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

(10) **DE 694 35 076 T2** 2009.03.26

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 389 011 B1**
(21) Deutsches Aktenzeichen: **694 35 076.1**
(96) Europäisches Aktenzeichen: **03 021 209.6**
(96) Europäischer Anmeldetag: **16.11.1994**
(97) Erstveröffentlichung durch das EPA: **11.02.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **27.02.2008**
(47) Veröffentlichungstag im Patentblatt: **26.03.2009**

(51) Int Cl.[8]: ***H04N 5/913*** (2006.01)

(30) Unionspriorität:

154866	**18.11.1993**	**US**
215289	**17.03.1994**	**US**
327426	**21.10.1994**	**US**

(73) Patentinhaber:
Digimarc Corp., Beaverton, Oreg., US

(74) Vertreter:
BOEHMERT & BOEHMERT, 80336 München

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

(72) Erfinder:
Rhoads, Geoffrey B., West Linn, OR 97068, US

(54) Bezeichnung: **Einbetten eines steganographischen Kodes in ein Bildsignal**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf die Einbettung robuster Kennungscodes in elektronische, optische and physikalische Medien und die nachfolgende, objektive Erkennung solcher Codes für Identifizierungszwecke auch nach einer inzwischen eingetretenen Verzerrung oder Entstellung der Medien.

[0002] Die Erfindung wird unter Bezugnahme auf verschiedene beispielhafte Anwendungen veranschaulicht, darunter die Codierung Für Identifizierung/Authentifizierung von elektronischen Abbildungen, seriellen Datensignalen (zum Beispiel Audio und Video), Emulsionsfilm und Papiergeld, ohne aber darauf beschränkt zu sein.

Hintergrund und Zusammenfassung der Erfindung

"Nie würde ich irgendeinem Drucker oder Verleger die Befugnis erteilen, eines meiner Werke zu unterdrücken oder zuverändern, indem ich ihn zum Gebieter über die Kopie erhebe."
Thomas Paine, *Rights of Man [Menschenrechte]*, 1792

"Der Drucker wagt es nicht, über den erlaubten Abdruck hinauszugehen."
Milton, *Aeropagetica*, 1644

[0003] Seit unvordenklichen Zeiten sind die nicht autorisierte Verwendung und die reine Piraterie von urheberrechtlich geschützten Quellen eine Quelle von verlorenem Einkommen, Verwechslung und Kunstfälschung gewesen.

[0004] Diese zur Geschichte gehörigen Probleme haben sich mit dem Aufkommen der Digitaltechnik potenziert. Mit ihr haben die Technik des Kopierens von Materialien und ihrer nicht autorisierten Weiterverbreitung neue Gipfel der Raffinesse und, was noch wichtiger ist, der Allgegenwart erreicht. Ohne objektive Mittel für den Vergleich einer angeblichen Kopie mit dem Original gibt es für Eigentümer und mögliche Rechtsstreitigkeiten nur eine subjektive Meinung dazu, ob die angebliche Kopie gestohlen oder in nicht autorisierter Art und Weise verwendet worden ist. Ferner gibt es keine einfachen Mittel, um den Weg zu einem ursprünglichen Käufer des Materials zurückzuverfolgen, was sich als wertvoll erweisen kann, um nachzuweisen, wo eine mögliche "Leckage" des Materials zuerst aufgetreten ist.

[0005] Verschiedenartige Verfahren zum Schutz handelsüblichen Materials sind erprobt worden. Eines besteht darin, Signale vor dem Vertrieb durch ein Kodierverfahren zu verschlüsseln und vor der Verwendung zu entschlüsseln. Diese Methode erfordert es jedoch, dass weder die ursprünglichen noch die später entschlüsselten Signale geschlossene, kontrollierte Netze verlassen, wenn sie nicht abgefangen und aufgezeichnet werden sollen. Des weiteren ist diese Anordnung von nur geringem Nutzen auf dem grossen Gebiet der Massenvermarktung von Audio- und visuellen Materialien, wo selbst wenige Dollar zusätzlicher Kosten eine grössere Markteinschränkung verursachen und das Signal für seine Wahrnehmung entschlüsselt werden muss, daher auch leicht aufgezeichnet werden kann.

[0006] Eine weitere Gruppe von Verfahren beruht auf einer Abwandlung der ursprünglichen Audio- oder Videosignale, indem ein unterschwelliges Kennungssignal beigefügt wird, das mit elektronischen Mitteln wahrnehmbar ist. Beispiele für solche Systeme sind in der Patentschrift US 4 972 471 und in der Europäischen Patentveröffentlichung EP 443 702 sowie auch in Komatsu und Mitautoren, "Authentication system using concealed image in telematics" [Authentifizierungssystem mit verborgenem Bild in der Telematik], Memoirs of the School of Science and Engineering, Waseda University, Nr. 52, Seiten 45–69 (1988) zu finden. Komatsu verwendet für dieses Verfahren die Bezeichnung "digitales Wasserzeichen". Eine elementare Einführung in diese Verfahren ist in dem Aufsatz: "Digital signatures" [Digitale Signaturen], Byte Magazine, November 1993, Seite 309, zu finden. Diese Verfahren haben das gemeinsame Merkmal, dass deterministische Signale mit wohldefinierten Muster und Sequenzen innerhalb der Quelle die Daten zur Identifizierung vermitteln. Für bestimmte Anwendungen ist das kein Nachteil. Allgemein ist dies jedoch aus verschiedenartigen Gründen eine ineffiziente Form der Einbettung von Daten zur Identifizierung: a) nicht die gesamte Quelle wird verwendet; b) deterministische Muster haben eine höhere Wahrscheinlichkeit, von einem potenziellen Piraten entdeckt und entfernt zu werden; und c) die Signale sind nicht allgemein 'holographisch', indem eine Identifizierung schwierig sein kann,

wenn nur Abschnitte des ganzen Werkes vorliegen. ('Holographisch' wird hier auf die Eigenschaft bezogen, dass Daten zur Identifizierung global durch das gesamte verschlüsselte Signal hindurch verteilt und selbst durch Überprüfung nur eines Bruchteils des verschlüsselten Signals voll erkennbar sind. Dieser Kodierungstyp wird hierin gelegentlich als "verteilt" bezeichnet.)

[0007] In den gegebenen Literaturhinweisen finden sich Beschreibungen verschiedener Programme, die Steganographie ausführen, was in einem Dokument als "...die alte Kunst, Daten in anderweit unauffälligen Daten zu verstecken" beschrieben wird. Diese Programme geben Computerbenutzern auf unterschiedliche Art und Weise die Möglichkeit, ihre eigenen Botschaften in digitalen Bild- oder Audiodateien zu verstecken. Alle verwenden dafür eine Stellungsumkehr des niedrigstwertigen Bits (des Bits niedrigster Ordnung in einem einzelnen Datenmuster) eines gegebenen Audiodatenflusses oder gerasterten Bildes. Einige dieser Programme betten Botschaften ziemlich direkt in das niedrigstwertige Bit ein, während andere eine Botschaft erst "vorverschlüsseln" oder kodieren und die verschlüsselten Daten dann in das niedrigstwertige Bit einbetten.

[0008] Wir verstehen diese Programme heute so, dass sie allgemein auf einer fehlerfreien Übertragung der digitalen Daten beruhen, um eine gegebene Botschaft als Ganzes richtig zu übermitteln. Typischerweise wird die Botschaft nur einmal durchgegeben, das heisst, sie wird nicht wiederholt. Weiter scheint es, dass diese Programme das niedrigstwertige Bit gänzlich "übernehmen", wobei die wirklichen Daten verwischt werden und die Botschaft entsprechend platziert wird. Das könnte darauf hinauslaufen, dass solche Kodes leicht ausgelöscht werden können, indem lediglich das niedrigstwertige Bit aller Datenwerte in einer gegebenen Bild- oder Audiodatei abgetrennt wird. Diese und andere Erwägungen legen nahe, dass die einzige Ähnlichkeit zwischen unserer Erfindung und der bestehenden Kunst der Steganographie darin besteht, Information mit minimaler Wahrnehmbarkeit in Dateien zu platzieren. Die spezifischen Mittel für das Einbetten und die Verwendung dieser vergrabenen Information weichen von diesem Punkte aus ab.

[0009] Ein weiterer angeführter Literaturhinweis ist das an Melen erteilte US-Patent 5 325 167. Als Hilfeleistung für die Echtheitsprüfung eines gegebenen Dokuments enthüllt eine hochgenaue Abtastung dieses Dokuments Muster und eine "mikroskopische Kornstruktur", die anscheinend eine Art eindeutigen Fingerabdrucks für die zugrundeliegenden Dokumentenmedien wie das Papier selbst oder nachträglich aufgebrachte Materialien wie den Toner ist. Melen lehrt ferner, dass das Abtasten und Speichern dieses Fingerabdrucks später zur Authentifizierung verwendet werden kann, indem ein mutmassliches Dokument abgetastet und mit dem ursprünglichen Fingerabdruck verglichen wird. Die Anmelderin weiss von einer ähnlichen Idee, die bei der sehr hochgenauen Aufzeichnung von Kreditkarten-Magnetstreifen eingesetzt wird, wie im Wall Street Journal, Seite B1, vom 8. Februar 1994 berichtet, wobei sehr feine magnetische Schwankungen dazu tendieren, von einer Karte zur nächsten eindeutig zu sein, so dass eine Authentifizierung von Kreditkarten durch vorausgehende Aufzeichnung dieser Schwankungen und späteren Vergleich mit Aufzeichnungen der angeblich gleichen Kreditkarte erreicht werden kann.

[0010] Beide der vorangehenden Verfahren beruhen anscheinend auf denselben Identifizierungsprinzipien, auf der die reife Wissenschaft der Fingerabdruckanalyse beruht, nämlich der innewohnenden Eindeutigkeit irgendeiner örtlichen physikalischen Eigenschaft. Diese Verfahren bauen dann auf eine einzelne Beurteilung und/oder Messung der "Ähnlichkeit" oder "Korrelation" zwischen einem verdächtigten Dokument und einer im voraus aufgezeichneten Originalkopie. Obwohl die Fingerabdruckanalyse dieses Verfahren zu einer grossen Kunstfertigkeit erhoben hat, bleiben sie dennoch anfechtbar gegenüber einer Behauptung, dass Musteraufbereitungen und das "Filtern" und die "Scannervorschriften" des Melenschen Patents unvermeidbar dazu tendieren, die daraus folgende Beurteilung der Ähnlichkeit systematisch in einer Richtung zu beeinflussen und ein esoterischeres "Gutachterzeugnis" erforderlich machen könnten, um das Vertrauen in eine gefundene Übereinstimmung oder Nichtübereinstimmung zu begründen. Es ist ein Ziel der vorliegenden Erfindung, diesen Verlass auf Gutachterzeugnis zu vermeiden und das Vertrauen in eine Übereinstimmung in die einfache, gewöhnliche Sprache von "Kopf oder Zahl" zu übersetzen, d. h., was sind die Chancen, dass man die richtige Seite der geworfenen Münze 16mal hintereinander richtig vorhersagen kann. Bei Versuchen, Bruckstücke eines Fingerabdrucks, Dokuments usw. zu identifizieren, wird diese Streitfrage des Vertrauens in eine Beurteilung noch verschärft, wobei es ein Ziel der vorliegenden Erfindung ist, das intuitive "Kopf oder Zahl"-Vertrauen auf das kleinstmögliche Bruchstück anzuwenden. Es sollte sich auch als eine recht grosse wirtschaftliche Unternehmung erweisen, wenn man für all und jedes Dokument, für all und jeden Kreditkarten-Magnetstreifen eindeutige Fingerabdrücke speichern und diese für spätere Gegenüberstellung schnell verfügbar halten wollte. Es ist ein Ziel der vorliegenden Erfindung, eine "Wiederverwendung" von Störungscodes und von "Schnee" zum Vorteil leichterer Speichererfordernisse zu ermöglichen.

[0011] In dem Shiang und Mitautoren erteilten US-Patent 4 921 278 wird eine Art von räumlichem Verschlüs-

selungsverfahren gelehrt, wobei eine Unterschrift oder eine Fotografie zu einem Signal ausgespreizt wird, das dem ungeübten Auge als Rauschen erscheinen würde, in Wirklichkeit aber eine als Moiré bezeichnete, wohldefinierte Struktur ist. Die Ähnlichkeiten zwischen der vorliegenden Erfindung und Shiangs System liegen anscheinend in der Verwendung von rauschähnlichen Muster, die dennoch Information beinhalten, sowie die Verwendung dieses Prinzips auf Kreditkarten und anderen Kennkarten.

[0012] Andere unter den zitierten Patenten beschäftigen sich mit anderen Verfahren zur Identifizierung und/oder Authentifizierung von Signalen oder Medien. Das Hyatt erteilte US-Patent 4 944 036 scheint auf die vorliegende Erfindung nicht zuzutreffen, vermerkt jedoch, das die Bezeichnung "Signatur" gleichermassen auf Signale angewendet werden kann, die eindeutige, auf einer physikalischen Struktur beruhende Merkmale beinhalten.

[0013] Trotz der voranstehenden und verschiedener anderer Arbeiten auf dem Gebiet der Identifizierung und Authentifizierung verbleibt immer noch ein Bedarf für eine zuverlässige und wirksame Methode, zwischen einer Kopie eines ursprünglichen Signals und dem ursprünglichen Signal eine positive Identifizierung zu leisten. Es wäre erwünscht, wenn diese Methode nicht nur eine Identifizierung leistete, sondern auch in der Lage wäre, Information zur Quellenversion zu liefern, um den Verkaufsort genauer zu erkennen. Die Methode sollte die innewohnende Qualität des verkauften Materials nicht aufs Spiel setzen, wie es durch das Einsetzen von lokalen Emblems auf Bildern geschieht. Die Methode sollte robust sein, so dass eine Identifizierung sogar dann erfolgen kann, wenn Kopien mehrfach erfolgt sind und/oder eine Kompression und Dekompression des Signals stattgefunden hat. Die Kennungsmethode sollte weitgehend unlöschbar und "unknackbar" sein. Die Methode sollte sogar mit Bruchstücken des ursprünglichen Signals wie zum Beispiel einem zehnsekundigen "Riff" eines Audiosignals oder mit dem "herausgeschnittenen und eingefügten" Unterabschnitt eines ursprünglichen Bildes funktionieren können.

[0014] Die Existenz einer solchen Methode hätte tiefgreifende Folgen für Piraterie, indem diese a) nicht autorisierte Nutzungen von Material kostenwirksam überwachen und "Schnellprüfungen" durchführen könnte; b) ein Abschreckungsmittel gegen nicht autorisierten Nutzungen werden könnte, wenn bekannt ist, dass die Methode im Einsatz ist, und die Konsequenzen gut bekannt gemacht worden sind; und c) in Rechtsstreitigkeiten eindeutigen Identitätsnachweis ähnlich wie bei einer Fingerabdruckidentifizierung liefern kann, und zwar mit potenziell höherer Zuverlässigkeit als ein Fingerabdruckverfahren.

[0015] Gemäss einer beispielhaften Ausführungsform der Erfindung, die in Anspruch 1 definiert ist, werden das vorstehende und zusätzliche Ziele durch Einbettung eines nicht wahrnehmbaren Kennungscodes in die Gesamtheit eines Quellensignals erreicht. In einer bevorzugten Ausführungsform wird dieses Einbetten durch codierte Modulierung des Quellensignals mit einem kleinen Rauschsignal erreicht. Genauer werden Bits eines binären Kennungscodes jeweils einzeln verglichen, um die Modulation des Quellensignals mit dem Rauschsignal zu steuern.

[0016] Die Kopie mit dem eingebetteten Signal (die "codierte" Kopie) wird zum Verkaufsmaterial, während das Original an einem sicheren Ort verwahrt wird. Die neue Kopie ist mit dem Original nahezu identisch, ausser bei allergenauester Untersuchung; somit ist ihr Handelswert nicht gefährdet. Nachdem die neue Kopie verkauft und verbreitet und potenziell durch Mehrfachkopien verzerrt worden ist, beschreibt die vorliegende Offenbarung im Detail die Verfahren, mit denen jegliches Verdachtssignal gegenüber dem Original positiv identifiziert werden kann.

[0017] Unter den weiteren Vorteilen ist es, weil die bevorzugten Ausführungsformen Kennungssignale verwenden, die global (holographisch) sind und natürliche Rauschquellen nachahmen, möglich, die Energie des Kennungssignals zu maximieren, im Gegensatz zu der Situation, in der dieses Signal nur 'irgendwo im ursprünglichen Material' vorliegt. Dadurch kann die Kennungscodierung angesichts der Tausende von Degradationsprozessen und Stoffumwandlungen der wirklichen Welt wie zum Beispiel des Ausschneidens und Beschneidens von Bildern umso robuster sein.

[0018] Die vorstehenden und weiteren Merkmale und Vorteile der vorliegenden Erfindung, werden aus der folgenden detaillierten Beschreibung derselben klarer hervorgehen, die unter Bezugnahme auf die beigefügten Zeichnungen erfolgt.

Kurze Beschreibung der Zeichnungen

[0019] Fig. 1 ist eine einfache und klassische Abbildung eines eindimensionalen digitalen Signals, das ent-

lang beider Achsen diskretisiert wurde.

[0020] Fig. 2 ist eine allgemeine Übersicht des Verfahrens, ein "nicht wahrnehmbares" Kennungssignal in ein anderes Signal einzubetten, mit eingehender Beschreibung der Verfahrensschritte.

[0021] Fig. 3 ist eine schrittweise Beschreibung, wie eine verdächtigte Kopie eines Originals identifiziert wird.

[0022] Fig. 4 ist eine schematische Ansicht eines Geräts zur Vorausbelichtung von Film mit Kenndaten gemäss einer weiteren Ausführungsform der vorliegenden Erfindung.

[0023] Fig. 5 ist ein Diagramm einer "Blackbox"-Ausführungsform der vorliegenden Erfindung.

[0024] Fig. 6 ist ein schematisches Blockdiagramm der Ausführungsform der Fig. 5.

[0025] Fig. 7 zeigt eine Variante der Ausführungsform von Fig. 6, die dafür eingerichtet ist, aufeinanderfolgende Sätze von Eingangsdaten mit unterschiedlichen Codewörtern, aber den gleichen Rauschdaten zu verschlüsseln.

[0026] Fig. 8 zeigt eine Variante der Ausführungsform von Fig. 6, die dafür eingerichtet ist, jedes Bild einer auf Videoband aufgenommenen Produktion mit einer eindeutigen Codenummer zu verschlüsseln.

[0027] Fig. 9A bis Fig. 9C sind Darstellungen einer Industriestandard-Rauschsekunde, die in einer Ausführungsform der vorliegenden Erfindung verwendet werden kann.

[0028] Fig. 10 zeigt eine für den Nachweis von Standard-Rauschcodes verwendete integrierte Schaltung.

[0029] Fig. 11 zeigt einen Prozessablauf zum Nachweis eines Standard-Rauschcodes, der in der Ausführungsform von Fig. 10 verwendet werden kann.

[0030] Fig. 12 ist eine Ausführungsform, die eine Mehrzahl von Detektoren gemäss einer weiteren Ausführungsform der vorliegenden Erfindung verwendet.

Eingehende Beschreibung

[0031] In der folgenden Erörterung einer veranschaulichenden Ausführungsform werden die Wörter "Signal" und "Bild" austauschbar verwendet, um sowohl eine wie auch zwei und sogar mehr als zwei Dimensionen des digitalen Signals zu bezeichnen. Beispiele werden routinemässig zwischen einem eindimensionalen digitalen Signal des Audiotyps und einem zweidimensionalen digitalen Signal des Bildtyps hin- und herwechseln.

[0032] Um eine veranschaulichende Ausführungsform der Erfindung in allen Einzelheiten zu beschreiben, müssen zuerst die grundlegenden Eigenschaften eines digitalen Signals beschrieben werden. Fig. 1 zeigt eine klassische Darstellung eines eindimensionalen digitalen Signals. Die x-Achse definiert die Indexzahlen der Folge von digitalen "Mustern", während die y-Achse der augenblicklichen Wert des Signals an diesem Muster ist, der nur in Gestalt einer endlichen Anzahl von als die "binäre Tiefe" eines digitalen Musters definierten Niveaus existieren darf. Das in Fig. 1 abgebildete Beispiel hat einen Wert von 2 zur vierten Potenz oder "vier Bits", was 16 erlaubte Zustände des Musterwerts ergibt.

[0033] Für Audiodaten wie zum Beispiel Klangwellen wird gemeinhin akzeptiert, dass der Digitalisierungsprozess ein kontinuierliches Phänomen sowohl im Zeitbereich wie im Signalpegelbereich diskretisiert. Der Digitalisierungsvorgang als solcher bringt insofern eine grundsätzliche Fehlerquelle ins Spiel, als damit keine Details aufgezeichnet werden können, die kleiner als die Diskretisierungsintervalle in jedem der beiden Bereiche sind. In der Industrie wird dies unter anderem als "Aliasing" im Zeitbereich und als "Quantisierungsrauschen" im Signalpegelbereich bezeichnet. Daher wird ein digitales Signal immer und grundsätzlich einen Hintergrundfehler haben. Reines Quantisierungsrauschen, im Sinne eines quadratischen Mittelwertes gemessen, hat bekanntermassen einen theoretischen Wert von eins geteilt durch die Quadratwurzel von zwölf oder etwa 0,29 DN, wo DN die 'Digital Number' (digitale Zahl) oder die kleinste Inkrementeinheit des Signalpegels ist. Zum Beispiel hat ein vollkommener 12-Bit-Digitalisierer 4096 erlaubte DN mit einem innewohnenden Effektivwert des Hintergrundgeräuschs von ~0.29 DN.

[0034] Alle bekannten physikalischen Messvorgänge fügen der Umwandlung eines kontinuierlichen Signals

in die digitale Form zusätzliches Rauschen hinzu. Das Quantisierungsrauschen addiert sich typischerweise in Quadratur (Quadratwurzel der mittleren Quadrate) zum "Analograuschen" des Messvorgangs, wie es manchmal bezeichnet wird.

[0035] Bei fast allen kommerziellen und technischen Vorgängen wird die Decibelskala als ein Mass für Signal und Rauschen in einem gegebenen Aufzeichnungsmedium verwendet. Der Ausdruck "Signal-Rausch-Verhältnis" wird allgemein benutzt, wie er auch in dieser Offenbarung benutzt werden wird. Zum Beispiel werden in dieser Offenbarung Signal-Rausch-Verhältnisse als Signalleistung und Rauschleistung ausgedrückt, somit stellen 20 dB eine zehnfache Zunahme der Signalamplitude dar.

[0036] Zusammengefasst wird durch die derzeit bevorzugten Ausführungsformen der Erfindung ein N-Bit-Wert durch Hinzufügen eines Verschlüsselungssignals sehr niedriger Amplitude, das wie reines Rauschen aussieht, in ein ganzes Signal eingebettet. Gewöhnlich beträgt N wenigstens acht und ist nach oben hin mit Rücksicht auf das schlussendliche Signal-Rausch-Verhältnis und "Bitfehler" beim Lesen und Entschlüsseln des N-Bit-Wertes begrenzt. Praktisch wird N nach anwendungsspezifischen Betrachtungen ausgewählt, wie zum Beispiel der Anzahl von eindeutigen, verschiedenen "Signaturen", die gewünscht werden. Zur Veranschaulichung beträgt, wenn N = 128, die Anzahl von eindeutigen digitalen Signaturen mehr als 10^{38} (2^{128}). Es darf angenommen werden, dass diese Zahl mehr als ausreichend ist, um sowohl das Material mit genügender statistischer Sicherheit zu identifizieren wie auch genaue Verkaufs- und Vertriebsdaten zu indizieren.

[0037] Die Amplitude oder Leistung dieses hinzugefügten Signals wird durch ästhetische und informatorische Betrachtungen jeder gegebenen, die vorliegende Methodologie verwendende Anwendung bestimmt. Zum Beispiel kann nicht-professionelles Video einen höheren eingebetteten Signalpegel vertragen, ohne für das durchschnittliche Menschenauge bemerkbar zu werden, während hochpräzises Audio nur einen verhältnismässig niedrigen Signalpegel aufnehmen kann, wenn das menschliche Ohr nicht eine unangenehme Zunahme des "Zischens" wahrnehmen soll. Diese Feststellungen sind allgemeiner Art, während jede Anwendung ihren eigenen Satz von Kriterien für die Auswahl des Signalpegels des eingebetteten Kennungssignals hat. Je höher der Pegel des eingebetteten Signals, desto stärker entstellte Kopien können noch identifiziert werden Andererseits, je höher der Pegel des eingebetteten Signals, desto unangenehmer könnte das wahrgenommene Rauschen werden und möglicherweise den Wert des vertriebenen Materials beeinträchtigen.

[0038] Um den Umfang der verschiedenen Anwendungen zu veranschaulichen, in denen die Grundsätze der vorliegenden Erfindungen angewendet werden können, geht die vorliegende Beschreibung auf zwei verschiedene Systeme ein. Das erste (in Abwesenheit eines besseren Namens als ein "Batch-Verschlüsselungs"system bezeichnet) wendet Kennungscodierung auf ein existierendes Datensignal an. Das zweite (in Abwesenheit eines besseren Namens als ein "Echtzeit-Verschlüsselungs"system bezeichnet) wendet Kennungscodierung auf ein Signal an, während dieses erzeugt wird. Der Fachmann wird erkennen, dass die Grundsätze der vorliegenden Erfindung über die hier insbesondere beschriebenen Situationen hinaus in einer Anzahl weiterer Situationen angewendet werden können.

[0039] Die Erörterungen dieser beiden Systeme können in beliebiger Reihenfolge gelesen werden. Für einige Leser mag das letztere intuitiver als das erstere sein, für andere mag das Gegenteil zutreffen.

BATCHVERSCHLÜSSELUNG

[0040] Der folgenden Diskussion einer ersten Klasse von Ausführungsformen wird am besten ein Abschnitt vorangestellt, in dem die massgeblichen Bezeichnungen definiert werden.

