



(11) **EP 2 385 521 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:  
**09.11.2011 Patentblatt 2011/45**

(51) Int Cl.:  
**G10L 19/00** <sup>(2006.01)</sup> **G10L 19/12** <sup>(2006.01)</sup>  
**H04K 1/00** <sup>(2006.01)</sup>

(21) Anmeldenummer: **11006299.9**

(22) Anmeldetag: **29.08.2007**

(84) Benannte Vertragsstaaten:  
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR**

(30) Priorität: **15.09.2006 DE 102006044181**  
**16.02.2007 DE 102007007627**

(62) Dokumentnummer(n) der früheren Anmeldung(en) nach Art. 76 EPÜ:  
**07801969.2 / 2 062 254**

(71) Anmelder: **RWTH Aachen**  
**52062 Aachen (DE)**

(72) Erfinder:  
• **Geiser, Bernd**  
**52072 Aachen (DE)**  
• **Vary, Peter**  
**52074 Aachen (DE)**

(74) Vertreter: **Röthinger, Rainer**  
**Wuesthoff & Wuesthoff**  
**Patent- und Rechtsanwälte**  
**Schweigerstrasse 2**  
**81541 München (DE)**

Bemerkungen:

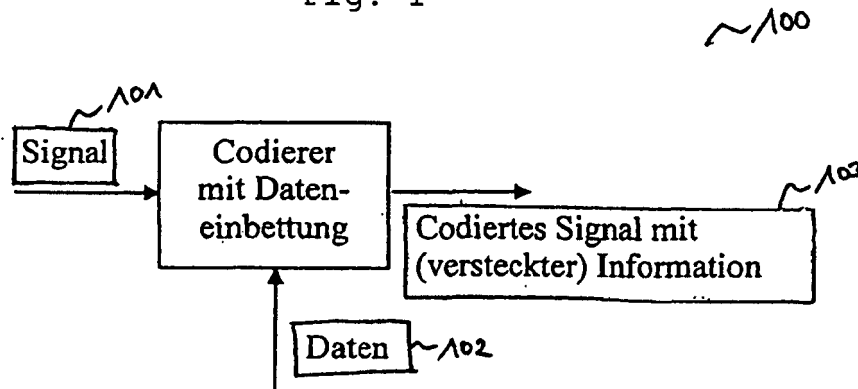
Diese Anmeldung ist am 29-07-2011 als  
Teilanmeldung zu der unter INID-Code 62 erwähnten  
Anmeldung eingereicht worden.

(54) **Steganographie in digitalen Signal-Codierern**

(57) Bei einem Verfahren zur Einbettung einer steganographischen Information in eine Signalinformation eines Signalcodierers soll eine Lösung geschaffen werden, die es ermöglicht, eine steganographische Information in eine Signalinformation eines Signalcodierers derart einzubetten, dass eine Reduktion der Sprachqualität weitestgehend vermieden wird. Die wird erreicht durch Bereitstellen einer Dateninformation, insbesondere einer Sprachinformation, Auswählen einer steganographischen Information aus einer Menge von steganographischen Informationen, Erzeugen eines Codewortes aus

einem bereitgestellten Codebuch mittels des Signal-Codierers auf Basis von das Codewort bildenden Codeelementen, derart, dass unter Verwendung des erzeugten Codeworts im Rahmen eines mit dem Codebuch assoziierbaren Übertragungsstandards die Dateninformation in eine das Codewort beinhaltende und/oder auf das Codewort verweisende Signalinformation codiert wird; und, dass das erzeugte Codewort eine zusätzliche, auf Basis der das Codewort bildenden Codeelemente berechenbare Eigenschaft aufweist, wobei die zusätzliche Eigenschaft die steganographische Information darstellt.

Fig. 1



EP 2 385 521 A1

## Beschreibung

**[0001]** Die Erfindung richtet sich auf ein Verfahren zur Einbettung einer steganographischen Information in eine Signalinformation eines Signal-Codierers.

**[0002]** Neben den analogen Ton-, Bild- und Videoübertragungen gewinnt die digitale Übertragung immer mehr Gewicht. Dies liegt unter anderem auch daran, dass digitale Signalinformationen einfacher bearbeitet, d.h. kopiert oder auch komprimiert werden können. So führt insbesondere die Komprimierung von digitalen Signalinformationen dazu, dass mittels Signalübertragungskanälen mit begrenzten Datenübertragungsraten mit hoher Informationsdichte Informationen übertragen werden können.

**[0003]** Neben der Komprimierung von Signalinformationen als eine Art der Bearbeitung hat sich in jüngster Zeit auch das Einbetten von "unsichtbaren" - steganographischen - Informationen in Signalinformationen durchgesetzt. Eine solche Einbettung von Zusatzinformationen ermöglicht beispielsweise eine Kennzeichnung von Urheberrechten - wenn es sich bei der Signalinformation beispielsweise um ein Musikstück handelt - oder allgemein gesprochen um eine allgemeine Herkunftsangabe, also ein "digitales Wasserzeichen".

**[0004]** Auch wenn sich eine derartige Einbettung von steganographischen Informationen in Musik- und/oder Videosignalen bereits weitgehend durchgesetzt hat, so ist eine Einbettung von steganographischen Informationen in eine codierte Signalinformation, insbesondere wenn sie in "Echtzeit" zu übertragen ist, weiterhin mit Schwierigkeiten verbunden. Dies ist in der Tatsache begründet, dass gewisse Codierungen keine Redundanz und damit keinen Raum für steganographische Informationen bieten, oder dass die steganographische Information beim Decodieren der codierten Signalinformation verloren geht.

**[0005]** Eine derartige Ausgangssituation, bei der Signalinformationen, im gegebenen Fall vornehmlich Sprachinformationen, über einen Kanal gesendet und empfangen werden, und in Echtzeit codiert und decodiert werden, und bei der nicht unbeschränkt Übertragungsressourcen zur Verfügung stehen, findet man beispielsweise in der Mobilfunktelefonie. Hier erlaubt das GSM-Netz bestenfalls eine Übertragungsrate von maximal 13,0 kbit/s. Eine uncodierte Sprachinformation, d.h. hier eine nicht komprimierte Sprachinformation, wäre aufgrund der sehr geringen Übertragungsrate auf Empfängerseite kaum mehr zu verstehen. Um trotzdem verständliche Sprachinformationen beispielsweise von einem Mobilfunkgerät auf ein anderes zu übertragen, haben sich die sogenannten Sprach-Codecs als ein probates Mittel zur komprimierten Sprachsignalübertragung herauskristallisiert. Sollen zusätzliche Informationen, d.h. steganographische Informationen, in eine solche Signalinformation eingebettet werden, so sind die sich aus der Codierung ergebenden Besonderheiten zu berücksichtigen.

**[0006]** Im Bereich der mobilen Telekommunikation werden beispielsweise in GSM (Global System for Mobile Communications) - Mobilfunknetzwerken oder UMTS (Universal Mobile Telecommunications Standard) - Mobilfunknetzwerken die zu übertragenden Sprachinformationen mittels des bekannten CELP (Code-book Excited Linear Predictive Coding) bzw. ACELP (Algebraic Code Excited Linear Prediction) oder zukünftig der AMR (Adaptive Multi-Rate) - Codierung codiert. Diese Sprachcodierungen basieren allesamt auf einem Modell der Spracherzeugung, bei dem in einer ersten Näherung die Bildung des Sprachsignals in einer Anregungsstufe und einer Filterungsstufe erzeugt wird. Ein Signalcodierer, wie beispielsweise ein CELP-Codierer, ein ACELP-Codierer oder ein AMR-Codierer, erzeugt einen Codebucheintrag, in der Regel einen Vektor aus einem sogenannten Codebuch, wobei die Codeelemente des Codebucheintrages - also in der Regel die Vektorkomponenten - Informationen bezüglich der (Filter-)Anregung enthalten. Filterkoeffizienten, Verstärkungsfaktoren etc. werden als Zeitinformation mittels dedizierter Codebücher codiert.

**[0007]** Ein Codebuch zur Anregungscodierung besteht in der Regel aus einer Menge von Vektoren, beispielsweise mit jeweils 10 Komponenten bei der ACELP-Codierung nach den Enhanced Full Rate (EFR) Standard, die die zu übermittelnde Sprachinformation für eine bestimmte Länge, beispielsweise 5 Millisekunden, codieren. Aus dem fest vorgegebenen Codebuch, welches insgesamt eine große Vielzahl von Vektoren umfasst, wobei die Vektoren nach bekannten Kriterien aufgebaut sind, wird in der Regel eine Teilmenge des Codebuches, ein Sub-Codebuch, verwendet, die oftmals ausreichend ist, um die gewöhnlichen Sprachinformationen mit einer guten Qualität übertragen zu können.

**[0008]** Zur Unterscheidung zwischen dem im Rahmen der Codierung vorgegebenen vollständigen Codebuch, wird das in der Praxis verwendete Sub-Codebuch als "praktisches Codebuch" bezeichnet.

**[0009]** Zum schnellen Auffinden eines geeigneten Codebucheintrages wird das praktische Codebuch nur heuristisch durchsucht, d.h. es wird keine vollständige Suche nach einem geeigneten Codebucheintrag durchgeführt.

