den mit Markierungen versehenen Inhalt) zu bilden, der dann gegen eine verbotene Kopierung geschützt ist, ohne dass die Markierung in dem Inhalt wahrnehmbar ist.

[0043] Im Folgenden wird anhand der Fig. 3 ein Gerät zur Ermittlung einer Markierung in einem empfangenen Inhalt beschrieben, wenn diese Markierung durch ein Gerät, wie dem Gerät von Fig. 2, in einen zu schützenden Inhalt eingefügt wurde.

[0044] Das Prinzip der Ermittlung oder Detektion basiert auf der Spektralanalyse des empfangenen Signals.

[0045] Das empfangene Signal stellt den empfangenen Inhalt dar, für den man zu ermitteln versucht, ob er mit einer Markierung versehen ist oder nicht. Dieser Inhalt ist von demselben Typ wie der vorangehend beschriebene zu schützende Inhalt. In dem folgenden Beispiel wird angenommen, dass der empfangene Inhalt ein Bild mit N Pixeln ist.

[0046] Der empfangene Inhalt wird zunächst zu einem Transformationsmodul **30** übertragen, das denselben Transformationsvorgang durchführt wie das Modul **10** des Gerätes von Fig. 2 für eine Markierungseinfügung, und so eine Datenfolge $r = \{r_n\}$, $\forall n \in [1..N]$ liefert, die den empfangenen Inhalt darstellt. In unserem Beispiel wird angenommen, dass die Luminanz r_n der Pixel des empfangenen Bildes als Ausgang von dem Transformationsmodul **30** gewonnen wird.

[0047] Wenn der empfangene Inhalt genau dem Markierungsinhalt entsprechen würde, der von dem Gerät von Fig. 2 ausgeht, das heißt wenn keine Transformation oder Verzerrung während der Übertragung zwischen den Gerät zur Einfügung einer Markierung und dem Ermittlungsgerät stattgefunden hat, dann hätte man:

$r = \{r_n\} = Y = \{y_n\}$

[0048] In der Praxis ist dies nicht immer der Fall, da das Signal manchmal Transformationen während seiner Übertragung unterliegt.

[0049] Wenn die Markierung in dem Gerät von Fig. 2 in eine Folge von verschachtelten Daten $\tilde{x}$ eingefügt worden ist, dann wird, um die mögliche Anwesenheit einer Markierung in dem empfangenen Inhalt zu ermitteln, die Datenfolge r zu einem Verschachteler **32** übertragen, der dieselbe Permutation p der Koeffizienten r_n durchführt wie diejenige, die durch die Verschachteler **20** und **14** der Fig. 2 erfolgt.

[0050] Eine Folge von verschachtelten Daten $\tilde{r} = \{r_{p(n)}\}$ wird als Ausgang von dem Verschachteler **32** gewonnen.

[0051] Es wurde vorangehend ersichtlich, dass dann, wenn die Markierung in eine Pseudorauschfolge eingefügt wurde, die durch ein Filter mit der Impulsantwort h und mit der Spektralantwort H(f) gefiltert wurde, die Leistungsspektraldichte der (verschachtelten) Daten oder der gewonnen Daten $\tilde{y}$ durch die Gleichungen (6) und (7) ausgedrückt wird.

[0052] Der Zweck der Verschachtelung der Datenfolge x und der Modulationsfolge n wird nunmehr ersichtlich. Wenn die Datenfolge x die Pixel eines Bildes darstellt, hat ihre Spektraldichte eine sehr strukturierte Form mit sehr großen Amplitudendifferenzen. Die Rolle der Verschachtelung der Daten besteht darin, die statistische Kohärenz dieser Datenfolge zu beseitigen, so dass die Spektraldichte der Folge der verschachtelten Daten $\tilde{x}$ einen im Wesentlichen flachen Verlauf hat, wie derjenige einer Pseudorauschfolge mit einer Gauß-Verteilung.

[0053] Wenn somit eine Markierung aus einer Pseudorauschfolge, gefiltert durch ein Filter mit einer Spektralantwort H(f), zu dieser verschachtelten Folge addiert wird, ergibt sich eine Datenfolge, deren Leistungsspektraldichte durch die Gleichung (7) ausgedrückt werden kann, in der der wichtige Ausdruck $|H(f)|^2$ ermittelt oder detektiert werden kann.