[0041] Das ursprüngliche Signal bezieht sich entweder auf das ursprüngliche digitale Signal oder auf die digitalisierte Kopie hoher Qualität eines nicht-digitalen Originals.

[0042] Das N-Bit-Kennwort bezieht sich auf einen eindeutigen binären Kennungswert, bei dem N typischerweise irgendwo im Bereich von 8 bis 128 liegt und der der schlussendlich über den offenbarten Umwandlungsprozess in das ursprüngliche Signal platzierte Kennungscode ist. In der veranschaulichten Ausführungsform beginnt jedes N-Bit-Kennwort mit der Wertefolge '0101', die dazu verwendet wird, eine Optimierung des Signal-Rausch-Verhältnisses in der Identifizierungsprozedur eines verdächtigten Signals (siehe Definition weiter unten) zu veranlassen.

[0043] Der Wert des m-ten Bits des N-Bit-Kennwortes ist entweder eine Null oder eine Eins, die dem Wert der m-ten Stelle, von links nach rechts gelesen, des N-Bit-Wortes entspricht. Zum Beispiel ist der Wert des ersten

(m = 1) Bits des Kennworts 01110100 mit N = 8 der Wert '0'; der Wert des zweiten Bits dieses Kennwortes ist '1', usw..

[0044] Das m-te individuelle eingebettete Codesignal bezieht sich auf ein Signal, das in seinen Abmessungen und in seiner Ausdehnung dem ursprünglichen Signal genau gleicht (zum Beispiel sind beide ein 512 × 512-Digitalbild) und (in der veranschaulichten Ausführungsform) eine unabhängige pseudo-zufällige Folge von digitalen Werten ist. "Pseudo" huldigt der Schwierigkeit, reine Zufälligkeit philosophisch zu definieren, und zeigt auch an, dass verschiedene akzeptable Möglichkeiten existieren, das "zufällige" Signal zu erzeugen. Mit jedem gegebenen ursprünglichen Signal werden genau N individuelle eingebettete Codesignale verbunden sein.

[0045] Der annehmbare wahrgenommene Rauschpegel bezieht sich auf eine anwendungsspezifische Festlegung, wieviel "zusätzliches Rauschen", d. h., wieviel Amplitude des nachstehend beschriebenen, zusammengesetzten eingebetteten Codesignals zum ursprünglichen Signal hinzugefügt werden können, damit noch ein akzeptables Signal verkauft oder anderweit vertrieben werden kann. In dieser Offenbarung wird eine Rauscherhöhung von 1 dB als typischer Wert verwendet, der akzeptabel sein könnte, jedoch ist dies ziemlich willkürlich.

[0046] Das zusammengesetzte eingebettete Codesignal bezieht sich auf das Signal, das in seinen Abmessungen und in seiner Ausdehnung genau dem ursprünglichen Signal entspricht (d. h. beide sind ein digitales 512×512-Bild) und die Hinzufügung und passende Abschwächung der N individuellen eingebetteten Codesignale enthält. Die individuellen eingebetteten Signale werden in einem willkürlichen Massstab erzeugt, aber die Amplitude des zusammengesetzten Signals darf nicht den vordefinierten annehmbaren, wahrnehmbaren Rauschpegel übersteigen, daher die Notwendigkeit einer "Abschwächung" der N hinzugefügten individuellen Codesignale.

[0047] Das vertriebsfähige Signal bezieht sich auf die nahezu ähnliche Kopie des ursprünglichen Signals, das aus dem ursprünglichen Signal und dem zusammengesetzten eingebetteten Codesignal besteht. Dieses ist das in der Aussenwelt vertriebene Signal, das nur geringfügig höhere, aber akzeptable "Rauscheigenschaften" als das Original hat.

[0048] Ein verdächtigtes Signal bezieht sich auf ein Signal, das die allgemeine Erscheinungsform des ursprünglichen und vertriebenen Signals hat, aber dessen mögliche Identifizierungs-Übereinstimmung mit dem Original in Frage gestellt wird. Das verdächtigte Signal wird dann analysiert, um zu sehen, ob Übereinstimmung mit dem N-Bit-Kennwort besteht.

[0049] Die genaue Methodologie dieser ersten Ausführungsform beginnt damit festzustellen, dass das N-Bit-Kennwort im ursprünglichen Signal verschlüsselt wird, indem jeder seiner m Bitwerte mit den entsprechenden individuellen verschlüsselten Codesignalen multipliziert, das sich ergebende Signal im zusammengesetzten Signal angesammelt, das voll aufaddierte zusammengesetzte Signal dann auf die annehmbare, wahrgenommene Rauschamplitude abgeschwächt und das sich ergebende zusammengesetzte Signal zum ursprünglichen Signal hinzugefügt wird, um zu dem vertriebsfähigen Signal zu werden.

[0050] Das ursprüngliche Signal, das N-Bit-Kennwort und alle N individuellen eingebetteten Codesignale werden dann an einen gesicherten Ort gebracht und dort verwahrt. Sodann wird ein verdächtiges Signal gefunden. Dieses Signal hat vielleicht vielfaches Kopieren, Kompressionen und Dekompressionen, ausschnittweises Aufbringen auf verschieden beabstandete digitale Signale, Umwandlungen von digital nach analog und zurück auf digitale Medien oder irgendeine Kombination dieser Vorgänge erlitten. SOFERN das Signal immer noch dem Original ähnelt, d. h. seine innewohnende Qualität nicht durch all diese Umwandlungen und Rauschhinzufügungen völlig zerstört ist, dann sollte je nach den Signal-Rausch-Eigenschaften des eingebetteten Signals der Identifizierungsvorgang mit einem bestimmten objektiven Grad von statistischem Vertrauen funktionieren. Das Ausmass von Entstellung des verdächtigten Signals und der ursprüngliche, akzeptable wahrnehmbare Rauschpegel sind zwei Schlüsselparameter, die eine erwartete statistische Sicherheit der Identifizierung bestimmen.

[0051] Der Identifizierungsprozess am verdächtigten Signal beginnt mit einer erneuten Stichprobennahme und Ausrichtung des verdächtigten Signals auf das digitale Format und die Ausdehnung des ursprünglichen Signals. Wenn zum Beispiel ein Bild um einen Faktor von zwei verkleinert worden ist, dann muss es digital um denselben Faktor vergrössert werden. Desgleichen muss, wenn ein Stück Musik "herausgeschnitten" worden ist, aber vielleicht noch die gleiche Abtastrate wie das Original hat, dieses ausgeschnittene Stück mit dem Original zur Deckung gebracht werden, was typischerweise dadurch geschieht, indem eine lokale digitale Quer-

korrelation der beiden Signale ausgeführt wird (was eine übliche digitale Operation ist), festgestellt wird, bei welchem Verzögerungswert die Korrelation ein Maximum erreicht, und dann dieser gefundene Verzögerungswert dazu verwendet wird, das ausgeschnittene Stück mit einem Segment des Originals zur Deckung zu bringen.

[0052] Nachdem das verdächtigte Signal über die Abtastabstände mit dem Original in Übereinstimmung und Deckung gebracht worden ist, sollten die Signalpegel des verdächtigten Signals im Sinne eines Effektivwertes mit dem Signalpegel des Originals in Übereinstimmung gebracht werden. Das kann durch eine Suche nach den Parametern für Versetzung, Verstärkung und Gamma erfolgen, die durch Verwendung der kleinsten Standardabweichung zwischen den beiden Signalen als Funktion der drei Parameter optimiert wird. An diesem Punkt nennen wir das verdächtigte Signal normalisiert und zur Deckung gebracht, oder bequemer einfach normalisiert.

[0053] In dem frisch zur Übereinstimmung gebrachten Paar wird nun das ursprüngliche Signal vom normalisierten verdächtigten Signal abgezogen, um ein Differenzsignal zu erzeugen. Das Differenzsignal wird dann mit jedem der N individuellen eingebetteten Codesignale querkorreliert, und der höchste Querkorrelationswert wird notiert. Der erste Vierbitcode ('0101') wird als ein Kalibrator sowohl auf die Mittelwerte des Nullwertes wie auf die des Einswertes angewendet, und er wird ferner zur weiteren Deckung der beiden Signale verwendet, sofern ein kleineres Signal-Rausch-Verhältnis gewünscht wird (i. e., die optimale Trennung des 0101-Signals zeigt eine optimale Deckung der beiden Signale an, und sie zeigt auch die wahrscheinliche Existenz des N-Bit-Kennungssignals an).

[0054] Die sich ergebenden höchsten Querkorrelationswerte bilden dann eine verrauschte Reihe von Gleitkommazahlen, die durch ihre Nähe zu den Mittelwerten von 0 und 1, die durch die 0101-Kalibrierfolge gefunden worden sind, in Nullen und Einsen umgewandelt werden können. Wenn das verdächtigte Signal tatsächlich vom Original abgeleitet worden ist, dann stimmt die sich aus dem obigen Prozess ergebende Kennnummer mit dem N-Bit-Kennwort des Originals überein, wobei entweder vorhergesagte oder unbekannte "Bitfehler"-Statistik zu berücksichtigen ist. Es folgt aus Signal-Rausch-Betrachtungen, ob irgendeine Art von 'Bitfehler" im Identifizierungsprozess vorliegt, was zu einer Identifizierungswahrscheinlichkeit in Gestalt von X% führt, wobei für X ein Wert von 99.9 oder was auch immer erwünscht sein könnte. Falls die verdächtigte Kopie tatsächlich keine Kopie des Originals ist, dann wird eine im wesentlichen zufällige Folge von Nullen und Einsen erzeugt, und eine Trennung zwischen den sich ergebenden Werten scheint nicht zu existieren. Damit soll gesagt sein, dass bei Auftragung der sich ergebenden Werte in einem Histogramm das Vorhandensein des N-Bit-Kennungssignals starke Doppelniveau-Eigenschaften zeigt, während das Nichtvorhandensein des Codes oder das Vorhandensein eines anderen Codes von einem anderen Signal eine Art von zufälliger Gaussscher Verteilung zeigt. Diese Trennung im Histogramm sollte allein schon für eine Identifizierung ausreichen, aber es ist ein noch strengerer Beweis für eine Identifizierung, wenn eine exakte binäre Sequenz objektiv reproduziert werden kann.

Spezifisches Beispiel

[0055] Angenommen, wir haben ein wertvolles Bild zweier Staatsoberhäupter bei einer Cocktailparty aufgenommen, also Bilder, für die im Handel mit Sicherheit ein vernünftiges Honorar erhalten werden kann. Wir wünschen dieses Bild zu verkaufen und zu gewährleisten, dass es nicht in einer nicht autorisierten oder nicht vergüteten Art und Weise verwendet wird. Dies, und die nachfolgenden Schritte, sind in **Fig. 2** zusammengefasst.

[0056] Angenommen, das Bild sei in einen Farbpositivabzug umgewandelt worden. Zuerst wird dieser mit einem normalen Schwarzweiss-Scanner hoher Qualität mit typischer spectrophotometrischer Empfindlichkeitskurve zu einer digitalisierten Form abgetastet. (Es ist möglich, am Ende bessere Signal-Rausch-Verhältnisse zu erhalten, wenn die Abtastung in jeder der drei Primärfarben des Farbbilds erfolgt, aber diese Feinheit ist für die Beschreibung des zugrundeliegenden Prozesses nicht von zentraler Bedeutung.)

[0057] Wir nehmen an, dass das abgetastete Bild nunmehr zu einem monochromen digitalen Bild aus 4000×4000 Pixeln mit einer durch 12-Bit-Grauwerte oder 4096 erlaubte Niveaus definierten Grauskalengenauigkeit wird. Wir bezeichnen dieses als das "ursprüngliche digitale Bild", während wir uns vergegenwärtigen, dass es dasselbe wie unser "ursprüngliches Signal" in den oben gegebenen Definitionen ist.

[0058] Während des Abtastvorgangs haben wir absolutes Schwarz willkürlich als einem digitalen Wert von '30' entsprechend gesetzt. Wir schätzen, dass auf dem ursprünglichen digitalen Bild ein effektives Hintergrundrauschen von 2 Digitalzahlen sowie ein theoretisches Rauschen (in der Industrie als "Schrotrauschen"

bekannt) der Quadratwurzel des Helligkeitswertes eines jeden gegebenen Pixels existiert. Als Formel haben wir

$$<\text{Effektiv-Rauschen}_{n,m}> = qw(4 + (V_{n,m} - 30)) \quad (1)$$

[0059] Hier sind n und m einfache Laufwerte der Zeilen und Spalten des Bildes, die von 0 bis 3999 reichen. Das Zeichen qw steht für Quadratwurzel. V ist die DN eines gegebenen indizierten Pixels im ursprünglichen digitalen Bild. Klammern <> um das Effektiv-Rauschen zeigen lediglich an, dass dies ein erwarteter Durchschnittswert ist, wobei es aber klar ist, dass ein jedes Pixel individuell einen Zufallsfehler hat. So finden wir für einen Pixelwert mit 1200 as der Digitalzahl oder dem "Helligkeitswert", dass sein erwarteter effektiver Rauschwert qw(1204) = 34,70 beträgt, was ziemlich nahe bei 34,64, der Quadratwurzel aus 1200, liegt.

[0060] Wir erkennen weiterhin, dass die Quadratwurzel des innewohnenden Helligkeitswertes eines Pixels nicht genau das ist, was das Auge als ein minimales unangenehmes Rauschen wahrnimmt, daher gelangen wir zu der Formel

$$<\text{Effektives hinzufügbares Rauschen}_{n,m}> = X \cdot qw(4 + (V_{n,m} - 30)^{\wedge}Y) \quad (2)$$

wo X und Y als empirische Parameter hinzugefügt worden sind, die wir anpassen werden, während "hinzufügbares" Rauschen sich auf unseren akzeptablen, wahrnehmbaren Rauschpegel aus den obigen Definitionen bezieht. Wir beabsichtigen nunmehr, experimentell festzustellen, welche genauen Werte von X und Y wir wählen können, aber wir werden das zu dem Zeitpunkt tun, zu dem wir die nächsten Prozessschritte ausführen.

[0061] Der nächste Schritt in unserem Prozess besteht darin, das N in unserem N-Bit-Kennwort auszuwählen. Wir beschliessen, dass ein 16-Bit-Hauptkennungswert mit seinen 65536 möglichen Werten genügend gross ist, um das Bild als unser Bild zu identifizieren, und dass wir nicht mehr als 128 Kopien des Bildes direkt verkaufen werden, die wir dann zu verfolgen wünschen, was sieben Bits und ein achtes Bit für ein ungerades/gerades Addieren der ersten sieben Bits (d. h. eine Fehlerkontrollbit für die ersten sieben) ergibt. Die Gesamtzahl der jetzt erforderlichen Bits beträgt jetzt vier für die 0101-Kalibrierfolge, 16 für die Hauptidentifizierung, acht für die Version und, als Zugabe, weitere vier als ein weiterer Fehlerkontrollwert für die ersten 28 Bits, was 32 Bits für N ergibt. Für die Werte der letzten vier Bits stehen viele industrielle Standard-Fehlerkontrollmethoden zur Auswahl.

[0062] Wir bestimmen nun zufällig die 16-Bit-Hauptkennnummer und finden zum Beispiel 1101 0001 1001 1110; unsere ersten Verkaufsversionen des Originals haben lauter Nullen als Kennzeichen der Version, und die Fehlerkontrollbits werden vorfallen, wo sie können. Wir haben nun unser eindeutiges 32-Bit-Kennwort, das wir in das ursprüngliche digitale Bild einbetten werden.

[0063] Um dies zu tun, erzeugen wir 32 unabhängige, zufällige 4000×4000-Codierbilder für jedes Bit unseres 32-Bit-Kennwortes. Die Art und Weise, wie diese zufälligen Bilder erzeugt werden, ist aufschlussreich. Zahlreiche Möglichkeiten existieren, sie zu erzeugen. Bei weitem die einfachste ist die, die Verstärkung des Abtastgeräts, das benutzt worden war, die ursprüngliche Fotografie abzutasten, hochzufahren, nur dass diesmal ein reines schwarzes Bild als Eingabe verwendet wird und dieses 32mal abgetastet wird. Der einzige Nachteil dieses Verfahrens besteht darin, dass sie eine grosse Menge Speicherplatz benötigt und dass Rauschen mit "festgelegtem Muster" ein Teil jedes unabhängigen "Rauschbildes" ist. Das Rauschen mit festgelegtem Muster kann aber durch normale "Dunkelbild"-Subtraktionsverfahren entfernt werden. Es sei angenommen, dass wir für den Durchschnittswert von absolut Schwarz die digitale Zahl '100' festsetzen, und dass wir statt eines effektiven Rauschens von 2 DN, das bei der normalen Verstärkereinstellung gefunden worden war, nunmehr ein effektives Rauschen von 10 DN um den Mittelwert eines jeden Pixels finden.

[0064] Als nächstes wenden wir ein Raummittenfrequenz-Bandfilter (räumliche Faltung) auf jedes der unabhängigen zufälligen Bilder an, wodurch im wesentlichen die sehr hohen und sehr niedrigen Raumfrequenzen daraus entfernt werden. Wir entfernen die sehr niedrigen Frequenzen, weil einfache, in der realen Welt vorkommende Fehlerquellen wie geometrische Krümmung, Flecken auf Abtasteinrichtungen, falsche Deckung und dergleichen am stärksten bei niederigen Frequenzen zur Geltung kommen, deshalb wollen wir unser Kennungssignal auf höhere Raumfrequenzen konzentrieren, um diese Arten der Entstellungen zu vermeiden. Desgleichen entfernen wir die höheren Frequenzen, weil die vielfache Erzeugung von Kopien eines gegebenen Bildes ebenso wie Umwandlungen durch Kompression und Dekompression dazu neigen, höhere Frequenzen sowieso auszulöschen, so dass es keinen Zweck hat, zu viel Kennungssignal in diese Frequenzen zu legen, wenn sie diejenigen sind, die am meisten dazu neigen, abgeschwächt zu werden. Daher werden unsere neu-

en, gefilterten und unabhängigen Rauschbilder von Raummittenfrequenzen beherrscht. Was die Praxis anlangt, so wird es nützlich sein, weil wir 12-Bit-Werte in unserem Abtastgerät verwenden, den Gleichstromwert wirksam entfernt haben, und unser neues effektives Rauschen geringfügig weniger als 10 Digitalzahlen betragen wird, dies im sich ergebenden Zufallsbild auf einen 6-Bit-Wert zu bringen, der von – 32 über 0 bis 31 reicht.

[0065] Als nächstes addieren wir alle die Zufallsbilder, die eine '1' in ihrem entsprechenden Bitwert des 32-Bit-Kennwortes haben, und sammeln das Ergebnis in einem 16-Bit-Bild aus ganzen Zahlen mit Vorzeichen. Dies ist die unabgeschwächte, nicht skalierte Version des zusammengesetzten, eingebetteten Signals.

[0066] Als nächstes probieren wir visuell, das zusammengesetzte, eingebettete Signal zum ursprünglichen digitalen Bild zu addieren, indem wir Parameter X und Y der Gleichung (2) variieren. In der Formel iterieren wir visuell, um X zu maximieren und gleichzeitig das geeignete Y zu finden:

$$V_{vert;\,n,m} = V_{orig;\,n,m} + V_{zus;\,n,m} \cdot X \cdot qw(4 + V_{orig;\,n,m}\text{^}Y) \qquad (3)$$

wo vert sich auf das vertreibbare Kandidatenbild bezieht, d. h. wir iterieren visuell, um herauszufinden, welches X und Y uns ein akzeptables Bild geben; orig bezieht sich auf den Pixelwert des ursprünglichen Bildes; und zus bezieht sich auf den Pixelwert des zusammengesetzten Bildes. Die n und m indizieren weiterhin die Zeilen und Spalten des Bildes und zeigen an, dass diese Operation an allen 4000×4000 Pixeln ausgeführt wird. Das Symbol V ist die DN eines gegebenen Pixels und eines gegebenen Bildes.

[0067] Wir machen nun die willkürliche Annahme, dass unsere visuellen Prüfungen ergeben haben, dass die Werte von X = 0,025 und Y = 0,6 akzeptabel sind, wenn wir das ursprüngliche Bild mit dem vertreibbaren Kandidatenbild vergleichen. Damit wird gesagt, dass das vertreibbare Bild mit dem "Extrarauschen" in einem ästhetischen Sinne annehmbar nahe an das Original herankommt. Man bemerke, dass, da unsere individuellen Zufallsbilder einen effektiven zufälligen Rauschwert um 10 DN hatten und dass die Summierung von ungefähr 16 dieser Bilder das zusammengesetzte Rauschen auf 40 DN erhöht, der Faktor X von 0,025 das hinzugefügte effektive Rauschen auf etwa 1 DN zurückbringt, d. h. halb soviel wie die Amplitude unseres innewohnenden Rauschens im Original. Das ist etwa 1 dB Rauschverstärkung bei den dunklen Pixelwerten, und entsprechend mehr bei den durch einen Y-Wert von 0,6 modifizierten helleren Werten.

[0068] Mit diesen beiden Werten von X und Y haben wir also nun unsere ersten Versionen einer vertreibbaren Kopie des Originals konstruiert. Andere Versionen werden lediglich mit einem neuen zusammengesetzten Signal arbeiten und möglicherweise, wenn als nötig erachtet, X geringfügig ändern. Wir schliessen nun das ursprüngliche digitale Bild zusammen mit dem 32-Bit-Kennwort für jede Version sowie die 32 unabhängigen zufälligen Vier-Bit-Bilder weg und warten auf unseren ersten Fall einer vermuteten Piraterie unseres Originals. Im Speicher sind das etwa 14 Megabytes für das ursprüngliche Bild und 32·0,5 bytes·16 Millionen = ~256 Megabytes für die individuellen verschlüsselten Zufallsbilder. Für ein einzelnes wertvolles Bild ist das ganz akzeptabel. Einige Ersparnis an Speicherraum kann durch einfache verlustlose Kompression erreicht werden.

Herausfinden einer vermuteten Piraterie unseres Bildes

[0069] Wir verkaufen unser Bild, und einige Monate später finden wir unsere beiden Staatsoberhäupter in genau der Pose, in der wir sie verkauft hatten, anscheinend aus unserem Bild geschnitten und herausgenommen und vor einen anderen, stilisierten Hintergrund platziert. Das neue, "verdächtige" Bild wird, sagen wir, in 100 000 Stück einer gegebenen Zeitschriftennummer gedruckt. Wir gehen nun daran zu bestimmen, ob ein Teil unseres ursprünglichen Bildes tatsächlich in nicht autorisierter Art und Weise verwendet worden ist. **Fig. 3** fasst die Einzelheiten zusammen.

[0070] Der erste Schritt besteht darin, eine Nummer der Zeitschrift zu nehmen, die Seite mit dem Bild herauszuschneiden, dann sorgfältig, aber nicht zu sorgfältig mit einer gewöhnlichen Schere die beiden Figuren aus ihrem Hintergrund herauszuschneiden. Wenn möglich, schneiden wir nur ein zusammenhängendes Stück und nicht die beiden Figuren separat heraus. Wir kleben dieses Stück auf einen schwarzen Hintergrund und tasten es in digitaler Form ab. Als nächstes markieren oder maskieren wir den schwarzen Hintergrund elektronisch, was durch visuelle Betrachtung leicht zu erreichen ist.

[0071] Nun beschaffen wir uns das ursprüngliche digitale Bild aus unserer sicheren Verwahrung, zusammen mit dem 32-Bit-Kennwort und den 32 individuellen eingebetteten Bildern. Wir platzieren das ursprüngliche digitale Bild mit Standard-Bildmanipulations-Software auf unseren Computerbildschirm und schneiden es grob entlang derselben Grenzen aus, wie unsere maskierte Fläche des verdächtigten Bildes, gleichzeitig maskieren

wir es in grob derselben Art. Das Wort "grob" wird benutzt, da ein genaues Ausschneiden nicht nötig ist; es ist lediglich für die Identifizierungsstatistik nützlich, wenn man vernünftig nahe herankommt.

[0072] Als nächstes bringen wir das maskierte, verdächtigte Bild wieder auf den Massstab, in dem es grob mit der Grösse unseres maskierten ursprünglichen digitalen Bildes übereinstimmt, d. h. wir skalieren das verdächtigte Bild digital auf oder ab und bringen es grob mit dem Original zur Deckung. Nachdem wir diese grobe Deckung erreicht haben, überlassen wir die beiden Bilder einem automatisierten Skalier- und Deckungsprogramm. Das Programm stellt eine Suche für die drei Parameter: x-Position, y-Position und Raummassstab, wobei die Güteziffer der mittlere quadratische Fehler zwischen den beiden Bildern ist, die bei irgendeiner gegebenen Massstabvariablen sowie Versetzungen auf der x- und y-Achse zu finden ist. Diese Bildverarbeitungsmethodologie ist ziemlich standardmässig. Typischerweise würde dies mit allgemein glatten Interpolationsverfahren und einer über Pixel hinausgehenden Genauigkeit geschehen. Die Suchmethode kann unter vielen ausgewählt werden, das Simplex-Verfahren ist typisch.

[0073] Nachdem die optimierten Variablen für den Massstab und für die x- und y-Position gefunden worden sind, kommt als nächstes nun eine weitere Suche zur Optimierung des Schwarzniveaus, des Helligkeitsgewinns und des Gammas der beiden Bilder. Die zu benutzende Gütezahl ist wiederum der mittlere quadratische Fehler, und wiederum können die Simplex-Technik oder andere Suchmethodologien können eingesetzt werden, um diese drei Variablen zu optimieren. Nachdem diese drei Variablen optimiert worden sind, wenden wir ihre korrigierten Werte auf das verdächtigte Bild an und richten es genau auf den Pixelabstand und die Maskierung des ursprünglichen digitalen Bildes und seiner Maske aus. Wir können das jetzt die Standard-Maske nennen.