**[0010]** Ein Verfahren, welches die Zerlegung eines festen Codebuches berücksichtigt, wird in dem Artikel "Watermarking Combined with CELP Speech Coding for Authentication" von Zhe-Ming Lu et al. (in IEICE TRANS. INF. & SYST., Vol. E88-D, No. 2 February 2005) offenbart. Dabei wird zunächst ein Codebuch in drei Sub-Codebücher zerlegt, aus denen wiederum zwei Codebücher generiert werden, welche unterschiedliche Eigenschaften aufweisen. Je nachdem, welche steganographische Information übermittelt werden soll, wird nun ein Codebucheintrag aus dem dafür bestimmten Sub-Codebuch ausgewählt und zur Codierung der zu übermittelnden Sprachinformation verwendet. Diese Sprachinformation kann auf Empfängerseite decodiert werden, wobei der eigentliche Decodierer auch gleichzeitig erkennen kann, aus welcher Zerlegung des Codebuches der Codebucheintrag stammt. Um eine hinreichend gute Codierung

aus einem der Sub-Codebücher bereitzustellen, wird in der Veröffentlichung auch das bekannte Analysis-by-Synthesis Verfahren beschrieben. Bei diesem Verfahren wird das ausgewählte Codewort bewertet, d.h. die Güte der Codierung wird überprüft. Dies geschieht im Wesentlichen dadurch, dass, nachdem eine Sprachinformation codiert wurde, die Codierung decodiert, d.h. synthetisiert, wird und das Ergebnis der Decodierung, welches wiederum eine Sprachinformation darstellt, mit der ursprünglichen Sprachinformation verglichen wird. Somit wird vorab auf Senderseite - Codierseite - eine Synthese durchgeführt, die, nach einer etwaigen Übertragung, ebenfalls auf Empfängerseite -Decodierseite - durchgeführt wird. Mit einer solchen Analysis-by-Synthesis Schleife ist es möglich, ein Codewort, d.h. in der Regel einen Vektor aus einem Codebuch, aufzufinden, welches zum einen die gewünschte Eigenschaft, d.h. aus dem entsprechend zerlegten Sub-Codebuch stammend, aufweist und dabei die Sprachinformation mit einer ausreichenden Qualität codiert.

**[0011]** Es zeigt sich jedoch, dass die feste Aufteilung eines praktischen Codebuchs - welches ja ohnehin schon eine Untermenge eines übergeordneten Codebuchs ist - in mehrere Sub-Codebücher die Anzahl der verwendbaren Codeworte pro Sub-Codebuch derart reduziert, dass eine hörbare Reduktion der Sprachqualität nicht ausgeschlossen ist.

**[0012]** Der Erfindung liegt daher die Aufgabe zugrunde, eine Lösung zu schaffen, die es ermöglicht, eine steganographische Information in eine Signalinformation eines Signalcodierers derart einzubetten, dass eine Reduktion der Sprachqualität weitestgehend vermieden wird.

**[0013]** Bei einem Verfahren zur Einbettung einer steganographischen Information in eine Signalinformation eines Signalcodierers wird die Aufgabe erfindungsgemäß gelöst durch Bereitstellen einer Dateninformation, insbesondere einer Sprachinformation, Auswählen einer steganographischen Information aus einer Menge von steganographischen Informationen, Erzeugen eines Codewortes aus einem bereitgestellten Codebuch mittels eines Signalcodierers auf Basis von das Codewort bildenden Codeelementen, derart, dass unter Verwendung des erzeugten Codewortes im Rahmen eines mit dem Codebuch assoziierbaren Übertragungsstandards die Dateninformation in eine das Codewort beinhaltende und/oder auf das Codewort verweisende Signalinformation codiert wird; und, dass das erzeugte Codewort eine zusätzliche, auf Basis der das Codewort bildenden Codeelemente berechenbare Eigenschaft aufweist, wobei die zusätzliche Eigenschaft die steganographische Information darstellt.

**[0014]** Ein solches Verfahren zur Einbettung einer steganographischen Information in eine Signalinformation eines Signalcodierers, bei dem ein Codewort aus einem bereitgestellten Codebuch mittels des Signalcodierers auf Basis von das Codewort bildenden Codeelementen erzeugt wird, ermöglicht es, ein Codewort bereitzustellen, welches zum einen eine berechenbare Eigenschaft aufweist, d.h. eine steganographische Information darstellt, und zum anderen gleichzeitig eine Signalinformation bereitstellt, welche für eine Dateninformation, insbesondere eine Sprachinformation, codiert. Dadurch, dass nicht von vorneherein eine Zerlegung des Codebuches durchgeführt wird, sondern statt dessen ein Codebucheintrag erzeugt wird, und zwar auf Basis der das Codewort bildenden Codeelemente, können Codeworte berücksichtigt werden, die nicht in dem praktischen Codebuch und/oder den Zerlegungen des praktischen Codebuches vorhanden waren. Dies erweitert die Anzahl der Codeelemente auf die zurückgegriffen werden kann erheblich, so dass entweder eine Zerlegung in mehr Sub-Codebüchern im Vergleich zum Stand der Technik oder aber bei einer gleichen Anzahl von Sub-Codebüchern eine verbesserte Sprachqualität im Vergleich zum Stand der Technik bereitgestellt werden kann.

**[0015]** Bevorzugt wird in einer Ausgestaltung der Erfindung eine Bewertung des erzeugten Codewortes im Rahmen eines mit dem bereitgestellten Codebuch assoziierbaren Übertragungsstandards mittels Decodierens des Codewortes und anschließenden Vergleichens der decodierten Dateninformation mit der ursprünglichen Dateninformation durchgeführt.

**[0016]** Dies hat den Vorteil, dass die Qualität des erzeugten Codewortes bezüglich der Codierungs-Decodierungstreue, d.h. dem Verlust der (Sprach-)Qualität aufgrund der Codierung und Decodierung, bewertet werden kann.

**[0017]** Weiterhin bevorzugt wird in Ausgestaltung des erfindungsgemäßen Verfahrens das Erzeugen des Codewortes aus dem bereitgestellten Codebuch mittels des Signalcodierers auf Basis der das Codewort bildenden Codeelemente unter Berücksichtigung der Bewertung durchgeführt.

**[0018]** Die Berücksichtigung der Bewertung bei der Erzeugung des Codewortes aus dem bereitgestellten Codebuch ermöglicht das Erzeugen von Codeworten, welche eine hohe Sprachqualität bezüglich der zu codierenden Information aufweisen.

**[0019]** In einer Ausgestaltung der Erfindung wird die Verwendung eines auf Basis des GSM (Global System for Mobile Communications)- und/oder des UMTS (Universal Mobile Telecommunications Standard)-Übertragungsstandards basierenden Codierers und Codebuches vorgesehen.

**[0020]** Dies hat den Vorteil, dass das Verfahren zur Einbettung einer steganographischen Information auch in Mobilfunknetzen verwendet werden kann.

**[0021]** Zur weiteren Ausgestaltung der Erfindung ist das Erzeugen eines Codewortes auf Basis der CELP-, der ACELP (Algebraic Code Excited Linear Prediction)- und /oder der AMR-Codierung vorgesehen.

**[0022]** Die hohe Verbreitung der CELP oder der ACELP Codierung ermöglicht die Verwendung des erfindungsgemäßen Verfahrens in vielen Bereichen der Technik, insbesondere der mobilen Telekommunikation. Dies gilt zukunftswei-

send analog auch für die AMR-Codierung.

**[0023]** Weiterhin wird in einer Ausgestaltung die Berechnung der Eigenschaft des Codewortes als Ergebnis einer Anwendung mindestens einer Operation auf mindestens eines der das Codewort bildenden Codeelemente durchgeführt.

**[0024]** So ist es möglich, auf Basis der das Codewort bildenden Codeelemente unter Anwendung mindestens einer, vorzugsweise mathematischen, Operation eine Eigenschaft des Codewortes zu bestimmen, welche die steganographische Information darstellt.

**[0025]** Weiterhin wird in Ausgestaltung des erfindungsgemäßen Verfahrens die Bereitstellung des Codewortes derart ausgeführt, dass das Codewort die Eigenschaft implizit erfüllt.

**[0026]** Dies hat den Vorteil, dass ein Codewort derartig erzeugt werden kann, dass es die Eigenschaft, welche die steganographische Information darstellt, bereits während seiner Erzeugung erfüllt.

**[0027]** Weiterhin wird in einer Ausgestaltung des erfindungsgemäßen Verfahrens die Auswahl der steganographischen Information derart durchgeführt, dass die steganographische Information zur Signalverbesserung, insbesondere bei Sprachübertragung, wie eine künstliche Bandbreitenerweiterung und/oder Störreduktion, verwendet wird.

**[0028]** Es wurde festgestellt, dass die zusätzliche übertragbare steganographische Information genutzt werden kann, um beispielsweise eine Eigenschaft der eigentlich zu übertragenden Dateninformation zu beschreiben, so dass die steganographische Information zur Signalverbesserung benutzt werden kann. Das bedeutet, dass - sofern das für die Dateninformation codierende Codewort nach dem erfindungsgemäßen Verfahren erzeugt wird - der marginale Verlust in der Übertragungsqualität durch die steganographische Zusatzinformation nicht nur kompensiert, sondern sogar überkompensiert werden kann.

**[0029]** Weiterhin wird in einer Ausgestaltung die Auswahl der steganographischen Information derart durchgeführt, dass die steganographische Information als digitales Wasserzeichen verwendet wird.

