

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-124950

(P2012-124950A)

(43) 公開日 平成24年6月28日(2012.6.28)

(51) Int.Cl.		F I		テーマコード(参考)
HO4N 7/167 (2011.01)		HO4N	7/167	5C164
HO4L 9/14 (2006.01)		HO4L	9/00 641	5J104

審査請求 有 請求項の数 4 OL (全 9 頁)

(21) 出願番号 特願2012-42655 (P2012-42655)
 (22) 出願日 平成24年2月29日(2012.2.29)
 (62) 分割の表示 特願2008-520725 (P2008-520725) の分割
 原出願日 平成18年3月30日(2006.3.30)
 (31) 優先権主張番号 102005033285.4
 (32) 優先日 平成17年7月15日(2005.7.15)
 (33) 優先権主張国 ドイツ(DE)

(71) 出願人 507061959
 インスティトゥート フュール ルントフ
 ンクテヒニク ゲー・エム・ペー・ハー
 Institute fuer Rund
 funktechnik GmbH
 ドイツ連邦共和国 デー-80939 ミ
 ュンヘン フロリアンスミュールシュトラ
 ーセ 60
 Florianismuehlstrass
 e 60 D-80939 Muench
 en, Bundesrepublik
 Deutschland

(74) 代理人 100062993
 弁理士 田中 浩

最終頁に続く

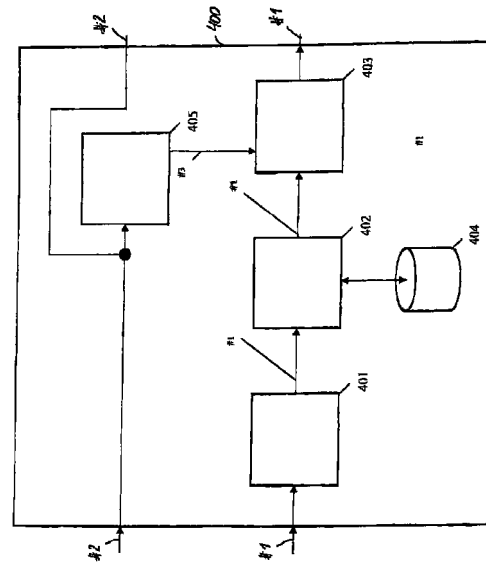
(54) 【発明の名称】 画像および/または音声情報のデジタル信号の入力デジタル・データストリームを受信する消費者用の電子機器

(57) 【要約】

【課題】 許可情報に基づいて画像/音声コンテンツを非暗号形式で利用できるようにする。

【解決手段】 画像/音声情報のデジタル信号の入力デジタル・データストリーム(1)を受信する電子機器において、デジタル信号は送信前に暗号化されてよく、入力デジタル・データストリームは許可情報(2)を含む。電子機器は、入力デジタル・データストリームから許可情報を取出す取出部(405)、入力デジタル・データストリームの入力デジタル信号が暗号化されているか否かを検出する検出部、暗号化デジタル信号を解読し解読デジタル信号を生成する解読部、及び画像/音声情報の非暗号デジタル信号を暗号化する暗号化部(403)を含む。入力デジタル・データストリームが非暗号デジタル信号を含み許可情報に暗号化を無効にする暗号命令信号(3)が含まれない場合、暗号化部は入力デジタル・データストリームの画像/音声情報のデジタル信号を暗号化する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

画像および/または音声情報のデジタル信号の入力デジタル・データストリーム(1)を受信する消費者用の電子機器であって、

前記デジタル信号は送信前に暗号化されたものであってもよく、前記入力デジタル・データストリームはさらに許可情報(2)を含むものであり、

前記入力デジタル・データストリームから前記許可情報を取り出す取出し部(405)と、

前記受信された入力デジタル・データストリームにおける前記デジタル信号が暗号化されているか否かを検出する検出部と、

前記受信された暗号化されたデジタル信号を暗号解読して、暗号解読されたデジタル信号を生成する暗号解読部(401)と、

を含み、

前記取出し部(405)は、さらに、前記許可情報に暗号命令信号(3)が含まれている場合に前記入力デジタル・データストリームから暗号命令信号を取り出すよう構成されており、