[0074] Der nächste Schritt besteht darin, das ursprüngliche digitale Bild ausschliesslich innerhalb des Bereichs der Standardmaske von dem neu normalisierten, verdächtigten Bild abzuziehen. Dieses neue Bild wird Differenzbild genannt.

[0075] Sodann schreiten wir vorwärts durch alle 32 individuellen, eingebetteten Zufallsbilder, indem wir eine örtliche Querkorrelation zwischen dem maskierten Differenzbild und dem maskierten individuellen, eingebetteten Bild vornehmen. 'Örtlich' bezieht sich auf den Gedanken, dass man nur über einen Versetzungsbereich von ±1 Pixel zwischen den nominellen, während der obigen Suchprozeduren gefundenen Deckungspunkten der beiden Bilder eine Korrelation beginnen muss. Die höchste Korrelation sollte sich sehr nahe am nominellen Deckungspunkt mit einer Versetzung von 0,0 befinden, und wir können die 3×3 Korrelationswerte summieren, um einen Gesamtkorrelationswert für jedes der 32 individuellen Bits unseres 32-Bit-Kennworts zu erhalten.

[0076] Nachdem wir dies für alle 32 Bitstellen und ihre entsprechenden Zufallsbilder getan haben, besitzen wir eine Quasi-Gleitpunktfolge von 32 Werten. Die ersten vier Werte stellen unser Kalibriersignal 0101 dar. Wir bilden nun den Mittelwert aus dem ersten und dritten Gleitpunktwert und nennen diesen Gleitpunktwert '0', und wir bilden den Mittelwert aus dem zweiten und vierten Wert und nennen diesen Gleitpunktwert '1'. Wir durchschreiten dann alle übrigen 28 Bitwerte und ordnen entweder eine '0' oder eine '1' zu, einfach darauf basierend, welchem Mittelwert sie näher liegen. Einfach gesagt, sollte der sich ergebende eingebettete 32-Bit-Code mit dem Code in unseren Aufzeichnungen übereinstimmen, wenn das verdächtigte Bild tatsächlich eine Kopie unseres Originals ist, während wir allgemeine Zufälligkeit erhalten sollten, sofern es keine Kopie ist. Die dritte und vierte Möglichkeit, nämlich, 3) dass es eine Kopie ist, aber nicht mit der Kennungszahl übereinstimmt, und 4) dass es keine Kopie ist, aber übereinstimmt, ergeben sich, im Falle von 3) sofern das Signal-Rausch-Verhältnis des Prozesses abgesackt ist, d. h. wenn das 'verdächtigte Bild' tatsächlich eine sehr schlechte Kopie des Originals ist, und im Falle von 4) im Grunde genommen mit einer Chance von eins in vier Milliarden, da wir eine 32-Bit-Kennnummer verwenden. Falls wir wirklich wegen 4) Sorge haben, können wir einfach durch ein zweites, unabhängiges Labor deren eigene Prüfungen mit einer anderen Number derselben Zeitschrift durchführen lassen. Eine letzte, möglicherweise Overkill-Überprüfung des ganzen Prozesses besteht darin, die Fehler-Prüfbits gegen die Ergebnisse aus den Werten zu überprüfen. In Situationen, in denen das Signal-Rausch-Verhältnis ein mögliches Problem ist, könnten diese Fehlerüberprüfungsbits ohne zu viel Schaden eliminiert werden.

Vorteile

[0077] Nachdem die erste Ausführungsform anhand eines ausführlichen Beispiels voll beschrieben worden ist, ist es zweckmässig, die rationelle Grundlage einiger der Prozessschritte und deren Vorteile zu nennen.

[0078] Die schlussendlichen Vorteile des vorstehenden Prozesses liegen darin, dass eine Kennnummer völlig

unabhängig von der Art und Weise und den Verfahren erhalten wird, mit denen das Differenzbild hergestellt wurde. Damit soll gesagt werden, dass man durch die Art und Weise, wie das Differenzbild hergestellt wird, wie Ausschneiden, zur Deckung bringen, skalieren usw., nicht die Chancen erhöhen kann, eine Kennnummer zu finden, wenn keine existiert; es kann nur das Signal-Rausch-Verhältnis des Identifizierungsprozesses verbessern, wenn eine wirkliche Kennnummer vorhanden ist. Die Verfahren zur Herstellung von Bildern zur Identifizierung können sich voneinander unterscheiden, was sogar die Möglichkeit für mehrfache, unabhängige Methodologien schafft, um zu einer Übereinstimmung zu kommen.

[0079] Die Fähigkeit, eine Übereinstimmung sogar an Teilmengen des ursprünglichen Signals oder Bildes zu erhalten, ist ein Schlüsselpunkt in der heutigen, informationsreichen Welt. Das Ausschneiden und Einblenden sowohl von Bildern wie von Klangauschnitten wird immer üblicher, so dass eine solche Ausführungsform dazu verwendet werden kann, eine Kopie zu entdecken, selbst wenn ursprüngliches Material auf diese Art und Weise entstellt worden ist. Schliesslich sollte das Signal-Rausch-Verhältnis bei der Gegenüberstellung erst dann beginnen, schwierig zu werden, wenn das kopierte Material selbst entweder durch Rauschen oder durch erhebliche Verzerrung erheblich verändert worden ist; aber diese beiden Veränderungen beeinträchtigen auch den kommerziellen Wert dieser Kopie, so dass der Versuch, das System zu vereiteln, nur mit einem riesigen Verlust an kommerziellem Wert erkauft werden kann.

[0080] Ein frühes Konzept dieser Erfindung war der Fall, in dem nur ein einziges "Schneebild" oder Zufallssignal zu einem ursprünglichen Bild hinzugefügt wurde, d. h. der Fall von N = 1. Dieses Signal zu "entschlüsseln" würde eine nachfolgende mathematische Analyse unter Verwendung von (im allgemeinen statistischen) Algorithmen beinhalten, um zu einer Beurteilung zu gelangen, ob dieses Signal vorliegt oder nicht. Dieses Herangehen wurde als bevorzugte Ausführungsform aufgegeben, weil ihm eine Grauzone bezüglich der Gewissheit, die Gegenwart oder Abwesenheit des Signals zu entdecken, anhaftete. Die Erfindung verschob die Frage der Gewissheit aus dem Bereich von fachmännischer statistischer Analyse in den Bereich, ein zufälliges binäres Ereignis wie "Kopf oder Zahl" zu erraten, indem sie zu einer Vielzahl von Bitebenen voranschritt, d. h. N > 1, zusammen mit einfachen, vordefinierten Algorithmen, die die Art und Weise vorschreiben, wie zwischen einer "0" und einer "1" gewählt wird. Das wird als leistungsstarkes Merkmal bezüglich der intuitiven Akzeptanz dieser Erfindung sowohl im Gerichtssaal wie auch auf dem Markt angesehen. Die Analogie, die die Gedanken des Erfinders bezüglich dieser ganzen Frage zusammenfasst, stellt sich wie folgt dar. Die Suche nach einem einzelnen Kennungssignal läuft darauf hinaus, "Kopf oder Zahl" nur ein einziges Mal zu anzusagen und sich auf Fachleute mit Geheimwissen zu verlassen, die Ansage zu machen; während die bevorzugte Ausführungsform dieser Erfindung mit N > 1 auf dem im wesentlichen intuitiven Prinzip beruht, "Kopf oder Zahl" N-mal hintereinander richtig anzusagen. Die Situation, d. h. die Probleme, das Vorhandensein eines einzelnen Signals zu "interpretieren", verschärft sich erheblich, wenn Bilder und Klangausschnitte immer kleiner werden.

[0081] Ein weiterer wichtiger Grund, dass der Fall mit N > 1 die gegenüber dem Fall mit N = 1 bevorzugte Ausführungsform ist, liegt darin, dass im Falle von N = 1 die Art und Weise, in der ein verdächtigtes Bild vorbereitet und manipuliert wird, sich direkt auf die Aussichten auswirkt, eine positive Identifizierung zu erreichen. Somit wird die Art und Weise, in der ein Fachmann eine Identifizierung feststellt, ein integraler Teil dieser Feststellung. Das Vorhandensein einer Vielzahl von mathematischen und statistischen Methoden, diese Feststellung zu treffen, lässt Raum für die Möglichkeit, dass in einigen Prüfungen positive Identifizierungen erreicht werden, während andere zu negativen Identifizierungen führen könnten, was zu weiteren undurchsichtige Erörterungen über die relativen Vorzüge der verschiedenen Herangehensweisen an die Identifizierung einlädt. Die bevorzugte Ausführungsform dieser Erfindung mit N > 1 vermeidet diese weitere Grauzone, indem ein Verfahren vorgestellt wird, wo kein noch so grosser Aufwand bei der Vorverarbeitung eines Signals (ausser derjenigen, die Wissen über die privaten Codesignale unerlaubterweise verwendet) die Aussichten erhöhen kann, "Kopf oder Zahl" N-mal hintereinander anzusagen.

[0082] Das vorliegende System wird seinen vollsten Ausdruck erlangen, wenn es ein Industriestandard wird und zahlreiche unabhängige Gruppen mit ihren eigenen Mitteln oder 'hausgemachten' Marken darangehen, eingebettete Kennnummern anzuwenden und sie zu entziffern. Eine Identifizierung durch zahlreiche unabhängige Gruppen wird die schlussendlich erreichbare Objektivität des Verfahrens weiter steigern und somit auch ihre Anziehungskraft als ein Industriestandard erhöhen.

Verwendung echter Polarität bei der Schaffung des zusammengesetzten eingebetteten Codesignals

[0083] Die vorangehende Diskussion bediente sich des Null- und Eins-Formalismus der Binärtechnik, um ihre Ziele zu erreichen. Genauer werden die Nullen und Einsen des N-Bit-Kennworts direkt mit ihren entsprechenden individuellen eingebetteten Codesignalen multipliziert, um das zusammengesetzte eingebettete Codesig-

nal zu bilden (Schritt 8, Fig. 2). Dieses Herangehen hat sicherlich seine eigene gedankliche Einfachheit, aber die Multiplikation eines eingebetteten Codesignals mit Null und die damit verbundene Speicherung dieses eingebetteten Codes enthalten eine Art von Ineffizienz.

[0084] Bevorzugterweise wird der Formalismus der Null-und-Eins-Natur des N-Bit-Kennwortes beibehalten, wobei aber nun die Nullen des Wortes eine Subtraktion ihres entsprechenden eingebetteten Codesignals hervorrufen. In Schritt 8 der Fig. 2 werden wir also, anstatt nur die individuellen eingebetteten Codesignale "hinzuzufügen", die einer '1' im N-Bit-Kennwort entsprechen, auch diejenigen individuellen eingebetteten Codesignale, die einer '0' im N-Bit-Kennwort entsprechen, 'abziehen'.

[0085] Auf den ersten Blick wird hierdurch mehr Scheinrauschen zum fertigen zusammengesetzten Signal hinzugefügt. Jedoch wird dadurch auch der energetische Abstand der Nullen von den Einsen erhöht, und somit kann die 'Verstärkung', die in Schritt 10 der Fig. 2 angelegt wird, entsprechend niedriger sein.

[0086] Wir können diese Verbesserung als Einsatz echter Polarität bezeichnen. Der Hauptvorteil dieser Verbesserung kann weitgehend als 'informative Effizienz' zusammengefasst werden.

'Wahrnehmungs-Orthogonalität' der individuellen eingebetteten Codesignale

[0087] Die vorangegangene Diskussion sieht die Verwendung von allgemein zufälligen, rauschähnlichen Signalen als individuellen eingebetteten Codesignalen vor. Dies ist vielleicht die einfachste Signalform, die sich erzeugen lässt. Es gibt jedoch eine Form der informativen Optimierung, die auf den Satz von individuellen eingebetteten Signalen angewandt werden kann und die die Anmelderin unter der Überschrift 'Wahrnehmungs-Orthogonalität' beschreibt. Dieser Ausdruck basiert lose auf dem mathematischen Konzept der Orthogonalität von Vektoren, aber hier mit der zusätzlichen Anforderung, dass diese Orthogonalität die Signalenergie der Daten zur Identifizierung maximieren sollte, während diese unterhalb einer gewissen Wahrnehmbarkeitsschwelle gehalten werden. Anders ausgedrückt, brauchen die eingebetteten Codesignals nicht notwendigerweise von zufälliger Natur sein.

Verwendung und Verbesserung der ersten Ausführungsform auf dem Gebiet der Emulsionsfilmfotografie

[0088] Die vorangehende Diskussion hat Methoden dargelegt, die auf fotografische Materialien anwendbar sind. Der folgende Abschnitt erforscht die Einzelheiten dieses Gebiets weiter und offenbart bestimmte Verbesserungen, die sich für einen breiten Anwendungsbereich eignen.

[0089] Das erste zu erörternde Gebiet umfasst die Vorausanwendung oder Vorausbelichtung einer Seriennummer auf herkömmliche fotografische Produkte wie Negativfilm, Papier für Abzüge, Diapositive usw. Dies ist allgemein eine Methode, um a priori eindeutige Seriennummern (und implizit auch Eigentümer- und Spureninformation) auf fotografische Materialien aufzubringen. Die Seriennummern selbst wären, im Gegensatz zu einer Verbannung auf die Ränder oder einem Aufdruck auf der Rückseite eines fotografischen Abzugs, die zum Kopieren alle einen getrennten Ort und ein separates Verfahren erfordern, ein bleibender Bestandteil des normal belichteten Bildes. Die 'Seriennummer', wie sie hier genannt wird, ist allgemein synonym mit dem N-Bit-Kennwort, nur dass wir jetzt eine üblichere industrielle Terminologie verwenden.

[0090] In Fig. 2, Schritt 11 verlangt die Offenbarung die Speicherung des "Original[bild]s" zusammen mit Codebildern. In Fig. 3, Schritt 9 ordnet sie dann an, dass das Original vom verdächtigten Bild abgezogen werde, wodurch mögliche Kennungscodes and alle möglichen angesammelten Geräusche und Entstellungen zurückbleiben. Die frühere Offenbarung hat also schweigend angenommen, dass ein Original ohne die zusammengesetzten eingebetteten Signale existiert.

[0091] Nun wird dies beim Verkauf von Papier für Abzüge und anderen Filmprodukten für die Vervielfältigung immer noch der Fall sein, d. h. ein "Original" ohne die eingebetteten Codes wird tatsächlich existieren, und die grundlegende Methodologie der ersten Ausführungsform kann verwendet werden. Der Originalfilm dient in vollkommener Weise als 'nichtverschlüsseltes Original'.

[0092] In dem Falle jedoch, wenn vorbelichteter Negativfilm verwendet wird, existiert das zusammengesetzte eingebettete Signal schon im voraus auf dem Originalfilm, und somit wird es niemals ein "Original" getrennt vom voreingebetteten Signal geben. Es ist dieser letzere Fall, der daher etwas näher untersucht werden soll, zusammen mit Betrachtungen, wie die oben diskutierten Prinzipien am besten zu benutzen sind (wobei die ersteren Fälle mit den vorher dargelegten Methoden zusammenhängen).

[0093] Der deutlichste Ausgangspunkt für den Fall eines vornummerierten Negativfilms, d. h. eines Negativfilms, auf dem jedes einzelne Bild mit einem sehr schwachen und eindeutigen, zusammengesetzten eingebetteten Signal vorbelichtet worden ist, liegt beim Schritt 9 der Fig. 3, wie vorher angedeutet. Es gibt bestimmt noch weitere Unterschiede, aber diese sind meistens logistischer Natur, zum Beispiel wie und wann die Signale im Film einzubetten sind, wie die Codenummern und die Seriennummer aufzubewahren sind usw. Die Vorbelichtung von Film würde offensichtlich eine wichtige Veränderung im allgemeinen Massenfertigungsprozess der Filmherstellung und -verpackung beinhalten.

[0094] Fig. 4 umreisst schematisch einen möglichen post-hoc-Mechanismus für die Vorbelichtung von Film. 'Post hoc' besagt, dass ein Prozess angewandt wird, nachdem der volle, übliche Filmfertigungsprozess bereits stattgefunden hat. Grössenbedingte Kostenvorteile könnten bewirken, dass diese Vorbelichtung direkt in die Filmfertigungskette eingefügt wird. In Fig. 4 ist abgebildet, was gemeinhin als ein Filmbeschreibsystem bekannt ist. Der Computer **106** zeigt das in Schritt 8 der Fig. 2 erzeugte zusammengesetzte Signal auf seinem Leuchtschirm an. Ein gegebenes Filmbild wird dann belichtet, indem dieser Leuchtschirm abgebildet wird, wobei das Belichtungsniveau allgemein sehr schwach ist, im allgemeinen nämlich nicht wahrnehmbar. Es ist klar, dass der Markt seine eigenen Forderungen stellen wird, wie schwach dieses sein sollte, d. h. das Niveau von hinzugefügter 'Körnigkeit', wie es der Praktiker ausdrücken würde. Jedes Filmbild wird der Reihe nach belichtet, wobei allgemein das auf der Kathodenstrahlröhre **102** angezeigte, zusammengesetzte Bild für jedes einzelne Filmbild geändert wird, wodurch jedem dieser Filmbilder eine verschiedene Seriennummer gegeben wird. Die Übertragungslinse **104** hebt die konjugierten Brennpunktebenen eines Filmbildes und der Kathodenstrahlröhren-Vorderseite hervor.

[0095] Wir kommen jetzt zurück zur Anwendung der Prinzipien der vorausgehenden Ausführungsform im Falle von vorbelichtetem Negativfilm. Zögen wir in Schritt 9 der Fig. 3 das "Original" mit seinem eingebetteten Code ab, dann würden wir offensichtlich auch den Code "löschen", da der Code ein integrierender Bestandteil des Originals ist. Glücklicherweise existieren Abhilfen, und Identifizierungen sind immer noch möglich. Es wird aber eine Herausforderung für die Fachkräfte, die diese Ausführungsform verfeinern, ein Signal-Rausch-Verhältnis des Identifizierungsprozesses im Falle vorbelichteter Negative zu haben, das dem Signal-Rausch-Verhältnis des Falles nahekommt, in dem ein nicht verschlüsseltes Original existiert.

[0096] Eine kurze Definition des Problems gehört an diese Stelle. Bei Vorliegen eines verdächtigten Bildes (Signals) soll der eingebettete Kennungscode gefunden werden, SOFERN ein Code überhaupt existiert. Das Problem besteht darin, die Amplitude jedes einzelnen, individuellen eingebetteten Codesignals innerhalb des verdächtigten Bildes zu finden, nicht nur im Zusammenhang mit Rauschen und Entstellung, wie früher erläutert, sondern nun auch im Zusammenhang mit der Kopplung zwischen einem eingefangenen Bild und den Codes. 'Kopplung' bezieht sich hier auf die Idee, dass das eingefangene Bild die Querkorrelation "zufällig verschiebt".

[0097] Wenn wir also dieses zusätzliche Element der Signalkopplung berücksichtigen, wird durch den Identifizierungsprozess nunmehr die Signalamplitude jedes einzelnen, individuellen eingebetteten Codesignals beurteilt (im Gegensatz zur Benutzung des Querkorrelations-Ergebnisses des Schritts 12 von Fig. 3). Sofern unser Identifizierungssignal im verdächtigten Bild existiert, werden die so gefundenen Amplituden aufgespalten in eine Polarität mit positiven Amplituden, denen eine Eins zugeordnet wird, und eine mit negativen Amplituden, denen eine Null zugeordnet wird. Unser eindeutiger Kennungscode offenbart sich hier. Falls andererseits kein solcher Kennungscode existiert oder es der Code von Dritten ist, wird eine Gausssche Zufallsverteilung der Amplituden mit einem zufälligen Mischmasch von Werten gefunden.

[0098] Uns bleibt, noch einige weitere Einzelheiten anzuführen, wie die Amplituden der individuellen eingebetteten Codes gefunden werden. Glücklicherweise ist auch genau dieses Problem in anderen technischen Anwendungen bereits behandelt worden. Ausserdem könnte man dieses Problem zusammen mit etwas Essen in ein mit Mathematikern und Statistikern gefülltes Zimmer werfen, und sicherlich käme nach einer vernünftigen Wartezeit ein halbes Dutzend optimierter Methodologien heraus. Es handelt sich um ein ziemlich sauber definiertes Problem.

[0099] Ein spezifisches Beispiel kommt aus dem Gebiet der astronomischen Abbildung. Hier existiert ein reifer Stand der Technik, ein "thermisches Rauschbild" von einem gegebenen CCD-Bild eines Objekts abzuziehen. Jedoch ist oft nicht genau bekannt, welcher Skalierungsfaktor beim Abziehen des thermischen Bildes verwendet werden sollte, und eine Suche nach dem richtigen Skalierungsfaktor wird durchgeführt. Genau das ist die Aufgabe dieses Schritts der vorliegenden Ausführungsform.

[0100] In der allgemeinen Praxis wird lediglich ein gemeinsamer Suchalgorithmus für den Skalierungsfaktor durchgeführt, wobei ein Skalierungsfaktor ausgewählt und ein neues Bild gemäss

NEUES BILD = ERWORBENES BILD – MASSSTAB·THERMISCHES BILD (4)

erzeugt wird.

[0101] Das neue Bild wird einer schnellen Fouriertransformation unterworfen, und irgendwann wird ein Skalierungsfaktor gefunden, der den integrierten Hochfrequenzinhalt des neuen Bildes minimiert. Dieser allgemeine Typ einer Suchoperation mit Minimierung einer spezifischen Grösse ist überaus verbreitet. Der so gefundene Skalierungsfaktor ist die gesuchte "Amplitude". In Betracht gezogene, aber noch nicht umgesetzte Verfeinerungen bestehen darin, die Kopplung der höheren Ableitungen des erworbenen Bildes und der eingebetteten Codes zu beurteilen und vom berechneten Skalierungsfaktor abzuziehen. In anderen Worten liegen bestimmte Verschiebungseffekte aus der vorher erwähnten Kopplung vor und sollten irgendwann sowohl durch theoretische wie auch durch empirische Experimente berücksichtigt und eliminiert werden.

Verwendung und Verbesserungen in der Erfassung von Signal- oder Bildveränderungen

[0102] Neben dem grundsätzlichen Bedürfnis nach Identifizierung eines Signals oder Bildes als Ganzes besteht auch ein ziemlich allgegenwärtiger Bedarf, mögliche Veränderungen an einem Signal oder Bild zu erfassen. Der folgende Abschnitt beschreibt, wie die vorangehende Ausführungsform mit bestimmten Abwandlungen und Verbesserungen als ein leistungsfähiges Werkzeug auf diesem Gebiet verwendet werden kann. Mögliche Szenarios und Anwendungen der Erfassung von Veränderungen sind unzählbar.

[0103] Um zuerst zusammenzufassen, nehmen wir an, ein gegebenes Signal oder Bild zu besitzen, das mit den grundsätzlichen, oben umrissenen Methoden positiv identifiziert worden ist. In anderen Worten kennen wir sein N-Bit-Kennwort, seine individuellen eingebetteten Codesignale und seinen zusammengesetzten eingebetteten Code. Wir können dann ziemlich leicht eine Raumkarte der Amplitude des zusammengesetzten Codes innerhalb unseres gegebenen Signals oder Bildes entwerfen. Des weiteren können wir diese Amplitudenkarte durch die Raumamplitude des bekannten zusammengesetzten Codes teilen, was eine normalisierte Karte ergibt, d. h. eine Karte, die um einen gewissen Gesamtmittelwert herum fluktuieren sollte. Durch einfache Prüfung dieser Karte können wir visuell all diejenigen Bereiche erkennen, die bedeutend verändert worden sind, und worin der Wert der normalisierten Amplitude unter eine gewisse, statistisch festgelegte Schwelle absinkt, die rein auf typischem Rauschen und auf Entstellung (Fehler) beruht.

[0104] Für die Details der Erstellung der Amplitudenkarte besteht eine vielseitige Auswahl. Eine Möglichkeit besteht darin, der gleichen Prozedur zu folgen, die wie oben beschrieben benutzt wird, um die Signalamplitude zu bestimmen, nur dass wir jetzt die Multiplikation jeder gegebenen Fläche des Signals oder Bildes mit einer um die zu untersuchende Fläche herum zentrierte Gausssche Wichtungsfunktion ansetzen und wiederholen.

Universelle im Vergleich zu kundenspezifischen Codes

[0105] In der Offenbarung ist bis hierher umrissen worden, wie jedes einzelne Quellensignal seinen eigenen, eindeutigen Satz von individuellen, eingebetteten Codesignalen hat. Dies bedingt, zusätzlich zum Original eine bedeutende Menge weiterer Codeinformation zu speichern, und viele Anwendungen könnten gwisse Einsparungen verdienen.

[0106] Eine solche Möglichkeit, etwas einzusparen, besteht darin, dass ein gegebener Satz von individuellen, eingebetteten Codesignalen einer Partie von Quellenmaterialien gemein ist. Zum Beispiel können eintausend Bilder alle den gleichen, grundlegenden Satz von individuellen, eingebetteten Signalen verwenden. Die Speicherplatzerfordernisse für diese Codes werden dann zu einem kleinen Bruchteil der Gesamterfordernisse an Speicherplatz für das Quellenmaterial.

[0107] Des weiteren können einige Anwendungen einen universellen Satz von individuellen eingebetteten Codesignalen verwenden, d. h. Codes, die in allen Fällen des vertriebenen Materials die gleichen bleiben. Dieser Typ von Anforderung wäre bei Systemen zu sehen, in denen gewünscht wird, das N-Bit-Kennwort selbst zu verstecken, aber dennoch Standardgerät zu haben, mit dem dieses Wort gelesen werden kann. Das ist für Systeme nützlich, die Ja-nein-Entscheidungen an Lesestandorten treffen. Diese Anordnung hat den potenziellen Nachteil, dass die universellen Codes mehr dazu neigen, aufgespürt oder gestohlen zu werden; sie sind daher nicht so sicher wie die Geräte und Methodologie der vorher offenbarten Anordnung. Vielleicht liegt genau

hier der Unterschied zwischen 'hoher Sicherheit' und 'luftdichter Sicherheit', einer Unterscheidung, die in der grossen Menge potenzieller Anwendungen wenig Bedeutung hat.

