(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6438459号
(P6438459)
(45)発行日　平成30年12月12日(2018.12.12)　(24)登録日　平成30年11月22日(2018.11.22)

(51)Int.Cl.　　F I
G09C 5/00 (2006.01)　G09C 5/00
H04L 9/08 (2006.01)　H04L 9/00　601C
G06F 21/16 (2013.01)　G06F 21/16

請求項の数 8　(全 12 頁)

(21)出願番号　特願2016-509502 (P2016-509502)
(86)(22)出願日　平成26年4月28日 (2014.4.28)
(65)公表番号　特表2016-522435 (P2016-522435A)
(43)公表日　平成28年7月28日 (2016.7.28)
(86)国際出願番号　PCT/EP2014/058628
(87)国際公開番号　WO2014/174122
(87)国際公開日　平成26年10月30日 (2014.10.30)
審査請求日　平成29年3月13日 (2017.3.13)
(31)優先権主張番号　13165597.9
(32)優先日　平成25年4月26日 (2013.4.26)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　504344495
ナグラビジョン　エス　アー
スイス　ＣＨ－１０３３　シュゾー－シュール－ローザンヌ，ルート　ドゥ　ジュネーヴ　２２－２４
(74)代理人　100085372
弁理士　須田　正義
(74)代理人　100129229
弁理士　村澤　彰
(72)発明者　ユナセック，ディディエ
スイス　ＣＨ－１８０７　ブロネ，シュマン　ドュ　プレ　デ　プランシュ　１６Ｃ

最終頁に続く

(54)【発明の名称】少なくとも１つのコンテンツキーによって暗号化された圧縮コンテンツに透かしを入れる方法

(57)【特許請求の範囲】
【請求項１】
クライアント装置によって受信された圧縮コンテンツに透かしを入れる方法において、前記クライアント装置は、少なくとも１つのコンテンツキー（ＣＡキー）によって暗号化された圧縮コンテンツと、前記少なくとも１つのコンテンツキー（ＣＡキー）及びプリマーキングデータ（ＷＭＤ）を含む第１の伝達キーによって暗号化されたＣＡＳデータとを受信し、前記クライアント装置は、
前記暗号化された圧縮コンテンツを受信する入力及び解読された圧縮コンテンツを生成する出力を有するデスクランブラー（１０３）と、
前記デスクランブラーの前記出力に直接接続しているＷＭ挿入器（１０４）と、
を備え、前記デスクランブラー及び前記ＷＭ挿入器はコンディショナー（２００）に接続し、前記コンディショナーは識別子を備える方法であって、
前記ＣＡＳデータを受信するステップと、
前記第１の伝達キーで前記ＣＡＳデータを解読して、前記コンテンツキー（ＣＡキー）及び前記プリマーキングデータを抽出するステップと、
前記プリマーキングデータのシグネチャを検証するステップと、そして前記シグネチャが有効である場合、
前記プリマーキングデータ及び前記識別子を前記ＷＭ挿入器へ転送するステップと、
前記デスクランブラー（１０３）用の前記コンテンツキー（ＣＡキー）を検査するステップと、

前記プリマーキングデータ及び前記識別子を用いて、前記デスクランブラーにより生成された前記解読された圧縮コンテンツに、前記WM挿入器によって透かしを入れるステップであって、前記プリマーキングデータが、変更が可能な位置を定義する少なくとも１つのコンテンツインデックスと、前記位置に挿入される少なくとも１つの代替値とを含むステップと、

を含む方法。

【請求項２】

前記ＣＡＳデータはパケットに編成され、各パケットはシグネチャ及びセット又は記録を含み、各記録はコンテンツインデックス及び所与のコンテンツインデックスに対する代替値を含み、前記WM挿入器によって透かしを入れるステップは、前記識別子のビットに基づいて前記コンテンツインデックスの示す位置の前記圧縮コンテンツのオリジナル値を変えるか又は保つことを決定する請求項１に記載の方法。

【請求項３】

前記クライアント装置は、オペレーティングシステムを実行することを担当するホストＣＰＵを備え、そして前記コンディショナー、前記デスクランブラー、及び前記WM挿入器は、セキュア環境に位置し、そしてこれらの要素間の前記接続にはホストＣＰＵがアクセス可能ではない請求項１～２のいずれか１項に記載の方法。

【請求項４】

前記ＣＡＳデータは、前記暗号化された圧縮コンテンツに埋め込まれて、前記デスクランブラーにより解読され、前記方法は、前記デスクランブラーの前記出力で前記プリマーキングデータを抽出して、それらを前記コンディショナーへ転送するステップと、前記プリマーキングデータからシグネチャを抽出して、前記コンディショナーによって前記シグネチャを検証するステップとを含む請求項１に記載の方法。