さらに、画像および/または音声情報の非暗号のデジタル信号を暗号化する暗号化部(403)を含み、

前記入力デジタル・データストリームが非暗号のデジタル信号を含み、かつ前記許可情報に暗号化を無効にするタイプの暗号命令信号(3)が含まれていない場合に、出力デジタル・データストリームを生成するために、前記暗号化部(403)は、前記入力デジタル・データストリームにおける画像および/または音声情報のデジタル信号を暗号化するよう構成されているものであること

を特徴とする、電子機器。(図1)

【請求項 2】

画像および/または音声情報のデジタル信号の入力デジタル・データストリーム(1)を受信する消費者用の電子機器であって、

前記デジタル信号は送信前に暗号化されたものであってもよく、前記入力デジタル・データストリームはさらに許可情報(2)を含むものであり、

前記入力デジタル・データストリームから前記許可情報を取り出す取出し部(405)と、

前記受信された入力デジタル・データストリームにおける前記デジタル信号が暗号化されているか否かを検出する検出部と、

前記許可情報に応答して前記デジタル・データストリームを暗号解読してデジタル信号を生成する暗号解読部(401)と、

を含み、

前記入力デジタル・データストリームはさらに暗号命令信号(3)を含み、前記取出し部(40)は、前記入力デジタル・データストリームから前記暗号命令信号を取り出すよう構成されており、

さらに、前記入力デジタル・データストリームの画像および/または音声情報の非暗号のデジタル信号を暗号化する暗号化部(403)を含み、

前記非暗号のデジタル信号は前記暗号解読部(401)において暗号解読されたものであってもよく、

前記入力デジタル・データストリームが暗号化されたデジタル信号を含み、かつ前記暗号命令信号(3)が暗号化を無効にするタイプのものである場合に、前記暗号化部(403)は、前記暗号化を無効にする種類の暗号命令信号に応答して、前記入力デジタル・データストリームの画像および/または音声情報の前記デジタル信号を暗号化せずに、画像および/または音声情報の非暗号のデジタル信号の出力デジタル・データストリームを生成するよう構成されており、

さらに、前記出力デジタル・データストリームを供給するための出力を含むこと

を特徴とする、電子機器。(図1)

【請求項3】

画像および/または音声情報のデジタル信号の入力デジタル・データストリーム(1)を受信する消費者用の電子機器であって、

前記デジタル信号は送信前に暗号化されたものであってもよく、前記入力デジタル・データストリームはさらに許可情報(2)を含むものであり、

前記入力デジタル・データストリームから前記許可情報を取り出す取出し部(405)と、

前記受信された入力デジタル・データストリームにおける前記デジタル信号が暗号化されているか否かを検出する検出部と、

前記受信された暗号化されたデジタル信号を暗号解読して、暗号解読されたデジタル信号を生成する暗号解読部(401)と、

を含み、

前記許可情報は暗号命令信号(3)を含み、前記取出し部(405)はさらに前記入力デジタル・データストリームから前記暗号命令信号を取り出すよう構成されており、

さらに、画像および/または音声情報の非暗号のデジタル信号を暗号化する暗号化部(403)を含み、

前記入力デジタル・データストリームが非暗号のデジタル信号を含み、かつ前記暗号命令信号(3)が暗号化を有効にするタイプのものである場合に、出力デジタル・データストリームを生成するために、前記暗号化部(403)は、暗号化を有効にする種類の暗号命令信号にตอบสนองして前記入力デジタル・データストリームにおける画像および/または音声情報のデジタル信号を暗号化するよう構成されているものであること

を特徴とする、電子機器。(図1)

【請求項4】

さらに、前記暗号命令信号を前記出力デジタル・データストリーム(1、2)に含ませるよう構成されていることを特徴とする、請求項1乃至3のいずれかに記載の電子機器

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、画像および/または音声(音響)情報のデジタル信号の入力デジタル・データストリームを受信する電子機器に関する。