**[0030]** Bei der Verwendung der steganographischen Information als digitales Wasserzeichen können nicht nur die Originalität und die Herkunft von Dateninformationen gekennzeichnet werden, vielmehr können auch Urheberrechte an Dateninformationen mit Hilfe der steganographischen Information in Form eines digitalen Wasserzeichens eingebracht werden. Dabei wird die Dateninformation im Rahmen des erfindungsgemäßen Verfahrens qualitativ kaum beeinträchtigt.

**[0031]** In weiterer Ausgestaltung der Erfindung wird ein Übertragen der das Codewort beinhaltenden oder auf das Codewort verweisenden Signalinformationen an einen Empfänger durchgeführt.

**[0032]** Vorteilhafterweise ist es durch ein Übertragen an einen Empfänger möglich, die Dateninformation und die steganographische Information in Form einer Signalinformation über eine räumliche Distanz zu übertragen.

**[0033]** Weiterhin wird in einer Ausgestaltung des erfindungsgemäßen Verfahrens ein empfangsseitiges Bereitstellen einer Dateninformation mittels Decodierens des Codewortes im Rahmen eines mit dem bereitgestellten Codebuch assoziierbaren Übertragungsstandards durchgeführt.

**[0034]** Durch die Decodierung des Codewortes können die in der Signalinformation beinhalteten Dateninformationen sowie die steganographische Information zurückgewonnen und verwendet werden.

**[0035]** Weiterhin bevorzugt wird in Ausgestaltung des erfindungsgemäßen Verfahrens ein empfangsseitiges Bereitstellen der steganographischen Information mittels Berechnens der zusätzlichen Eigenschaft des Codewortes auf Basis der das Codewort bildenden Codeelemente durchgeführt.

**[0036]** Je nach Ausgestaltung des Empfängers ist es möglich, die steganographische Information, welche sich in der Signalinformation beinhaltet, zu berechnen. Diese Möglichkeit kann optional genutzt werden, d.h. Systeme, welche nicht in der Lage sind, die steganographische Information zurück zu berechnen, werden lediglich die Dateninformation aus der Signalinformation extrahieren, ohne an die steganographische Information zu gelangen.

**[0037]** Schließlich wird in einer Ausgestaltung des Verfahrens weiterhin ein Ausführen des Verfahrens in einer Mobilfunkvorrichtung ausgeführt.

**[0038]** Das Verfahren eignet sich insbesondere für die Signalinformationsübertragung, d.h. Sprach- oder sonstige Information, mittels Mobilfunkvorrichtungen, welche in einem Mobilfunknetz betreibbar sind.

**[0039]** Die vorgenannten sowie beanspruchten und in den Ausführungsbeispielen beschriebenen zu verwendenden Bauteile unterliegen in ihrer Größe, Form, Gestaltung, Materialauswahl und technischen Konzeptionen keinen besonderen Ausnahmebedingungen, so dass die in dem Anwendungsgebiet bekannten Auswahlkriterien uneingeschränkt Anwendung finden können.

**[0040]** Weitere Einzelheiten, Merkmale und Vorteile des Gegenstandes der Erfindung ergeben sich aus den Unteransprüchen sowie aus der nachfolgenden Beschreibung der zugehörigen Zeichnungen, in der - beispielhaft - ein bevorzugtes Ausführungsbeispiel der Erfindung dargestellt ist.

**[0041]** Zu den beschriebenen Codierungsverfahren gemäß Ausführungsbeispielen der Erfindung werden entsprechende Codierer bereitgestellt sowie entsprechende Verfahren zum Dekodieren und entsprechende Dekodierer.

Figur 1 zeigt einen Codierer 100 gemäß einem Ausführungsbeispiel der Erfindung.

Figur 2 zeigt ein Codier/Decodiersystem 200 gemäß einem Ausführungsbeispiel der Erfindung.

Figur 3 zeigt einen Codierer 300 gemäß einem Ausführungsbeispiel der Erfindung.

Figur 4 zeigt einen Codierer 400 gemäß einem Ausführungsbeispiel der Erfindung.

5 Figur 5 zeigt ein Codebuch 500 gemäß einem Ausführungsbeispiel der Erfindung.

**[0042]** Fig.1 zeigt einen Codierer 100 gemäß einem Ausführungsbeispiel der Erfindung.

**[0043]** Dem Codierer 100 wird ein zu codierende Signal 101, beispielsweise ein Sprachsignal 100, zugeführt. Außerdem werden dem Codierer 100 einzubettende Daten 102 zugeführt. Der Codierer erzeugt aus dem zu codierenden  
10 Signal 101 ein codiertes Signal 103, in das die einzubettenden Daten 102 eingebettet sind, das heißt, aus dem ein entsprechender Decodierer die einzubettenden Daten 102 ermitteln kann.

**[0044]** Das codierte Signal 103 wird beispielsweise an einen Empfänger übermittelt, beispielsweise mittels eines Computernetzwerks oder mittels eines Funknetzwerks.

**[0045]** Bei dem im Folgenden beschriebenen Ausführungsbeispiel wird angenommen, dass der Codierer 100 in einem  
15 Mobilfunknetzwerk gemäß GSM (Global System for Mobile Communications) eingesetzt wird. Bei anderen Ausgestaltungen der Erfindung kann der Codierer auch im Rahmen eines Mobilfunknetzwerks gemäß UMTS (Universal Mobile Telecommunications Standard), CDMA2000 (CDMA: Code Division Multiple Access) oder gemäß FOMA (Freedom of Mobile Access) eingesetzt werden.

**[0046]** In dem im Folgenden beschriebenen Ausführungsbeispiel wird angenommen, dass das zu codierende Signal  
20 101 ein Sprachsignal ist, das von dem Codierer 100 gemäß einem ACELP (Algebraic Code Excited Linear Prediction) - Sprachkompressionsverfahren, beispielsweise gemäß einem "Enhanced Full-Rate"-ACELP-Sprachkompressionsverfahren codiert werden soll, wie es in einem GSM-Mobilfunknetz eingesetzt wird.

**[0047]** Der Codierer 100 verwendet zur Informationseinbettung, das heißt zur Einbettung der einzubettenden Daten  
25 102 in das codierte Signal 103 in einer Ausführungsform zur Codierung des sogenannten Restsignals ein festes (anders ausgedrückt stochastisches) Codebuch, welches in N Sub-Codebücher zerlegt wird. Zur eigentlichen Restsignal-Codierung wird je nach einzubettender Information gemäß einem Binning-Schema (binning scheme) das entsprechende Sub-Codebuch herangezogen.

**[0048]** Da das Codebuch bei einem CELP-Sprach-Codierer nicht erschöpfend (sondern lediglich heuristisch) durch-  
30 sucht wird, können die Sub-Codebücher einen zum durchsuchten Teil des festen Codebuches durchaus vergleichbaren Umfang haben und die Qualität der CELP-Codierung leidet nur wenig unter der Informationseinbettung. Ferner kann die die Informationseinbettung mit geringer algorithmischer Komplexität durchgeführt werden.

**[0049]** Bei dem im Folgenden beschriebenen Ausführungsbeispiel verwendet der Codierer 100 ein Codebuch, das wie folgt definiert ist:

**[0050]** Das in diesem Ausführungsbeispiel verwendete Codebuch C ist das Codebuch des GSM EFR (Enhanced Full  
35 Rate) Codecs und ist gegeben durch die Vektoren  $\underline{c}$  der ACELP-Pulspositionen, (in diesem Ausführungsbeispiel ohne Vorzeichen) für jeden Subrahmen der Länge 5ms:

$$C = \{ \underline{c} = (c_0, \dots, c_9) \}$$

40 mit

$$c_0, c_5 \in \{0, 5, 10, 15, 20, 25, 30, 35\}, c_1, c_6 \in \{1, 6, 11, 16, 21, 26, 31, 36\}$$

45  $c_2, c_7 \in \{2, 7, 12, 17, 22, 27, 32, 37\}, c_3, c_8 \in \{3, 8, 13, 18, 23, 28, 33, 38\}$

und

50  $c_4, c_9 \in \{4, 9, 14, 19, 24, 29, 34, 39\}$

**[0051]** Ein Codewort  $\underline{c}$  aus dem Codebuch (d.h. der Menge aller möglichen Codeworte) C ist somit ein Vektor mit  
zehn Komponenten, wobei jede Komponente eine Position eines Pulses innerhalb eines Subrahmens beschreibt. Das  
Codebuch C hat in diesem Ausführungsbeispiel einen Umfang von  $2^{(10 \cdot \log_2(8))} = 2^{30}$  Codewörtern.

**[0052]** In einem anderen Ausführungsbeispiel sind die Komponenten der Vektoren  $\underline{c}$ , wie gemäß EFR vorgesehen,  
55 vorzeichenbehaftet. Die Verwendung von vorzeichenbehafteten Komponenten ermöglicht eine verbesserte Informationseinbettung. In einer Ausführungsform wird bei EFR jedoch aus Komplexitätsgründen auf die Verwendung von vorzeichenbehafteten Komponenten verzichtet.

**[0053]** Das Codebuch C wird in einer Ausführungsform derart in zwei Sub-Codebücher C(1) und C(2) zerlegt, dass pro Codewort in das codierte Signal 102 ein Bit der einzubettenden Daten 101 eingebettet werden kann und dementsprechend ein Bit der einzubettenden Daten 101 pro Subrahmen übermittelt wird, was bei einer Subrahmendauer von 5ms einer Datenrate von 200bit/s entspricht.