【請求項５】

前記ＣＡＳデータは、エンタイトルメント制御メッセージに含まれる請求項１～３のいずれか１項に記載の方法。

【請求項６】

前記ＣＡＳデータはパケットに編成され、各パケットはシグネチャ及びセット又は記録を含み、各記録はコンテンツインデックス及び所与のコンテンツインデックスに対する代替値を含み、前記WM挿入器によって透かしを入れるステップは、前記識別子のビットに基づいて前記コンテンツインデックスの示す位置の前記圧縮コンテンツのオリジナル値を変えるか又は保つことを決定し、プリマーキング記録は、コンテンツインデックスに対するオリジナル値を含み、前記WM挿入器（１０４）は、前記コンテンツインデックスの示す位置の圧縮コンテンツのオリジナル値が前記プリマーキング記録の前記オリジナル値と同じであることを検証し、そして更に前記コンディショナー（２００）に前記検証の結果を知らせる請求項２～５のいずれか１項に記載の方法。

【請求項７】

エンタイトルメント制御メッセージ（ＥＣＭ）はアクセス条件を含み、前記コンテンツキーが前記デスクランブラー（１０３）へ転送される前に、これらのアクセス条件は前記コンディショナー（２００）により検査される請求項１～６のいずれか１項に記載の方法。

【請求項８】

暗号化された圧縮コンテンツを解読して、透かしを入れるクライアント装置において、前記圧縮コンテンツはプリマーキングデータを含み、そして少なくとも１つのコンテンツキー（ＣＡキー）によって暗号化され、前記コンテンツキーは、第１の伝達キーによって暗号化されたエンタイトルメント制御メッセージ（ＥＣＭ）において前記クライアント装置により受信されるクライアント装置であり、

前記暗号化された圧縮コンテンツを受信する入力及び解読された圧縮コンテンツを生成する出力を有するデスクランブラー（１０３）と、

前記エンタイトルメント制御メッセージ及び前記解読されたプリマーキングデータを受

信することを担当して、前記エンタイトルメント制御メッセージを前記第１の伝達キーで解読して、前記コンテンツキー（ＣＡキー）を抽出するコンディショナー（２００）であって、識別子を含むコンディショナー（２００）と、

前記プリマーキングデータ及び前記識別子を用いて前記解読された圧縮コンテンツに透かしを入れることを担当し、前記プリマーキングデータが、変更が可能な位置を定義する少なくとも１つのコンテンツインデックスと、前記位置に挿入される少なくとも１つの代替値とを含む、前記デスクランブラーの前記出力に直接接続しているＷＭ挿入器（１０４）と、

を備えるクライアント装置であって、

前記デスクランブラー及び前記ＷＭ挿入器は前記コンディショナー（２００）に接続し、前記コンディショナー（２００）は、前記プリマーキングデータのシグネチャを検証する手段を備え、そしてシグネチャが有効である場合、前記プリマーキングデータ及び前記識別子を前記ＷＭ挿入器へ転送する手段を備えるクライアント装置において、前記デスクランブラーは、前記暗号化したコンテンツと共に前記プリマーキングデータを解読することを担当して、前記解読されたプリマーキングデータをフィルター処理して、前記コンディショナーへ導く手段を有することを特徴とするクライアント装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツキーによって暗号化された圧縮コンテンツに透かしを入れる方法に関する。

【背景技術】

【０００２】

透かしを入れることは、保護されたコンテンツにタグを付けるために利用する技術である。このタグは、保護されたコンテンツの無許可の使用又は違法コピーを検出するために用いられる。透かしを入れる技術は、デジタルマークをコンテンツに埋め込むことを含む。外観の視点から、埋め込まれたデジタルマークは、不可視又は可視であり得る。情報・性状の視点から、このデジタルマークは、コンテンツの所有者がモニタしたいものに依存して固有値又は汎用シンボルであり得る。特に固有値の場合、マークがこの装置の識別子を含むので、透かしの挿入は最終的なクライアント装置において行わなければならない。

【０００３】

透かしを入れる技術の目的は、その表現の１つをコンテンツに拡げることによって埋め込まれたマーク／隠された情報を可能な限り隠すことである。品質上のいかなる妥協もなしにマーク挿入の裁量を確実にするために、挿入は、通常、所与の装置に対して複雑な更に表示するコンピューティング能力を必要とする。従って、完全な計算は、しばしば、前処理と後処理に分けられる。前処理は重要な演算の大部分を実行し、それは、マークを効果的に挿入するために非常により簡単な後処理を助ける透かしメタデータ（ＷＭＤ）と呼ばれているいくつかのキューを生成する。「どこを変更するか」、「どのように変更するか」は、通常は、ＷＭＤに含まれる情報である。これはプリマーキング記録のファイルの形であることができて、各々は、マークを付けられるブロックのアドレスの形をしており、少なくとも１つの代替値を有するコンテンツインデックスを含む。クライアント装置で、各記録は処理されて、代替値は、コンテンツに含まれる識別子のビットに従って選択される（又は選択されない）。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】米国特許出願公開第２０１０／１２８８７１号明細書