【0002】

実施形態は、音声(音響)および/または画像コンテンツ(内容)を再送信(Weiteruebertragen: 転送、再伝送)し並びに処理および/または再生および/または蓄積(Speichern)する方法および装置(Einrichtung: 設備)に関し、また音声および/または画像コンテンツを処理および/または再生および/または蓄積する機器(Geraet: 装置)に関する。

【背景技術】

【0003】

保護された音声(音響)および/または画像コンテンツ(内容)を含む予め記録された記録媒体の、パーソナル・コンピュータ・プログラムによる不法(illegale: 非合法的)コピーに対して、その不法コピーを困難にしたりは防止する多くの技術的防御手段が提供されている。このようなコピー保護システムに対して、“コンテンツの保護およびコピー管理(CPCM: Content Protection and Copy Management)”システムは、或る指定されたライセンス(許可)条項および条件(license terms and conditions)においてのみそのコンテンツの記録媒体の使用を許可する。CPCMシステムの基本的な思想(アイデア)は、そのコンテンツの許可されたそれぞれの使用に対して別々の信号を与えることであり、その信号は、画像および/または音声コンテンツに付加され、適した受信機によって評価される。画像および/または音声の米国制作者(プロデューサ)は、コンテン

10

20

30

40

50

ツのコピーのみならず、最小のディテール（精細度、詳細）にまでいたる前記コンテンツを用いて実行される任意の処理（動作、操作）を制御する相異なる最大55までの信号伝送（シグナリング）を想定しており、それによって、“許可された領域”内でのみ（即ち、許可された区域（エリア）、例えば許可されたユーザの宅内（家庭内）でのみ）のスペースに制限されたコンテンツの使用が許可される。

【0004】

しかし、消費者（コンシューマ）の電子機器におけるそのような非常に多くの信号の変換は複雑であり、コストを上昇させることが予想される。消費者の電子機器のみならず将来のPCにおいても適した方法が実現されよう。既に使用されている方法は、いわゆる条件付きアクセス（Conditional Access：CA）システムであり、このシステムによってペイTV（有料TV：Pay-TV）プロバイダは、スマート・カードを介して、暗号化（verschlüsselt：コード化、符号化）された形式で送信された画像および/または音声コンテンツへのアクセスが制御される。しかし、これらのシステム単独では、CPMシステムの拡張された要求に対しては不十分であり、適当な形態で増強（拡張）する必要がある。スマート・カードによって暗号化されたコンテンツが機器（デバイス）の出力において利用可能になると直ぐに、そのコンテンツはCAシステムの排他的（独占的）使用の場合に制限なしで再生し、処理しまたは蓄積（記録）することが可能になる。その拡張は所謂マクロビジョン（macrovision）信号であり、その信号は、テレビジョン受像機のスクリーン上にペイTV放送の再生のみを許可し、VCR（ビデオカセット・レコーダ、VTR）での記録は許可しないもの、と想定される。

10

20

【0005】

一方、暗号化（Verschuesselung：encoding、コード化、符号化）にのみ（排他的に）基づくCPMシステムは、公共放送会社にとって、および“無料放送サービス（Free-to-Air）”放送プロバイダにとっても、基本的に（原則として）許容できない。これらの放送会社によって放送されるコンテンツは将来においても非暗号化（unverschlüsselt：unencoded）状態を維持しなければならず、制限なしに記録が可能でなければならない。消費者の宅内の種々の再生装置相互間のインタフェースへの転送（伝送）もまた非暗号形式で実現されるべきである。しかし、無線（ワイヤレス）LANのような無線システムでは、消費者の宅内で伝送されたコンテンツの暗号化は、近隣者による傍受を防止するために有意義である（有効である、意味がある）。特に、インターネットへのアクセス機能を有するPC（パーソナル・コンピュータ）および放送受信用のセットトップ・ボックス（set-top boxes）は、ケーブルによる配線の費用なしにそのような無線ホーム・システムを使用して消費者の宅内でその他の装置との間にネットワークを形成する。

