(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-546019
(P2008-546019A)
(43)公表日　平成20年12月18日(2008.12.18)

(51)Int.Cl.			F I			テーマコード（参考）
G09C	5/00	(2006.01)	G09C	5/00		5B057
H04N	1/387	(2006.01)	H04N	1/387		5C076
G06T	1/00	(2006.01)	G06T	1/00	500B	5J104
G10L	19/00	(2006.01)	G10L	19/00	230	

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

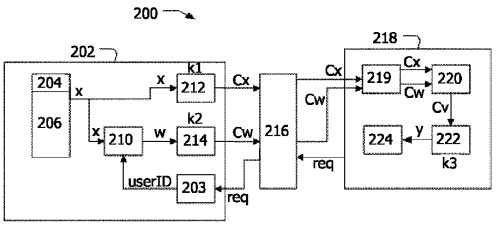
(21)出願番号　特願2008-514292 (P2008-514292)
(86)(22)出願日　平成18年6月2日 (2006.6.2)
(85)翻訳文提出日　平成19年11月28日 (2007.11.28)
(86)国際出願番号　PCT/IB2006/051773
(87)国際公開番号　WO2006/129293
(87)国際公開日　平成18年12月7日 (2006.12.7)
(31)優先権主張番号　05104828.8
(32)優先日　平成17年6月3日 (2005.6.3)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦
(74)代理人　100122769
弁理士　笛田　秀仙
(72)発明者　レムマ　アウェーケ　エヌ
オランダ国　５６５６　アーアー　アインドーフェン　プロフ　ホルストラーン　６

最終頁に続く

(54)【発明の名称】安全なウォーターマーキングに対する準同型暗号

(57)【要約】
メディア信号xにウォーターマークを埋め込む方法及びシステムが開示される。前記方法は、暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供するステップと、暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供するステップと、暗号化された結合メディア信号c_yを得るように結合器において少なくとも部分的に暗号化されたメディア信号c_x及び少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合するステップと、第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得るステップとを有する。本発明は、信用されていないデバイス内の安全なウォーターマーク埋め込みに対する構成を提供する。



【特許請求の範囲】
【請求項１】
メディア信号xにウォーターマークを埋め込む方法において、
暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供するステップと、
暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供するステップと、
暗号化された結合メディア信号c_yを得るように結合器において前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合するステップと、
第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得るステップと、
を有する方法。
【請求項２】
前記結合器が乗算器である、請求項１に記載の方法。
【請求項３】
前記少なくとも部分的に暗号化されたウォーターマーク信号c_wに含まれる第１のウォーターマーク及び前記復号されたウォーターマーク入りメディア信号yの第２のウォーターマークの両方が同一である、請求項１に記載の方法。
【請求項４】
前記第３の復号鍵k3が、前記第１の暗号化鍵k1とは異なり、前記少なくとも部分的に暗号化されたメディア信号c_xを復号しない、請求項１に記載の方法。
【請求項５】
前記第３の復号鍵k3が、前記第２の暗号化鍵k2とは異なり、前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを復号しない、請求項１に記載の方法。
【請求項６】
前記第３の復号鍵k3が、前記第１の暗号化鍵k1及び前記第２の暗号化鍵k2とは異なる、請求項１に記載の方法。
【請求項７】
前記少なくとも部分的に暗号化されたメディア信号c_xが、
$c_x = (1+K)^x r^{k1} \bmod K^2$ 又は $c_x = (1+K)^x r^{N \cdot k1} \bmod K^2$
の関係によって暗号化され、ここでN、K及びrが正の整数であり、k1 = K-k2が前記第１の暗号化鍵である、請求項１又は２に記載の方法。
【請求項８】
前記少なくとも部分的に暗号化されたウォーターマーク信号c_wが、
$c_w = (1+K)^w r^{k2} \bmod K^2$ 又は $c_w = (1+K)^w r^{N \cdot k2} \bmod K^2$
の関係によって暗号化され、ここでN、K及びrが正の整数であり、k2 = K-k1が前記第２の暗号化鍵である、請求項１、２又は７に記載の方法。
【請求項９】
前記復号されたウォーターマーク入りメディア信号yを得るステップが、
$y = ((c_y^N-1) \bmod k3^2)/Nk3 \bmod k3$ 又は $y = ((c_y-1) \bmod k3^2)/k3 \bmod k3$
を計算し、ここで$c_y = c_x c_w$であり、Nが正の整数であり、k3 = k1+k2が前記第３の復号鍵である、請求項１、２、７又は８に記載の方法。
【請求項１０】
前記少なくとも部分的に暗号化されたメディア信号c_xが、
$c_x = g^{rk1} g^x$
の関係によって暗号化され、ここでg及びrが正の整数であり、k1が前記第１の暗号化鍵である、請求項１又は２に記載の方法。
【請求項１１】
前記少なくとも部分的に暗号化されたウォーターマーク信号c_wが、$c_w = g^{rk2} g^w$の関係