Verwendung bei Druck, Papieren, Dokumenten, kunststoffumhüllten ID-Karten und anderen Materialien, wo umfassende eingebettete Codes eingedruckt werden können

[0108] Der Begriff 'Signal' wird oft eng dazu verwendet, digitale Dateninformation, Audiosignale, Bilder usw. zu bezeichnen. Eine breitere Interpretation von 'Signal', die auch allgemeiner angestrebt ist, schliesst alle Arten von Modulation jeglicher Materialien ein. So wird die Mikrotopologie eines Stücks gewöhnlichen Papiers ein 'Signal' (zum Beispiel seine Höhe in Abhängigkeit von der x- und y-Koordinaten). Die Rückstrahleigenschaften eines flachen Kunststoffstücks werden (auch als Raumfunktion) ein Signal. Der springende Punkt ist, dass fotografische Emulsionen, Audiosignale und digitalisierte Information nicht die einzigen Signalarten sind, bei denen die Grundsätze der vorliegenden Erfindung genutzt werden können.

[0109] Zum Beispiel kann eine Maschine, die sehr stark einer Blindenschrift-Druckmaschine ähnelt, so konstruiert werden, dass sie eindeutige 'rauschähnliche' Einkerbungen eindruckt, wie oben umrissen. Diese Einkerbungen können mit einem Druck angebracht werden, der viel kleiner ist als der bei Blindenschrift typisch angewandte, und zwar so viel kleiner, dass die Muster von einem normalen Benutzer des Papiers nicht bemerkt werden. Aber durch Befolgung der Schritte der vorliegenden Offenbarung und ihrer Anwendung via Mikroeinkerbung kann ein eindeutiger Kennungscode auf jedes gegebene Blatt Papier aufgebracht werden, sei es als täglicher Bedarf für Schreibpapier oder für wichtige Dokumente, gesetzliche Zahlungsmittel oder andere gesicherte Materialien bestimmt.

[0110] Das Lesen des Kennungsmaterials in einer solchen Ausführungsform erfolgt allgemein einfach dadurch, dass das Dokument optisch aus einer Auswahl von Gesichtswinkeln gelesen wird. Dies könnte eine billige Methode für die Ableitung der Mikrotopologie von Papieroberflächen werden. Sicher sind auch andere Formen der Ablesung der Papiertopologie möglich.

[0111] Im Falle von kunststoffumhüllten Materialien wie ID-Karten, zum Beispiel Führerscheinen, kann eine ähnliche Maschine zur Herstellung blindenschriftartiger Eindrücke verwendet werden, um eindeutige Kennungscodes einzudrucken. Feine Schichten photoreaktiver Materialien können auch innerhalb des Kunststoffs eingebettet und 'belichtet' werden.

[0112] Es ist klar, dass, wo immer ein Material existiert, das durch 'rauschähnliche' Signale modifiziert werden kann, dieses Material auch ein geeigneter Träger für eindeutige Kennungscodes und für die Nutzung der Prinzipien der Erfindung ist. Es bleibt nur, die Daten zur Identifizierung wirtschaftlich aufzubringen und den Signalpegel unter einer Annehmbarkeitsschwelle zu halten, die in jeder einzelnen Anwendung speziell zu definieren ist.

Anhang A: Beschreibung

[0113] Anhang A enthält den Source-Code einer Realisierung und Überprüfung der vorstehenden Ausführungsform für ein Schwarz-Weiß-Abbildungssystem mit 8 Bit.

ECHTZEITCODIERER

[0114] Während in der ersten Klasse von Ausführungsformen am üblichsten ein Standard-Mikroprozessor oder Computer verwendet wird, um die Codierung eines Bildes oder Signals auszuführen, ist es auch möglich, eine kundenspezifische Codierungsvorrichtung zu nutzen, die vielleicht schneller als ein typischer Prozessor des von Neumann-Typs ist. Ein solches System kann mit allen Arten serieller Datenströme eingesetzt werden.

[0115] Musik- und Videobandaufzeichnungen sind Beispiele für serielle Datenströme, und zwar Datenströme, die oft ohne Erlaubnis kopiert werden. Es würde bei den Vollzugsanstrengungen helfen, wenn autorisierte Aufzeichnungen mit Kennungsdaten codiert wären, so dass illegale Kopien zu dem Original zurückverfolgt werden könnten, von dem sie gemacht worden sind.

[0116] Piraterie ist nur ein Belang, der die Notwendigkeit der vorliegenden Erfindung belegt. Authentifizierung ist eine weitere. Oft ist es wichtig zu bestätigen, dass ein gegebener Datensatz wirklich das ist, was er zu sein den Eindruck macht (und das oft mehrere Jahre nach seiner Herstellung).

[0117] Das System **200** der Fig. 5 kann eingesetzt werden, um diese und weitere Bedürfnisse zu berücksichtigen. System **200** kann als ein schwarzer Kasten **202** für Kennungscodierung angesehen werden. Das System **200** empfängt ein Eingangssignal (manchmal als "Master" oder "nichtverschlüsseltes" Signal bezeichnet) und ein Codewort und erzeugt (allgemein in Echtzeit) ein mit Kennung codiertes Ausgangssignal. (Üblicherweise liefert das System Schlüsseldaten zur Verwendung bei späterer Decodierung.)

[0118] Der Inhalt des "schwarzen Kastens" **202** kann verschiedene Formen annehmen. Ein beispielhaftes Black-Box-System wird in Fig. 6 gezeigt und schliesst eine Nachschlagtabelle **204**, eine digitale Rauschquelle **206**, einen ersten und zweiten Skalierer **208**, **210**, ein Addier-Subtrahier-Glied **212**, einen Speicher **214** und ein Register **216** ein.

[0119] Das Eingangssignal (das in der veranschaulichten Ausführungsform ein mit einer Rate von einer Million Muster pro Sekunde geliefertes Signal aus Daten mit 8 bis 20 Bit ist, aber in anderen Ausführungsformen ein Analogsignal sein könnte, wenn geeignete A/D- und D/A-Wandlung vorgesehen ist) wird von einem Eingang **218** an den Adresseneingang **220** der Nachschlagtabelle **204** angelegt. Für jedes Eingangsmuster (d. h. jede Nachschlagtabellenadresse) liefert die Tabelle ein entsprechendes digitales Ausgangswort aus 8 Bits. Dieses Ausgangswort wird als Skalierfaktor verwendet, der an den einen Eingang des ersten Skalierers **208** angelegt wird.

[0120] Der erste Skalierer **208** hat einen zweiten Eingang, an den ein digitales Rauschsignal aus 8 Bits von der Quelle **206** angelegt wird. (In der veranschaulichten Ausführungsform umfasst die Rauschquelle **206** eine Analograuschquelle **222** und einen Analog-Digital-Wandler **224**, obwohl wiederum andere Ausführungen verwendet werden können.) Die Rauschquelle in der veranschaulichten Ausführungsform hat einen mittleren Ausgangswert von Null bei einer Halbwertsbreite (FWHM) von 50 bis 100 digitalen Zahlen (zum Beispiel von –75 bis +75).

[0121] Der erste Skalierer **208** multipliziert die beiden 8-Bit-Wörter an seinen Eingängen (Skalenfaktor und Rauschen), um – für jedes Muster des Eingangssystems im System – ein 16-Bit-Ausgangwort zu erzeugen. Da das Rauschsignal einen Mittelwert von Null hat, hat der Ausgang des ersten Skalierers gleichermassen einen Mittelwert von Null.

[0122] Der Ausgang des ersten Skalierers **208** wird an den Eingang des zweiten Skalierers **210** angelegt. Der zweite Skalierer dient einer globalen Skalierfunktion, indem er die absolute Grössenordnung des Kennungssignals festlegt, das schlussendlich in das Eingangs-Datensignal eingebettet werden soll. Der Skalierfaktor wird durch eine Skaliersteuervorrichtung **226** festgelegt (diese kann verschiedene Formen annehmen, die von einem einfachen Rheostaten bis zu einer graphisch ausgeführten Steuerung in einer graphischen Benutzerschnittfläche reichen), die es gestattet, dass dieser Faktor in Übereinstimmung mit den Anforderungen der verschiedenen Anwendungen abgeändert werden kann. Der zweite Skalierer **210** liefert an seiner Ausgangsleitung **228** ein skaliertes Rauschsignal. Jedes Muster dieses skalierten Rauschsignals wird nacheinander im Speicher **214** gespeichert.

[0123] (In der veranschaulichten Ausführungsform kann der Ausgang des ersten Skalierers **208** (dezimal) von –1500 bis +1500 reichen, während der Ausgang des zweiten Skalierers **210** bei niedrigen einstelligen Ziffern (zum Beispiel zwischen –2 und +2) liegt)

[0124] Register **216** speichert ein Mehrfachbit-Kennungscodewort. In der veranschaulichten Ausführungsform besteht dieses Codewort aus 8 Bits, obwohl längere Codewörter (mit bis zu Hunderten von Bits) üblicherweise benutzt werden. Diese Bits werden nacheinander einzeln herbeigezogen, um zu prüfen, wie das Eingangssignal mit dem skalierten Rauschsignal moduliert wird.

[0125] Insbesondere wird ein Zeiger **230** nacheinander durch die Bitpositionen des Codeworts im Register **216** geschickt, um ein Steuerbit von "0" oder "1" an einen Steuereingang **232** des Addier-Subtrahier-Gliedes **212** zu liefern. Wenn für ein spezifisches Eingangssignalmuster das Steuerbit eine "1" ist, wird das skalierte Rauschsignalmuster auf der Leitung **232** zum Eingangssignalmuster addiert. Wenn das Steuerbit eine "0" ist, dann wird das skalierte Rauschsignalmuster vom Eingangssignalmuster subtrahiert. Der Ausgang **234** des Addier-Subtrahier-Gliedes **212** liefert das Augangssignal des schwarzen Kastens.

[0126] Die Addition oder Subtraktion des skalierten Rauschsignals entsprechend den Bits des Codeworts bewirkt eine Modulation des Eingangssignals, die allgemein nicht wahrnehmbar ist. In Kenntnis des Inhalts des Speichers **214** kann aber ein Benutzer später die Verschlüsselung decodieren, indem er die im ursprünglichen

Verschlüsselungsprozess verwendete Codenummer bestimmt. (Die Verwendung des Speichers **214** ist, wie unten erklärt, eigentlich wahlfrei.)

[0127] Es ist ersichtlich, dass das verschlüsselte Signal in wohlbekannter Art und Weise vertrieben werden kann, einschliesslich seiner Umwandlung in gedruckte Bilder und seiner Speicherung auf magnetischen Medien (Floppy-Disk, Analog- oder DAT-Band usw.), CD-ROM usw. usw.

Decodieren

[0128] Eine Vielfalt von Verfahren kann benutzt werden, um den Kennungscode zu bestimmen, mit dem ein verdächtigtes Signal verschlüsselt worden ist. Zwei werden hierunter diskutiert. In den meisten Anwendungen ist das erste weniger bevorzugt als das zweite, wird aber hierin diskutiert, damit der Leser einen vollständigeren Zusammenhang erhält, in dem die Erfindung zu verstehen ist.

[0129] Genauer ist die erste Decodiermethode eine Differenzmethode, die darauf beruht, entsprechende Muster des ursprünglichen Signals vom verdächtigten Signal abzuziehen, um Differenzmuster zu erhalten, die dann (typischerweise individuell) auf deterministische Codierindizien hin untersucht werden (zum Beispiel auf die gespeicherten Rauschdaten). Dieses Herangehen kann somit als eine auf "Mustern basierende, deterministische" Decodiertechnik bezeichnet werden.

[0130] Die zweite Decodiermethode macht vom ursprünglichen Signal keinen Gebrauch. Sie untersucht auch keine spezifischen Muster, um vorbestimmte Rauscheigenschaften aufzufinden. Vielmehr wird die Statistik des verdächtigten Signals (oder eines Ausschnitts davon) als Ganzes betrachtet und analysiert, um die Anwesenheit von Kennungscodierung zu erkennen, die das ganze Signal durchdringt. Die Bezugnahme auf Durchdringung bedeutet, dass der ganze Kennungscode aus einem kleinen Bruchstück des verdächtigten Signals erkannt werden kann. Letzteres Vorgehen kann daher als eine "holographische, statistische" Decodiertechnik bezeichnet werden.

[0131] Beide Methoden beginnen damit, das verdächtige Signal mit dem Original zur Deckung und Übereinstimmung zu bringen. Das bedeutet Skalierung (zum Beispiel in Amplitude, Dauer, Farbabgleich usw.) und Sampling (oder wiederholtes Sampling), um die ursprüngliche Samplingrate wiederherzustellen. Wie in der früher beschriebenen Ausführungsform existiert eine Vielfalt von wohlverstandenen Verfahren, mit denen die mit dieser Zupassungsfunktion verbundenen Operationen durchgeführt werden können.

[0132] Wie bemerkt, wird im ersten Decodierverfahren so vorgegangen, dass das ursprüngliche Signal vom zur Deckung gebrachten, verdächtigten Signal abgezogen wird, wobei ein Differenzsignal verbleibt. Die Polarität aufeinanderfolgender Differenzsignalmuster kann dann mit den Polaritäten der entsprechenden gespeicherten Rauschsignalmuster verglichen werden, um den Kennungscode zu bestimmen. Das heisst, wenn die Polarität des ersten Differenzsignalmusters mit der des ersten Rauschsignalmusters übereinstimmt, dann ist das erste Bit des Kennungscodes eine "1". (In einem solchen Fall sollten die Polaritäten des 9., 17., 25. usw. Musters auch alle positiv sein.) Wenn die Polarität des ersten Differenzsignalmusters der des entsprechenden Rauschsignalmusters entgegengesetzt ist, dann ist das erste Bit des Kennungscodes eine "0".

[0133] Indem die vorstehende Analyse mit acht aufeinanderfolgenden Muster des Differenzsignals durchgeführt wird, kann die Folge der Bits, aus denen das ursprüngliche Codewort besteht, bestimmt werden. Wenn während der Decodierung, wie in der bevorzugten Ausführungsform, der Zeiger **230** mit dem ersten Bit beginnend Bit für Bit durch das Codewort gezogen wird, dann können die ersten acht Muster des Differenzsignals analysiert werden, um den Wert des 8-Bit-Codeworts eindeutig zu bestimmen.

[0134] In einer rauschfreien Welt (hier, ein Rauschen, das unabhängig von dem ist, mit dem die Kennungscodierung ausgeführt wird) würde die vorangehende Analyse immer den richtigen Kennungscode liefern. Ein Prozess, der nur in einer rauschfreien Welt anwendbar ist, hat aber tatsächlich eine begrenzte Nützlichkeit.

[0135] (Weiter kann eine genaue Identifizierung von Signalen in rauschfreien Situationen durch eine Reihe anderer, einfacherer Verfahren gehandhabt werden, zum Beispiel Kontrollsummen, statistisch unwahrscheinliche Korrespondenz zwischen verdächtigten und ursprünglichen Signalen usw.)

[0136] Obwohl rausch-induzierte Abweichungen beim Decodieren – zu einem gewissen Grad – dadurch überwunden werden können, dass grosse Anteile des Signals analysiert werden, führen aber solche Abweichungen doch zu einer praktischen Obergrenze der Sicherheit des Prozesses. Ferner ist der Bösewicht, dem man

gegenübertreten muss, nicht immer so wohlwollend wie zufälliges Rauschen. Vielmehr tritt er zunehmend in Gestalt von von Menschen verursachter Entstellung, Verzerrung, Manipulation usw. auf. In solchen Fällen kann der erwünschte Grad von Sicherheit bei der Identifizierung nur durch andere Vorgehensweisen erreicht werden.

[0137] Die derzeit bevorzugte Vorgehensweise (die "holographische, statistische" Decodiermethode) baut darauf, das verdächtigte Signal mit bestimmten Rauschdaten zu rekombinieren (typischerweise die in Speicher **214** gespeicherten Daten) und die Entropie des sich ergebenden Signals zu analysieren. "Entropie" braucht nicht in ihrer striktesten mathematischen Definition verstanden zu werden, es ist lediglich das knappste Wort, um Zufälligkeit (Rauschen, Glätte, Schnee usw.) zu beschreiben.

[0138] Die meisten seriellen Daten sind nicht zufällig. Das heisst, dass ein Muster gewöhnlich – in einem bestimmten Grade – mit angrenzenden Muster korreliert. Im Gegensatz dazu ist Rauschen typischerweise zufällig. Wenn ein Zufallssignal (zum Beispiel Rauschen) zu einem Nichtzufallssignal addiert (oder von ihm subtrahiert) wird, wächst allgemein die Entropy des sich ergebenden Signals. Das heisst, dass das sich ergebende Signal mehr Zufallsschwankungen als das ursprüngliche Signal hat. Dies ist der Fall mit dem durch den vorliegenden Verschlüsselungsprozess erzeugten verschlüsselten Ausgangssignal; es besitzt mehr Entropie als das ursprüngliche, nicht verschlüsselte Signal.

[0139] Wenn im Gegensatz dazu die Addition eines Zufallssignals zu (oder Subtraktion von) einem Nichtzufallssignal die Entropie vermindert, dann passiert etwas Ungewöhnliches. Es ist diese Anomalie, die im bevorzugten Decodierprozess verwendet wird, um eingebettete Kennungscodierung zu erfassen.

[0140] Um diese auf Entropie basierende Decodiermethode voll zu verstehen, ist es zuerst nützlich, eine Eigenschaft des ursprünglichen Verschlüsselungsprozesses hervorzuheben, nämlich die ähnliche Behandlung jedes achten Musters.

[0141] In dem oben diskutierten Verschlüsselungsprozess inkrementiert der Zeiger **230** um ein Bit für jedes folgende Muster des Eingangssignals, wenn er das Codewort durchläuft. Wenn das Codewort acht Bits lang ist, dann kehrt der Zeiger bei jedem achten Signalmuster zu derselben Bitposition im Codewort zurück. Wenn dieses Bit eine "1" ist, wird Rauschen zum Eingangssignal hinzugefügt; wenn dieses Bit eine "0" ist, dann wird Rauschen vom Eingangssignal abgezogen. Auf Grund des zyklischen Fortschreitens des Zeigers **230** hat jedes achte Muster eines verschlüsselten Signals daher eine gemeinsame Eigenschaft, indem nämlich alle diese Muster entweder um die entsprechenden Rauschdaten (die negativ sein können) vermehrt oder um diese vermindert sind, je nachdem, ob das Bit des Codeworts, das dann jeweils durch den Zeiger **230** angesprochen wird, eine "1" oder eine "0" ist.

[0142] Um diese Eigenschaft auszunutzen, behandelt der auf Entropie beruhende Decodierprozess jedes achte Muster des verdächtigten Signals in gleicher Weise. Genauer beginnt der Prozess damit, zum 1., 9., 17., 25. usw. Muster des verdächtigten Signals die entsprechenden skalierten, im Speicher **214** gespeicherten Rauschsignalwerte hinzuzufügen (d. h. die am 1., 9., 17., 25. usw. Speicherplatz gespeicherten Daten). Die Entropie des sich ergebenden Signals (d. h. des verdächtigten Signals, in dem jedes achte Muster modifiziert ist) wird dann berechnet.

[0143] (Die Berechnung der Entropie oder Zufälligkeit eines Signals ist unter den Fachkräften auf diesem Gebiet wohl verstanden. Eine allgemein akzeptierte Methode besteht darin, an jedem Stichprobenpunkt die Ableitung des Signals zu bilden, diese Werte zum Quadrat zu erheben und dann über das gesamte Signal zu summieren. Jedoch kann eine Vielfalt anderer, wohlbekannter Methoden wahlweise verwendet werden.)

[0144] Der vorangehende Schritt wird dann wiederholt, diesmal aber, indem die gespeicherten Rauschwerte vom 1., 9., 17., 25. usw. Muster abgezogen werden.

[0145] Eine dieser beiden Operationen hebt den Verschlüsselungsprozess auf und vermindert die Entropie des sich ergebenden Signals, die andere vertieft ihn. Wenn durch Addition der Rauschdaten aus Speicher 214 zum verdächtigten Signal dessen Entropie vermindert wird, dann müssen diese Daten früher vom ursprünglichen Signal subtrahiert worden sein. Das weist darauf hin, dass Zeiger **230** auf ein "0"-Bit wies, als diese Muster verschlüsselt wurden. (Eine "0" am Steuereingang des Addier-Subtrahier-Gliedes **212** veranlasste dieses, das skalierte Rauschen vom Eingangssignal zu subtrahieren.)

[0146] Wenn im Gegensatz dazu eine Subtraktion der Rauschdaten von jedem achten Muster des verdäch-

tigten Signals dessen Entropie vermindert, dann muss der Verschlüsselungsprozess dieses Rauschen früher addiert haben. Dies weist darauf hin, dass Zeiger **230** auf ein "1"-Bit wies, als Muster 1, 9, 17, 25 usw. verschlüsselt wurden.

[0147] Indem man vermerkt, ob die Entropie durch Addieren (a) oder Subtrahieren (b) der gespeicherten Rauschdaten zum/vom verdächtigten Signal sinkt, kann man feststellen, dass das erste Bit des Codewort eine "0" (a) oder eine "1" (b) ist.

[0148] Die vorangehenden Operationen werden dann für die Gruppe beabstandeter Muster des verdächtigten Signals ausgeführt, die mit dem zweiten Muster beginnt (d. h. 2, 10, 18, 26...). Die Entropie des sich ergebenden Signals zeigt an, ob das zweite Bit des Codeworts eine "0" oder eine "1" ist. Gleichermassen wird mit den folgenden sechs Gruppen von beabstandeten Muster im verdächtigten Signal verfahren, bis alle acht Bits des Codeworts erkannt worden sind.

[0149] Es ist einzusehen, dass die voranstehende Vorgehensweise gegen Entstellungsmechanismen unempfindlich ist, die die Werte der individuellen Muster abändern; stattdessen betrachtet der Prozess die Entropie des Signals als Ganzes und ergibt einen hohen Grad von Sicherheit bei den Ergebnissen. Des weiteren können sogar kleine Auszüge aus dem Signal auf diese Weise analysiert werden, sodass Piraterie selbst kleiner Details eines Originalwerks nachgewiesen werden kann. Die Ergebnisse sind also statistisch robust, sowohl beim Vorliegen natürlicher wie beim Vorliegen von durch Menschen verursachten Entstellungen des verdächtigten Signals.

[0150] Es ist weiterhin einzusehen, dass die Verwendung eines N-Bit-Codewortes in dieser Echtzeit-Ausführungsform Vorteile liefert, die den oben in Verbindung mit dem Batchverschlüsselungssystem diskutierten analog sind. (Tatsächlich kann die vorliegende Ausführungsform so aufgefasst werden, dass sie N verschiedene Rauschsignale verwendet, gerade wie im Batchverschlüsselungssystem. Das erste Rauschsignal ist ein Signal, das dieselbe Ausdehnung wie das Eingangssignal hat und das skalierte Rauschsignal im 1., 9., 17., 25. usw. Muster einschliesst (unter der Annahme, dass N = 8), wobei Nullen in den dazwischenliegenden Muster vorliegen. Das zweite Rauschsignal ist ein ähnliches Signal, das das skalierte Rauschsignal im 2., 10., 18., 26. usw. Muster einschliesst, wobei Nullen in den dazwischenliegenden Muster vorliegen. Und so fort. Diese Signale werden alle kombiniert, um ein zusammengesetztes Rauschsignal zu ergeben.) Einer der einem solchen System innewohnenden wichtigen Vorteile ist der hohe Grad von statistischer Sicherheit (einer Sicherheit, die sich mit jedem nachfolgenden Bit des Kennungscodes verdoppelt), dass die Übereinstimmung wirklich eine Übereinstimmung ist. Das System verlässt sich nicht auf eine subjektive Bewertung eines verdächtigen Signals bezüglich eines einzelnen, deterministisch eingebetteten Codesignals.

Veranschaulichende Abänderungen

[0151] Aus der vorangehenden Beschreibung ist erkenntlich, dass zahlreiche Abwandlungen an den veranschaulichten Systemen angebracht werden können, ohne die Grundprinzipien zu verändern. Einige dieser Abänderungen werden unten beschrieben.

[0152] Der oben beschriebene Decodierprozess versucht, gespeicherte Rauschdaten zum verdächtigten Signal sowohl zu addieren wie von ihm zu subtrahieren, um herauszufinden, welche Operation die Entropie vermindert. In anderen Ausführungsformen braucht nur eine dieser Operationen ausgeführt zu werden. In einem alternativen Decodierprozess zum Beispiel werden die gespeicherten Rauschdaten, die jedem achten Muster des verdächtigten Signals entsprechen, nur zu den benannten Muster addiert. Wenn die Entropie des sich ergebenden Signals dadurch erhöht wird, dann ist das entsprechende Bit des Codeworts eine "1" (d. h. dieses Rauschen ist früher, während des Verschlüsselungsprozesses, hinzugefügt worden, so dass sein wiederholtes Hinzufügen nur die Zufälligkeit des Signals verstärken kann). Wenn die Entropie des sich ergebenden Signals dadurch vermindert wird, dann ist das entsprechende Bit des Codeworts eine "0". Ein weiterer Entropietest für den Fall, dass die gespeicherten Rauschmuster subtrahiert werden, ist nicht erforderlich.

[0153] Die statistische Zuverlässigkeit des Identifizierungsprozesses (Codierung und Decodierung) kann so ausgelegt werden, dass im wesentlichen jede Sicherheitsschwelle (zum Beispiel 99.9%, 99.99%, 99.999% usw.) durch geeignete Auswahl der globalen Skalierfaktoren übertroffen werden kann. Zusätzliche Sicherheit kann bei jeder gegebenen Anwendung (in den meisten Anwendungen unnötigerweise) erzielt werden, indem der Decodierprozess nochmals überprüft wird.