[0054] Das Prinzip der Detektion basiert daher auf der Spektralanalyse der Folge $\tilde{r}$ und einem so genannten "Maximum Likelihood Ratio Hypothesis Test" (Hypothese des Verhältnisses mit der Maximum-Likelihood-Schätzung (MLR-Hypothese-Test), wobei die getestete Hypothese folgendermaßen ist: Wenn die Folge der verschachtelten Daten $\tilde{r}$ Rauschen enthält, ist es ein Rauschen, dass durch ein Filter gefiltert wurde, dessen Spektralantwort einen Modulo ähnlich zu |H(f)| hat. Wenn die Antwort JA ist, wird daraus abgeleitet, dass das in der Folge $\tilde{r}$ vorhandene Rauschen eine Markierung ist, und im entgegengesetzten Fall wird man darauf schließen, das der empfangene Inhalt nicht mit einer Markierung versehen ist.

[0055] In der Praxis beruht diese Analyse auf Berechnungen für die Spektralanalyse und die Wahrscheinlichkeit der Prüfung von Hypothesen, die im Detail beschrieben sind in dem Artikel von K. Dzhaparidze, "Parameter Estimation and Hypothesis Testing in Spectral Analysis of Stationary Time Series", Springer Series in Statistics, Springer-Verlag, 1986, worauf für weitere Details verwiesen wird.

[0056] In Fig. 3 wird die Folge der empfangenen verschachtelten Daten $\tilde{r}$ zu einem Modul **34** übertragen, das eine Periodogram-Berechnung durchführt. Diese Berechnung hat den Zweck der Schätzung der Leistungsspektraldichte der Folge $\tilde{r}$, eine Menge $I_N(f)$, die durch die folgende Gleichung (8) gegeben ist,

$$I_N(f) = \frac{1}{N}\left|\sum_{k=1}^{N} \tilde{r}_k * \exp(2\pi j f k)\right|^2 \qquad (8)$$

wird am Ausgang gewonnen.

[0057] Diese Menge wird dann zu einem Modul **36** übertragen, das einen MLR-Hypothese-Test durchführt, um so zu ermitteln, ob der empfangene Inhalt mit einer Markierung versehen ist (Ausgangsantwort "Y") oder nicht (Ausgangsantwort "N").

[0058] Das Modul **36** prüft die Wahrscheinlichkeit von zwei Hypothesen:

– Gemäß der ersten Hypothese G_0 ist der empfangene Inhalt nicht mit einer Markierung versehen, somit ist die Spektraldichte der Folge $\tilde{r}$ im Wesentlichen flach und kann durch die folgende Gleichung (9) geschätzt werden:

$$g_0(f) = \sigma_r^2 + \mu_r^2 \cdot \delta(f) \qquad (9)$$

– Gemäß der zweiten Hypothese G_1 ist der empfangene Inhalt mit einer Markierung versehen, und die Spektraldichte der Folge $\tilde{r}$ kann durch die folgende Gleichung (10) geschätzt werden:

$$g_1(f) = \mu_m^2 \cdot \sigma_v^2 \cdot |H(f)|^2 + C \qquad (10)$$

[0059] Darin ist C eine Konstante, und σ_v ist gleich 1 (man wählt vorzugsweise die Pseudorauschfolge v bei dem Wert des Einfügegeräts, so dass σ_v gleich 1 ist, jedoch kann man ebenso andere Werte wählen). Außerdem ist μ_m bei dem Wert des Einfügegeräts genormt und ist zum Beispiel gleich 3.

[0060] Zur Schätzung der Wahrscheinlichkeit der Hypothesen G_0 und G_1 berechnet das Modul **36** zwei Zahlen $U_{N,0}(\tilde{r})$ und $U_{N,1}(\tilde{r})$ bezeichnet die Wahrscheinlichkeiten der Hypothesen G_0 und G_1 gemäß der folgenden Gleichung (11):

$$U_{Nj}(\tilde{r}) = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\log\, g_i(f) + \frac{I_n(f)}{g_i(f)} \right) df \quad \text{mit} \quad i \in \{0,1\} \qquad (11)$$

[0061] Wenn dann diese beiden Zahlen verglichen werden, folgert das Modul **36** daraus:
– wenn $U_{N,1}(\tilde{r}) > U_{N,0}(\tilde{r})$ ist, dann ist die Antwort des Detektors "Y" und zeigt an, dass der empfangene Inhalt mit einer Markierung versehen ist, und
– wenn $U_{N,1}(\tilde{r}) < U_{N,0}(\tilde{r})$ ist, dann ist die Antwort des Detektors "N" und zeigt an, dass der empfangene Inhalt nicht markiert ist.