によって暗号化され、ここでg及びrが正の整数であり、k2が前記第２の暗号化鍵である、請求項１又は２に記載の方法。

【請求項１２】

前記復号されたウォーターマーク入りメディア信号yを得るステップが、

$g^{x+w} = c_y/g^{rk3}$を計算するステップであって、$c_y = c_x c_w$であり、rが正の整数であり、k3 = k1+k2が前記第３の復号鍵である、当該計算するステップと、

前記復号されたウォーターマーク入りメディア信号yを得るためにルックアップテーブルを使用して離散的な指数関数g^{x+w}を解くステップと、

を有する、請求項１０又は１１に記載の方法。

【請求項１３】

前記方法がデバイスにおいて実行され、前記デバイスが、信用されていない環境を持つ信用されていないデバイスであり、及び／又は前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供するステップが、前記デバイスにおいて前記メディア信号xの前記少なくとも部分的に暗号化されたメディア信号c_xを受信するステップを有し、前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供するステップが、前記デバイスにおいて前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを受信するステップを有する、請求項１に記載の方法。

【請求項１４】

独立した瞬間において及び独立したチャネルを介して前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを独立して提供するステップを有する、請求項１ないし１３のいずれか一項に記載の方法。

【請求項１５】

前記方法が、ソフトウェア又はプログラム要素において実行され、前記ソフトウェア又はプログラム要素が、信用されていない環境で実行される、請求項１ないし１４のいずれか一項に記載の方法。

【請求項１６】

メディア信号xにウォーターマークを埋め込むシステムにおいて、

暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供する手段と、

暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供する手段と、

暗号化された結合メディア信号c_yを得るように結合器において前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合する手段と、

第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得る手段と、

を有するシステム。

【請求項１７】

コンピュータにより処理する、メディア信号xにウォーターマークを埋め込むコンピュータプログラムを包含するコンピュータ読み取り可能媒体において、前記コンピュータプログラムが、

暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供する第１のコードセグメントと、

暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供する第２のコードセグメントと、

暗号化された結合メディア信号c_yを得るように結合器において前記少なくとも部分的に暗号化されたメディア信号c_x及び前記少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合する第３のコードセグメントと、