**[0054]** Die Codewörter der Sub-Codebücher unterscheiden sich darin, dass die Summe der Komponenten  $c_i$  eines Codewortes aus dem einen Sub-Codebuch gerade und aus dem anderen Sub-Codebuch ungerade ist. Beispielsweise erfüllen alle Codeworte aus C(1) die Bedingung

$$\sum_{i=0}^9 c_i = 2 \cdot \text{trunc} \left( \frac{1}{2} \sum_{i=0}^9 c_i \right),$$

(d.h. Summe der Komponenten ist gerade) und alle Codeworte aus C(2) die Bedingung

$$\sum_{i=0}^9 c_i = 2 \cdot \text{trunc} \left( \frac{1}{2} \sum_{i=0}^9 c_i \right) + 1$$

(d.h. Summe der Komponenten ist ungerade) wobei trunc die Abrundungsoperation, das heißt das Abrunden auf die nächstkleinere ganze Zahl, bezeichnet.

**[0055]** Soll eine erste Nachricht (in diesem Beispiel bestehend aus einem Bit, beispielsweise dem Bitwert 0) übermittelt werden, so wird ein Codewort aus C(1) zur Codierung (der aktuellen Signalwerte des zu codierenden Signals 101) verwendet, und soll eine zweite Nachricht (in diesem Beispiel bestehend aus einem Bit, beispielsweise dem Bitwert 1) übermittelt werden, so wird ein Codewort aus C(1) zur Codierung verwendet. Ein Empfänger bzw. ein Decodierer kann basierend auf der Zugehörigkeit eines empfangenen Codewortes zu C(1) oder zu C(2) ermitteln, ob die erste Nachricht oder die zweite Nachricht eingebettet worden ist.

**[0056]** In einer anderen Ausführungsform wird die Unterteilung von C nach gerader und ungerader Parität der Summe der Komponenten der Codeworte durchgeführt. Beispielsweise gehört ein Codewort zu C(1) wenn

$$\sum_{i=0}^9 c_i$$

in Binärdarstellung eine gerade Anzahl von Einsen aufweist und zu C(2) andernfalls.

**[0057]** In einer Ausführungsform werden vier Bits pro Subrahmen eingebettet und damit eine Datenrate von 400bit/s erreicht. Dies geschieht durch eine Unterteilung des Codebuchs C in vier Sub-Codebücher C(1) bis C(4), wobei die Codeworte der Sub-Codebücher beispielsweise die folgenden Bedingungen erfüllen:

$$C(1): \sum_{i=0}^4 c_{2i} = 2 \cdot \text{trunc} \left( \frac{1}{2} \sum_{i=0}^4 c_{2i} \right),$$

$$C(2): \sum_{i=0}^4 c_{2i+1} = 2 \cdot \text{trunc} \left( \frac{1}{2} \sum_{i=0}^4 c_{2i+1} \right),$$

$$C(3): \sum_{i=0}^4 c_{2i} = 2 \cdot \text{trunc} \left( \frac{1}{2} \sum_{i=0}^4 c_{2i} \right) + 1$$

$$C(4): \sum_{i=0}^4 c_{2i+1} = 2 \cdot \text{trunc} \left( \frac{1}{2} \sum_{i=0}^4 c_{2i+1} \right) + 1.$$

anschaulich wird hierbei die Unterscheidung basierend auf Geradzahligkeit bzw. Ungeradzahligkeit der Summe der Komponenten mit geradem bzw. ungeraden Index durchgeführt.

**[0058]** Analog zu der obigen Alternative kann auch bei der Unterteilung des Codebuchs C in vier Sub-Codebücher dies basierend auf der Parität einer Binärdarstellung der Summe von Komponenten mit geradem bzw. ungeradem Index durchgeführt werden, also basierend auf der Parität von

$$\sum_{i=0}^4 c_{2i}$$

bzw.

$$\sum_{i=0}^4 c_{2i+1}.$$

**[0059]** In den obigen Bedingungen für die Codebücher C(1) und C(2) bzw. C(1) bis C(4) kann alternativ statt einer Komponente  $c_i$  selbst auch der Ausdruck  $\text{trunc}(c_i/5)$  verwendet werden, der eine Pulsposition innerhalb eines sogenannten Tracks eindeutig bezeichnet. Alternativ kann auch die jeweils Graycodierte Version  $\text{GRAY}(c_i)$  bzw.  $\text{GRAY}(\text{trunc}(c_i/5))$  verwendet werden, wie sie zur Kanalcodierung bei EFR vorgesehen ist. Unter Berücksichtigung der tatsächlichen Übertragung der Codeworte über einen GSM-Mobilfunkkanal erweist sich diese Möglichkeit zur Codebuchzerlegung als besonders vorteilhaft. Damit wird erreicht, dass besonders wenige Kanalbits einen Einfluss auf die eingebetteten Daten haben, wodurch die Bitfehlerrate der übertragenen eingebetteten Daten bei gestörter Übertragung sinkt.

**[0060]** Allgemein kann das Codebuch C in einer Ausführungsform derart zerlegt werden, dass die Codeworte des Sub-Codebuchs, das zur Codierung verwendet wird, wenn ein Nachrichtenbit  $m_i$  übermittelt werden soll, die Bedingung

$$m_i = \bigoplus_{j \in A_i} b_j \text{ erfüllen, wobei } A_i \text{ eine Indexmenge, } b_j \text{ die Komponenten des jeweiligen Codeworts bezeichnen.}$$

Die Summation wird dabei modulo 2 durchgeführt, so dass gefordert wird, dass die Summe modulo 2 mehrerer Codewortbits  $b_j$  gleich dem einzubettenden Nachrichtenbit  $m_i$  ist.

**[0061]** Zur Rekonstruktion einer eingebetteten Nachricht in einem empfangenen bzw. zu decodierenden Codewort ist es lediglich erforderlich, dass der Decodierer ermittelt, zu welchem Sub-Codebuch das Codewort gehört. Werden die Codeworte ungestört an den Decodierer übermittelt, so können auch die eingebetteten Informationen fehlerlos rekonstruiert werden.

**[0062]** Die oben beschriebene Vorgehensweise zur Einbettung von Informationen kann auch bei anderen Codierern eingesetzt werden, beispielsweise bei allen CELP Sprach-Codierern aber auch bei anderen Signal-Codierern wie Video-Codierern, Bild-Codierern etc.

**[0063]** Die Übertragung von Seiteninformationen (eingebetteten Informationen) mittels Steganographie kann auch zur Signalverbesserung eingesetzt werden und stellt eine Lösung für das Problem der Rückwärtskompatibilität dar. Ein Empfänger ohne Kenntnis der eingebetteten Informationen kann das (Sprach-) Signal, in das die Informationen einge-

bettet wurden, wie gewohnt, das heißt wie im Falle keiner Einbettung von Informationen mit nur geringen Verlusten decodieren. Kennt der Empfänger hingegen die eingebetteten Informationen, so können die Seiteninformationen zur Signalverbesserung verwendet werden. Ein entsprechendes Ausführungsbeispiel wird im Folgenden mit Bezug auf Fig. 2 beschrieben.

**[0064]** Fig.2 zeigt ein Codier/Decodiersystem 200 gemäß einem weiteren Ausführungsbeispiel der Erfindung.

**[0065]** Das Codier/Decodiersystem 200 weist einen Codierer 201 wie mit Bezug auf Fig.1 beschrieben auf. Entsprechend werden dem Codierer 201 ein zu codierendes Signal 202 und einzubettende Daten 203 zugeführt. Die einzubettenden Daten werden zur Signalverbesserung verwendet und werden dementsprechend von einer Signal-Analyse-Einrichtung 204, dem das zu codierende Signal 202 zugeführt wird, in für eine Signalverbesserung codierenden Signals 202 geeigneter Weise erzeugt.

**[0066]** Analog zu Fig.1 gibt der Codierer 201 ein codiertes Signal 205 aus, in das die einzubettenden Daten 203 eingebettet sind. Das codierte Signal 205 kann nun an einen Empfänger übermittelt werden, beispielsweise, wie oben beschrieben, mittels eines Mobilfunk-Kommunikationsnetzwerks.

**[0067]** Weist der Empfänger einen "konventionellen" Decodierer 206 auf, das heißt einen Decodierer, der die eingebetteten Daten nicht aus dem codierten Signal 205 ermitteln kann, so decodiert der Decodierer 206 lediglich das codierte Signal 205 zu einem decodierten Signal 207, welches (bis auf Übertragungsfehler und Codier/Decodierverluste) dem zu codierenden Signal 202 entspricht.

**[0068]** Weist der Empfänger einen "erweiterten" Decodierer 208 auf, das heißt einen Decodierer, der die eingebetteten Daten aus dem codierten Signal 205 ermitteln kann, so werden die eingebetteten Daten extrahiert und die extrahierten Daten 209 von einer Signalverbesserungseinheit 210 zur Signalverbesserung verwendet, welche ein decodiertes und (gegenüber dem decodierten Signal 207) verbessertes Signal 211 erzeugt.

**[0069]** Als Signalverbesserung kann z.B. künstliche Bandbreitenerweiterung, oder Störreduktion eingesetzt werden. Auch die Koeffizienten eines sendeseitig bestimmten Postfilters können per Steganographie übertragen werden.