[0062] Es ist auch in einer bevorzugten Weise möglich, die Differenz $U_{N,1}(\tilde{r}) – U_{N,0}(\tilde{r})$ zu berechnen und die obigen Vergleiche nur dann durchzuführen, wenn diese Differenz größer ist als ein vorbestimmter Schwellwert. Das erfolgt, um eine bessere Genauigkeit der Ermittlung oder Detektion zu garantieren.

[0063] Die oben an Hand der Fig. 2 und Fig. 3 beschriebenen Verfahren zur Einfügung und Ermittlung der Markierung machen es möglich, ein neues Markiersystem zu erzeugen, das in Fig. 4 dargestellt ist. In diesem neuen System und gemäß einem bevorzugten Aspekt der Erfindung dient ein Parameter, der als der "Private Schlüssel" (private key) K_{PRI} bezeichnet wird, für die Einfügung (**100**) einer Markierung W in einen Inhalt C, während ein anderer Parameter, der als der "Öffentliche Schlüssel" (public key) K_{PUB} bezeichnet wird für die Ermittlung (**200**) einer Markierung in einem empfangenen Inhalt CT dient. Die Ausdrücke "Privater Schlüssel" und "Öffentlicher Schlüssel" werden analog bei öffentlichen Schlüssel-Verschlüsselungssystemen benutzt. Es sei bemerkt, dass die Markierung W hier binär ist, das bedeutet, das entweder der Inhalt C markiert ist oder nicht. W enthält jedoch kein Datenwort für sich selbst.

[0064] In der oben beschriebenen Ausführungsform wird der private Schlüssel K_{PRI} durch die Pseudozufalls-Rauschfolge v gebildet, ebenso durch die Impulsantwort h des Filters **16** (Fig. 2). Die Folgen $v = \{v_n\}$ und $h = \{h_n\}$ sind unbedingt notwendig oder unverzichtbar für die Berechnung der Folge $w = \{w_n\}$, die selbst, nachdem sie mit der verschachtelten Modulationsfolge $\tilde{m}$ multipliziert worden ist, in die Daten eingefügt wird, die den zu schützenden Inhalt darstellen.

[0065] Der öffentliche Schlüssel, der zur Ermittlung der Markierung in dem empfangenen Inhalt dient, wird seinerseits durch den Modulus der Spektralfolge des Filters **16** |H(f)| geformt. Tatsächlich wird in den durchgeführten Spektralanalyseberechnungen (Module **34** und **36** von Fig. 3) zur Ermittlung der Anwesenheit einer Markierung in einem empfangenen Inhalt CT nur die Kenntnis von |H(f)| benötigt. Insbesondere ist es nicht notwendig, v und h (der private Schlüssel) zu kennen, um die Ermittlung der Markierung durchzuführen. In der Praxis genügt, wie früher in der Beschreibung ersichtlich wurde, die Kenntnis von |H(f)| nicht dafür, H(f) und somit h zu kennen.

[0066] Es wird daher ein System geschaffen, in dem die Kenntnis des privaten Schlüssels es nicht ermöglicht, den privaten Schlüssel daraus zu folgern. Ebenso ist es, wenn man den privaten Schlüssel nicht kennt, für das Gerät unmöglich die Detektion der Markierung durchzuführen, um diese zu beseitigen oder zu ändern. Die Ermittlung kann daher in einer nicht-sicheren Umgebung erfolgen, ohne die Gefahr, dass die Markierung gelöscht wird.

Patentansprüche

1. Verfahren zum Einfügen einer Markierung in Daten (x), die einen zu schützenden Inhalt darstellen, mit folgenden Schritten:

a) Erzeugung einer Modulationsfolge (m) aus den Daten (x), die den Maximalbetrag an Rauschen darstellen, der den Daten hinzugefügt werden kann,
b) Zuführung einer Pseudozufalls-Rauschfolge (v) zu dem Eingang eines Filters mit einer vorbestimmten Impulsantwort (h),
c) Multiplikation der gefilterten Pseudozufalls-Rauschfolge (w) mit der Modulationsfolge und
d) Hinzufügung der gefilterten Pseudozufalls-Rauschfolge (w), multipliziert mit der Modulationsfolge, zu den Daten.