第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得る第４のコードセグメントと、

を有する、コンピュータ読み取り可能媒体。
【請求項１８】
暗号化が第１の暗号化鍵k1を使用して実行される、メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xと、
暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wと、
を結合して有する、暗号化された結合メディア信号c_yにおいて、
前記結合信号が、第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを提供するために復号可能であり、前記ウォーターマーク入りメディア信号yが、復号されたウォーターマークを埋め込まれている、暗号化された結合メディア信号。
【請求項１９】
電子音楽配信（ＥＭＤ）システムにおける請求項１ないし１５のいずれか一項に記載の方法の使用。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、データの安全な送信の分野に関連する。より具体的には、本発明は、電子音楽配信システムにおいてメディア信号にウォーターマークを埋め込む方法及び装置に関し、より具体的には、電子音楽配信システムにおける安全なウォーターマーキングに対する準同型暗号（homomorphic encryption）に関する。
【背景技術】
【０００２】
音楽データを配信する従来の電子音楽配信（ＥＭＤ）システム１００が、図１に示される。ＥＭＤシステム１００は、サーバ１０２、クライアント１１８及びインターネットのような配信ネットワーク１１６を有する。一般に、サーバ１０２は、コンテンツプロバイダと配信ネットワーク１１６を介してコンテンツを要求したユーザとの間で相互認証を実行した後に得られたセッション鍵データを使用することにより著作権情報のようなコンテンツ情報及びコンテンツデータを暗号化する。前記暗号化された情報は、クライアント１１８に転送され、クライアント１１８は、前記暗号化された情報を復号し、前記要求されたコンテンツを得る。
【０００３】
より特定的には、ネットワーク１１６を介してクライアント１１８からサーバ１０２に送信されたコンテンツに対する要求が認証された後に、コンテンツプロバイダ１０４は、要求されたコンテンツ１０６をウォーターマークエンジン１１０に送信し、コンテンツ情報１０８をペイロードデバイス１１２に送信する。コンテンツ情報１０８は、シリアルコピーマネジメントシステム（ＳＣＭＳ）情報、コンテンツデータに著作権情報を埋め込むデジタルウォーターマーク情報、及びサーバ１０２の送信プロトコルに著作権情報を埋め込む情報を含みうる。
【０００４】
ペイロードデバイス１１２は、埋め込まれるべき適切なペイロードを計算し、ペイロードpLをウォーターマークエンジン１１０に転送する。前記ウォーターマークエンジンは、コンテンツ１０６にペイロードpLを埋め込む。ウォーターマークエンジン１１０からの結合されたデータは、次いで、暗号化デバイス１１４により暗号化される。前記結合されたデータは、従来は、単一の暗号化鍵により暗号化される。暗号化された信号E(y)は、次いで、インターネット１１６上でクライアント１１８に送信される。クライアント１１８は、この場合、復号デバイス１２０において暗号化された信号E(y)を復号する。ウォーターマーク入りであるが復号されたコンテンツは、次いで、前記ユーザによる使用のためにユーザデータベース１２２に記憶される。
【０００５】

現在、サーバプロセスは、３ＧＨｚペンティアムIVプロセッサ上で実時間の約４０倍で実行する。これは多くの場合に許容可能であるが、数百万の同時アクセスを必要とする大量コンテンツ配信に対して十分ではないかもしれない。この場合、マルチキャスティング及びキャッシングに対する可能性を持つ固定の低複雑度サーバが望ましい。サービスフレキシビリティのような実施されたことが望ましいこれら及び他の特徴は、ウォーターマーク埋め込みがクライアント側で行われる場合に達成されることができる。一般には、しかしながら、クライアント側の埋め込みは、ウォーターマーキングシステムをハッキングに対して弱くし、したがって、回避されるべきである。特に、前記クライアントがウォーターマーク入り及びウォーターマーク無しの両方のコンテンツを所有することが可能にされる場合、悪意を持って前記ウォーターマークを除去又は修正し、基礎となるアルゴリズムを推定することさえ、極度に容易である。結論として、暗号学的に安全な埋め込み解決法を提供することにより実施されるクライアント側の埋め込みに対する必要性が存在する。

【０００６】

ウォータークリプト（watercrypt）とも称される、安全なウォーターマーク埋め込みに対する１つの解決法は、ドイツ、ダルムシュタット、ＣＭＳ２００１カンファレンスにおいて提示された、Roland Parviainen及びPeter Parnesによる"Large scale distributed watermarking of multicast media through encryption"に開示されている。このアイデアは、ウォーターマークw_1及びw_2をそれぞれ備えた２つの暗号化されたメディアストリームx_1及びx_2を持つことである。暗号化及びウォーターマーキングは、フレームごと（パケット）のベースで行われ、すなわち、１つのパケットでいずれかのウォーターマークw_1又はw_2を抽出することが可能であるようにする。全てのパケットは、異なる鍵$K_e[i]$で暗号化される。したがって、合計2kのランダム暗号化鍵$K_e[1]$, $K_e[2]$, ..., $K_e[2k]$が必要とされる。x_1及びx_2の両方が、ユーザごとに送信される。