**[0070]** Insbesondere die Anwendung der künstlichen Bandbreitenerweiterung ist vorteilhaft, da das Telefonnetz historisch bedingt auf eine akustische Bandbreite von 3.1kHz (300Hz-3.4kHz) begrenzt ist, eine Übertragung von Breitbandsprache (50Hz-7kHz) jedoch nur mit enormem Aufwand seitens der Netzbetreiber und der Endgerätehersteller zu bewerkstelligen wäre. Änderungen im (Mobilfunk-)Übertragungsnetz sind zur Realisierung der oben beschriebenen Ausführungsformen hingegen nicht erforderlich. Entsprechende (leistungsfähige) Bandbreitenerweiterungsalgorithmen sind beispielsweise in der Veröffentlichung von Peter Jax, Bernd Geiser, Stefan Schandl, Hervé Taddei, und Peter Vary, "An Embedded Scalable Wideband Codec Based on the GSM EFR Codec", in Proceedings of ICASSP, Toulouse, Mai 2006 beschrieben. Weiterhin wird in der Veröffentlichung von Peter Jax und Peter Vary, "Bandwidth Extension of Speech Signals: A Catalyst for the Introduction of Wideband Speech Coding?", IEEE Communications Magazine, vol. 44, no. 5, Mai 2006 die Einführung breitbandiger Sprachübertragung über den Umweg der Bandbreitenerweiterung (ggf. mit Unterstützung von digitalen Wasserzeichen) erwähnt.

**[0071]** Im Folgenden wird eine weitere Möglichkeit für eine Zerlegung des oben definierten Codebuchs C (EFR-ACELP Codebuch) beschrieben.

**[0072]** Zunächst wird zum besseren Verständnis kurz die Suchstrategie des EFR-Codecs erläutert:

1) Zunächst wird die erste Pulsposition  $i_0 \in \{0, \dots, 39\}$  heuristisch ermittelt und bleibt während der gesamten Suche fest. Der zu  $i_0$  gehörige "Track" ist beispielsweise  $x = 4$  oder  $x = 9$ . Für die  $x$ -te Komponente  $c_x$  des entsprechenden Codeworts gilt  $c_x = i_0$ .

2) Die Position des zweiten Pulses  $i_1 \in \{0, \dots, 39\}$  wird ebenfalls heuristisch ermittelt, wobei für jede der vier Iterationen des unten stehenden Algorithmus (Schritt 3) ein anderer Wert angenommen wird. Beispielsweise gehöre für die erste Iteration zur gewählten Position  $i_1$  der Track  $y=3$  oder  $y=8$ , d.h.  $C_y = i_1$ .

3) Für die verbleibenden acht Tracks werden für jede von vier Iterationen die Pulse sukzessive in Paaren zu je zwei Tracks durch erschöpfende Suche optimiert. In jeder der vier Iterationen werden die Track-Paare durch Permutation neu zusammengestellt, wobei  $c_x$  und  $c_y$  nicht wiederverwendet werden

**[0073]** Beispielsweise wird für das Track-Paar  $c_0 / c_6$  die Optimierung entsprechend dem folgenden Pseudocode durchgeführt:

```
for(i = 0, 5, 10, ..., 35) // Iteration über alle zulässigen Elemente für  $c_0$ 
for(j = 1, 6, 11, ..., 36) // Iteration über alle zulässigen Elemente für  $c_6$ 
  Teste Puls-Paar ( $c_0=i, c_6=j$ ) entsprechend CELP-Kriterium auf Optimalität
```

**[0074]** Bei dieser Suchstrategie gemäß EFR werden insgesamt 1024 Kombinationen (4 Iterationen \* 4 Track-Paare



\* 8 Puls-Positionen \* 8 Puls-Positionen = 1024 Kombinationen) untersucht und daraus die optimalen Puls-Paare ausgewählt.

**[0075]** Zur Einbettung von Informationen, im Folgenden Beispiel eines einzelnen (Wasserzeichen-)bits  $b$ , in ein Codewort  $\underline{c} = (c_0, \dots, c_9)$  wird gemäß einem Ausführungsbeispiel der Erfindung der obige Algorithmus wie im Folgenden beschrieben abgeändert.

**[0076]** Wenn bei einer Suche bereits ein Puls für einen Track, beispielsweise  $c_1$ , ermittelt wurde, kann bei der Wahl des (identisch aufgebauten) Tracks  $c_6$  durch ein Wasserzeichenbit  $b$  in das Puls-Positionenpaar  $c_1$  und  $c_6$  eingebettet werden, indem  $c_6$  in Abhängigkeit des Bits  $b$  gewählt wird. Die paarweise Suche wird dazu beispielsweise wie folgt modifiziert:

```
c6_offset = 5 * ((c1 + b + 1) mod 2)
for(i = 0, 5, 10, ..., 35) // Iteration über alle zulässigen Elemente für c0
for(j = 1, 11, 21, 31) // Iteration über alle zulässigen Elemente für c6 (gegenüber oben halbe Anzahl)
  Teste Puls-Paar (c0=i, c6=j+c6_offset) entsprechend CELP-Kriterium auf Optimalität
```

**[0077]** Das eingebettete Bit  $b$  kann im Empfänger bzw. Decodierer durch die Operation

$$b = (c_1 + c_6) \bmod 2$$

ermittelt werden.

**[0078]** Statt  $c6\_offset = 5 * ((c1 + b + 1) \bmod 2)$  können auch andere Kombinationen von bereits ermittelten Pulspositionen und einzubettenden Bits verwendet werden. In dem obigen Beispiel wurde der Suchraum für die Pulsposition  $c_6$  in zwei gleiche Teile (ungerade/gerade Werte) aufgeteilt. Weitere Aufteilungen (etwa erste/zweite Worthälfte) sind auch möglich, wobei die Gleichung für  $c6\_offset$  entsprechend anzupassen ist.

**[0079]** Die Anzahl der untersuchten Pulsposition-Kombinationen ist durch das auf diese Weise eingebettete Bit auf

$$4 \text{ Iterationen} * (3 \text{ Paare} * 8 \text{ Pos.} * 8 \text{ Pos.} + 1 \text{ Paar} * 8 \text{ Pos.} * 4 \text{ Pos.}) = 896 \text{ Kombinationen}$$

gesunken.

**[0080]** Zur Einbettung mehrerer Bits in ein Codewort  $\underline{c}$  kann der Suchraum für  $c_6$  noch einmal halbiert werden, oder ein identisches Verfahren für ein zweites Pulspaar angewendet werden. Es ist günstig, gerade solche Pulse im Rahmen der Informationseinbettung durch  $c6\_offset$  (bzw. das Bit  $b$ ) zu koppeln, die in einem Track liegen. Anderenfalls kann, aufgrund der Vorzeichencodierung des EFR, im Empfänger keine eindeutige Zuordnung der Pulse mehr vorgenommen werden. Durch entsprechenden Zusatzaufwand im Sender kann diese Beschränkung aufgehoben werden. Im Empfänger sind  $c_1$  und  $c_6$  nicht voneinander zu unterscheiden. Die Datenextraktion via  $b = (c_1 + c_6) \bmod 2$  macht daher keine Probleme, allerdings ist es schwierig, beispielsweise  $b = (c_1 + c_5) \bmod 2$  zu berechnen, da (je nach Vorzeichen) "versehentlich"  $b = (c_6 + c_5) \bmod 2$  berechnet werden könnte. Der sendeseitige "Zusatzaufwand" besteht darin, die Vorzeichencodierung in den Optimierungsschleifen zu berücksichtigen und quasi pro Optimierungsschritt vorwegzunehmen.

**[0081]** Durch die reduzierte Anzahl von untersuchten Kombinationen (896 statt 1024 in dem obigen Beispiel) ergibt sich eine geringere Codierqualität durch Wasserzeicheneinbettung. Dies kann durch eine erweiterte Suche, das heißt eine Erweiterung des Suchraums, kompensiert werden. Dazu werden die Tracks nicht mehr in Paaren sondern in Gruppen zu 3 oder 4 (oder auch mehr) Tracks gemeinsam durchsucht. Die gemeinsame Suche (ohne Wasserzeicheneinbettung) für 3 Tracks (z.B.  $c_0$ ,  $c_6$  und  $c_7$ ) wird beispielsweise wie folgt realisiert:

```
for(i2 = 0, 5, 10, ..., 35) // Iteration über die zulässigen Werte von c0
for(i3 = 1, 6, 11, ..., 36) // Iteration über die zulässigen Werte von c6
for(i4 = 2, 7, 12, ..., 37) // Iteration über die zulässigen Werte von c7
  Suche optimales Tripel (c0=i2, c6=i3, c7=i4)
```

**[0082]** Für jedes Tripel bedeutet dies, dass  $8*8*8 = 512$  Kombinationen durchsucht werden. Wird die gesamte Suche für die 8 variablen Pulspositionen (gemäß den Schritten 1 und 2 sind ja zwei Pulspositionen fest) so aufgeteilt, dass 2 Tripel und 1 Paar gemeinsam optimiert werden, so ergibt sich, dass

4 Iterationen \* (2 Tripel \* 8 Pos. \* 8 Pos. \* 8 Pos. + 1 Paar \*  
8 Pos. \* 8 Pos.) = 4352 Kombinationen

untersucht werden, was gegenüber den 1024 Kombinationen gemäß EFR einen erheblichen Mehraufwand bedeutet.