2. Verfahren nach Anspruch 1 mit folgenden Schritten:
e) Durchführung einer Pseudozufalls-Verschachtelung (p) der Modulationsfolge (m) vor dem Schritt (c),
f) Durchführung derselben Pseudozufalls-Verschachtelung (p) der Daten (x) vor dem Schritt (d) und
g) Durchführung einer inversen Verschachtelung nach dem Schritt d), um so die markierten Daten zu bilden.

3. Verfahren zur Ermittlung einer Markierung in Daten (r), die einen empfangenen Inhalt darstellen, gekennzeichnet durch folgenden Schritte:
i) Durchführung einer Spektralanalyse der Daten
ii) Schätzung daraus, ob die Daten eine Pseudozufalls-Rauschfolge enthalten, die durch ein Filter mit einer vorbestimmten Spektralantwort (H(f)) gefiltert worden sind, und
iii) Folgerung der Anwesenheit der Markierung aus der Schätzung.

4. Verfahren nach Anspruch 3 zur Ermittlung einer Markierung in Daten (r), die einen empfangenen Inhalt darstellen, wobei die Markierung gemäß dem Verfahren nach Anspruch 2 eingefügt wird, gekennzeichnet durch folgende Schritte:
iii) Durchführung einer Pseudozufalls-Verschachtelung (p) der empfangenen Daten (r) vor dem Schritt i), die zu der im Schritt f) durchgeführten Verschachtelung identisch sind.

5. Gerät zur Einfügung einer Markierung in Daten (x), die einen zu schützenden Inhalt darstellen, mit:
– Mitteln zur Erzeugung einer Pseudozufalls-Rauschfolge (v),
– Mitteln (**12**) zur Erzeugung einer Modulationsfolge (m) aus den Daten (x), die den maximalen Betrag an Rauschen anzeigt, der den Daten hinzugefügt werden kann,
gekennzeichnet durch:
– Filtermittel (**16**) mit einer vorbestimmten Impulsantwort (h) zum Empfang der Pseudozufalls-Rauschfolge (v) und zur Lieferung einer gefilterten Pseudozufalls-Rauschfolge (w),
– Multipliziermittel (**18**) zur Multiplikation der gefilterten Pseudozufalls-Rauschfolge (w) mit der Modulationsfolge (m) und
– Mittel (**22**) zur Zufügung der gefilterten Pseudozufalls-Rauschfolge (w), multipliziert mit der Modulationsfolge (m) zu den Daten (x).

6. Gerät nach Anspruch 5, gekennzeichnet durch:
– erste Mittel (**20**) einer Pseudozufalls-Verschachtelung der Daten (x), die den zu schützenden Inhalt darstellen, zur Zuführung verschachtelter Daten ($\tilde{x}$),
– zweite Mittel (**14**) einer Pseudozufalls-Verschachtelung, die identisch sind zu den ersten Mitteln (**20**) zum Empfang der Modulationsfolge (m), um so eine verschachtelte Modulationsfolge ($\tilde{m}$) zu liefern, dass die verschachtelte Modulationsfolge den Multiplikationsmitteln (**18**) zugeführt wird zur Multiplikation mit der gefilterten Pseudozufalls-Rauschfolge (w),
wobei die verschachtelten Daten ($\tilde{x}$) den Hinzufügungsmitteln (**22**) zugeführt werden, um so der gefilterten Pseudozufalls-Rauschfolge (w) hinzugefügt zu werden, multipliziert mit der verschachtelten Modulationsfolge ($\tilde{m}$), und
– Mittel (**24**) zur inversen Verschachtelung der ersten Verschachtelungsmittel (**20**), verbunden mit dem Ausgang der Addiermittel (**22**), um so die markierten Daten zu bilden.

7. Gerät nach Anspruch 6 mit:
– Mitteln (**10**) zur Umsetzung des zu schützenden Inhalts in die den Inhalt darstellende Daten (x) und
– Mitteln (**26**) zur inversen Umsetzung der markierten Daten in einen markierten Inhalt.

8. Gerät zur Ermittlung einer Markierung in einen empfangenen Inhalt darstellenden Daten (r), gekennzeichnet durch:
– Mittel (**34**) zur Bildung der Leistungspektraldichte der Daten:
– Wahrscheinlichkeitsmittel (**36**) für die Testung von Hypothesen, um so zu schätzen, ob die Daten eine Pseudozufalls-Rauschfolge enthalten, die durch ein Filter mit einer vorbestimmten Spektralantwort (H(f)) gefiltert

worden sind, und
– Mittel zur Ableitung der Anwesenheit der Markierung aus dieser Schätzung.