【特許文献２】欧州特許第２３９１１２５号明細書

【特許文献３】欧州特許第２４５８８９０号明細書

【発明の概要】

【発明が解決しようとする課題】
【０００５】
従って、ＷＭＤの秘密並びにそれらの挿入は、特に後処理が実行されるときに、クライアント装置内部で、それらをフィルター処理する、取り外す、及び／又は切り取る能力を防止するために確実にされるべきである。クライアント装置で、既存の電子透かし処理技術は、通常、場合によっては、保護されていなくてまだマークされないコンテンツがクライアント装置のソフトウェアによってアクセス可能であり得ることを意味する装置のアプリケーションソフトウェア（ホストＣＰＵ）により制御される。従って、電子透かし処理のセキュリティは、装置上で動作するソフトウェアのセキュリティ、即ち、装置がうまく攻撃されるか又は実際に開かれるときに（ソフトウェア認証でない）、電子透かし処理を変更して、バイパスすることがどんなに簡単であるかに依存する。
【０００６】
特許文献１は、メインストリームを復元して、同時に復元されたストリームをマールすることを可能にするデータを含む二次ストリームが生成される解決策を記載している。結果として、同じストリームはスクランブリングデータ及び透かしデータを含む。受信すると、このストリームは、変更されたストリームにおいて置き換えられる１セットのデータとして処理される。
【０００７】
特許文献２は、すべての装置に共通のストリームに基づいて個々のマーク付けを（受信装置で）可能にする解決策を記載している。制御対象は、オリジナル値、代替値、及び位置を含む。セキュリティユニットは、オリジナル値を検索するために代替値に適用される数学操作を決定する。数学操作が装置ごとに固有であるように、数学操作は受信装置の内部パラメータに従って変えられて、スクランブリングデータのストリームが分析される場合、この装置を探知することを可能にする。
【課題を解決するための手段】
【０００８】
本発明の目的は、クライアント装置により受信されたコンテンツ、特に圧縮ビデオコンテンツに透かしを入れることを実施することである。
【０００９】
本発明は、少なくとも１つのコンテンツキー（ＣＡキー）によって暗号化された圧縮コンテンツに透かしを入れる方法を提案し、前記圧縮コンテンツと、前記少なくとも１つのコンテンツキー（ＣＡキー）及びプリマーキングデータ（ＷＭＤ）を含む第１の伝達キーによって暗号化されたＣＡＳデータとはクライアント装置により受信される。
クライアント装置は、
暗号化された圧縮コンテンツを受信する入力及び解読された圧縮コンテンツを生成する出力を有するデスクランブラー（１０３）と、
デスクランブラーの出力に直接接続しているＷＭ挿入器（１０４）とを備える。
前記デスクランブラー及び前記ＷＭ挿入器はコンディショナー（２００）に接続する。
前記コンディショナーは、
ＣＡＳデータを受信するステップと、
前記第１の伝達キーでＣＡＳデータを解読して、コンテンツキー（ＣＷ）及びプリマーキングデータを抽出するステップと、
プリマーキングデータのシグネチャを検証するステップと、そしてシグネチャが有効である場合、
コンテンツキー（ＣＡキー）をデスクランブラー（１０３）へ、そしてプリマーキングデータをＷＭ挿入器へ転送するステップと、
プリマーキングデータ及び識別子を用いて、デスクランブラーにより生成された解読された圧縮コンテンツに、ＷＭ挿入器によって透かしを入れるステップであって、前記プリマーキングデータが、変更が可能な位置を定義する少なくとも１つのコンテンツインデックスと、前記位置に挿入される少なくとも１つの代替値とを含むステップを実行する。