**[0083]** Werden jedoch z.B. im Zuge der Optimierung des ersten Tripels 3 Wasserzeichenbits, im Zuge der Optimierung des zweiten Tripels 2 Wasserzeichenbits wie oben beschrieben eingebettet, während für das Pulspositionen-Paar keine Einbettung vorgenommen wird, so ergibt sich die Zahl der zu untersuchenden Kombinationen zu

4 Iterationen \* (1 Tripel \* 4 Pos. \* 4 Pos. \* 4 Pos. + 1 Tri-  
pel \* 8 Pos. \* 4 Pos. \* 4 Pos. + 1 Paar \* 8 Pos. \* 8 Pos.) =  
1024 Kombinationen,

d.h. exakt die Anzahl der untersuchten Kombinationen im Standard-EFR-Codec. Die Wasserzeichendatenrate liegt in diesem Fall bei  $(2+3)\text{bit}/5\text{ms} = 1\text{ kbit/s}$ .

**[0084]** Schließlich ist eine weitere Möglichkeit zur Erweiterung des Suchraumes die Erhöhung der Iterationszahl, d.h. die Untersuchung weiterer Track-Permutationen.

**[0085]** Die einem Ausführungsbeispiel zu Grunde liegende Idee kann darin gesehen werden, dass die Informations-einbettung dem Signal-Codierer bekannt ist, was durch eine gemeinsame Dateneinbettung und Signalcodierung erreicht wird, das heißt es wird beispielsweise die Wasserzeichen-Einbettung in den Codierer integriert. Dies kann innerhalb einer Analyse-durch-Synthese Schleife durchgeführt werden ("closed-loop"), wie es in Fig.3 dargestellt ist.

**[0086]** Fig.3 zeigt einen Codierer 300 gemäß einem weiteren Ausführungsbeispiel der Erfindung.

**[0087]** Dem Codierer werden ein zu codierendes Signal und einzubettende Daten 302 zugeführt.

**[0088]** Ein codiertes Signal 303 wird aus dem zu codierenden Signal 301 mittels einer Schleife erzeugt, die ein Codebuch 304, eine Syntheseeinrichtung 305 und einen Vergleicher 306 aufweist. Dabei wird eine mögliche Codierung des zu codierenden Signals 301 von dem Codebuch 304 erzeugt und es wird mittels der Syntheseeinrichtung 305 und dem Vergleicher 306 überprüft, wie gut es das zu codierende Signal 301 widerspiegelt und gegebenenfalls, basierend auf der Ausgabe des Vergleichers 306, abgeändert.

**[0089]** Die einzubettenden Daten 302 werden im Laufe des Codierungsprozesses in das codierte Signal 303 eingebettet, beispielsweise gemäß einer der oben beschriebenen Vorgehensweisen.

**[0090]** Beispielsweise wird basierend auf den einzubettenden Daten 302 ein Sub-Codebuch des Codebuchs 304 ausgewählt, wie es in Fig.4 dargestellt ist.

**[0091]** Fig.4 zeigt einen Codierer 400 gemäß einem weiteren Ausführungsbeispiel der Erfindung.

**[0092]** Analog zu dem in Fig.3 dargestellten Codierer 300 werden dem Codierer einzubettende Daten 402 und ein zu codierendes Signal 401 zugeführt und er erzeugt ein codiertes Signal 403, in das die einzubettenden Daten 402 eingebettet sind. Neben einer Syntheseeinrichtung 405 und einem Vergleicher 406 analog zu dem Codierer 300 in Fig.3 weist der Codierer 400 eine Mehrzahl von Sub-Codebüchern 404 also ein in mehrere Sub-Codebücher 404 unterteiltes Codebuch auf. Basierend auf den einzubettenden Daten werden die Sub-Codebücher bei der Codierung des zu codierenden Signals 401 ausgewählt. Beispielsweise wird einem Datenwort des zu codierenden Signals 401 ein Codewort aus einem ersten Sub-Codebuch zugeordnet, wenn eine erste Seiteninformation aus den einzubettenden Daten 402, beispielsweise ein Bit mit dem Wert 0, eingebettet werden soll und es wird ein Codewort aus einem zweiten Sub-Codebuch zugeordnet, wenn eine zweite Seiteninformation aus den einzubettenden Daten 402, beispielsweise ein Bit mit dem Wert 1, eingebettet werden soll.

**[0093]** Die Aufteilung eines Codebuchs in mehrere Sub-Codebücher ist in Fig.5 illustriert.

**[0094]** Fig.5 zeigt ein Codebuch 500 gemäß einem weiteren Ausführungsbeispiel der Erfindung.

**[0095]** Das Codebuch 500 ist mit C bezeichnet. Aus Effizienzgründen wird, wenn der Codewortumfang des Codebuchs 500 sehr groß ist, das Codebuch 500 beim Codieren nur teilweise durchsucht, d.h. es werden Codeworte zur Codierung nur aus einer Codebuch-Teilmenge 501, welche mit C' (praktisches Codebuch) bezeichnet ist, ausgewählt.

**[0096]** Bei den obigen Ausführungsbeispielen wird das Codebuch 500 zur Dateneinbettung wie oben erläutert in Codebücher zerlegt, beispielsweise in vier Sub-Codebücher 502, welche mit C(1) bis C(4) bezeichnet sind.

**[0097]** Da ein Sub-Codebuch 502 einen geringeren Codewortumfang hat als die Codebuch-Teilmenge 501 und damit die Qualität der Signalcodierung (abhängig von der Anzahl der Sub-Codebücher 502) gegenüber einer Verwendung der gesamten Codebuch-Teilmenge 501 sinken würde, wird in einem Ausführungsbeispiel der Codeumfang der Sub-

Codebuch 502 erweitert, so dass insgesamt eine erweiterte Codebuch-Teilmenge 503 zur Codierung verwendet wird. Dabei steigt die algorithmische Komplexität nur geringfügig an, die Qualität der Codierung sinkt nicht und es kann in Sonderfällen sogar eine Qualitätssteigerung erzielt werden.

[0098] In einer Ausführungsform wird ein algebraisches Codebuch verwendet. Im Gegensatz zu einem gewöhnlichen Codebuch in Tabellenform existiert ein algebraisches Codebuch nur im Sinne einer algebraischen Konstruktionsvorschrift. Dies bedeutet, dass die einzelnen Codebuch-Einträge (Codewörter) im Zuge der Signalcodierung durch einen Codewortgenerator erzeugt werden. Das "Binning Scheme" zur Informationseinbettung, das heißt die Zerlegung des Codebuchs in Sub-Codebücher und Auswahl des zur Codierung verwendeten Sub-Codebuchs in Abhängigkeit der einzubettenden Information, bei einem Codierer mit algebraischem Codebuch besteht nun nicht mehr lediglich in der Aufteilung des Codebuchs in eine Anzahl von Sub-Codebüchern, sondern darüber hinaus auch in der Modifikation des Codewortgenerators dahingehend, dass jeweils nur zu dem durch die aktuell einzubettende Nachricht i ausgewählten Sub-Codebuch C(i) gehörige Codewörter ausgegeben werden.

## Patentansprüche

1. Verfahren zur Einbettung einer steganographischen Information in eine Signalinformation eines Signal-Codierers (100), **gekennzeichnet durch**

- Bereitstellen einer Dateninformation, insbesondere einer Sprachinformation, als zu codierendes Signal (101),
- Auswählen einer steganographischen Information als einzubettende Daten (102), wobei die steganografische Information aus einer Menge von steganographischen Informationen ausgewählt wird,
- Erzeugen eines Codewortes aus einem bereitgestellten Codebuch (500) mittels des Signal-Codierers (100) auf Basis von das Codewort bildenden Codeelementen, derart, dass

- unter Verwendung des erzeugten Codeworts im Rahmen eines mit dem Codebuch assoziierbaren Übertragungsstandards die Dateninformation in eine das Codewort beinhaltende und/oder auf das Codewort verweisende Signalinformation als codiertes Signal (103) codiert wird; und, dass
- das erzeugte Codewort eine zusätzliche, auf Basis der das Codewort bildenden Codeelemente berechenbare Eigenschaft aufweist, wobei die zusätzliche Eigenschaft die steganographische Information darstellt.

2. Verfahren nach Anspruch 1, **gekennzeichnet durch** Erzeugen des Codewortes derart, dass das Codebuch (500) in eine Anzahl von Sub-Codebüchern aufgeteilt ist und dass **durch** den Signal-Codierer (100) jeweils nur ein zu dem **durch** die aktuell einzubettende steganografische Information ausgewählten Sub-Codebuch gehöriges Codewort ausgegeben wird.

3. Verfahren nach Anspruch 1 oder 2, **gekennzeichnet durch** eine Bewertung des erzeugten Codewortes im Rahmen eines mit dem bereitgestellten Codebuch assoziierbaren Übertragungsstandards mittels Decodierens des Codewortes und anschließenden Vergleichens der decodierten Dateninformation mit der ursprünglichen Dateninformation und ferner **gekennzeichnet durch** das optionale Erzeugen des Codewortes aus dem bereitgestellten Codebuch mittels des Signal-Codierers (100) auf Basis der das Codewort bildenden Codeelemente unter Berücksichtigung der Bewertung.

4. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** die Verwendung eines auf Basis des GSM- und/oder des UMTS-Übertragungsstandards basierenden Codierers (100) und Codebuchs.

5. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** Erzeugen des Codewortes aus einem bereitgestellten algebraischen Codebuch (500) im Sinne einer algebraischen Konstruktionsvorschrift und/oder auf Basis der CELP-, der ACELP- oder der AMR-Codierung.

6. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** die Berechnung der Eigenschaft des Codewortes als Ergebnis einer Anwendung mindestens einer Operation auf mindestens eines der das Codewort bildenden Codeelemente.

7. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** die Bereitstellung des Codewortes derart, dass das Codewort die Eigenschaft implizit erfüllt.

8. Verfahren nach Anspruch 7, **gekennzeichnet durch** Erzeugung des Codeworts derart, dass es die Eigenschaft,

welche die steganografische Information darstellt, bereits während seiner Erzeugung erfüllt.

9. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** die Auswahl der steganographischen Information derart, dass die steganographische Information empfangsseitig zur Signalverbesserung, insbesondere bei Sprachübertragung, wie eine künstliche Bandbreitenerweiterung und/oder Störreduktion, verwendet wird.
10. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** die Auswahl der steganographischen Information derart, dass die steganographische Information als digitales Wasserzeichen verwendet wird.
11. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** ein Übertragen der das Codewort beinhaltenden oder auf das Codewort verweisenden Signalinformation an einen Empfänger.
12. Verfahren nach Anspruch 11, **gekennzeichnet durch** ein empfangsseitiges Bereitstellen einer Dateninformation mittels Decodierens des Codewortes im Rahmen eines mit dem bereitgestellten Codebuch assoziierbaren Übertragungsstandards.
13. Verfahren nach Anspruch 11 oder 12, **gekennzeichnet durch** ein empfangsseitiges Bereitstellen der steganographischen Information mittels Berechnens der zusätzlichen Eigenschaft des Codewortes auf Basis der das Codewort bildenden Codeelemente.
14. Verfahren nach einem der vorhergehenden Ansprüche, **gekennzeichnet durch** ein Ausführen des Verfahrens in einer Mobilfunkvorrichtung.
15. Verfahren nach einem der vorhergehenden Ansprüche, wobei dem Signal-Codierer (100) die einzubettende Information zugeführt wird.
16. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Signal-Codierer (100) ein erstes Codeelement und ein zweites Codeelement des Codewortes ermittelt, wobei das zweite Codeelement in Abhängigkeit des ersten Codeelements und der einzubettenden Information ermittelt wird.
17. Signal-Codierer (100) zur Einbettung einer steganographischen Information in eine Signalinformation des Signal-Codierers (100), **gekennzeichnet durch**
  - eine Einrichtung zum Empfangen einer Dateninformation, insbesondere einer Sprachinformation, als zu codierendes Signal (101),
  - eine Einrichtung zum Empfangen einer steganographischen Information als einzubettende Daten (102), wobei die steganografische Information aus einer Menge von steganographischen Informationen ausgewählt wird,
  - eine Einrichtung zum Erzeugen eines Codewortes aus einem bereitgestellten Codebuch (500) mittels des Signal-Codierers (100) auf Basis von das Codewort bildenden Codeelementen, derart, dass
    - unter Verwendung des erzeugten Codeworts im Rahmen eines mit dem Codebuch assoziierbaren Übertragungsstandards die Dateninformation in eine das Codewort beinhaltende und/oder auf das Codewort verweisende Signalinformation als codiertes Signal (103) codiert wird; und dass
    - das erzeugte Codewort eine zusätzliche, auf Basis der das Codewort bildenden Codeelemente berechenbare Eigenschaft aufweist, wobei die zusätzliche Eigenschaft die steganographische Information darstellt.
18. Verfahren zur empfangsseitigen Bereitstellung einer steganographischen Information, die von einem Signal-Codierer (100) in eine Signalinformation eingebettet wurde durch Erzeugen eines Codewortes aus einem bereitgestellten Codebuch (500) mittels des Signal-Codierers (100) auf Basis von das Codewort bildenden Codeelementen, derart, dass
  - unter Verwendung des erzeugten Codeworts im Rahmen eines mit dem Codebuch assoziierbaren Übertragungsstandards eine Dateninformation als zu codierendes Signal (101) in eine das Codewort beinhaltende und/oder auf das Codewort verweisende Signalinformation als codiertes Signal (103) codiert ist; und dass
  - das erzeugte Codewort eine zusätzliche, auf Basis der das Codewort bildenden Codeelemente berechenbare Eigenschaft aufweist, wobei die zusätzliche Eigenschaft die steganographische Information darstellt;

wobei die empfangsseitige Bereitstellung der steganografischen Information das Berechnen der zusätzlichen Eigenschaft des Codeworts auf Basis der das Codewort bildenden Codeelemente umfasst.

5      **19.** Verfahren nach Anspruch 18, wobei empfangsseitig ein erstes Codeelement und ein zweites Codeelement des Codewortes ermittelt werden, wobei die steganografische Information in Abhängigkeit des ersten Codeelements und des zweiten Codeelements ermittelt wird.

10      **20.** Verfahren nach Anspruch 18 oder 19, ferner umfassend Ermitteln der eingebetteten Daten aus einem codierten Signal (205) und Verwenden der so ermittelten Daten (209) zur Signalverbesserung, insbesondere zur künstlichen Bandbreitenerweiterung und/oder Störreduktion, oder zur Ermittlung der Koeffizienten eines senderseitig bestimmten Postfilters.