9. Gerät nach Anspruch 8 zur Ermittlung einer Markierung, die durch ein Einfügegerät gemäß einem der Ansprüche 6 oder 7 eingefügt wurde, gekennzeichnet durch:
– Mittel (**32**) zur Pseudozufalls-Verschachtelung der den empfangenen Inhalt darstellenden Daten (r) zur Durchführung derselben Verschachtelung (p) wie die ersten Verschachtelungsmittel (**20**) des Einfügegeräts, wobei die verschachtelten Daten ($\tilde{r}$) den Mitteln (**34**) zur Bildung der Leistungsspektraldichte zugeführt werden.

10. Gerät nach Anspruch 9 zur Ermittlung einer Markierung, die durch ein Einfügegerät nach Anspruch 7 eingefügt wurde, gekennzeichnet durch:
– Mittel (**30**) zur Umsetzung des empfangenen Inhalts in den Inhalt darstellende Daten (r), wobei die Umsetzmittel für die Durchführung derselben Umsetzung wie die Umsetzmittel (**10**) des Einfügegeräts sind.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

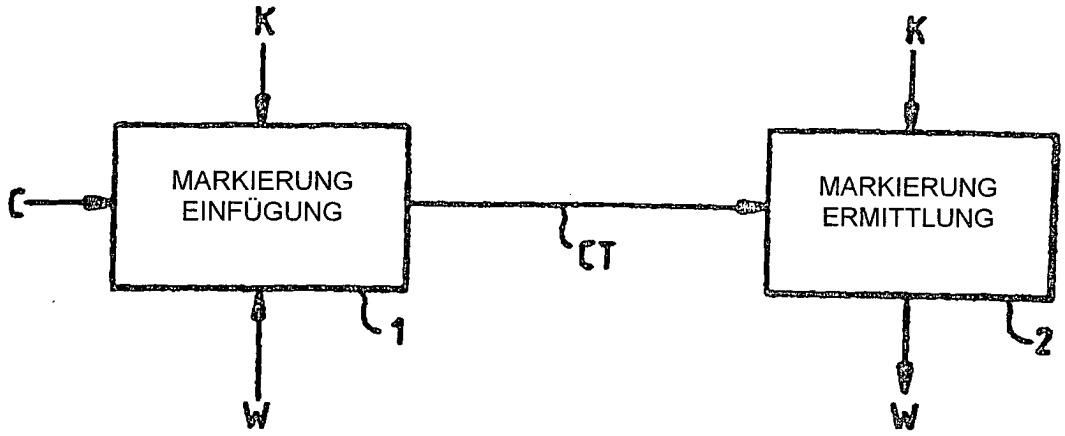

FIG.1

STAND DER TECHNIK

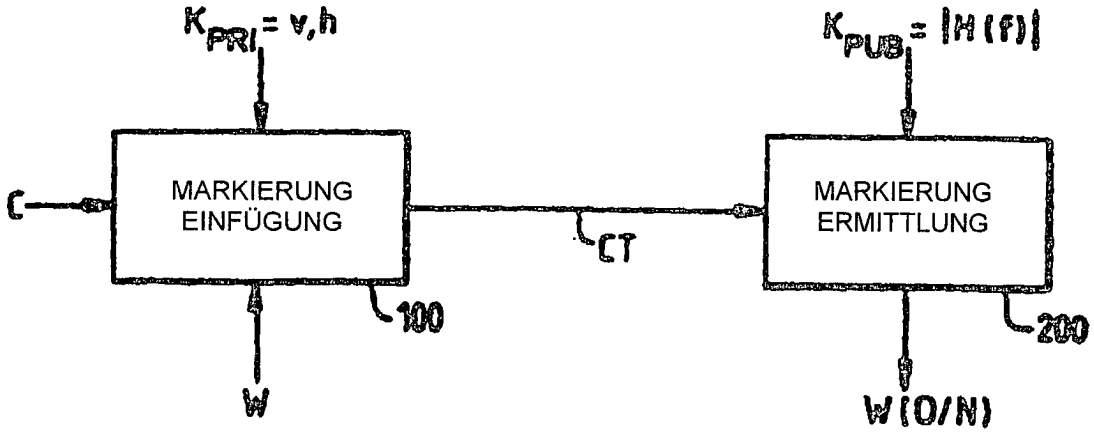

FIG.4

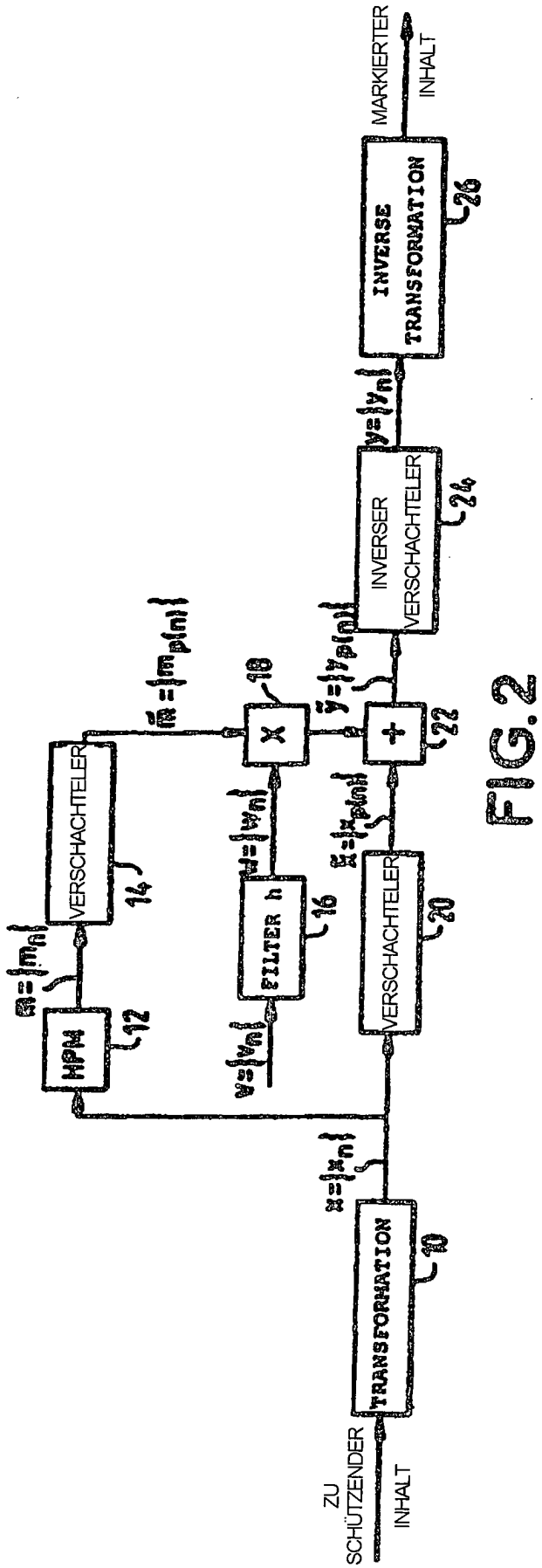
ZU SCHÜTZENDER INHALT
TRANSFORMATION
10
VERSCHACHTELER
20
+
22
INVERSER VERSCHACHTELER
24
INVERSE TRANSFORMATION
26
MARKIERTER INHALT
HPM
12
VERSCHACHTELER
14
FILTER h
16
X
18

FIG. 2

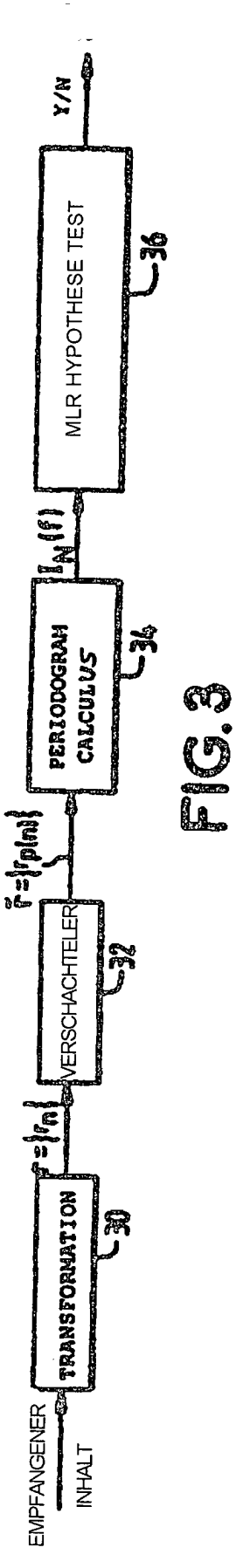
EMPFANGENER INHALT
TRANSFORMATION
30
VERSCHACHTELER
32
PERIODOGRAM CALCULUS
34
MLR HYPOTHESE TEST
36
Y/N

FIG. 3