[0154] Eine Möglichkeit der nochmaligen Überprüfung des Decodierprozesses besteht darin, die gespeicher-

ten Rauschdaten entsprechend den Bits des erkannten Codeworts vom verdächtigten Signal zu entfernen, was ein "wiederhergestelltes" Signal ergibt (d. h. wenn für das erste Bit des Codeworts die "1" gefunden wird, dann werden die am 1., 9., 17. usw. Platz des Speichers **214** gespeicherten Rauschmuster von den entsprechenden Muster des verdächtigten Signals abgezogen). Die Entropie des wiederhergestellten Signals wird gemessen und als Basislinie in weiteren Messungen verwendet. Als nächstes wird der Prozess wiederholt, diesmal, indem die gespeicherten Rauschdaten entsprechend einem modifizierten Codewort vom verdächtigten Signal abgezogen werden. Das modifizierte Codewort ist das gleiche wie das erkannte Codewort, ausser dass ein Bit gekippt wird (zum Beispiel das erste). Die Entropie des sich ergebenden Signals wird bestimmt und mit der Basislinie verglichen. Wenn Kippen des Bits im erkannten Codewort eine erhöhte Entropie ergab, dann ist die Richtigkeit dieses Bits im erkannten Codewort bestätigt. Der Prozess wird wiederholt, jedesmal mit einem anderen Bit des erkannten Codeworts gekippt, bis alle Bits des Codeworts so überprüft worden sind. Jede Veränderung sollte ein Anwachsen der Entropie gegenüber der Basislinie ergeben.

[0155] Für die im Speicher **214** gespeicherten Daten gibt es eine Vielfalt von Alternativen. In der vorangehenden Diskussion enthält Speicher **214** die skalierten Rauschdaten. In anderen Ausführungsformen können stattdessen nicht die skalierten Rauschdaten gespeichert sein.

[0156] In noch weiteren Ausführungsformen kann es wünschenswert sein, zumindest einen Teil des Eingangssignals selbst im Speicher **214** zu speichern. Zum Beispiel kann der Speicher acht Bits mit Vorzeichen dem Rauschmuster zuordnen und weitere 16 Bits verwenden, um die höchstwertigen Bits eines 18- oder 20-Bit-Audiosignalmusters zu speichern. Das bringt verschiedene Vorteile. Ein Vorteil ist der, dass dadurch erleichtert wird, ein "verdächtigtes" Signal zur Deckung zu bringen. Ein weiterer Vorteil ist der, dass im Falle der Verschlüsselung eines Eingangssignals, das bereits verschlüsselt worden war, die Daten im Speicher **214** verwendet werden können, um zu erkennen, welcher der beiden Verschlüsselungsprozesse zuerst erfolgte. Das heisst, dass es ausgehend von den Eingangssignaldaten im Speicher **214** (auch wenn sie unvollständig sind) allgemein möglich ist festzustellen, mit welchem der beiden Codewörter es verschlüsselt worden ist.

[0157] Noch eine weitere Alternative für Speicher **214** ist die, dass er gänzlich weggelassen werden kann.

[0158] Eine Möglichkeit, dies zu erreichen, ist die Verwendung einer deterministischen Rauschquelle im Verschlüsselungsprozess, zum Beispiel ein algorithmischer Rauschgenerator, der mit einer bekannten Schlüsselzahl angeimpft wurde. Die mit derselben Schlüsselzahl angeimpfte, selbe deterministische Rauschquelle kann im Decodierprozess verwendet werden. In einer solchen Anordnung braucht statt des grossen, gewöhnlich im Speicher **214** gespeicherten Datensatzes nur die Schlüsselzahl für ihren späteren Gebrauch beim Decodieren gespeichert werden.

[0159] Alternativ kann ein unverseller Decodierprozess durchgeführt werden, wenn das während der Verschlüsselung hinzugefügte Rauschsignal keinen Mittelwert von Null hat und dem Decodierer die Länge N des Codeworts bekannt ist. Dieser Prozess verwendet denselben Entropietest wie die vorangehenden Verfahren, aber durchläuft mögliche Codewörter, indem er entsprechend den Bits des in Überprüfung befindlichen Codeworts einen kleinen Füllrauschwert (zum Beispiel einen Wert, der kleiner als der erwartete mittlere Rauschwert ist) zu jedem N-ten Muster des verdächtigten Signals hinzufügt oder von ihm abzieht, bis eine Entropieverminderung bemerkt wird. Eine solche Vorgehensweise wird jedoch für die meisten Anwendungen nicht bevorzugt, weil sie weniger Sicherheit als andere Ausführungsformen bietet (zum Beispiel kann sie durch rohe Gewalt geknackt werden).

[0160] Viele Anwendungen sind mit der in Fig. 7 veranschaulichten Ausführungsform gut bedient, in der verschiedene Codewörter verwendet werden, um mehrere verschieden verschlüsselte Versionen eines Eingangssignals zu erzeugen, deren jede dieselben Rauschdaten einsetzt. Genauer schliesst die Ausführungsform **240** der Fig. 7 einen Rauschspeicher **242** ein, in den während der Kennungs-Codierung des Eingangssignals mit einem ersten Codewort Rauschen aus der Quelle **206** eingeschrieben wird. (Zur bequemeren Veranschaulichung ist die Rauschquelle der Fig. 7 ausserhalb des Echtzeitcodierers **202** gezeigt.) Danach können zusätzliche, kennungscodierte Versionen des Eingangssignals erzeugt werden, indem die gespeicherten Rauschdaten aus dem Speicher gelesen und gemeinsam mit dem zweiten bis N-ten Codewort benutzt werden, um das Signal zu verschlüsseln. (Während binär-sequenzielle Codewörter in Fig. 7 veranschaulicht werden, können in anderen Ausführungsformen beliebige Folgen von Codewörtern benutzt werden.) Mit einer solchen Anordnung kann eine grosse Anzahl von verschieden verschlüsselten Signalen erzeugt werden, ohne einen Langzeit-Rauschspeicher proportional grosser Abmessungen zu verlangen. Stattdessen wird eine festgelegte Menge von Rauschdaten gespeichert, gleichviel ob ein Original einmal oder tausendmal verschlüsselt wird.

[0161] (Wenn gewünscht, können mehrere verschieden codierte Ausgangssignale gleichzeitig statt hintereinander erzeugt werden. Eine solche Ausführungsform schliesst eine Mehrzahl von Addier-Subtrahier-Kreisen **212** ein, jeder mit dem gleichen Eingangssignal und mit dem gleichen skalierten Rauschsignal, aber mit unterschiedlichen Codewörtern betrieben. Jeder erzeugt dann ein verschieden verschlüsseltes Ausgangssignal.)

[0162] Bei Anwendungen, die eine grosse Anzahl von verschieden verschlüsselten Versionen des gleichen Originals haben, ist einzusehen, dass der Decodierprozess nicht immer jedes Bit des Codeworts erkennen muss. Manchmal könnte die Anwendung zum Beispiel verlangen, nur eine Gruppe von Codes zu identifizieren, zu denen das verdächtigte Signal gehört. (Zum Beispiel könnten Bits hoher Ordnung im Codewort eine Organisation anzeigen, an die mehrere verschieden codierte Versionen des gleichen Quellenmaterials geliefert worden sind, während Bits niedriger Ordnung spezifische Kopien identifizieren. Um die Organisation zu identifizieren, mit der ein verdächtigtes Signal assoziiert wird, könnte es unnötig sein, Bits niedriger Ordnung zu prüfen, da die Organisation aus den Bits hoher Ordnung allein identifiziert werden. kann.) Der Decodierprozess lässt sich abkürzen, wenn die Kennungserfordernisse durch Erkennung einer Teilmenge der Codewortbits im verdächtigten Signal erfüllt werden können.)

[0163] Einige Anwendungen können am besten bedient werden, indem der Verschlüsselungsprozess verschiedene Male innerhalb eines integralen Werkes neu begonnen wird, und dies manchmal mit einem unterschiedlichen Codewort. Betrachte beispielsweise auf Videoband aufgenommene Produktionen (zum Beispiel Fernsehprogramme). Jedes Bild einer auf Videoband aufgenommenen Produktion and mit einer eindeutigen Codenummer, die in Echtzeit mit einer Anordnung **248** wie in Fig. 8 gezeigt verarbeitet wurde, zur Identifizierung codiert werden. Jedesmal, wenn ein vertikaler Rücksprung durch den Synchrondemodulator **250** erkannt wird, kehrt die Rauschquelle **206** an ihren Anfangspunkt zurück (zum Beispiel, um die soeben erzeugte Folge zu wiederholen), und ein Kennungscode erhöht sich auf den nächsten Wert. Jedes Bild auf dem Videoband wird dadurch eindeutig kennungs-codiert. Typischerweise wird das verschlüsselte Signal zur langfristigen Speicherung auf einem Videoband gespeichert (obwohl andere Medien einschliesslich Laserdisc verwendet werden können).

[0164] Um auf das Verschlüsselungsgerät zurückzukommen, nutzt die Nachschlagtabelle **204** im veranschaulichten Ausführungsbeispiel die Tatsache aus, dass Muster des Eingangsdatensignals mit hoher Amplitude (ohne eine unangenehme Degradation des Ausgangssignals) ein höheres Niveau an verschlüsselter Kennungscodierung als Eingangsmuster niedriger Amplitude vertragen können. Zum Beispiel entsprechen Eingangsdatenmuster mit Dezimalwerten von 0, 1 oder 2 vielleicht (in der Nachschlagtabelle **204**) Skalierungsfaktoren von Eins (oder sogar Null), während Eingangsdatenmuster mit Werten über 200 vielleicht Skalierungsfaktoren von 15 entsprechen. Allgemein gesprochen stehen die Skalierungsfaktoren und die Eingangsmusterwerte in einer Quadratwurzelbeziehung. Das heisst, dass ein vierfacher Anstieg im Wert des abgetasteten Eingangssignals einem ungefähr zweifachen Anstieg im Wert des damit assoziierten Skalierungsfaktors entsprechen.

[0165] (Der in Klammern gegebene Verweis auf Null als ein Skalierungsfaktor spielt auf Fälle an, in denen zum Beispiel das Quellensignal zeitlich oder räumlich keinen Informationsinhalt hat. In einem Bild zum Beispiel kann eine Region, die durch mehrere zusammenhängende Musterwerte von Null gekennzeichnet ist, einer tiefschwarzen Region des Bildes entsprechen. Ein Skalierungsfaktor von Null kann hier angebracht sein, da im wesentlichen keine Bilddaten geraubt werden können.)

[0166] Um mit dem Verschlüsselungsprozess fortzusetzen, werden Fachleute das Potenzial für "Spurfehler" in der veranschaulichten Ausführungsform erkennen. Wenn zum Beispiel das Eingangssignal aus 8-Bit-Mustern besteht und die Muster sich über den gesamten Bereich von 0 bis 255 (dezimal) erstrecken, dann kann die Addition oder Subtraktion von skaliertem Rauschen zum/vom Eingangssignal Ausgangssignale erzeugen, die nicht durch acht Bits dargestellt werden können (zum Beispiel –2 oder 257). Es existiert eine Anzahl von gut verstandenen Verfahren, um diese Situation in Ordnung zu bringen, darunter einige proaktive und einige reaktive. (Zu diesen bekannten Verfahren gehört es vorzuschreiben, dass das Eingangssignal keine Muster im Bereich von 0 bis 4 oder von 251 bis 255 haben soll, was eine Modulation durch das Rauschsignal mit Sicherheit gestattet, oder Vorkehrungen einzuschliessen, um Eingangssignalmuster, die andernfalls Spurfehler verursachen würden, zu erkennen und adaptiv zu modifizieren.)

[0167] Während in der veranschaulichten Ausführungsform beschrieben wird, dass das Codewort sequenziell ein Bit nach dem anderen durchschritten wird, um die Modulation aufeinanderfolgender Bits des Eingangssignals zu steuern, ist aber einzusehen, dass die Bits des Codeworts für diese Zwecke auch anders als sequenziell verwendet werden können. In Wirklichkeit können Bits des Codewortes in Übereinstimmung mit jeglichem

vorbestimmten Algorithmus ausgewählt werden.

[0168] Die dynamische Skalierung des Rauschsignals, die auf dem augenblicklichen Wert des Eingangssignals basiert, ist eine Optimierung, die in vielen Ausführungsformen weggelassen werden kann. Das heisst, dass die Nachschlagtabelle **204** und der erste Skalierer **208** gänzlich weggelassen werden können und das Signal von der digitalen Rauschquelle **206** direkt (oder durch den zweiten, globalen Skalierer **210**) an das Addier-Subtrahier-Glied angelegt werden kann.

[0169] Es ist weiterhin einzusehen, dass die Verwendung einer Rauschquelle mit einem Mittelwert von Null die veranschaulichte Ausführungsform vereinfacht, aber für die Erfindung nicht nötig ist. Ein Rauschsignal mit einem anderen Mittelwert kann leicht verwendet werden, und Gleichstromkompensation kann (wenn nötig) anderswo im System erfolgen.

[0170] Die Verwendung einer Rauschquelle **206** ist auch freigestellt. Eine Vielfalt anderer Signalquellen kann je nach den von den Anwendungen abhängenden Zwangen verwendet werden (zum Beispiel der Schwelle, bei welcher das verschlüsselte Kennungssignal wahrnehmbar wird). In vielen Fällen ist der Pegel des eingebetteten Kennungssignals niedrig genug, so dass das Kennungssignal keine zufällige Gestalt zu haben braucht; es ist nicht wahrnehmbar, gleich welcher Natur es ist. Eine Pseudo-Zufallsquelle **206** wird jedoch üblicherweise gewünscht, weil sie das grösste Signal-Rausch-Verhältnis S/N des Kennungscodesignals (ein etwas ungeschickter Ausdruck in diesem Falle) für einen nicht wahrnehmbaren Pegel des eingebetteten Kennungssignals liefert.

[0171] Es ist einzusehen, dass eine Kennungscodierung nicht stattzufinden braucht, nachdem ein Signal zu einer als Daten gespeicherten Form reduziert worden ist (d. h., "in sachlicher Form fixiert", in den Worten des U.S.-Urheberrechtsgesetzes). Betrachte zum Beispiel den Fall populärer Musiker, deren Auftritte oft gesetzeswidrig aufgezeichnet werden. Durch Kennungscodierung des Audiosystems, bevor es die Lautsprecher der Konzerthalle ansteuert, können nicht autorisierte Aufzeichnungen des Konzerts zu einen bestimmten Ort und eine bestimmte Zeit zurückverfolgt werden. Gleichermassen können Audioquellen wie Notrufe live auf Nummer 911 vor ihrer Aufzeichnung verschlüsselt werden, um ihre spätere Authentisierung zu erleichtern.

[0172] Während die Ausführungsform mit schwarzem Kasten als eine autonome-Einheit beschrieben worden ist, ist zu erkennen, dass sie als eine Komponente in eine Anzahl verschiedener Hilfsprogramme oder Instrumente integriert werden kann. Eines davon ist ein Scanner, der Kennungscodes in die abgetasteten Ausgangsdaten einbetten kann. (Die Codes können einfach dazu dienen festzuhalten, dass die Daten durch einen spezifischen Scanner erzeugt worden sind.) Ein anderes ist die kreative Software wie zum Beispiel die populären Zeichen-/Grafik-/Animations-/Malprogramme, die von Adobe, Macromedia, Corel und ähnlichen Firmen angeboten werden.

[0173] Schliesslich ist zu erkennen, dass eine Vielfalt anderer Implementierungen alternativ verwendet werden können, obwohl der Echtzeit-Codierer **202** unter Bezugnahme auf eine bestimmte Hardware-Implementierung veranschaulicht worden ist. In einigen werden andere Hardware-Konfigurationen verwendet. Andere nutzen Software-Routinen für einige oder alle der veranschaulichten Funktionsblöcke. (Die Software-Routinen können auf vielen programmierbaren Allzweckcomputern wie 80×86-PC-kompatible Computer, Workstations auf Basis eines RISC-Prozessors usw. ausgeführt werden.)

RAUSCHTYPEN. QUASI-RAUSCHEN UND OPTIMIERTES RAUSCHEN

[0174] Bis hierher wurden in dieser Offenbarung Gausssches Rauschen, "Weisses Rauschen" und direkt von der Anwendungsinstrumentierung erzeugtes Rauschen als einige von vielen Beispielen für Trägersignale vorausgesetzt, die sich dafür eignen, ein einzelnes Informationsbit durch ein ganzes Bild oder Signal hindurchzutragen. Es ist möglich, bei der "Konstruktion" von Rauscheigenschaften noch proaktiver zu sein, um bestimmte Ziele zu erreichen. Die "Konstruktion", in der Gausssches oder Instrumentenrauschen verwendet wird, richtete sich etwas auf "absolute" Sicherheit. In diesem Abschnitt der Offenbarung werden andere Überlegungen für die Konstruktion von Rauschsignalen, die als die schlussendlichen Träger der Kennungsdaten betrachtet werden können, vorgestellt.

[0175] In einigen Anwendungen könnte es von Vorteil sein, das Rauschträgersignal (zum Beispiel das N-te eingebettete Codesignal in der ersten Ausführungsform; die skalierten Rauschdaten in der zweiten Ausführungsform) so zu konstruieren, dass im Verhältnis zu seiner Wahrnehmbarkeit mehr absolute Signalstärke für das Kennungssignal geliefert wird. Ein Beispiel ist wie folgt. Es ist anerkannt, dass ein wahres Gausssches

Rauschsignal den Wert '0' am häufigsten hat, gefolgt von 1 und –1 mit einander gleichen Wahrscheinlichkeiten, aber geringeren als für '0', 2 und –2 als nächste usw. Es ist klar, dass der Wert Null keine Information trägt, wie sie für die Zwecke dieser Erfindung verwendet wird. Daher wäre eine einfache Anpassung oder Konstruktion, dass ein neuer Prozess jedesmal dann eingeleitet wird, wenn in der Erzeugung des eingebetteten Codesignals eine Null vorkommt, wodurch der Wert "zufällig" entweder in eine 1 oder eine –1 umgewandelt wird. Logisch ausgedrückt, eine Entscheidung würde gefällt: wenn '0', dann zufällig (1, –1). Das Histogramm eines solchen Prozesses würde wie eine Verteilung des Gausschen/Poissonschen Typs ausehen, mit Ausnahme der Tatsache, dass die 0-Zelle leer wäre und die 1- und –1-Zelle um je die Hälfte des normalen Histogrammwertes der 0-Zelle vermehrt wäre.

[0176] In diesem Falle würde Kennungssignalenergie immer an alle Teile des Signals angelegt. Zu einigen der Tradeoffs gehört, dass ein (wahrscheinlich vernachlässigbares) Absinken der Sicherheit der Codes auftritt, weil eine "deterministische Komponente" an der Erzeugung des Rauschsignals beteiligt ist. Der Grund, warum dies völlig vernachlässigbar sein könnte, ist der, dass wir immer noch zu einer "Kopf-oder-Zahl"-Situation kommen, bei der die 1 oder –1 zufällig ausgewählt wird. Ein weiterer Tradeoff besteht darin, dass dieser Typ des konstruierten Rauschens eine höhere Schwelle der Wahrnehmbarkeit hat und nur für Anwendungen geeignet ist, in denen das niedrigstwertige Bit eines Datenflusses oder Bildes im Verhältnis zum kommerziellen Wert des Materials bereits vernachlässigbar ist, was heisst, dass niemand den Unterschied erkennen und der Wert des Materials keinen Schaden erleiden würde, wenn das niedrigstwertige Bit (für alle Signalmuster) dem Signal entzogen würde. Wie jeder Fachmann sehen kann, ist diese Blockierung des Null-Wertes im obigen Beispiel nur eine von vielen Möglichkeiten, die Rauscheigenschaften des Signalträgers zu "optimieren". Wir bezeichnen dies auch als "Quasi-Rauschen", in dem Sinne, dass natürliches Rauschen in einer vorbestimmten Art und Weise in Signale umgewandelt werden kann, die in jeder Hinsicht als Rauschen gelesen werden. Kryptographische Verfahren und Algorithmen können ebenfalls leicht, und oft definitionsgemäss, Signale hervorbringen, die als völlig zufällig empfunden werden. Daher kann das Wort "Rauschen" verschiedene Bedeutungen haben, die primär zwischen dem, was ein Beobachter oder Zuhörer subjektiv als Rauschen bezeichnet, und dem, was mathematisch definiert ist, liegen. Der Unterschied des mathematischen Rauschens liegt darin, dass dieses Rauschen andere Sicherheitseigenschaften hat, und ferner in der Einfachheit, mit der es entweder "aufgespürt" werden kann oder mit der Instrumente das Vorhandensein dieses Rauschens "automatisch erkennen" können.

"Universelle" eingebettete Codes

[0177] Im Hauptteil dieser Offenbarung wird gelehrt, dass für Zwecke der absoluten Sicherheit die rauschähnlichen eingebetteten Codesignale, die die Informationsbits des Kennungssignals enthalten, für jedes und alle verschlüsselten Signale eindeutig sein sollten oder, etwas weniger restriktiv, dass die eingebetteten Codesignale sparsam erzeugt werden sollten, zum Beispiel durch Verwendung der gleichen eingebetteten Codes für Partien von 1000 Stück Film. Sei dem wie es wolle, es gibt noch ein ganz anderes Herangehen an diesen Sachverhalt, bei dem die Verwendung von, wie wir sie nennen werden, "universellen" eingebetteten Codesignalen grosse neue Anwendungen für diese Technologie eröffnen kann. Die Wirtschaftlichkeit dieser Nutzungen wäre derart, dass die tatsächlich verminderte Sicherheit dieser universellen Codes (sie könnten zum Beispiel durch die altehrwürdigen kryptographischen Decodierverfahren analysiert, und somit potenziell vereitelt oder umgekehrt werden) relativ zu den wirtschaftlichen Gewinnen, die die beabsichtigen Anwendungen einbringen würden, ökonomisch vernachlässigbar wäre. Piraterie und widerrechtliche Nutzungen bekämen lediglich vorhersehbare "Kosten" und nur eine Quelle nicht einkassierter Einnahmen; also ein einfacher Geschäftsposten in einer wirtschaftlichen Analyse des Ganzen. Eine gute Analogie dazu besteht in der Kabelindustrie und der Verwürfelung von Videosignalen. Jedermann scheint zu wissen, dass listige, technisch geschickte Personen, die allgemein die Gesetze befolgende Bürger sein können, auf eine Leiter steigen und ein paar Drähte in ihrem Kabelanschlusskasten umstecken können, um sämtliche gebührenpflichtigen Kanäle gratis zu haben. Der Kabelfernsehindustrie ist das bekannt, sie trifft aktive Massnahmen und verfolgt diejenigen, die erwischt werden, aber der aus dieser Praxis stammende "Einnahmenverlust" überwiegt, jedoch ist er als Prozentsatz des Gewinns aus dem Verwürfelungssystem als Ganzes fast vernachlässigbar klein. Das Verwürfelungssystem als Ganzes ist trotz des Fehlens "absoluter Sicherheit" ein wirtschaftlicher Erfolg.

[0178] Das gleiche gilt für Anwendungen dieser Technologie, wo um den Preis, die Sicherheit etwas zu verringern, grosse wirtschaftliche Chancen eröffnet werden. In diesem Abschnitt wird zuerst beschrieben, was unter universellen Codes zu verstehen ist, sodann wird zu einigen der interessanten Nutzungen übergegangen, bei denen diese Codes verwendet werden können.

[0179] Universelle eingebettete Codes beziehen sich allgemein auf den Gedanken, dass die Kenntnis der ge-

nauen Codes verbreitet werden kann. Die eingebetteten Codes werden nicht in einen dunklen Geldschrank gelegt, um nie wieder berührt zu werden, bis Rechtsstreitigkeiten aufkommen (worauf in anderen Teilen dieser Offenbarung angespielt wird), sondern werden stattdessen an verschiedene Punkte verteilt, wo an Ort und Stelle analysiert werden kann. Diese Verteilung dürfte allgemein immer noch innerhalb einer bezüglich der Sicherheit kontrollierten Umgebung erfolgen, was bedeutet, dass Schritte unternommen werden, um eine Kenntnis der Codes auf diejenigen zu begrenzen, die sie kennen müssen. Instrumente, die versuchen, urheberrechtlich geschütztes Material automatisch nachzuweisen, sind ein unpersönliches Beispiel für "etwas", das die Codes kennen muss.

[0180] Es gibt viele Möglichkeiten, den Gedanken universeller Codes zu implementieren, wobei jede ihre eigenen Vorzüge bei jeder gegebenen Anwendung hat. Zum Zwecke, diese Technik zu lehren, unterteilen wir diese Vorgehensweisen in drei breite Kategorien: universelle Codes, die sich auf Bibliotheken stützen, universelle Codes, die sich auf deterministische Formel stützen, und universelle Codes, die sich auf im voraus definierte Industrie-Standardmuster stützen. Eine grobe Faustregel besagt, dass die erste Kategorie sicherer ist als die beiden anderen, aber auch, dass die letzteren beiden möglicherweise wirtschaftlicher implementiert werden können als die erste.