【００１０】
本発明は、添付図によってより良く理解される。
【図面の簡単な説明】
【００１１】
【図１】透かしを入れるフローの実施例を示す。
【図２】透かし挿入プロセスのブロック図を示す。
【図３】透かしを入れるプロセスのフロー図を示す。
【図４】透かしデータがデータフローに含まれる実施例を示す。
【発明を実施するための形態】
【００１２】
条件付きアクセスデータは、１つ又は複数のコンテンツキーによって暗号化されたコンテンツ（ビデオ又は音声データ或いはその組合せ）を含む。このコンテンツへのアクセスはＣＡＳデータのおかげで可能であり、これらのデータは、暗号化されたコンテンツを解読する１つのキー又は複数のキー（ＣＡキー）、及びプリマーキングデータＷＭを含む。ＷＭＤは、暗号解読されたコンテンツの変更がどこでなされることができるかについてＷＭ挿入器が決定できる一組の記録である。これは、通常、一組の記録の形であり、各記録は、位置（又はアドレス、オフセット、インデックス）及び少なくとも１つの代替値を含む。この代替値は、コンテンツの特定位置のオリジナル値を置換できる（又は埋め込まれるビットに依存して、できない）。２つの代替値の場合には、透かしとして埋め込まれるビットは、どちらか一方の値を選択するために用いることができる。ＣＡＳデータはまた、コンテンツを解読するためにデコーダにより満たされる条件を記載しているコンテンツと関連したアクセス条件を含む。コンディショナーは、クライアント装置のアクセス条件を記載しているアクセス権を含む。アクセス権は、好ましくは、前記コンディショナーのための固有キーによって暗号化されたエンタイトルメント制御メッセージ（ＥＭＭ）によってコンディショナーにロードされる。条件付きアクセスデータは同報通信されるか、ユニキャストされるか、又は受取人の要求に応じて送られる。ＣＡＳデータは、条件付きアクセスデータの一部（例えば、特定のＰＩＤ値を有するサブストリーム）であり得るか、又はクライアント装置に別に送ることができる。
【００１３】
サーバー側で、圧縮コンテンツは１つ又は複数のキーによって暗号化され、第２のケースにおいて、コンテンツは区分されて、各区分は異なるキーによって暗号化される。サーバーはまた、圧縮コンテンツの可能性があるマーキング位置を（暗号化ステップの前に）検出するために、分析モジュールによって一組の記録として透かしデータ（ＷＭＤ）を作成する。分析モジュールの結果は、記録当たり少なくとも１つの代替値を生成することであり、この代替値は、圧縮コンテンツで置換されるときに、コンテンツを視覚的に変えないが、後で検出できる。ＷＭＤ又はプリマーキング記録は、記録ごとに変更されるコンテンツのコンテンツインデックス（即ち、変更をなすことができる位置）及び挿入する代替値を含む。プリマーキング記録は特定の識別子により決定されず、更なる処理なしに（それゆえに、クライアント装置の必要な複雑さを減らす）ローカル識別子によってマークを埋め込むことは、クライアント装置で透かしを助けることができる値だけである。
【００１４】
一旦クライアント装置において受信されると、ＣＡＳデータが条件付きアクセスデータに埋め込まれるという場合に、それらは抽出されて、条件付きアクセス条件において定められたセキュリティ対策の実行を担当する、コンディショナーに転送される（図２参照）。このモジュールは、ＣＡＳデータを解読して、ＣＡＳデータからキー（ＣＡキー）を抽出し、それからコンテンツを解読するためにそれをＣＡデスクランブラーへ転送するために必要な第１の伝達キーを含む。キーに加えて、このモジュールはまた、第２の伝達キーによって暗号化されたＷＭＤを抽出する。ＷＭＤがＣＡキーと同じメッセージにあるという場合に、１つの伝達キーはメッセージを暗号化するために用いる。特定の実施形態にお

いて、第１及び第２のキーは、同じ伝送であって、ＣＡＳデータ及びWMDを解読するために用いられる。コンディショナーとＣＡデスクランブラーとの間の通信が、両方の要素で初期化されたキーによって暗号化されて、保護されている点に留意する必要がある。これらの２つの要素の間の通信が安全であることを確実にする別の方法は、専用バスを使用すること、即ちクライアント装置で動作するホストＣＰＵ（２０３）がアクセス可能でないことである。

【００１５】

類似の保護は、コンディショナーとWM挿入器との間の通信に適用される。

【００１６】

提案された解決策は、WMDをスパイから保護するだけでなく、WMDをいかなる簡単なフィルタリング又は取外しからも保護する。解決策はまた、WMDのローバスト検出を実施して、マークの正しい挿入も強化する。本発明の典型的な態様は、WMDを受信するコンディショナー、コンテンツを暗号解読するＣＡデスクランブラー、及びWMDを用いてマークを挿入する透かし挿入器を含むことができる。

【００１７】

図１は、透かしを入れるプロセスの典型的な応用例である。例えば、ヘッドエンド１００はコンテンツを前処理して、正しい場所を発見して、マークを圧縮コンテンツに挿入して、WMDを形成する。そのステージで、透かしデータは、クライアント装置に依存せず、すべてのクライアント装置に共通である。この情報は、条件付きアクセスシステム（ＣＡＳ）により保護されているコンテンツと共に、例えば、衛星を使用して、最終的なクライアント装置に送信１０１される。保護されたコンテンツ１１０は装置に入る。図１に示すこの実施例で、コンテンツ及びWMDを暗号解読するために用いるＣＡキーは、コンテンツ自体の中で送信される。コンディショナー１０２は、保護されたＣＡキー及び保護されたWMDを、それらを送信するために用いるチャネルから抽出する。それはまた、この２つのテューブル：ＣＡキ-WMDを解読して、認証する。

【００１８】

別の実施形態によって、コンディショナーは、ＣＡＳデータをセキュア要素、即ちセキュアＣＰＵ２０５に送信する（図２参照）。このセキュア要素は、クライアント装置の一部、例えば、セキュリティ動作専用の保護されたソフトウェア環境であり得る。それは、切離し可能なセキュリティ要素、例えば、スマートカード、ドングル、又はＰＣＭＣＩＡモジュールでもあり得る。一旦ＣＡＳデータがセキュア要素により解読されて、認証されると、ＣＡキー及びWMDはコンディショナーに戻される。これらの２つの要素の間の通信は、好ましくは、ペアリングキーによって安全にされる、即ち、同じキーが初期化段階の間にコンディショナー及びセキュア要素にロードされる。