30

【先行技術文献】

【特許文献】

【0006】

【特許文献1】米国特許出願公開第2003/076955号明細書

【発明の開示】

【0007】

本発明の目的は、暗号化（verschlüsselt）されたまたは非暗号（unverschlüsselt）の音声および/または画像コンテンツの送信および受信のための単一システム内で末端のユーザによって自由にアクセスできるコンテンツの非暗号化処理および/または再生および/または蓄積（記録）のために公共放送会社および“無料放送システム（Free-to-Air）”プログラム（番組）プロバイダの要求に適合する手段を提供することである。

40

【0008】

この目的は、特別な使用許可情報（Nutzungsberechtigungsinformation：use authorization information、使用権限情報）が、受信信号中に含まれており、また音声および/または画像コンテンツが受信時に非暗号形式で末端（エンド）ユーザ（最終使用者）にとって利用可能であることを示し、さらにその音声および/または画像コンテンツがオプションとして（任意選択的に）カスケード（順次送信、連結、縦続）され暗号化されて送信

50

された場合においても付加状態を維持し；さらに、その特別な使用許可情報によって、暗号形式で転送（Weiteruebertragen：伝送）された画像および／または音声コンテンツを処理および／または再生および／または蓄積（記録）するときに転送カスケード（従続接続段）の少なくとも最後（端部、最後の段）までにおいてその画像および／または音声コンテンツが暗号解読（復号）されるような、上述のタイプの方法および装置（デバイス）によって実現される。

【 0 0 0 9 】

実施形態による方法および装置で使用される機器（Geraet：装置）が実施形態 3 に示されている。

【 0 0 1 0 】

本発明は、特別な使用許可情報と共に非暗号形式で末端のユーザが自由に利用（入手）可能な画像および／または音声コンテンツを提供するという思想に基づくものであり、その特別な使用許可情報は、その伝播路の途中でまたは伝播路（伝送路）に沿って複数回の暗号化および暗号解読（Entschluesselung：復号）される时候にも画像および／または音声コンテンツに“付加（添付）（klebt）”された状態にあるか、またはその情報が音声および／または画像コンテンツとは独立して伝送／蓄積されてもそのコンテンツに論理的にリンク（結合、連結）した状態を維持しており、また、それによって、暗号化が行われる場合に末端のユーザにおいてその画像および／または音声コンテンツの暗号解読（復号）を、使用可能で有効な様々な場所、少なくともその伝播路の末端までにおいて行わせる。

【 図面の簡単な説明 】

【 0 0 1 1 】

【 図 1 】 図 1 は、本発明による消費者用電子機器のブロック回路図である。

【 図 2 】 図 2 は、暗号または非暗号の画像信号および／または音声信号を受信し、これらを図 1 による消費者用電子機器に送信するための、末端ユーザの宅内に存在する島状（孤立）ネットワークのブロック回路図である。

【 図 3 】 図 3 は、任意の種類 of 伝送ネットワークから受信した画像および／または音声コンテンツの再送信のための受信機とメモリのカスケード接続のブロック回路図である。

【 発明を実施するための形態 】

【 0 0 1 2 】

以下、図示の実施形態を参照して本発明をさらに詳細に説明する。

1．実施形態において、任意の種類 of 伝送ネットワークから暗号または非暗号形式で受信した信号の画像および／または音声コンテンツを転送、および処理および／または再生および／または蓄積する方法において、

前記受信した信号は前記画像および／または音声コンテンツの許可された使用を示す使用許可情報（2）を含み、

前記使用許可情報（2）は、前記画像および／または音声コンテンツが受信時に非暗号形式で末端ユーザにとって利用可能であることを通知する非暗号化命令（3）を含み、

前記使用許可情報（2）は、前記画像および／または音声コンテンツのオプションとしてカスケード化（連結）された暗号化転送の場合でも、前記画像および／または音声コンテンツに付加された状態を維持し、または前記画像および／または音声コンテンツと同時に

（並行して）物理的に分離して送信される場合でも、適当な手段によって論理的にリンク（結合）された状態を維持し、

さらに、前記非暗号化命令（3）は、暗号形式で転送された前記画像および／または音声コンテンツを処理および／または再生および／または蓄積するときに、転送カスケード（縦続接続）の最後の段またはそれより前の段において前記画像および／または音声コンテンツの暗号解読（復号）を行わせる。