Universelle Codes: 1) Bibliotheken universeller Codes

[0181] Die Verwendung von Bibliotheken universeller Codes bedeutet einfach, dass die Methoden dieser Erfindung wie beschrieben eingesetzt werden, ausser der Tatsache, dass nur ein begrenzter Satz der individuellen, eingebetteten Codesignale erzeugt wird und dass jedes gegebene codierte Material irgendeine Untermenge dieses begrenzten "universellen Satzes" benutzen wird. Ein Beispiel soll hier angeführt werden. Ein Hersteller von Papier für fotografische Abzüge könnte wünschen, jedes Stück des verkauften 8×10-Zoll-Papiers mit einem eindeutigen Kennungscode vorzubelichten. Er wünscht ferner, Software für die Erkennung der Kennungscodes an seine Grosskunden, Servicebüros, Niederlagen und individuelle Fotografen zu verkaufen, so dass alle diese Leute nicht nur überprüfen können, dass ihr eigenes Material richtig markiert ist, sondern auch feststellen können, ob Drittmaterialien, die erworben werden sollen, mit dieser Technologie als urheberrechtlich geschützt identifiziert worden sind. Diese letztere Information hilft ihnen, neben vielen anderen Vorteilen die Urheberrechtsinhaber nachzuweisen und Rechtsstreitigkeiten zu vermeiden. Um diesen Plan "wirtschaftlich" umzusetzen, realisiert der Hersteller, dass Terabytes unabhängiger Daten erzeugt würden, wenn für jedes Blatt Papier für Abzüge eindeutige, individuelle eingebettete Codes eingesetzt werden, und diese Daten brauchen Speicherplatz sowie Zugang durch Erkennungs-Software. Stattdessen entscheidet der Hersteller, 16-Bit-Kennungscodes in das Papier einzubetten, die sich von einem Satz von nur 50 unabhängigen "universellen" eingebetteten Codesignalen ableiten. Einzelheiten, wie das gemacht wird, finden sich im nächsten Abschnitt, aber der springende Punkt liegt darin, dass nunmehr seine Erkennungs-Software nur einen begrenzten Satz von eingebetteten Codes in seiner Codebibliothek zu enthalten braucht, typischerweise in der Grössenordnung von 1 bis 10 Megabytes an Daten für 50 × 16 individuelle, eingebettete Codes, ausgespreizt über eine 8 × 10-Zoll-Fotoabzug (unter Berücksichtigung digitaler Kompression). Der Grund, 50 statt nur gerade 16 Codes auszuwählen, ist der, ein wenig zusätzliche Sicherheit zu haben, denn wenn dieselben 16 eingebetteten Codes für sämtliche Fotopapierbögen benutzt würden, wäre nicht nur die Obergrenze für Seriennummern auf 2^{16} begrenzt, sondern immer weniger spitzfindige Piraten könnten die Codes knacken und sie mit Software-Hilfsprogrammen entfernen.

[0182] Es gibt viele verschiedene Möglichkeiten, dieses Schema zu implementieren, wobei die folgende nur eine beispielhafte Methode ist. Die Weisheit des Firmenmanagements besagt, dass ein Kriterion für die eingebetteten Codesignale von 300 Pixels pro Zoll bei den meisten Anwendungen genügend Auflösung darstellt. Das bedeutet, dass ein zusammengesetztes eingebettetes Codebild 3000×2400 Pixels enthält, das mit einem sehr niedrigen Pegel auf jedes 8 × 10-Zoll-Blatt belichtet werden muss. Dies ergibt 7,2 Millionen Pixels. Unter Benutzung unseres gestaffelten Codiersystems, wie es in der Blackbox-Implementierung der **Fig. 5** und **Fig. 6** beschrieben ist, enthält jedes individuelle eingebettete Codesignal nur 7,2 Millionen geteilt durch 16, oder ungefähr 450 K an wirklich informationsbeladenen Pixeln, d. h. jeder 16. Pixel entlang einer gegebenen Rasterzeile. Diese Werte liegen typischerweise im Bereich von 2 bis –2 in digitalen Zahlen, bzw. sie sind hinlänglich beschrieben durch eine 3-Bit-Zahl mit Vorzeichen. Der rohe Informationsinhalt eines eingebetteten Codes ist dann ungefähr 3/8 Bytes mal 450 K oder etwa 170 Kilobytes. Durch digitale Kompression kann dies weiter vermindert werden. Alle diese Entscheidungen gehorchen den normalen Prinzipien der ingenieurmässigen Optimierung, wie sie durch jede gegebene Anwendung definiert werden und im Fach gut bekannt sind. Wir finden also, dass 50 dieser unabhängigen eingebetteten Codes einige wenige Megabytes ausmachen. Das ist ein ziemlich vernünftiges Mass zur Verteilung in Gestalt einer 'Bibliothek" universeller Codes innerhalb der Erkennungs-Software. Fortgeschrittene Standard-Verschlüsselungsgeräte könnten verwendet werden, um die ge-

naue Natur dieser Codes zu maskieren, sofern zu befürchten wäre, dass Sonntagspiraten die Erkennungs-Software lediglich deshalb kaufen würden, um die universellen eingebetteten Codes zu rekonstruieren. Die Erkennungs-Software könnte einfach die Codes entschlüsseln, bevor die in dieser Offenbarung gelehrten Erkennungstechniken angewandt werden.

[0183] Die Erkennungs-Software selbst würde sicher eine Vielfalt von Merkmalen haben, aber ihre Hauptaufgabe wäre zu bestimmen, ob innerhalb eines gegebenen Bildes irgendein universeller Urheberrechts-Code vorhanden ist. Die Schlüsselfrage ist dann, WELCHE 16 der insgesamt 50 universellen Codes darin enthalten sein mögen, wenn überhaupt, und sofern 16 gefunden werden, welches ihre Bitwerte sind. Die entscheidenden Variablen, die die Antworten auf diese Fragen bestimmen, sind: Deckung, Rotation, Vergrösserung (Massstab) und Ausdehnung. Im allgemeinsten Falle, wenn überhaupt keine zweckdienlichen Hinweise vorhanden sind, müsen alle Variablen unabhängig über sämtliche gegenseitigen Kombinationen variiert werden, und jeder der 50 universellen Codes muss dann durch Addition und Subtraktion überprüft werden, um zu sehen, ob die Entropie abnimmt. Streng genommen ist das eine enorme Aufgabe, aber viele dienliche Hinweise lassen sich finden, die die Aufgabe sehr erleichtern, zum Beispiel, wenn ein ursprüngliches Bild vorliegt, das mit der verdächtigen Kopie verglichen werden kann, oder wenn die allgemeine Ausrichtung und Ausdehnung des Bildes relativ zu einem 8 × 10-Zoll-Fotopapier bekannt ist, womit dann durch einfache Zentriertechniken alle Variablen in einem akzeptablen Ausmass bestimmt werden können. Es ist dann lediglich nötig, die 50 universellen Codes zu durchlaufen, um eine etwaige Verminderung der Entropie zu finden. Wenn ein Code das bewirkt, dann sollten es 15 weitere ebenfalls. Ein Protokoll muss aufgestellt werden, wonach eine gegebene Reihenfolde der 50 Codes in eine Folge vom höchstwertigen zum niedrigstwertigen Bit des ID-Codeworts übersetzt wird. Wenn wir also finden, dass die universelle Codezahl "4" vorhanden und ihr Bitwert "0" ist, dass aber die universellen Codes "1" bis "3" bestimmt nicht vorhanden sind, dann ist unser höchstwertiges Bit unserer N-Bit-ID-Codezahl eine "0". Desgleichen, wenn wir finden, dass der nächstniedrigste vorhandene universelle Code die Zahl "7" ist und sich als eine "1" herausstellt, dann ist unser nächsthöchstwertiges Bit eine "1". Wenn richtig ausgeführt, kann dieses System sauber zum Urheberrechts-Inhaber zurückverfolgen, sofern dieser die Seriennummer seines Fotopapiervorrats bei einem Register oder beim Papierhersteller selbst registriert hatte. Das heisst, wir suchen im Register nach und finden, dass ein Papier, das die universellen eingebetteten Codes 4, 7, 11, 12, 15, 19, 21, 26, 27, 28, 34, 35, 37, 38, 40 und 48 benutzt und den eingebetteten Code 0110 0101 0111 0100 hat, Leonardo de Boticelli gehört, einem ungekannten Wildfaunafotografen und Gletscher-Kameramann, dessen Adresse in Nordkanada ist. Wir wissen es, weil er seinen Film- und Papiervorrat pflichtgetreu registrierte-einige Minuten Arbeit, als er den Vorrat kaufte, den er in den portofreien Umschlag plumpsen liess, den die Herstellerfirma freundlicherweise zur Verfügung stellte, um den Prozess lächerlich einfach zu machen. Wahrscheinlich schuldet irgendjemand Leonardo einen Tantiemenscheck, und sicherlich hat das Register diesen Prozess der Tantiemenzahlungen als einen Teil seiner Dienstleistungen automatisiert.

[0184] Es muss zum Schluss bemerkt werden, dass wirklich spitzfindige Piraten und andere mit rechtswidrigen Absichten tatsächlich eine Vielfalt von kryptographischen und nicht so kryptographischen Methoden einsetzen können, um diese universellen Codes zu knacken, sie zu verkaufen und Software und Hardware herzustellen, die dabei helfen, die Codes zu entfernen oder zu entstellen. Wir werden aber diese Methoden nicht als Teil dieser Offenbarung lehren. Jedenfalls ist das ein Teil des Preises, der für die Bequemlichkeit der universellen Codes und die durch sie sich eröffnenden Anwendungen gezahlt werden muss.

Universelle Codes: 2) Auf deterministischen Formeln beruhende universelle Codes

[0185] Die Bibliotheken universeller Codes erfordern die Speicherung und Übermittlung von Megabytes an unabhängigen, allgemein zufälligen Daten, die als die Schlüssel dienen, mit denen das Vorhandensein und die Identität von Signalen und Bildern erschlossen wird, die mit universellen Codes markiert worden sind. Alternativ können verschiedene deterministische Formeln verwendet werden, die "erzeugen", was zufällige Daten oder Einzelbilder zu sein scheinen, wodurch es unnötig wird, alle diese Codes im Speicher zu speichern und jeden einzelnen der "50" universellen Codes zu befragen. Deterministische Formeln können auch dabei helfen, den Prozess der Bestimmung des ID-Codes zu beschleunigen, sobald bekannt ist, dass einer in einem gegebenen Signal oder Bild vorhanden ist. Andererseits eignen sich deterministische Formeln dafür, von wenig raffinierten Piraten aufgespürt zu werden. Einmal aufgespürt, eignen sie sich für einfachere Mitteilung wie Bekanntmachung über das Internet an hundert Nachrichtengruppen. Es mag sehr wohl viele Anwendungen geben, bei denen man sich über Aufspürung und Veröffentlichung keine Sorgen macht, und deterministische Formeln zur Erzeugung der individuellen eingebetteten Codes könnten da gerade die Antwort sein.

[0186] Diese Kategorie ist so etwas wie ein Hybrid der ersten beiden und richtet sich am meisten an Implementierungen der Prinzipien dieser Technologie in echt grossem Massstab. Die Anwendungen, die diese Klasse einsetzen, sind von dem Typ, bei dem starke Sicherheit viel weniger wichtig ist als eine Implementierung im grossen Massstab bei geringen Kosten und die sehr viel grösseren wirtschaftlichen Vorteile, die dadurch möglich werden. Eine beispielhafte Anwendung ist die Platzierung von Erkennungseinheiten für Identifizierung direkt in Haushalt-Audio- und Videogeräte (wie ein Fernsehgerät) einer bescheidenen Preisklasse. Derartige Erkennungseinheiten würden typischerweise Audio und/oder Video überwachen, um nach diesen Urheberrechts-Kennungscodes Ausschau zu halten und danach auf der Basis der Befunde einfache Entscheidungen auszulösen, wie zum Beispiel die Aufzeichnungsfunktionen blockieren oder freimachen oder aber programm-spezifische Gebührenmesser zählen lassen, deren Daten dann zu einem zentralen Audio/Videodiensteanbieter zurück übermittelt werden und auf die monatlichen Rechnungen gesetzt werden. Gleicherweise kann man vorhersehen, dass "schwarze Kästen" in Bars und an anderen öffentlichen Orten (durch Abhören mit einem Mikrophon) eine Überwachung urheberrechtlich geschützter Materialien ausüben und genaue Berichte zur Verwendung durch ASCAP, BMI und dergleichen erzeugen.

[0187] Es ist ein Kernprinzip einfacher universeller Codes, dass in Signale, Bilder oder Bildfolgen einige "rauschartige" und sich nahtlos wiederholende, industriegenormte Grundmuster injiziert werden, so dass kostengünstige Erkennungseinheiten entweder A) das reine Vorhandensein einer Urheberrechts-Flag" und, B) zusätzlich zu A, genaue Daten zur Identifizierung ermitteln können, durch die kompliziertere Entscheidungen und Tätigkeiten erleichtert werden.

[0188] Um diese besondere Ausführungsform der vorliegenden. Erfindung zu realisieren, müssen die Grundprinzipien der Erzeugung der individuellen, eingebetteten Rauschsignale vereinfacht werden, um an kostengünstige Schaltungsanordnungen zur Signalverarbeitung angepasst zu sein, während ihre Eigenschaften einer wirkungsvollen Zufälligkeit und holographischen Durchdringung aufrechterhalten bleiben. Mit einer Annahme dieser einfachen Codes im grossen Massstab durch die Industrie kämen die Codes selbst einer veröffentlichten Information nahe (so etwa wie die Kabelverschlüsselungskästen sich de facto fast in der öffentlichen Domäne befinden), wodurch für entschlossene Piraten der Weg frei ist, Schwarzmarkt-Gegenmassnahmen zu entwickeln, aber diese Situation wäre der bei der Verschlüsselung von Kabelfernsehen und bei objektiver wirtschaftlicher Analyse solcher gesetzeswidriger Aktivitäten bestehenden Situation recht ähnlich.

[0189] Ein der Anmelderin bekanntes Beispiel des Standes der Technik auf diesem allgemeinen Gebiet des proaktiven Urheberrechts-Nachweises ist das von vielen Firmen der Audioindustrie angenommene Serial Copy Management System. Nach bestem Wissen der Anmelderin verwendet dieses System ein Nichtaudio-"Flag"signal, das keinen Teil des Audiodatenstromes darstellt, aber trotzdem auf den Audiodatenstrom aufgepfropft ist und anzeigen kann, ob die damit verbundenen Audiodaten vervielfältigt werden sollten oder nicht. Ein mit diesem System verbundenes Problem besteht darin, dass es auf Medien und Geräte beschränkt ist, die dieses zusätzliche "Flag"signal unterstützen können. Eine weitere Unzulänglichkeit besteht darin, dass das Flaggensystem keine Identitätsdaten mit sich führt, die bei komplexeren Entscheidungen nützlich sein könnten. Noch eine weitere Schwierigkeit besteht darin, dass eine mit hoher Qualität ausgeführte Audioabtastung eines Analogsignals einer perfekten digitalen Kopie von digitalen Mastern beliebig nahe kommt und nichts vorgesehen zu sein scheint, diese Möglichkeit zu unterbinden.

[0190] Die Grundsätze dieser Erfindung können auf diese und andere Probleme in Audio-, Video- und all den anderen, vorher diskutierten Anwendungen angewendet werden. Eine beispielhafte Anwendung einfacher universeller Codes ist die folgende. Eine alleiniger Industriestandard von "1,000 000 Sekunden Rauschen" würde als der grundlegendste Indikator für das Vorhandensein oder Nichtvorhandensein der Urheberrechts-Markierung jedes gegebenen Audiosignals definiert. **Fig.** 9 zeigt ein Beispiel, wie die Wellenform einer industriellen Standard-Rauschsekunde aussehen könnte, und zwar sowohl im Zeitbereich **400** wie im Frequenzbereich **402**. Definitionsgemäss ist sie eine kontinuierliche Funktion und könnte an jede Kombination von Abtastraten und Bitquantisierung angepasst werden. Sie hat eine normalisierte Amplitude und kann beliebig mit jeder beliebigen Amplitude des digitalen Signals skaliert werden. Der Signalpegel und die ersten M-ten Ableitungen des Signals sind an den beiden Grenzen **404** (Fig. 9C) kontinuierlich, so dass bei Wiederholung der Wellenform der "Bruch" im Signal nicht (als Wellenform) sichtbar oder hörbar sein, wenn durch ein Audiosystem der Oberklasse abgespielt. Die Wahl von 1 Sekunde in diesem Beispiel ist willkürlich, da die genaue Länge des Intervalls aus Betrachtungen wie Hörbarkeit, Status eines quasi-weissen Rauschens, nahtlose Wiederholbarkeit, Einfachheit der Erkennungsverarbeitung und die Geschwindigkeit, mit der eine Urheberrechtsmarkierung bestimmt werden kann, abgeleitet wird. Die Injektion dieses wiederholten Rauschsignals in ein Signal oder Bild

(wiederum bei Pegeln, die unterhalb der menschlichen Wahrnehmung liegen) würde das Vorliegen von urheberrechtlich geschütztem Material anzeigen. Dies ist im wesentlichen ein Ein-Bit-Kennungscode, und die Einbettung weiterer Daten zur Identifizierungs wird weiter unten in diesem Abschnitt diskutiert. Die Verwendung dieser Kennungstechnik kann sich weit über die hier diskutierten billigen Haushaltrealisierungen hinaus erstrecken, indem Studios die Technik verwenden und Überwachungsstationen eingerichtet werden könnten, die buchstäblich Hunderte von Informationskanälen gleichzeitig überwachen und auf markierte Datenströme hin untersuchen, und die weiterhin nach den beigesellten Identitätscodes forschen können, die in Netze für die Fakturierung und die Tantiemenverfolgung eingebunden werden könnten.

[0191] Diese standardisierte Rausch-Grundsignatur wird nahtlos immer wiederholt und zu den Audiosignalen addiert, die mit der Urheberrechts-Grundkennung markiert werden sollen. Ein Teil des Grundes für das Wort "einfach" ist hier sichtbar: es ist klar, dass Piraten von diesem Industrie-Standardsignal wissen, aber ihre von diesem Wissen abgeleiteten, rechtswidrigen Nutzungen wie Löschen oder Entstellen werden im Verhältnis zu dem wirtschaftlichen Wert der Technik als Ganzes für den Massenmarkt wirtschaftlich sehr gering sein. Für die meisten Spitzen-Audiogeräte wird dieses Signal einige 80 bis 100 dB oder sogar noch weiter unterhalb des vollen Volumens liegen; für jede Situation können die geeigneten Pegel gewählt werden, obwohl es sicher Empfehlungen geben wird. Die Amplitude des Signals kann je nach den Audiosignalpegeln moduliert werden, auf die die Rauschsignatur angewandt wird, d. h. die Amplitude kann bedeutend höher sein, wenn eine Trommel geschlagen wird, aber nicht so dramatisch, das sie hörbar oder unangenehm wird. Diese Massnahmen sind lediglich eine Hilfe für die zu beschreibende Erkennungs-Schaltungsanordnung.

[0192] Erkennung der Gegenwart dieser Rauschsignatur durch billige Geräte kann auf einer Vielfalt von Wegen erreicht werden. Ein solcher Weg beruht auf grundlegenden Modifikationen der einfachen Grundsätze der Audiosignal-Leistungsmessung. Software-Erkennungsprogramme können ebenfalls geschrieben werden, und kompliziertere mathematische Erkennungsalgorithmen können auf Audio angewandt werden, um Erkennungsidentifizierungen sicherer zu machen. In solchen Ausführungsformen erfolgt die Erkennung der Urheberrechts-Rauschsignatur, indem der über die Zeit gemittelte Leistungspegel eines Audiosignals mit dem über die Zeit gemittelten Leistungspegel des gleichen Audiosignals verglichen wird, von dem die Rauschsignatur abgezogen worden ist. Wenn das Audiosignal, von dem die Rauschsignatur abgezogen wurde, einen geringeren Leistungspegel als das unveränderte Audiosignal hat, dann ist die Urheberrechtssignatur gegenwärtig, und eine entsprechende Statusanzeige muss erfolgen. Zu den hauptsächlichen technischen Feinheiten bei diesem Vergleich gehört, mit Diskrepanzen bei der Audioabspielgeschwindigkeit (zum Beispiel könnte ein Gerät im Vergleich zu genauen Einsekunden-Intervallen 0,5% zu "langsam" sein) und mit der unbekannten Phase der Einsekunden-Rauschsignatur innerhalb eines gegebenen Audios fertig zu werden (im Grunde genommen kann ihre "Phase irgendwo zwischen 0 und 1 Sekunde liegen). Eine andere Feinheit, die zwar nicht so zentral wie die obigen beiden ist, aber dennoch beachtet werden sollte, besteht darin, dass die Erkennungsschaltkreise keine höhere Amplitude der Rauschsignatur abziehen sollten als ursprünglich in das Audiosignal eingebettet. Zum Glück kann man das erreichen, indem man lediglich eine kleine Amplitude des Rauschsignals abzieht, und wenn der Leistungspegel dann absinkt, ist das ein Anzeichen, dass man sich "in Richtung auf eine Mulde" in den Leistungspegeln bewegt. Noch eine weitere, damit verwandte Feinheit besteht darin, dass die Leistungspegeländerungen im Vergleich zu den Gesamtleistungspegeln sehr klein sein werden, und Berechungen müssen allgemein mit geeigneter Bit-Genauigkeit durchgeführt werden, zum Beispiel 32 Bitwertoperationen und Kumulationen bei 16 bis 20 Bit Audio in Berechnungen der über die Zeit gemittelten Leistungspegel.

[0193] Es ist klar, dass Konstruktion und Einbau dieser Verarbeitungs-Schaltungsanordnungen für den Vergleich der Leistungspegel in Billiganwendungen eine technische Optimierungsaufgabe sind. Ein Kompromiss wird zwischen der Genauigkeit einer Identifizierung und den ""Shortcuts" zu finden sein, die in der Schaltungsanordnung möglich sind, um ihren Preis und ihre Komplexität zu reduzieren. Eine bevorzugte Ausführungsform für die Platzierung dieser Erkennungs-Schaltungsanordnung in den Instrumenten ist die einer einzelnen, programmierbaren integrierten Schaltung, die spezifisch für diese Aufgabe entworfen wurde. Fig. 10 zeigt einen solchen integrierten Schaltkreis **506**. Hier tritt das Audiosignal, **500**, entweder als ein digitales Signal oder als ein innerhalb der IC **500** zu digitalisierendes Audiosignal ein, während der Ausgang eine Flag **502** ist, die auf ein Niveau gesetzt wird, wenn die Urheberrechts-Rauschsignatur gefunden wurde, und auf ein anderes Niveau, wenn sie nicht gefunden wurde. Ebenfalls dargestellt ist die Tatsache, dass die standardisierte Rauschsignaturen-Wellenform im Festwertspeicher **504** innerhalb des IC **506** gespeichert ist. Wegen der Notwendigkeit, einen endlichen Abschnitt des Audio zu überwachen, bevor eine Erkennung stattfinden kann, gibt es eine geringfügige zeitliche Verzögerung zwischen dem Anlegen eines Audiosignals an den IC **506** und die Ausgabe einer gültigen Flag **502**. In diesem Falle ist es vielleicht nötig, einen Ausgang **508** "Flag gültig" zu haben, wo der IC die Aussenwelt informiert, ob er genügend Zeit hatte, um eine richtige Bestimmung bezüglich des Vorhandenseins oder Nichtvorhandenseins der Urheberrechts-Rauschsignatur auszuführen.

[0194] Es gibt eine grosse Vielfalt spezifischer Konstruktionen und Konstruktions-Philosophien, die angewendet werden, um die grundsätzliche Funktion des IC **506** der Fig. 10 auszufüllen. Audioingenieure und Ingenieure für die digitale Signalverarbeitung sind in der Lage, mehrere grundsätzlich unterschiedliche Konstruktionen zu entwerfen. Eine solche Konstruktion ist in Fig. 11 durch einen Prozess **599** illustriert, der seinerseits weiter konstruktiv zu optimieren ist, wie diskutiert werden wird. Fig. 11 zeigt ein Flussdiagramm für entweder ein Netzwerk zur Verarbeitung von Analogsignalen, ein Netzwerk zur Verarbeitung von digitalen Signalen oder die Programmschritte in einem Softwareprogramm. Wir finden ein Eingangssignal **600**, das einem Pfad folgend an einen über die Zeit gemittelten Leistungsmesser **602** angelegt wird, während der erzeugte Leistungsausgang selbst als ein Signal P_{sig} behandelt wird. Oben rechts finden wir die Standard-Rauschsignatur **504**, die mit 125% der normalen Geschwindigkeit, **604**, ausgelesen wird, wodurch seine Tonhöhe verändert wird und das "tonhöhenveränderte Rauschsignal" **606** zustande kommt. Dann wird dieses tonhöhenveränderte Rauschsignal in Schritt **608** vom Eingangssignal abgezogen, und dieses neue Signal wird an einen über die Zeit gemitteltem Leistungsmesser der gleichen Form wie bei **602** angelegt, hier als **610** bezeichnet. Der Ausgang dieser Operation ist ebenfalls ein zeitproportionales Signal, hier als $P_{s\text{-}pcn}$ **610** bezeichnet. Schritt **612** zieht dann das Leistungssignal **602** vom Leistungssignal **610** ab, was ein Ausgangsdifferenzsignal P_{out} **613** ergibt. Falls die universelle Standard-Rauschsignatur wirklich im Eingangs-Audiosignal **600** vorhanden ist, dann entsteht der Fall 2, **616**, in dem ein Schwebungssignal **618** mit einer Periode von ungefähr vier Sekunden im Ausgangssignal **613** auftritt, und es verbleibt, dieses Schwebungssignal mit einem Schritt wie **622** in Fig. 12 nachzuweisen. Fall 1, **614**, ist ein stetes Rauschsignal, das keine periodische Schwebung aufweist. Die 125% im Schritt **604** sind eine willkürliche Wahl, während konstruktive Erwägungen einen optimalen Wert festlegen würden, der zu anderen Schwebungssignalfrequenzen **618** führt. Während eine Wartezeit von vier Sekunden wie in diesem Beispiel ziemlich lang ist, speziell wenn man mindestens zwei oder drei Schwebungen erfassen möchte, umreisst Fig. 12, wie die grundsätzliche Konstruktion der Fig. 11 wiederholt und auf verschiedene verzögerte Versionen des Eingangssignals angesetzt werden könnte, d. h. Eingangssignale, die zum Beispiel um 1/20 Sekunde verzögert sind und 20 Parallelkreise konzertiert arbeiten, jeder an einem um 0,05 Sekunden gegenüber den Nachbarn verzögerten Abschnitt des Audio. Auf diese Weise würde ein Schwebungssignal ungefähr alle 1/5 Sekunden auftreten und wie eine Wanderwelle entlang den Reihen von Schwebungs-Erkennungskreisen aussehen. Das Vorhandensein oder Nichtvorhandensein dieser Schwebungs-Wanderwelle triggert die Erkennungsflagge **502**. Inzwischen gäbe es einen Audiosignalmonitor **624**, der sicherstellen würde, dass zum Beispiel mindestens zwei Sekunden des Audio gehört worden sind, bevor das Flag-gültig-Signal **508** gegeben wird.