【００１９】

保護されたコンテンツ１１１は、ＣＡデスクランブラー１０３に送信される。コンディショナー１０２が保護されたＣＡキー及び保護されたWMDをうまく解読して、ＣＡキー及びWMDを認証する場合、それは、ＣＡキーをＣＡデスクランブラー１０３に、そしてWMDをWM挿入器１０４に送信できる。ＣＡデスクランブラー１０３は、コンテンツ１１２を脱保護するためにＣＡキーを使用する。保護されていないコンテンツはWM挿入器１０４に入る。WM挿入器１０４は、マークを正しい場所で挿入するために、WMD（コンディショナー１０２から来る）とコンテンツとを同期させる役割を果たす。それから、マークされて暗号解読されたコンテンツ１１３は、ビデオデコーダ１０５に伝えられて、それはマークされたコンテンツを復号化する。ＴＶ１０６は、マークされて圧縮されないコンテンツを受信する。

【００２０】

認証はシグネチャに基づく。例えば、透かしデータは、データの起点を認証するためのシグネチャを含む。シグネチャは、ペイロードのダイジェストの暗号化の結果（例えば、プリマーキング記録）である。ダイジェストは、ヘッドエンド前処理１００（例えば、ハッシュ関数を使用する）により算出されて、シグネチャを生成するために、シグネチャキ

ーによって暗号化される。このシグネチャはメッセージに加えられて、メッセージは、好ましくは、伝達キーによって暗号化される。受信側で、メッセージは先ず解読されて、ダイジェストはペイロードで算出される。シグネチャキーと一致するキーの場合は、受信されたシグネチャは解読されて、結果は算出されたダイジェストと比較される。両方の値が同じである場合、メッセージは真正である。シグネチャキーは、対称キー又は非対称キー（公開／私用キー）であり得る。

【００２１】

図２は、ローバスト透かし挿入システムを例示するブロック図である。装置は、コンディショナー１０２、ＣＡデスクランブラー１０３、ホストＣＰＵ２０３、ＷＭ挿入器１０４、及び任意にセキュアＣＰＵ２０５を備えることができる。

【００２２】

セキュアＣＰＵ２０５は、使用される場合、透かしを入れるプロセスの制御及びカスタム化を確実にする回路、論理、及び／又はコードを備えることができる。信頼できないソフトウェア（ファームウェア）がそこにおいて動作することができないように、セキュアＣＰＵ２０５はホストＣＰＵ２０３から完全に分離されるべきである。

【００２３】

コンディショナー１０２は、保護されたＣＡキー及び保護されたＷＭＤを受信（抽出）し解読して認証する回路、論理、及び／又はコードを備えることができる。コードが用いられる場合、このコードは、セキュアＣＰＵ２０５によって暗号化されて、認証される。コンディショナー１０２はまた、変更不可能な信用値２０４（識別子、タイムスタンプなど）にアクセスする。コンディショナー１０２はまた、ＷＭ挿入器１０４を作動させることを担当する。ＣＡＳデータに含まれる条件は、コンテンツの中への透かしとして実施される識別子を選択するようにという命令を含むことができる。それは、コンディショナーのセキュア環境に好ましくは格納される、クライアント装置の固有識別子、又はＣＡＳデータに含まれる識別子（例えば、コンテンツの発信者の識別子）であり得る。

【００２４】

ＣＡデスクランブラー１０３は、コンディショナー１０２から来るＣＡキーで保護されたコンテンツを暗号解読するために、回路、論理、及び／又はコードを備えることができる。コードが用いられる場合、このコードは解読されて、セキュアＣＰＵ２０５により認証されて、問題なく格納される。

【００２５】

ＷＭ挿入器１０４は、コンディショナー１０２から来るＷＭＤ及び識別子を用いて、保護されていないコンテンツにマークを挿入するために、回路、論理、及び／又はコードを備えることができる。コードが用いられる場合、このコードはセキュアＣＰＵ２０５により解読されて、認証される。ＷＭ挿入器１０４の別の重要なタスクは、マークをどこに挿入するべきかについて指示するＷＭＤをコンテンツと同期させることである。

【００２６】

ホストＣＰＵ２０３は、装置の全体の機能を確実にする回路、論理、及び／又はコードを備えることができる。ホストＣＰＵ２０３は、ＣＡデスクランブラー１０３とＷＭ挿入器１０４との間で、ＣＡキー、ＷＭＤ、及び保護されていないコンテンツにアクセスすることができない。

【００２７】

セキュアリンク２１０、２１１、及び２１２は、ホストＣＰＵ２０３がアクセスできない私用のバス、論理、及び／又はＲＡＭを含むことができる。セキュアリンクにより連結された実体だけが、伝送されたデータにアクセスすることができる。例えば、ＣＡデスクランブラー１０３及びコンディショナー１０２だけが、ＣＡキーにアクセスすることができる。

【００２８】

上述のプロセスから離れて、本発明の目的は、保護されたＷＭＤの簡単なフィルタリングを防止することでもある。保護されたＣＡキーは攻撃者によって取り外されることがで

きず、さもなければコンテンツは解読されない。保護されたＷＭＤの場合は、目的は、ホストＣＰＵ２０３の観点から、それらの検出を可能な限り隠すことである。理想的なシナリオは、保護されたＷＭＤがコンディショナー１０２により抽出されて、それから可視であり得るということである。しかしながら多くのケースで、保護されたＷＭＤは、それにもかかわらずホストＣＰＵ２０３によってアクセス可能であり、従って目的は、ホストＣＰＵ２０３に、保護されたＷＭＤをコンディショナー１０２に渡すことを実施させることである。保護されたＷＭＤをコンディショナー１０２に渡すことを実施する手段について話す前に、以下のリストは、保護されたＣＡキー及び保護されたＷＭＤが来ることができるいくつかの可能なチャネルを要約する。