2．実施形態において、任意の種類 of 伝送ネットワークから暗号または非暗号形式で受信した信号の画像および／または音声コンテンツを転送、および処理および／または再生および／または蓄積する装置において、

10

20

30

40

50

前記受信した信号は前記画像および／または音声コンテンツの許可された使用を示す使用許可情報(2)を含み、

前記使用許可情報(2)は、前記画像および／または音声コンテンツが受信時に非暗号形式で末端ユーザにとって利用可能であるべきことを通知する非暗号化命令(3)を含み、前記使用許可情報(2)は、前記画像および／または音声コンテンツのオプションとしてカスケード化された暗号化転送の場合でも付加された状態を維持し、または前記画像および／または音声コンテンツと同時に送信される場合でも適当な手段によって論理的にリンクされた状態を維持するが前記画像および／または音声コンテンツから物理的に分離しており、

さらに、前記非暗号化命令(3)は、暗号形式で転送された前記画像および／または音声コンテンツを処理および／または再生および／または蓄積するときに、転送カスケードの最後の段またはそれより前の段において分析されて、前記画像および／または音声コンテンツの暗号解読(復号)を行わせるようにする。

3. 実施形態において、任意の種類ネットワークから暗号または非暗号形式で受信され前記1に記載の方法に従って暗号形式で転送される信号の画像および／または音声コンテンツの処理および／または再生および／または蓄積する機器において、

前記受信した信号は前記画像および／または音声コンテンツの許可された使用を示す使用許可情報(2)を含み、

前記使用許可情報(2)中に含まれる非暗号化命令(3)は、暗号形式で転送された前記画像および／または音声コンテンツを処理および／または再生および／または蓄積するときに、読み出されて分析されて、前記画像および／または音声コンテンツの暗号解読(復号)が行われるようにする。

【0013】

図1に示す消費者用電子機器400は、図示されていない伝送ネットワークから、暗号形式または非暗号形式の画像および／または音声コンテンツ1と使用許可情報2とを受信する。本発明によれば、使用許可情報2は、常に画像および／または音声コンテンツ1に付加された状態を維持しているか、またはこれが画像および／または音声コンテンツ1と共に同時にまたは並行して伝送されたとしても適した手段によってそのコンテンツに論理的にリンクされた状態を維持しているが、その使用許可情報2は、そのコンテンツ1が末端ユーザの再生または蓄積(記録)装置へのその伝送路の途中で(に沿って)暗号化または暗号解読(復号)されているか否かに関係なくその画像および／または音声から物理的に分離される。その使用許可情報2は、画像および／または音声コンテンツが暗号化されている場合には各送信または転送における少なくとも終了位置までにおいて画像および／または音声コンテンツの暗号解読(復号)を行わせる。

【0014】

図1における典型例では、機器400への暗号化された(verschlusstes)入力信号はその機器内に設けられた暗号解読器(Entschluester:復号器)401に供給され、そこで暗号解読(復号)される。非暗号の(unverschlusstes:暗号化されていない)入力信号は、変化することなく暗号解読器401中を通過する(durchgeschleift)。暗号解読器401の出力における非暗号(平文)の画像および音声コンテンツは、後続段402で処理されて、必要に応じてメモリ404に格納(蓄積)される。その処理された画像および／または音声コンテンツは、制御入力を介して分析器(Auswerter:評価器、判定器)405に接続された暗号化器(Verschluester:符号化器)403に供給される。分析器405は、送信(伝送)された使用許可情報2全体を分析(判定、評価)し、そこに含まれ得る非暗号化(nicht zu verschluesteln:non-encoding、暗号化させない)命令3を濾波して取り出す。この命令3は、暗号化器403に送られ、そこで暗号化を阻止する。従って、暗号化器403は、使用許可情報2中に命令3が存在しない場合にのみその処理された画像および／または音声コンテンツを暗号化する。暗号化器403の出力は、次いで使用許可情報2が付加された機器400の出力を形成する。