[0195] Obwohl oben das Audio-Beispiel beschrieben worden ist, sollte es jedem Fachmann klar sein, dass derselbe Typ der Definition eines sich wiederholenden, universellen Rauschsignals oder Bildes auf viele anderen, bereits diskutierten Signale, Bilder, Abbildungen und physikalische Medien angewendet werden könnte.

[0196] Der obige Fall handelt nur von einer einzelnen Bitdatenebene, d. h. das Rauschsignatursignal ist entweder vorhanden (1) oder nicht vorhanden (0). In vielen Anwendungen wäre es schön, auch Seriennummerdaten zu erkennen, die dann für komplexere Entscheidungen, Protokolldaten für Rechnungen usw. verwendet werden könnten. Die gleichen Grundsätze wie die obigen waren anwendbar, aber nun gäbe es N unabhängige Rauschsignaturen wie in **Fig.** 9 abgebildet, statt nur einer einzelnen solchen Signatur. Typischerweise wäre eine solche Signatur die Hauptsignatur, an der die blosse Existenz einer Urheberrechtsmarkierung erkannt wird, und diese hätte allgemein grösseren Einfluss als die anderen, und die anderen "Identifizierungs"-Rauschsignaturen geringerer Leistung wären dann im Audio eingebettet. Erkennungs-Schaltkreise würden, nachdem das Vorhandensein der primären Rauschsignatur festgestellt wurde, die anderen N Rauschsignaturen durchlaufen, indem sie die gleichen Schritte wie oben beschrieben einsetzen. Wo ein Schwebungssignal entdeckt wird, ist der Bitwert '1' angezeigt, aber wo kein Schwebungssignal entdeckt wird, ist ein Bitwert von '0' angezeigt. Es könnte typisch sein, dass N einen Wert von 32 hat, womit 2^{32} Identifizierungscodes für jegliche, diese Erfindung einsetzende Industrie zur Verfügung stünden.

Verwendung dieser Technologie, wenn die Länge des Identifizierungscodes 1 ist

[0197] Die Prinzipien dieser Erfindung können offensichtlich in Fällen angewendet werden, wo nur ein einziges Vorhandensein oder Nichtvorhandensein eines Kennungssignals – eines Fingerabdrucks, wenn man so will – verwendet wird, um die Sicherheit zu schaffen, dass irgendein Signal oder Bild urheberrechtlich geschützt ist. Das obige Beispiel der Industriestandard-Rauschsignatur ist ein Beispielfall. Wir haben nicht mehr die zusätzliche Sicherheit der Kopf-oder-Zahl-Analogie, wir haben nicht länger die Fähigkeit für Spurencodes oder Seriennummern, aber viele Anwendungen brauchen diese Attribute vielleicht nicht, und die grössere Einfachheit eines einzelnen Fingerabdrucks könnte diese anderen Attribute immer aufwiegen.

Die "Tapeten"-Analogie

[0198] Der Ausdruck "holographisch" ist in dieser Offenbarung verwendet worden, um zu beschreiben, wie eine Kennungscodenummer in weitgehend integraler Form durch ein ganzes verschlüsseltes Signal oder Bild hindurch verteilt wird. Dies bezieht sich auch auf den Gedanken, dass jedes gegebene Fragment des Signals oder Bildes die gesamte, eindeutige Kennungscodenummer enthält. Wie bei den physikalischen Realisierungen der Holographie gibt es dabei Grenzen, wie klein ein Fragment werden kann, bevor man diese Eigenschaft zu verlieren beginnt, wobei in der eigentlichen Holographie die Auflösungsgrenzen der holographischen Medien in dieser Beziehung der Hauptfaktor sind. Im Falle eines nicht entstellten Vertriebssignals, für das die Verschlüsselungsvorrichtung von Fig. 5 verwendet wurde und ausserdem unser wie oben "konstruiertes Rauschen" benutzt wurde, wo die Nullen zufällig zu einer 1 oder –1 umgewandelt wurden, ist die Ausdehnung des erforderlichen Fragments lediglich N zusammenhängende Muster eines Signals oder einer Bildrasterzeile, wobei N wie früher definiert die Länge unserer Kennungscodenummer ist. Dies ist ein Informationsextrem, denn praktische Situationen, in denen Rauschen und Entstellung wirksam werden, sollten allgemein eine, zwei oder mehr Grössenordnungen mehr Muster erfordern als diese einfache Anzahl N. Fachleute werden erkennen, dass viele Variablen mitwirken, wenn man genaue statistische Ergebnisse für die Grösse des kleinsten Fragments, mit dem eine Identifizierung erfolgen kann, erhalten will.

[0199] Für Lernzwecke verwendet die Anmelderin auch die Analogie, dass die eindeutige Kennungscodenummer wie eine "Tapete" über ein Bild (oder Signal) gespannt ist. Das heisst, dass sie über das ganze Bild hinweg immer und immer wiederholt wird. Diese Wiederholung der ID-Codenummer kann regelmässig sein, wie bei Benutzung des Codierers der Fig. 5, oder selbst zufällig, wobei die Bits im ID-Code **216** der Fig. 6 nicht in normaler, sich wiederholender Weise durchlaufen werden, sondern bei jedem Muster zufällig ausgewählt werden, und die zufällige Auswahl dann zusammen mit dem Wert des Ausgangs **228** selbst gespeichert wird. Jedenfalls ändert sich der Informationsträger des ID-Codes, nämlich das individuelle eingebettete Codesignal, über das Bild oder Signal hinweg. Somit wird mit der Tapetenanalogie zusammengefasst, dass sich der ID-Code immer und immer wiederholt, dass sich aber die Muster, die bei jeder Wiederholung eingedruckt werden, nach einem allgemein nicht entwendbaren Schlüssel zufällig verändern.

Verlustbehaftete Datenkompression

[0200] Wie schon erwähnt, verträgt die Kennungscodierung der bevorzugten Ausführungsform eine verlustbehaftete Datenkompression und nachfolgende Dekompression. Eine solche Kompression findet zunehmende Verwendung, insbesondere in Situationen wie dem Massenvertrieb von digitalisierten Unterhaltungsprogrammen (Filmen usw.).

[0201] Während Daten, die entsprechend der bevorzugten Ausführungsform der vorliegenden Erfindung codiert worden sind, alle der Anmelderin bekannten Arten von verlustbehafteter Datenkompression vertragen können, sind jedoch die Kompressions-/Dekompressionsnormen CCITT G3, CCITT G4, JPEG; MPEG und JBIG diejenigen, die erwartungsgemäss die kommerziell wichtigsten sein sollten. Die CCITT-Normen finden breite Verwendung zur Schwarzweiss-Dokumentenkompression (zum Beispiel Fax und Dokumentenspeicherung). Für stehende Bilder wird JPEG am meisten verwendet. Für Filmaufnahmen wird MPEG am meisten verwendet. JBIG ist ein wahrscheinlicher Nachfolger der CCITT-Norm zur Verwendung bei Schwarzweissbildern. Solche Verfahren sind den auf dem Gebiet der verlustbehafteten Datenkompression Tätigen wohl bekannt; eine gute Übersicht findet sich bei Pennebaker und Mitautoren, JPEG, Still Image Data Compression Standard [JPEG, Datenkompressionsnorm für stehende Bilder], Van Nostrand Reinhold, New York (1993).

Hin zur eigentlichen Steganographie und zur Verwendung dieser Technik zur Übermittlung komplexerer Botschaften oder Information

[0202] Diese Offenbarung konzentriert sich auf, wie es oben genannt wurde, tapetenartige Ausbreitung eines einzelnen Kennungscodes über ein ganzes Signal hinweg. Dies ist anscheinend ein wünschenswertes Merkmal für viele Anwendungen. Jedoch gibt es andere Anwendungen, wo es wünschenswert erscheinen könnte, Botschaften zu übermitteln oder sehr lange Ketten einschlägiger Daten zur Identifizierung in Signale und Bilder einzubetten. Eine der vielen möglichen, derartigen Anwendungen wäre es, wenn ein gegebenes Signal oder Bild durch mehrere unterschiedliche Gruppen manipuliert werden soll and bestimmte Bereiche eines Bildes für die Identifizierung jeder Gruppe und das Einsetzen der einschlägigen Manipulationsinformation reserviert werden.

[0203] In diesen Fällen kann sich das Codewort **216** in Fig. 6 tatsächlich in irgendeiner vorbestimmten Art und

Weise in Abhängigkeit von der Signal- oder Bildposition ändern. In einem Bild zum Beispiel könnte sich der Code für jede einzelne Rasterzeile des digitalen Bildes ändern. Er könnte ein 16-Bit-Codewort **216** sein, aber jede Abtastzeile hätte ein neues Codewort, daher könnte ein Bild mit 480 Abtastzeilen eine Botschaft von 980 Bytes (480×2 Bytes) übermitteln. Ein Empfänger dieser Botschaft müsste entweder Zugriff zu dem im Speicher **214** gespeicherten Rauschsignal haben oder die universelle Codestruktur des Rauschcodes kennen, sofern diese Codiermethode verwendet wurde. Nach bestem Wissen der Anmelderin ist dies eine neue Herangehensweise auf dem reifen Gebiet der Steganographie.

[0204] In allen drei der vorangehenden Anwendungen universeller Codes wird es oft erwünscht sein, zusätzlich zum universellen Code einen kurzen privaten Code (von vielleicht 8 oder 16 Bits) anzuhängen, den die Benutzer zusätzlich zum universellen Code in eigener Verwahrung halten würden. Dies bietet dem Benutzer noch etwas mehr Sicherheit gegen mögliches Löschen der universellen Codes durch spitzfindige Piraten.

Schlussfolgerung

[0205] Angesichts der grossen Anzahl von verschiedenen Ausführungsformen, in denen die Grundsätze meiner Erfindung angewandt werden können, sollte anerkannt werden, dass die ausführlichen Ausführungsbeispiele nur veranschaulichend sind und nicht als den Rahmen meiner Erfindung begrenzend angesehen werden sollten. Als meine Erfindung beanspruche ich vielmehr all die Ausführungsformen, die innerhalb des Bereichs der folgenden Ansprüche liegen.

Patentansprüche

1. Verfahren zum Einbetten eines steganographischen Kodes in ein Bildsignal, das eine Anzahl von Elementen enthält, denen jeweils am Wert zugeordnet ist, wobei das Verfahren umfasst:
das Generieren eines variablen Multi-Bit-Identifikationskodes; und
das Verändern des Bildsignals entsprechend einem eingebetteten Signal, um den Identifikationskode darin einzubetten, wobei die eingebetteten und veränderten Signale jeweils eine Anzahl von Elementen enthalten, denen jeweils ein Wert zugeordnet ist, wobei ein Element des Veränderten Signals einen Wert hat, der sich von dem von korrespondierenden Elementen in sowohl den Bildsignalen als auch den eingebetteten Signalen unterscheidet, und wobei der Identifikationskode und Pseudo-Zufallsreferenzdaten verwendet werden, um das eingebettete Signal zu generieren, wobei die Zuordnung zwischen dem eingebetteten Signal und dem Identifikationskode ohne Verfügbarkeit der Referenzdaten nicht erkennbar ist;
wobei das Verändern des Bildsignals das Einbetten des Identifikationskodes an Elementen in das Bildsignal einschließt, so dass der Identifikationskode redundant auf die Elemente in dem Bildsignal verteilt wird, und Instanzen des redundant verteilten Identifikationskodes werden in unterschiedlichen Elementen in dem Bildsignal unterschiedlich entsprechend von Daten repräsentiert, die unabhängig von dem Bildsignal sind, wobei bei der Einbettung Elemente des Identifikationskodes verwendet werden, um Bildeigenschaften in korrespondierenden Elementen in dem Bildsignal zu verändern, so dass die Veränderungen den Identifikationskode in einer im Wesentlichen nicht erkennbaren Weise transportieren.

2. Verfahren gemäß Anspruch 1, wobei das Bildsignal ein Bild umfasst, das auf ein Dokument gedruckt werden soll, und der Kode automatisch aus einem gescannten Bild des Dokuments lesbar ist.

3. Verfahren gemäß Anspruch 1, wobei das Bildsignal Video umfasst und der Multi-Bit-Identifikationskode über mehrere Einzelbilder verteilt wird.

4. Verfahren gemäß Anspruch 1 oder 2, wobei die Daten, die unabhängig von dem Bildsignal sind, einen Schlüssel umfassen.

5. Verfahren gemäß Anspruch 1 oder 2, wobei die Daten, die unabhängig von dem Bildsignal sind, eine Zufallszahl umfassen.

6. Verfahren gemäß Anspruch 5, wobei die Zufallszahl eine Pseudo-Zufallszahl umfasst.

Es folgen 7 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 4

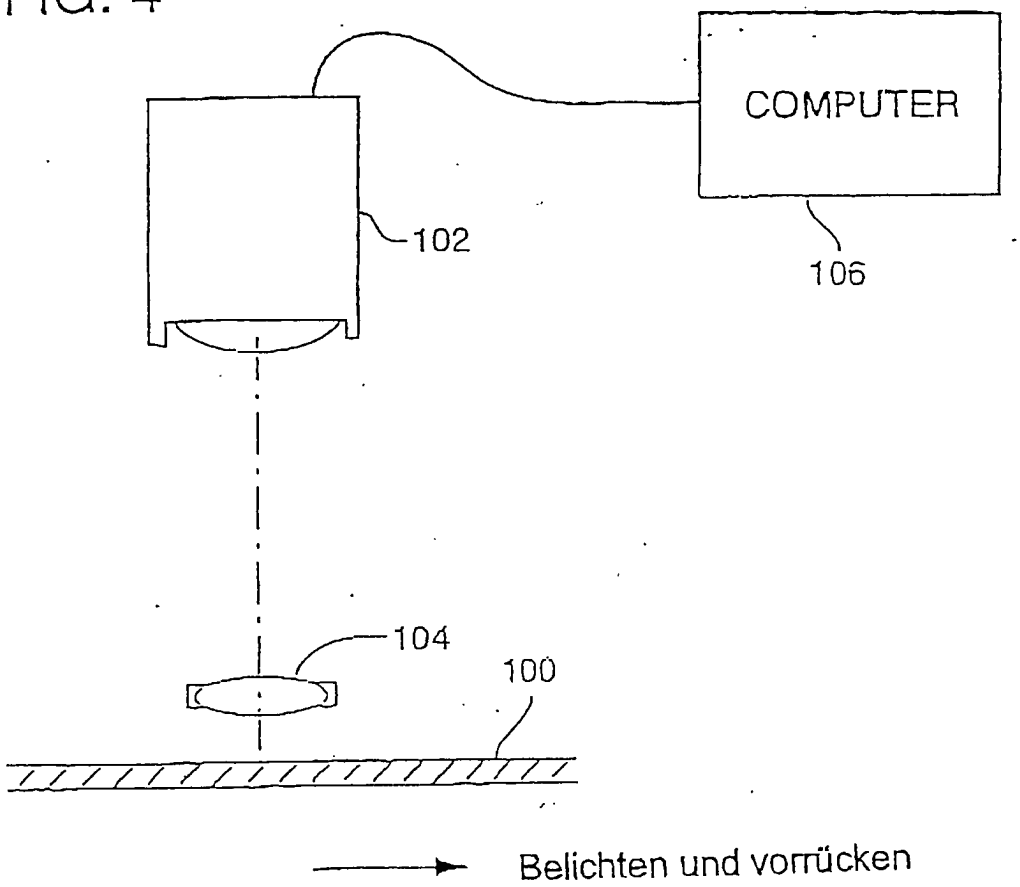
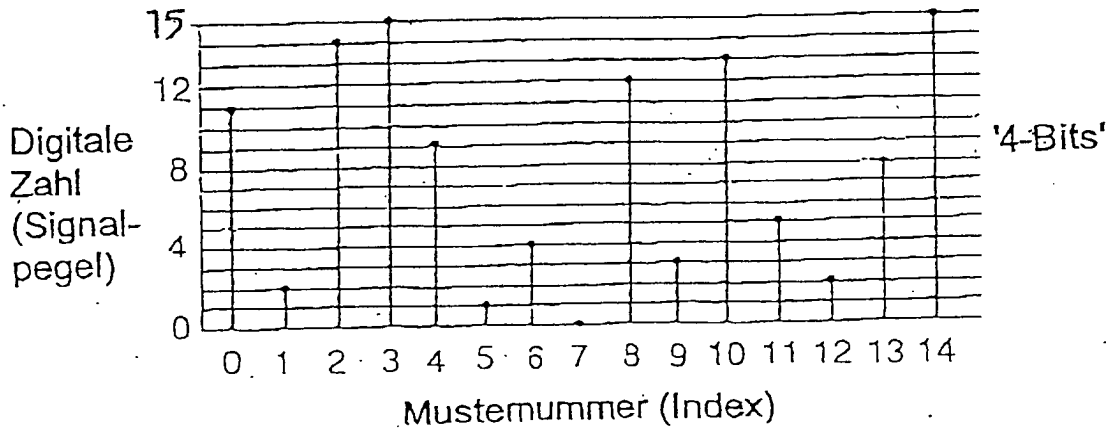
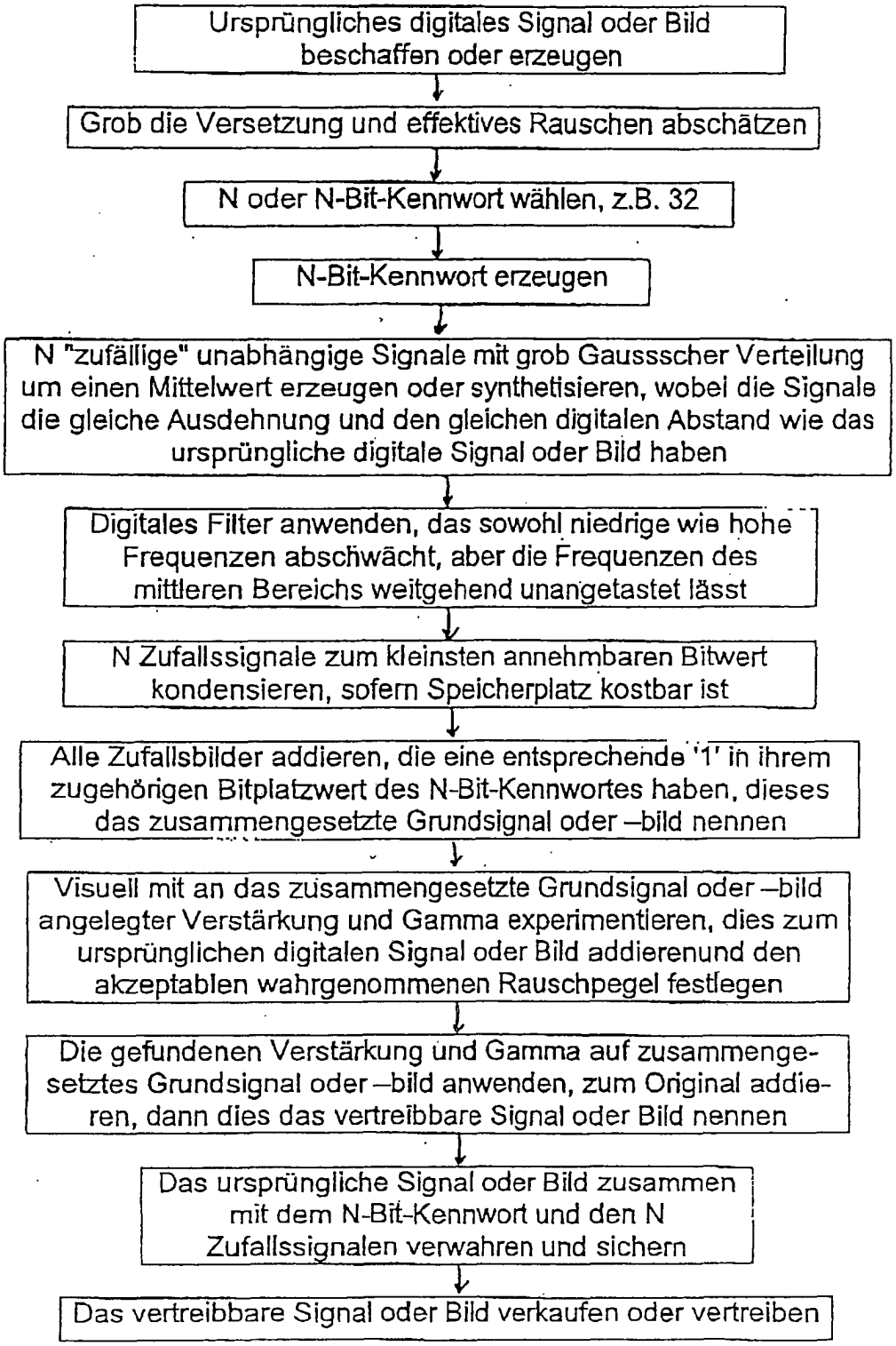


FIG. 1



Figur 2


Ursprüngliches digitales Signal oder Bild beschaffen oder erzeugen
Grob die Versetzung und effektives Rauschen abschätzen
N oder N-Bit-Kennwort wählen, z.B. 32
N-Bit-Kennwort erzeugen
N "zufällige" unabhängige Signale mit grob Gaussscher Verteilung um einen Mittelwert erzeugen oder synthetisieren, wobei die Signale die gleiche Ausdehnung und den gleichen digitalen Abstand wie das ursprüngliche digitale Signal oder Bild haben
Digitales Filter anwenden, das sowohl niedrige wie hohe Frequenzen abschwächt, aber die Frequenzen des mittleren Bereichs weitgehend unangetastet lässt
N Zufallssignale zum kleinsten annehmbaren Bitwert kondensieren, sofern Speicherplatz kostbar ist
Alle Zufallsbilder addieren, die eine entsprechende '1' in ihrem zugehörigen Bitplatzwert des N-Bit-Kennwortes haben, dieses das zusammengesetzte Grundsignal oder –bild nennen
Visuell mit an das zusammengesetzte Grundsignal oder –bild angelegter Verstärkung und Gamma experimentieren, dies zum ursprünglichen digitalen Signal oder Bild addierenund den akzeptablen wahrgenommenen Rauschpegel festlegen
Die gefundenen Verstärkung und Gamma auf zusammengesetztes Grundsignal oder –bild anwenden, zum Original addieren, dann dies das vertreibbare Signal oder Bild nennen
Das ursprüngliche Signal oder Bild zusammen mit dem N-Bit-Kennwort und den N Zufallssignalen verwahren und sichern
Das vertreibbare Signal oder Bild verkaufen oder vertreiben

Figur 3

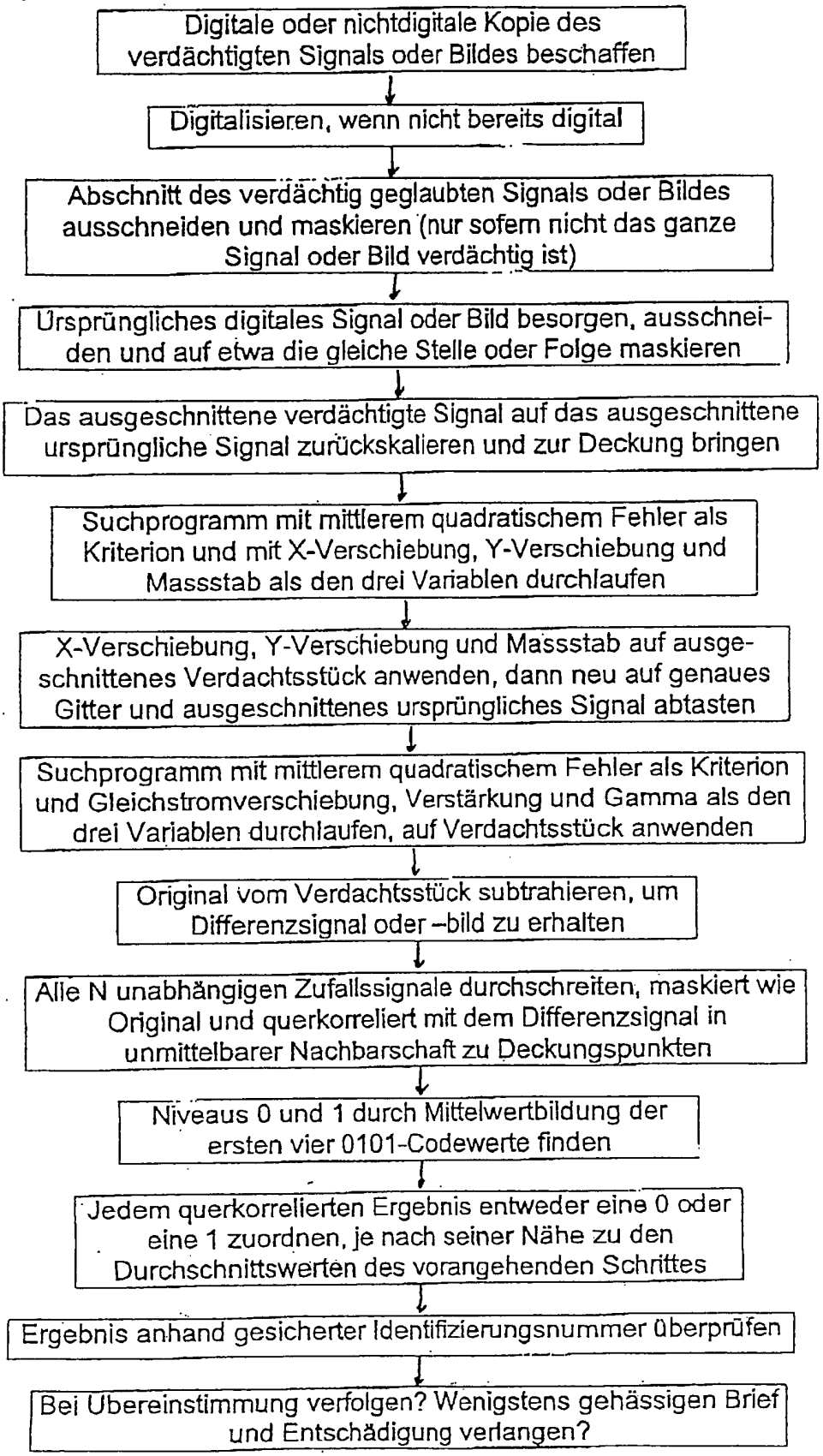

Digitale oder nichtdigitale Kopie des verdächtigten Signals oder Bildes beschaffen
Digitalisieren, wenn nicht bereits digital
Abschnitt des verdächtig geglaubten Signals oder Bildes ausschneiden und maskieren (nur sofern nicht das ganze Signal oder Bild verdächtig ist)
Ursprüngliches digitales Signal oder Bild besorgen, ausschneiden und auf etwa die gleiche Stelle oder Folge maskieren
Das ausgeschnittene verdächtigte Signal auf das ausgeschnittene ursprüngliche Signal zurückskalieren und zur Deckung bringen
Suchprogramm mit mittlerem quadratischem Fehler als Kriterion und mit X-Verschiebung, Y-Verschiebung und Massstab als den drei Variablen durchlaufen
X-Verschiebung, Y-Verschiebung und Massstab auf ausgeschnittenes Verdachtsstück anwenden, dann neu auf genaues Gitter und ausgeschnittenes ursprüngliches Signal abtasten
Suchprogramm mit mittlerem quadratischem Fehler als Kriterion und Gleichstromverschiebung, Verstärkung und Gamma als den drei Variablen durchlaufen, auf Verdachtsstück anwenden
Original vom Verdachtsstück subtrahieren, um Differenzsignal oder –bild zu erhalten
Alle N unabhängigen Zufallssignale durchschreiten, maskiert wie Original und querkorreliert mit dem Differenzsignal in unmittelbarer Nachbarschaft zu Deckungspunkten
Niveaus 0 und 1 durch Mittelwertbildung der ersten vier 0101-Codewerte finden
Jedem querkorrelierten Ergebnis entweder eine 0 oder eine 1 zuordnen, je nach seiner Nähe zu den Durchschnittswerten des vorangehenden Schrittes
Ergebnis anhand gesicherter Identifizierungsnummer überprüfen
Bei Übereinstimmung verfolgen? Wenigstens gehässigen Brief und Entschädigung verlangen?