保護されたＣＡキー及び保護されたＷＭＤは、サーバーからイーサネット（登録商標）を通じて直接来ることができる。

保護されたＣＡキー及び保護されたＷＭＤは、マニフェスト（ＤＡＳＨのような）に格納できる。

保護されたＣＡキー及び保護されたＷＭＤは、コンテンツに埋め込むことができる。

例えば、コンディショナー１０２はＥＣＭの保護されたＣＡキーを受信することができて、保護されたＷＭＤは、ＣＡデスクランブラー１０３の前にコンディショナー１０２によって抽出できる（図１）。図２に示される別の実施例は、ＷＭＤがコンテンツに埋め込まれて、ＣＡデスクランブラーの後に利用できるだけである（デスクランブラーの出力からの点線２３０）ことを示す。ＷＭＤは、その時保護される、即ちＣＡキーで暗号化される。ＷＭＤのサブストリームが抽出されて、コンディショナーに渡るように、フィルターはＣＡデスクランブラーの出力に位置する。ＣＡデスクランブラーから抽出されたＷＭＤは、コンディショナーによって知られている特定のＷＭキーによって、更に暗号化することができる。ＷＭＤの確実性を制御するために、これらのデータはシグネチャを更に含むことができる。これらのデータはパケットに編成されて、各パケットはパケットシグネチャを含む。シグネチャは、実現の実施例として、パケットの他のデータのハッシュ値であり、このハッシュ値はシグネチャキーによって暗号化されている。コンディショナーがＷＭＤを受信すると、それはパケットシグネチャを解読して、それをパケットのデータのハッシュ値と比較する。シグネチャがうまく検証される場合、コンディショナーは現在のＣＡキーを検証して、将来のＣＡキーをＣＡデスクランブラーに供給し続け、反対に、上記のブロッキング機構は使用可能にされる。

【００２９】

この構成において、コンディショナー２００は、最初に、ＷＭＤを受信する前に、ＣＡキーをＣＡデスクランブラー１０３にロードしなければならない。このために、コンディショナーは、ＣＡキーがデスクランブラーにロードされるときに初期化されるタイマーを備える。第１の所定時間後に、ＷＭＤがコンディショナーにより受信されない場合、後者はデスクランブラーをブロックする。これは、偽のＣＡキーをデスクランブラーに送信するか、又は新規なＣＡキーの更なる伝送をブロックすることにより行うことができる。タイマーは、第２の所定時間後にブロックを解除するために用いることができる。この第２の時間が過ぎると、コンディショナーは現在のＣＡキーを転送して、ＷＭＤの受信を待つ。ＷＭＤが第１の所定時間の間に受信されない場合、タイマーは再初期化されて、コンディショナーはブロッキングモードに再び入る。

【００３０】

ＣＡキー及びＷＤＭが一緒に送られる実施形態において、保護されたＷＭＤをコンディショナー１０２に与えることを実施する主要な着想は、ＣＡキーとＷＤＭをシグネチャ機構（例えば、ＳＨＡ－２５６）によって暗号で結び付けることである。このコンピュータ操作は、コンディショナー１０２において処理されることができるだけである。例えば、ビデオ・オン・デマンド・コンテンツは、固有のＣＡキーで暗号化されて、すべての保護されたＷＭＤはファイルに格納される。コンテンツを解読するために、コンディショナー１０２は保護されたＣＡキー及びすべての保護されたＷＭＤを受信し、さもなければＣＡキー及びＷＭＤに行われたシグネチャ検査は失敗し、そしてコンディショナー１０２がＣ