【0015】

10

20

30

40

50

図 2 は、末端ユーザの宅内の無線島状 (Inselnetz : ローカルエリア、孤立) ネットワーク 1 0 を示している。そのネットワーク 1 0 は W - L A N 送信機 2 0 0 および W - L A N 受信機 3 0 0 を含んでいる。W - L A N 送信機 2 0 0 は、インタフェースを介して入力段 1 0 0 に結合されており、その入力段 1 0 0 は任意の種類 of 伝送ネットワークからの、例えばインターネットまたは放送ネットワークからの使用許可情報 2 とともに暗号形式または非暗号形式の画像および / または音声コンテンツを受信する。入力段 1 0 0 は、主 (1 次) 受信機およびオプションとして (必要に応じて) 暗号解読器 (復号器) 1 0 0 を含んでいる。

【 0 0 1 6 】

W - L A N 送信機 2 0 0 は暗号形式の画像および / または音声コンテンツ 1 を W - L A N 受信機 3 0 0 に無線で送信する。W - L A N 受信機 3 0 0 は、他のインタフェースを介して消費者用電子機器 4 0 0 に接続され、その機器は図 1 に従って実施形態化 (具体化) されてもよい。使用許可情報 2 は、島状ネットワーク 1 0 を通って転送される (hindurchgeschleift) か、または使用許可情報 2 が画像および / または音声コンテンツ 1 と同時に送信されるとしても適当な手段によって論理的にリンクされた状態を維持するが、その画像および / または音声コンテンツから物理的に分離され、それによって使用許可情報 2 は転送された画像および / または音声コンテンツと共に消費者用電子機器 4 0 0 に送信される。

10

【 0 0 1 7 】

図 3 は、暗号解読器および暗号化器を有する消費者用電子機器 4 0 0、5 0 0 および 6 0 0 のカスケード (縦続) 接続によって画像および / または音声コンテンツ 1 を使用許可情報 2 に結合する原理を示している。暗号解読 (復号) および / または暗号化 (符号化) が各機器 1 0 0、4 0 0 または 5 0 0 内で行われるか否かには関係なく、各消費者用電子機器 4 0 0 および 5 0 0 と同様に入力段 1 0 0 の出力において、画像および / または音声コンテンツ 1 は使用許可情報 2 とともに存在する (供給される)。従って、図示された機器 (デバイス) のカスケード (縦続接続) 中の最後段の機器 6 0 0 は、使用許可情報 2 と共に画像および / または音声コンテンツ 1 を受信し、その使用許可情報 2 は、その間にそのコンテンツ 1 がどこかで暗号化されていれば、機器 6 0 0 内でその画像および / または音声コンテンツ 1 の暗号解読 (復号) を行わせる。