FIG. 5

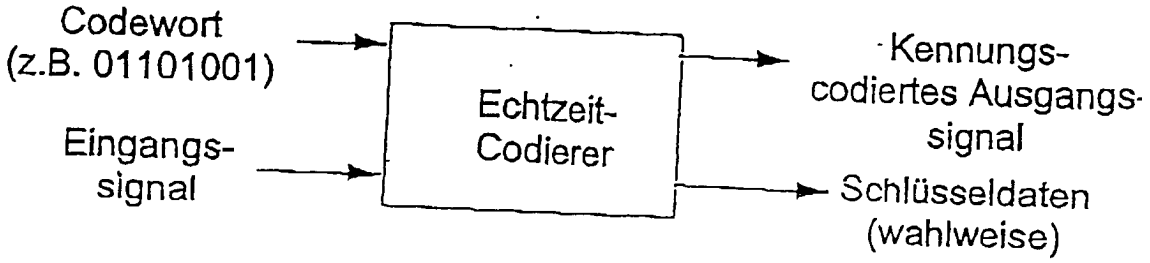
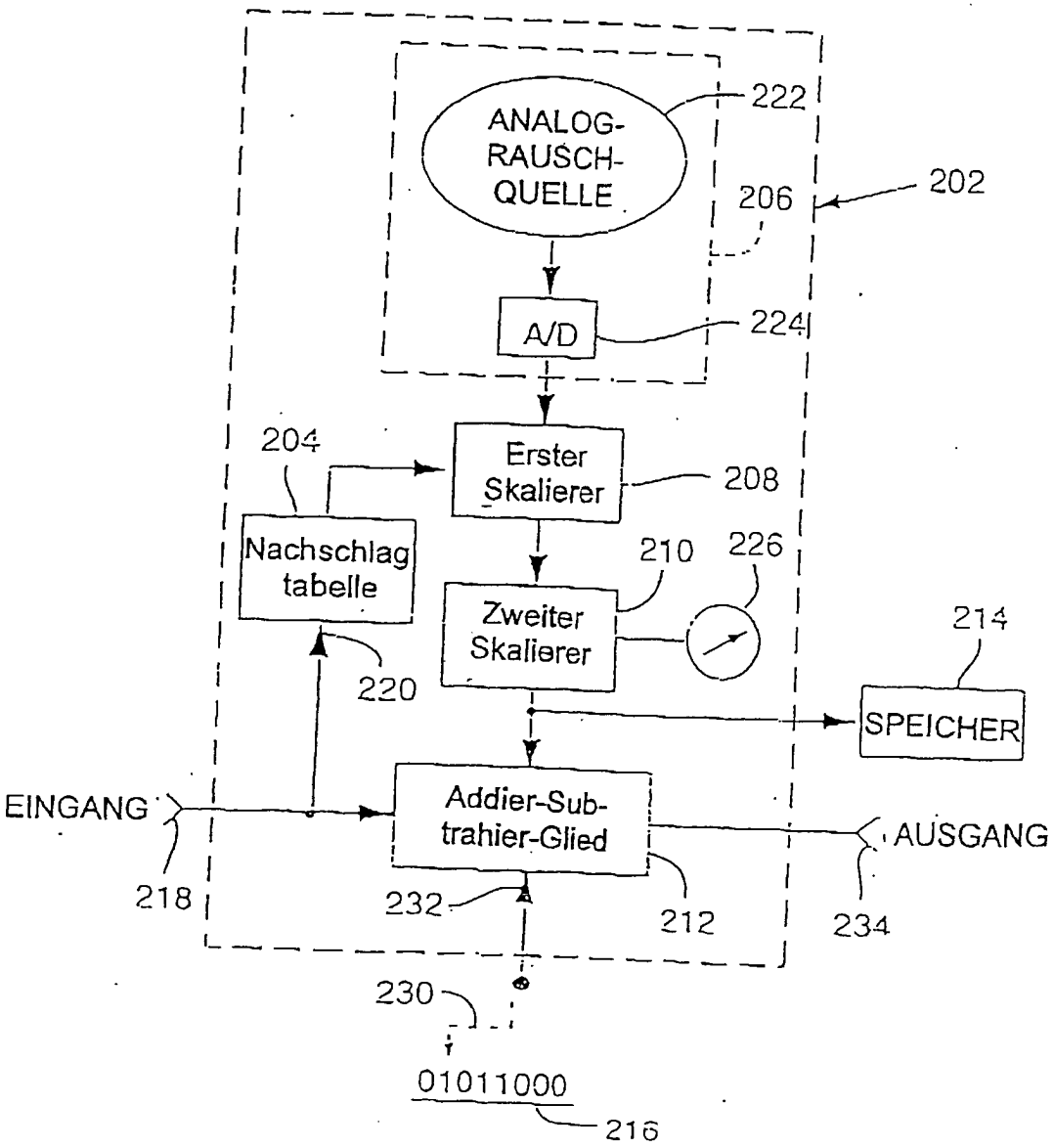

Codewort
(z.B. 01101001)
Eingangs-
signal
Echtzeit-
Codierer
Kennungs-
codiertes Ausgangs-
signal
Schlüsseldaten
(wahlweise)

FIG. 6


ANALOG-
RAUSCH-
QUELLE
222
206
202
A/D
224
204
Erster
Skalierer
208
Nachschlag
tabelle
210
226
Zweiter
Skalierer
214
220
SPEICHER
EINGANG
Addier-Sub-
trahier-Glied
AUSGANG
218
232
212
234
230
01011000
216

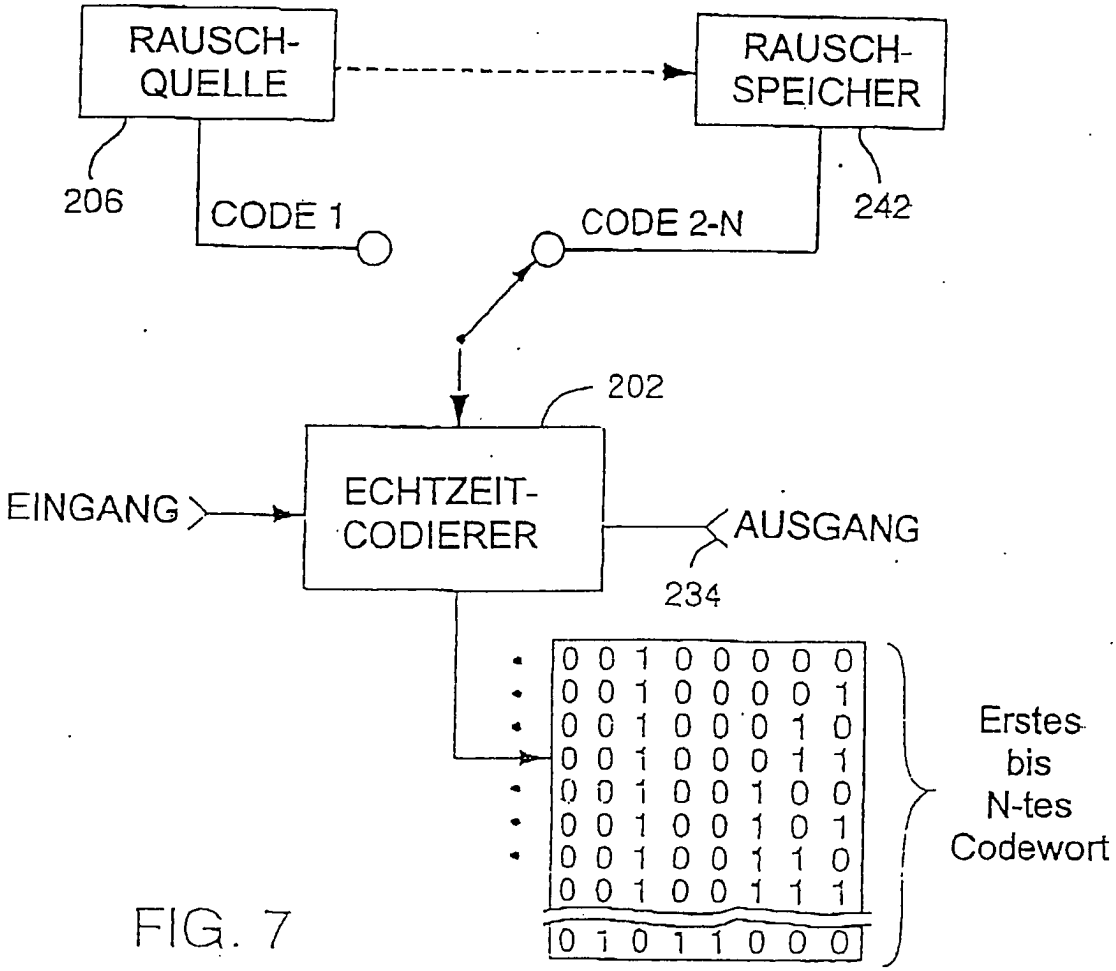

RAUSCH-
QUELLE
RAUSCH-
SPEICHER
206
CODE 1
CODE 2-N
242
202
EINGANG
ECHTZEIT-
CODIERER
AUSGANG
234
0 0 1 0 0 0 0 0
0 0 1 0 0 0 0 1
0 0 1 0 0 0 1 0
0 0 1 0 0 0 1 1
0 0 1 0 0 1 0 0
0 0 1 0 0 1 0 1
0 0 1 0 0 1 1 0
0 0 1 0 0 1 1 1
0 1 0 1 1 0 0 0
Erstes
bis
N-tes
Codewort

FIG. 7

FIG. 8

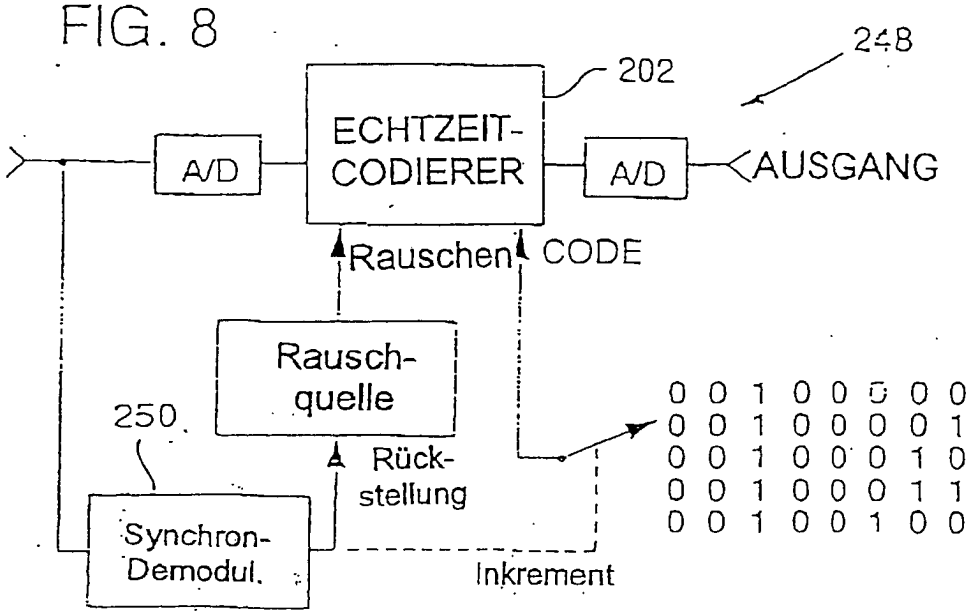

248
202
ECHTZEIT-
CODIERER
A/D
A/D
AUSGANG
Rauschen
CODE
Rausch-
quelle
250
Rück-
stellung
Synchron-
Demodul.
Inkrement
0 0 1 0 0 0 0 0
0 0 1 0 0 0 0 1
0 0 1 0 0 0 1 0
0 0 1 0 0 0 1 1
0 0 1 0 0 1 0 0

FIG. 9A

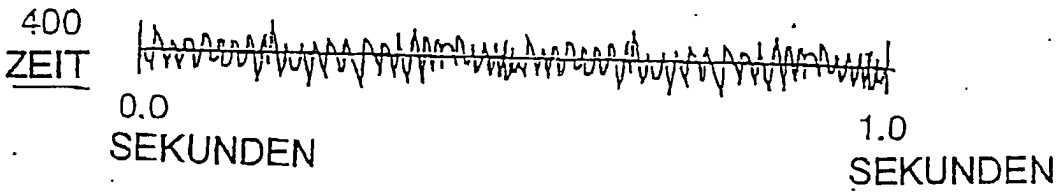


FIG. 9B

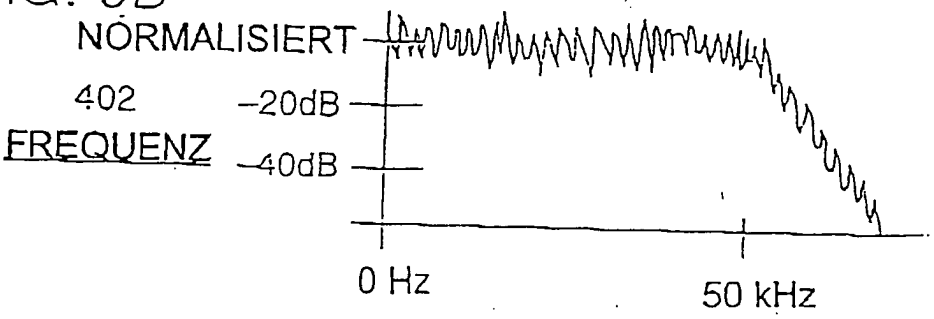


FIG. 9C

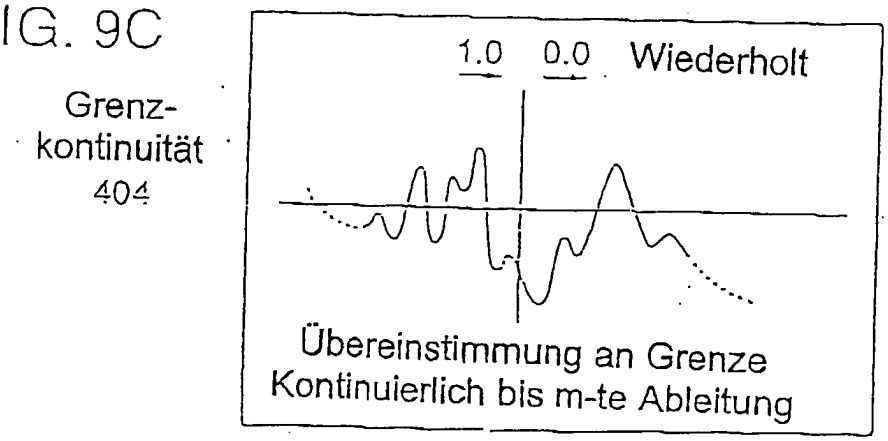


FIG. 10

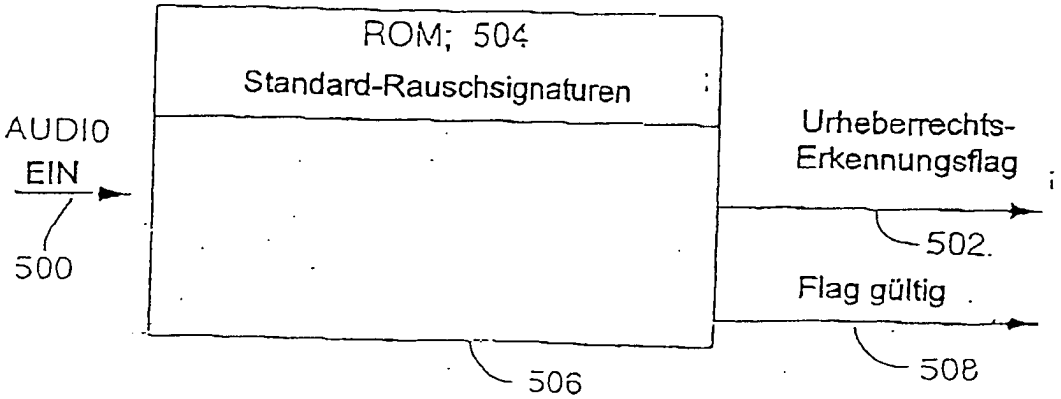


FIG. 11

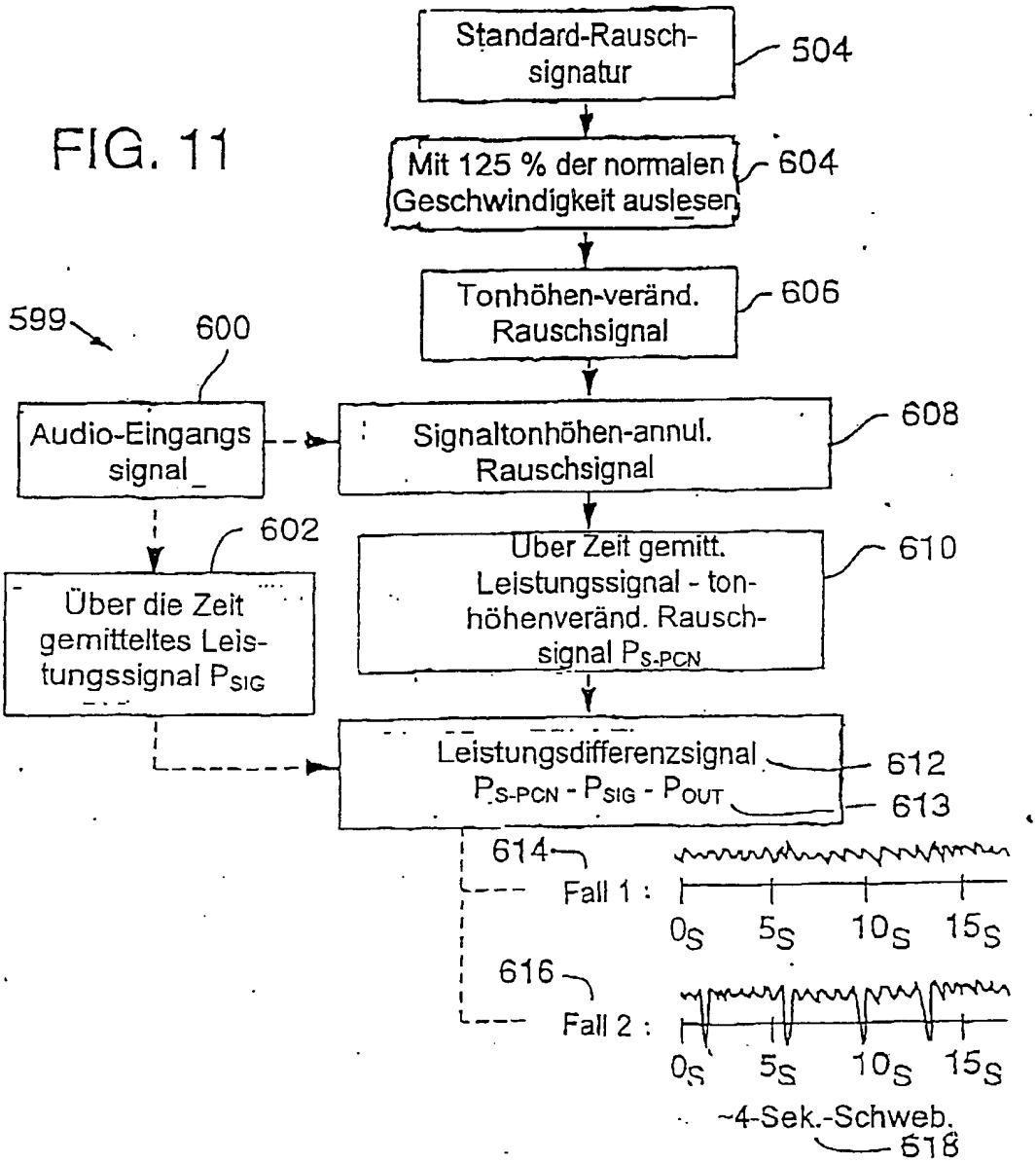
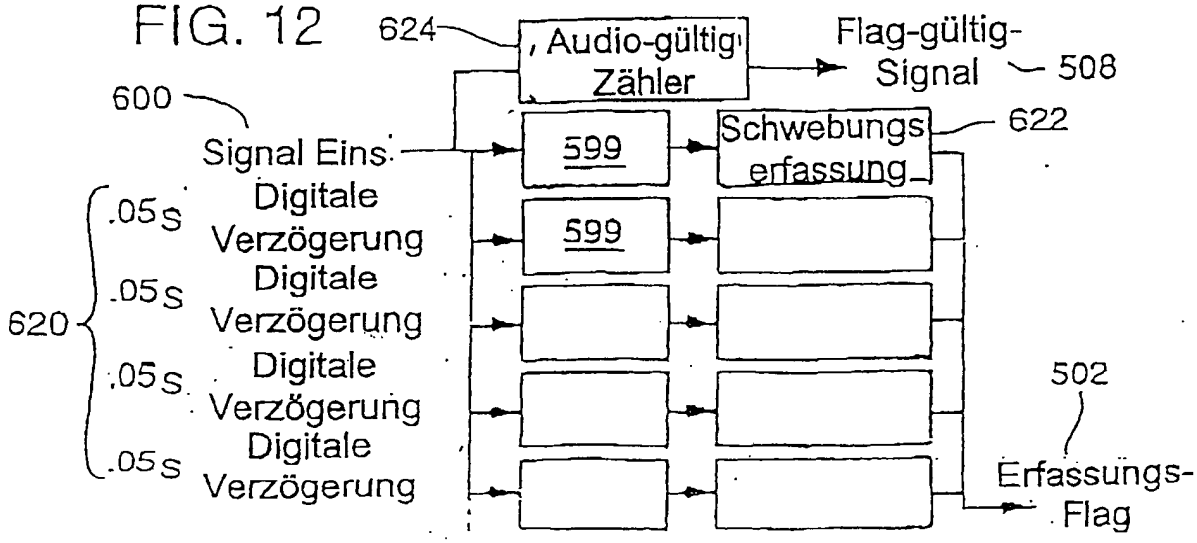

Standard-Rausch-signatur
504
Mit 125 % der normalen Geschwindigkeit auslesen
604
Tonhöhen-veränd. Rauschsignal
606
599
600
Audio-Eingangs signal
Signaltonhöhen-annul. Rauschsignal
608
602
Über die Zeit gemitteltes Leistungssignal P_{SIG}
Über Zeit gemitt. Leistungssignal - tonhöhenveränd. Rauschsignal P_{S-PCN}
610
Leistungsdifferenzsignal $P_{S-PCN} - P_{SIG} - P_{OUT}$
612
613
614
Fall 1 :
0S 5S 10S 15S
616
Fall 2 :
0S 5S 10S 15S
~4-Sek.-Schweb.
618

FIG. 12


624
Audio-gültig Zähler
Flag-gültig-Signal
508
600
Signal Eins
599
Schwebungserfassung
622
620
.05S Digitale Verzögerung
.05S Digitale Verzögerung
.05S Digitale Verzögerung
.05S Digitale Verzögerung
599
502
Erfassungs-Flag