ＡキーをＣＡデスクランブラー１０３に提供しないので、コンテンツは解読されない。
【００３１】
しかしながら、ＣＡキーとWMDとの間の暗号の結合は必ずしも可能でない。例えば、ＣＡキーは保護された媒体データと完全に無相関であり、それはＭＰＥＧ-ＴＳ伝送においてWMDに密接にリンクされている。WMD自体は、一種の媒体データとしてＣＡキーで保護されることもできる。この場合、保護されたWMDは、ホストＣＰＵ２０３の観点にとって不可視である。コンディショナー１０２だけは、それらを検出して、それらを使用できる。これを例示するために、図４は、ＭＰＥＧ-２　ＴＳコンテンツの伝送を示す。この例では、WMDは、特定のパケット化された基礎ストリーム（ＰＥＳ）に含まれており、それから、コンテンツの他のＰＥＳと共に混ぜられる。このＰＥＳのペイロードは、コンディショナー１０２だけに知られているキーによって暗号化されている。これらのＰＥＳ及び通常のＰＥＳは、ＴＳパケットにカプセル化されて、それから、スクランブラー（例えば、ＤＶＢ-ＣＳＡＶ２）によって暗号化される。ホストＣＰＵ２０３の観点から、通常のＰＥＳを含むＴＳパケットとWMD　ＰＥＳを含むものとの間の差がない。ＣＡデスクランブラー１０３はＴＳパケットを解読し、それから、コンディショナー１０２は特定のフラグを用いて保護されたWMDを検出する。それから、それはそれらを解読して、WM挿入器１０４にそれらを渡すことができる。
【００３２】
図１に示す別の実施例は、透かしを入れるプロセスを実施する方法に重点を置いている。コンディショナー１０２は、ＣＡデスクランブラー１０３の前に配置される。コンディショナー１０２は、保護されたWMDを抽出して、それらを解読する。この場合、保護されたWMDの検出はより容易であり、そしてホストＣＰＵ２０３によって潜在的に行うことができる。保護されたWMDのフィルタリングを防止するために、特許文献３で公開された特許出願に記載されているマーキング技術が用いられる。この技術によって保護されたWMDがフィルター処理される場合、コンテンツは相当な劣化を受ける。この実施例によれば、ＣＡデスクランブラーによって暗号解読されるコンテンツは、オリジナルのもの及びいわゆる変更コンテンツと同じでない。この変更コンテンツはなお、ヘッドエンドによって変えられるいくつかの値（例えば、相関係数）を含み、オリジナル値は透かしデータの一部である。WM挿入器により実行される、透かしを入れるプロセスの間、前透かし記録は２つの値を含み、一方はオリジナル値であり、そして他方は代替値である。視覚影響が最小限であるように、この代替値は選択される。
【００３３】
図３は、典型的な透かしを入れるプロセスのフロー図である。ステップ３０１において、ステップ３００の開始後、コンディショナー１０２は、ＣＡキー及びWMDを受信し、解読して、認証することを担当する。ステップ３０２において、コンディショナーは、ＣＡキー及びWMDに行われたシグネチャを解読して、検査する。ＣＡキー及びWMDが正しく認証されることができない場合、コンディショナー１０２がＣＡキーをＣＡデスクランブラー１０３に提供しないので、コンテンツは解読されない（ステップ３０４）。このトリックを用いて、ホストＣＰＵ２０３は、いかなる変更又はフィルタリングもなしに、保護されたＣＡキー及び保護されたWMDをコンディショナー１０２に渡さなければならない。すべてがうまくいっている場合、コンディショナー１０２はまた、ＣＡデスクランブラー１０３のためのＣＡキーと同時にWMD及び信用値をWM挿入器に提供することを担当している（ステップ３０３）。信用値は装置を独自に識別するために用いる。例えば、この信用値は、装置の構成でセットされて、ロックされることができる。
【００３４】
装置の一部として、この信用値は、コンディショナーによってアクセス可能であり、そして更に、装置のいかなる実体によっても変更可能ではない。いくつかのコンピュータ操作は、このペイロードの頑強性を改善するために、透かしペイロードとして使われる前にコンディショナー内のこの信用値に行うことができる。例えば、信用値は、タルドシュコードのような、ＥＣＣ又は結託防止コードにより変形される／高められることが可能であ

る固有識別子であり得る。

【００３５】

それから、ステップ３０５で、ＣＡデスクランブラーは保護されたコンテンツを暗号解読する。その後、ステップ３０７で、この保護されないコンテンツはWM挿入器に提供されて、マークされる。WM挿入器は、マークをコンテンツに正しく挿入するために、ＷＭＤ及び信用値を使用する。保護されないコンテンツは、それが正しくマークされる前にホストＣＰＵによって決してアクセス可能ではない。ステップ３０８において、別のＣＡキー及び／又は新規な保護されたＷＭＤが来ている場合、プロセスはステップ３０１へ飛ぶ。

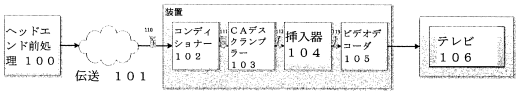
【００３６】

WM挿入器は、圧縮コンテンツがデスクランブラーによって実際に解読されるものであることを検査することを担当する検証モジュールを備えることができる。第１の検証は圧縮データの受信に基づいている。データがWM挿入器の入力で受信されない場合、メッセージは、ＣＡキーをデスクランブラーに提供するために、コンディショナーに送り返され、次にコンディショナーは停止する。