20

【 符号の説明 】

30

【 0 0 1 8 】

1 非暗号形式の画像及び / 又は音声コンテンツ

2 使用許可情報

1 + # 2 暗号形式の画像及び / 又は音声と使用許可情報

3 非暗号化命令

1 0 島状ネットワーク

1 0 0 主受信機 + オプションの復号器

2 0 0 W - L A N 送信機

3 0 0 W - L A N 受信機

4 0 0 オプションとして復号器及び / 又は暗号化器を有する消費者用電子機器

40

4 0 1 デコーダ

4 0 2 処理および / または記録

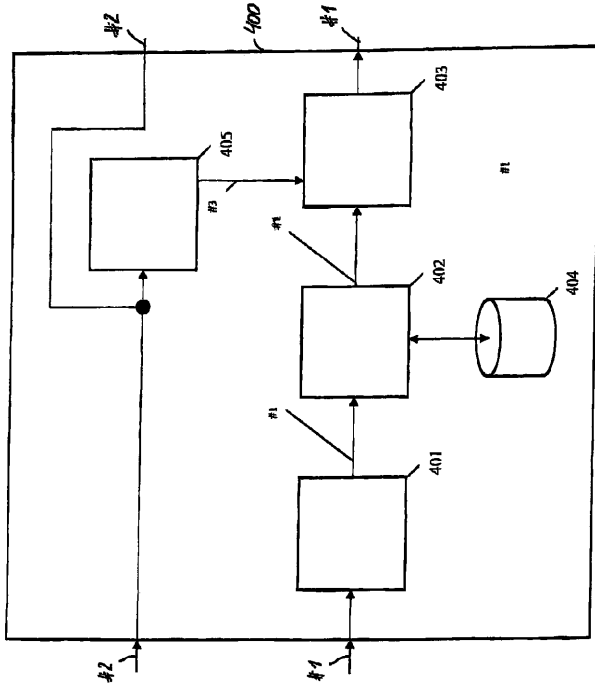
4 0 3 エンコーダ

4 0 4 メモリ

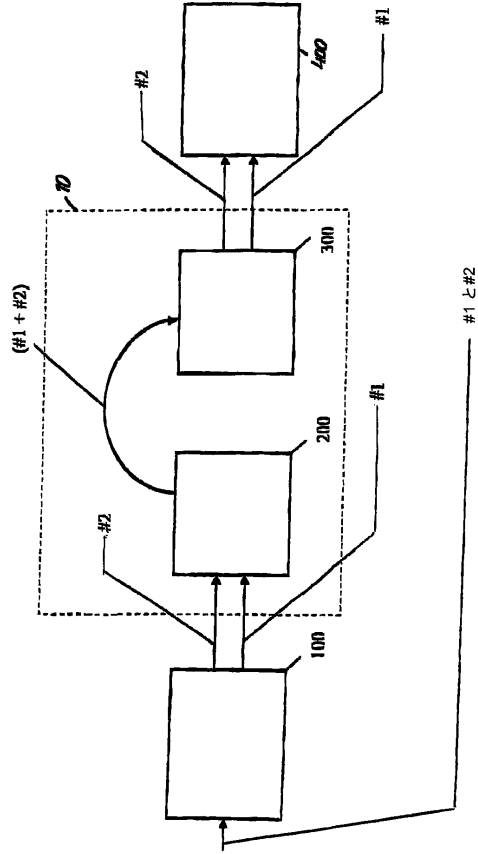
4 0 5 分析器

5 0 0 オプションとして復号器及び / 又は暗号化器を具え、暗号形式でのみ蓄積する消費者用電子装置

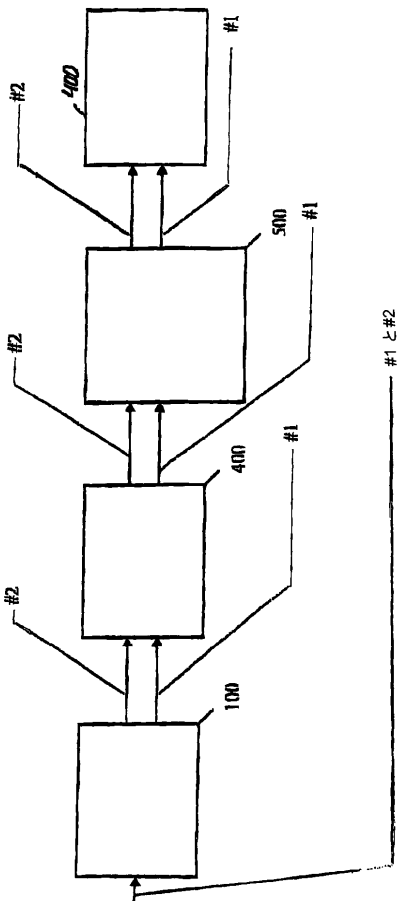
【 図 1 】



【 図 2 】



【 図 3 】



フロントページの続き

(74)復代理人 100145023

弁理士 川本 学

(72)発明者 セドルメイヤー, ロベルト

ドイツ連邦共和国 8 5 7 3 7 イスマニン ファザー ネンシュトラーセ 3 8

Fターム(参考) 5C164 TA07S UB06P UB10S UC26P

5J104 AA01 AA32 AA33 BA02 BA03 NA02 NA37 PA05