**21.** Decodierer (208), der zur Durchführung des Verfahrens nach einem der Ansprüche 18 bis 20 ausgebildet ist.

15

20

25

30

35

40

45

50

55

Fig. 1

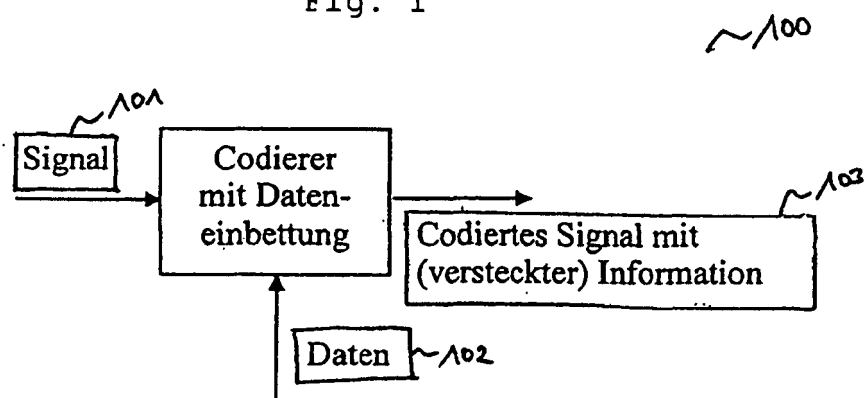


Fig. 2

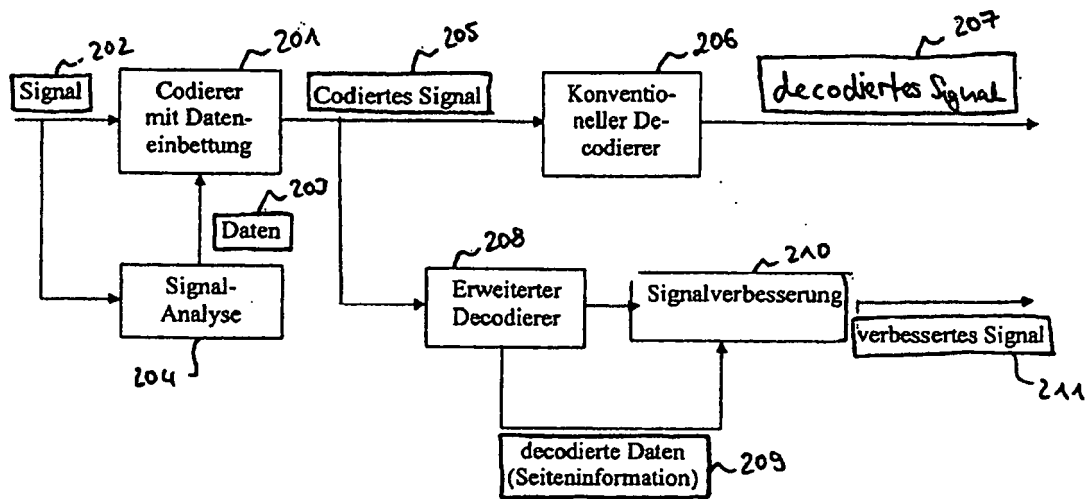


Fig. 3

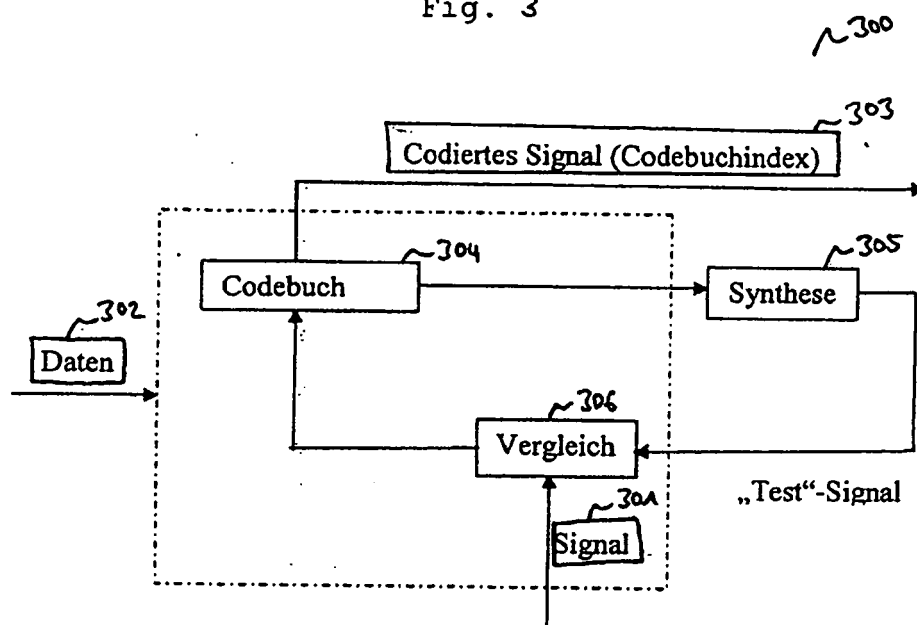




Fig. 4

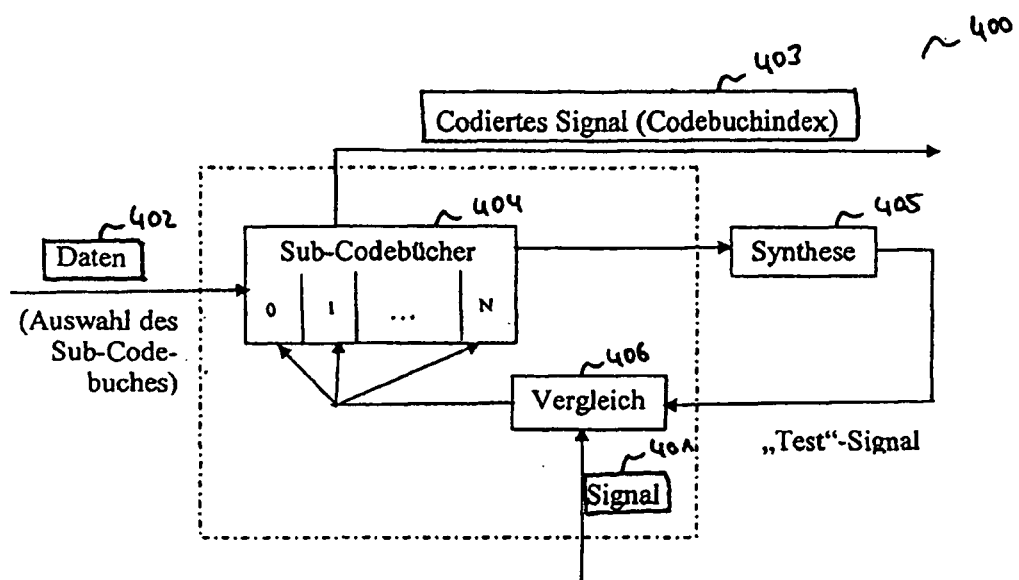
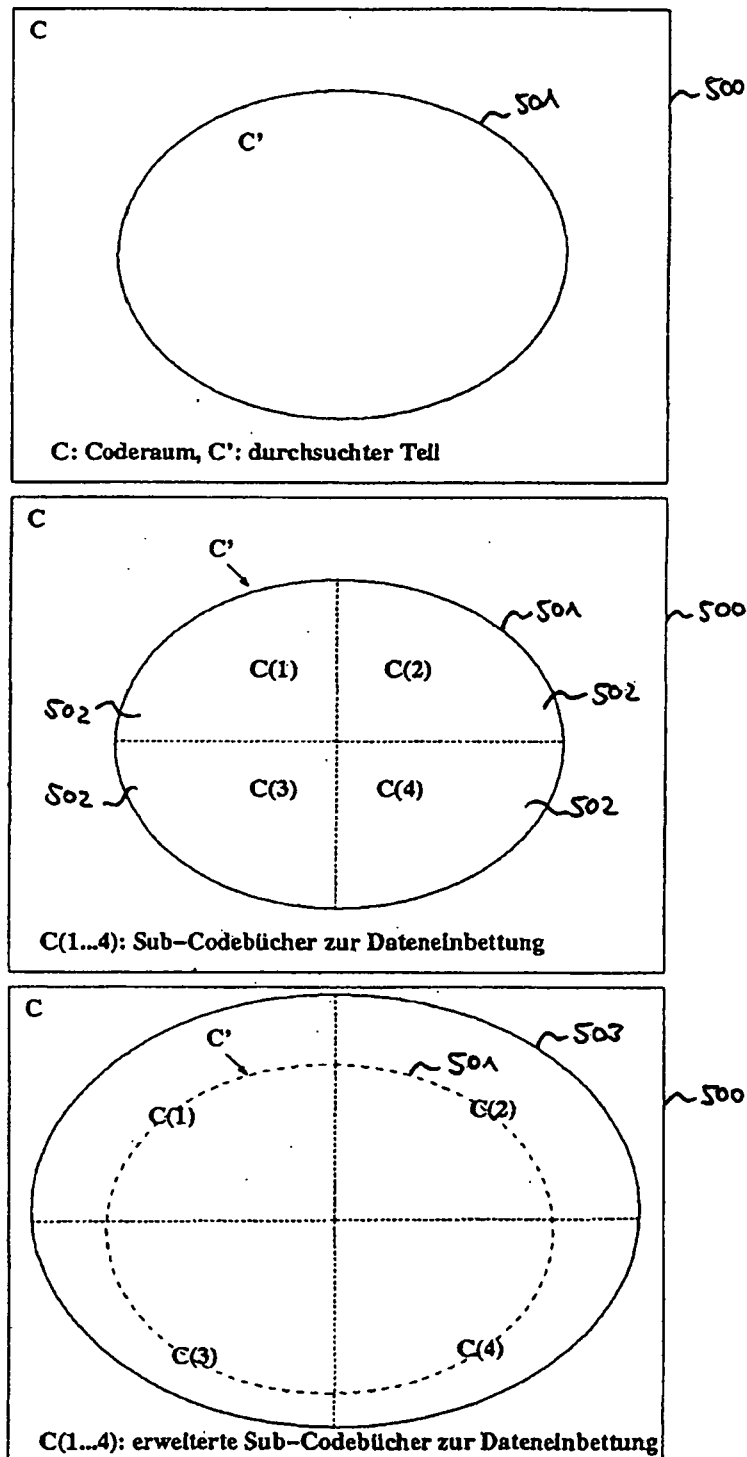


Fig. 5





## EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung  
EP 11 00 6299

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	NICOLAS CHÉTRY AND MIKE DAVIES: "Embedding side information into a speech codec residual", EUROPEAN SIGNAL PROCESSING CONFERENCE, 4. September 2006 (2006-09-04), - 8. September 2006 (2006-09-08), XP002460947, Florence, Italy	1-4,6-21	INV. G10L19/00 G10L19/12 H04K1/00
Y	* das ganze Dokument *	5	
Y	JP 11 272299 A (TOYO COMMUNICATION EQUIP) 8. Oktober 1999 (1999-10-08) * Abbildungen 2-4 * * Absätze [0016], [0018], [0029] - [0042] *	5	
A	MUNETOSHI IWAKIRI ET AL: "Embedding a text into conjugate structure algebraic code excited linear prediction audio codes", COMPUTER SYSTEM SYMPOSIUM, INFORMATION PROCESSING SOCIETY OF JAPAN, JP, Bd. 39, Nr. 3, 1. September 1998 (1998-09-01), Seiten 2623-2630, XP007916951, * Zusammenfassung *	1,5,17, 18,21	RECHERCHIERTE SACHGEBIETE (IPC) G10L
A,D	ZHE-MING LU ET AL: "Watermarking combined with CELP speech coding for authentication", IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS INST. ELECTRON. INF. & COMMUN. ENG, Bd. 1E88-D, Nr. 2, Februar 2005 (2005-02), Seiten 330-334, XP002460948, JAPAN ISSN: 0916-8532 * das ganze Dokument *	1-21	
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort Berlin		Abschlußdatum der Recherche 30. September 2011	Prüfer Santos Luque, Rocio
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

 1  
EPO FORM 1503 03.02 (P04C03)



## EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung  
 EP 11 00 6299

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
A	EP 1 049 259 A (KOWA CO [JP]) 2. November 2000 (2000-11-02) * Zusammenfassung * -----	1,2,17, 18,21	
			RECHERCHIERTE SACHGEBIETE (IPC)
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort <b>Berlin</b>		Abschlußdatum der Recherche <b>30. September 2011</b>	Prüfer <b>Santos Luque, Rocio</b>
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument ..... & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

 1  
 EPO FORM 1503 03-82 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT  
 ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 11 00 6299

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.

Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am

Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

30-09-2011

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
JP 11272299	A	08-10-1999	JP	3355521 B2	09-12-2002
-----					
EP 1049259	A	02-11-2000	DE	69839312 T2	09-04-2009
			JP	3022462 B2	21-03-2000
			JP	11205153 A	30-07-1999
			WO	9937028 A1	22-07-1999
			US	6539356 B1	25-03-2003
-----					

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

## IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

*Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.*

### In der Beschreibung aufgeführte Nicht-Patentliteratur

- **ZHE-MING LU et al.** Watermarking Combined with CELP Speech Coding for Authentication. *IEICE TRANS. INF. & SYST.*, Februar 2005, vol. E88-D (2) [0010]
- **PETER JAX ; BERND GEISER ; STEFAN SCHANDL ; HERVÉ TADDEI ; PETER VARY.** An Embedded Scalable Wideband Codec Based on the GSM EFR Codec. *Proceedings of ICASSP*, Mai 2006 [0070]
- **PETER JAX ; PETER VARY.** Bandwidth Extension of Speech Signals: A Catalyst for the Introduction of Wideband Speech Coding?. *IEEE Communications Magazine*, Mai 2006, vol. 44 (5) [0070]