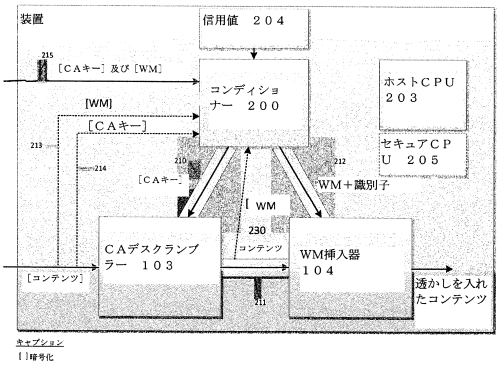
【００３７】

（以前のものに加えるか又は単独で実施できる）別の検証は、透かしを入れるコンテンツを認識することを目的とする。WM記録は、コンテンツインデックス及び代替値だけでなくて、コンテンツインデックスにより指された位置のコンテンツのオリジナル値も含む。透かしを入れるステップの間、WM挿入器は、識別子のビットの値に従って代替値（又はオリジナルのものを残す）によって、コンテンツのオリジナル値を変えることを決める。この動作に加えて、WM挿入器は、暗号解読された圧縮コンテンツからオリジナル値を読み取って、それをプリマーキング記録に含まれるオリジナル値と比較できる。値が同じである場合、現在進行中のコンテンツは真正のものである。コンテンツから読み取るオリジナル値が異なる場合、それは、別の圧縮コンテンツがWM挿入器の入力に供給されたことを意味する。この場合、メッセージは、適切な動作（例えば、ＣＡキーを無効にする）を行うために、コンディショナーに送られる。

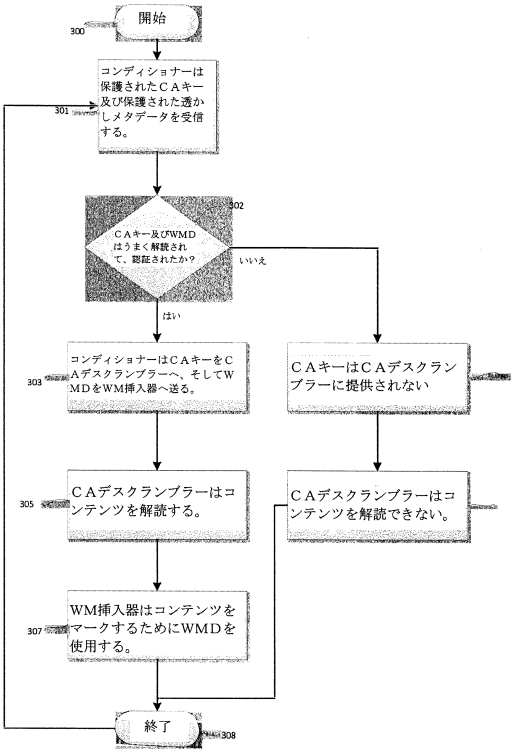
【図１】


ヘッドエンド前処理 １００
伝送 １０１
装置
コンディショナー １０２
ＣＡデスクランブラー １０３
挿入器 １０４
ビデオデコーダ １０５
テレビ １０６

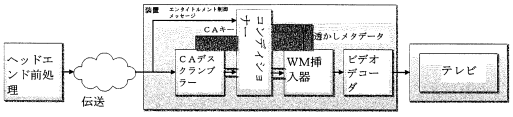
【図２】


装置
信用値 ２０４
［ＣＡキー］及び［WM］
コンディショナー ２００
ホストＣＰＵ ２０３
セキュアＣＰＵ ２０５
[WM]
［ＣＡキー］
［ＣＡキー］
WM＋識別子
WM
230
コンテンツ
［コンテンツ］
ＣＡデスクランブラー １０３
WM挿入器 １０４
透かしを入れたコンテンツ
キャプション
［］暗号化

【図３】


開始
300
コンディショナーは保護されたＣＡキー及び保護された透かしメタデータを受信する。
301
ＣＡキー及びWMDはうまく解読されて、認証されたか？
302
いいえ
はい
コンディショナーはＣＡキーをＣＡデスクランブラーへ、そしてWMDをWM挿入器へ送る。
303
ＣＡキーはＣＡデスクランブラーに提供されない
ＣＡデスクランブラーはコンテンツを解読する。
305
ＣＡデスクランブラーはコンテンツを解読できない。
WM挿入器はコンテンツをマークするためにWMDを使用する。
307
終了
308

【図４】


ヘッドエンド前処理
伝送
装置
エンタイトルメント制御メッセージ
CAキー
ＣＡデスクランブラー
コンディショナー
透かしメタデータ
WM挿入器
ビデオデコーダ
テレビ

フロントページの続き

(72)発明者 セルベ, パトリック
スイス ＣＨ－１０３３ シュゾーーシュールーローザンヌ、シュマン ドゥ スールーモン ３８
(72)発明者 トラン, ミン ソン
フランス Ｆ－９２３４０ ブール ラ レーヌ、ブルバール ドュ マレシャル ジョフル ９０
(72)発明者 サルダ, ピエール
スイス ＣＨ－１０４０ エシャランス、シュマン シュール ロッシュ ５

審査官 行田 悦資

(56)参考文献 特開２００２－１５８９６３（ＪＰ，Ａ）
特開２００１－００８０２２（ＪＰ，Ａ）
特開２００２－１１８７３６（ＪＰ，Ａ）
特開２００１－０２２２７１（ＪＰ，Ａ）
特開２００４－０６４５８２（ＪＰ，Ａ）
特開２０００－１５２２１４（ＪＰ，Ａ）
特開２００５－３１８０６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ ５／００
Ｇ０６Ｆ ２１／１６
Ｈ０４Ｌ ９／０８