【０００７】

各ユーザは、信号x_1及びx_2が復号されるシーケンスを決定する復号鍵$K_d[i]$の一意的なシーケンスを与えられる。x_1及びx_2がバイナリ"０"及び"１"として符号化される場合、合計N = kビットの情報が、このようなウォーターマークを用いて運ばれることができる。このアプローチの欠点は、２つのパーティが、無効なペイロード又は他のクライアントを示す新しい有効なペイロードのいずれかを生成するために、交互のセグメントを連結するだけで、２つの復号されたシーケンスを容易に結合することができることである。このような攻撃は、システム全体を危険にさらすかもしれず、アルゴリズムをＥＭＤのようなアプリケーションに対して適用不可能にする。

【０００８】

安全な領域においてウォーターマークを埋め込むのに使用されることができる他の構成は、Niv Ahituv、Yeheskel Lapid及びSeev Neumannによる"Processing Encrypted Data", Communications of the ACM, Volume 30 no. 9, 1987に開示されている。この論文において、減算又は加算により特定の銀行口座の残高を更新する目的で暗号化されたデータを処理するアイデアが論じられている。彼らは、規則、

$E_{k1,k2}(A+B) = E_{k1}(A)+E_{k2}(B)$、及び

$E_k(a \times B) = E_k(A) \times a$

を満たす準同型暗号化関数を使用することを提案している。

【０００９】

この解決法は、しかしながら、特定のアルゴリズムに基づく実際の実施を欠いている。更に、この開示された方法は、モジュロ演算を仮定し、オーバーフロー条件下で機能しない。

【００１０】

したがって、ウォーターマークを埋め込む改良された方法は有利であり、特に、配信システムの信用されていないクライアント側においてウォーターマークを安全に埋め込むことを可能にする方法及びシステムは有利である。

【発明の開示】

【発明が解決しようとする課題】
【００１１】
したがって、本発明は、好ましくは、当技術分野における上で識別された欠陥及び不利点の１つ以上を単独で又は組み合わせて軽減、緩和又は除去することを追求し、添付の特許請求項による、配信システムのクライアント側においてウォーターマークを安全に埋め込むデバイス、方法、コンピュータ読み取り可能媒体及びメディア信号を提供することにより、少なくとも上述の問題を少なくとも部分的に解決する。
【課題を解決するための手段】
【００１２】
本発明による一般的な解決法は、信用されていないデバイス内の安全なウォーターマーク埋め込みに対する構成を提供する。
【００１３】
本発明の態様によると、デバイスにおいてメディア信号にウォーターマークを埋め込む方法、装置及びコンピュータ読み取り可能媒体が開示される。
【００１４】
本発明の一態様によると、デバイスにおいてメディア信号にウォーターマークを埋め込む方法が提供される。前記方法は、暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号の少なくとも部分的に暗号化されたメディア信号を提供するステップと、暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号を提供するステップと、暗号化された結合メディア信号を得るように結合器において前記少なくとも部分的に暗号化されたメディア信号及び前記少なくとも部分的に暗号化されたウォーターマーク信号を結合するステップと、第３の復号鍵k3を使用して前記暗号化された結合メディア信号を復号することにより復号されたメディア信号を得るステップとを有する。
【００１５】
本発明の他の態様によると、デバイスにおいてメディア信号にウォーターマークを埋め込むシステムが提供される。前記システムは、暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号の少なくとも部分的に暗号化されたメディア信号を提供する手段と、暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号を提供する手段と、暗号化された結合メディア信号を得るように結合器において前記少なくとも部分的に暗号化されたメディア信号及び前記少なくとも部分的に暗号化されたウォーターマーク信号を結合する手段と、第３の復号鍵k3を使用して前記暗号化された結合メディア信号を復号することにより復号されたメディア信号を得る手段とを有する。
【００１６】
本発明の他の態様によると、コンピュータにより処理する、デバイスにおいてメディア信号にウォーターマークを埋め込むコンピュータプログラムを包含するコンピュータ読み取り可能媒体が提供される。前記コンピュータプログラムは、暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号の少なくとも部分的に暗号化されたメディア信号を提供する第１のコードセグメントと、暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号を提供する第２のコードセグメントと、暗号化された結合メディア信号を得るように結合器において前記少なくとも部分的に暗号化されたメディア信号及び前記少なくとも部分的に暗号化されたウォーターマーク信号を結合する第３のコードセグメントと、第３の復号鍵k3を使用して前記暗号化された結合メディア信号を復号することにより復号されたメディア信号を得る第４のコードセグメントとを有する。
【００１７】
本発明の更に他の態様によると、メディア信号が提供される。より具体的には、暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号の少なくとも部分的に暗号化されたメディア信号と、暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも

部分的に暗号化されたウォーターマーク信号とを結合して有する、暗号化された結合メディア信号が提供され、前記結合信号が、第３の復号鍵k3を使用して前記暗号化された結合メディア信号を復号することにより復号されたメディア信号を提供するために復号可能であり、前記メディア信号は、復号されたウォーターマークを埋め込まれている。

【００１８】

本発明は、クライアントが信用されない場合でさえ、前記クライアントが前記クライアントにより受信されたコンテンツからウォーターマークを除去することができるリスク無しで、前記コンテンツが配信システムのクライアント側でウォーターマークされることを可能にする点で、従来技術に対する利点を少なくとも持つ。

【００１９】

本発明が持つことができるこれら及び他の態様、特徴及び利点は、添付の図面を参照して本発明の実施例の以下の記載から説明され、明らかになる。

【発明を実施するための最良の形態】

【００２０】

以下の記載は、電子音楽配信システムに応用可能な本発明の実施例に焦点を当てる。しかしながら、本発明がこの応用に限定されず、ウォーターマーキング技術を採用する多くの他の配信システム、例えば画像データベース等に応用されることができると理解されたい。図２は、本発明の一実施例による電子音楽配信（ＥＭＤ）システム２００の基本的なアーキテクチャを図示する。この後に論じられる解決法は図２のＥＭＤアーキテクチャに基づくが、多くの他の応用に対しても同じ原理が応用されることができる。このＥＭＤに関連して、以下の仮定を行う。サーバ及びクライアントからなるメディア配信サービスを持つ。前記サーバは信用されており、前記クライアントは信頼されていない。前記クライアントは、ウォーターマーク無しのコンテンツ又はウォーターマーク信号にアクセスすることができるべきでない。本発明は、もちろん、同様の仮定を満たす全てのシステムに対して応用可能である。

【００２１】

ＥＭＤシステム２００は、幾つかある特徴の中で特に、サーバ２０２、クライアント２１８及びインターネットのような配信ネットワーク２１６を有する。クライアント２１８がコンテンツプロバイダからコンテンツを要求することを望む場合、前記クライアントは、ネットワーク２１６上でサーバ２０２に対して要求reqを送信する。例えば、クライアント２１８は、例えばＭＰ３形式のファイルによりアクセス可能な電子音楽又はビデオを再生するデバイスであり、例えばユーザにより初期化される前記デバイスは、サーバ２０２を制御するプロバイダにより提供された音楽の特定の曲を要求する。管理プロセッサ２０３は、この要求を受信し、既知の形で前記要求を認証し、例えば正しいユーザが識別される及び／又は前記音楽の曲の後のダウンロードに対して引き落とされることを保証する。一度認証されると、コンテンツプロバイダ２０４は、ここではメディア信号xの形式で、要求されたコンテンツ２０６を暗号化デバイス２１２に送信する。暗号化デバイス２１２は、第１の暗号化鍵k_1を使用してコンテンツ２０６を少なくとも部分的に暗号化し、少なくとも部分的に暗号化されたメディア信号c_xを与える。加えて、コンテンツプロバイダ２０４は、前記要求されたコンテンツに対するコンテンツ情報（メディア信号x）をウォーターマークエンジン２１０に送信する。ウォーターマークエンジン２１０は、要求しているユーザからユーザＩＤ及び前記コンテンツ情報を取り、埋め込まれるべき適切なペイロードを計算する。ペイロード情報信号wは、次いで、暗号化デバイス２１４に送信される。暗号化デバイス２１４は、次いで、第２の暗号化鍵k_2を使用して少なくとも部分的にペイロード情報信号wを暗号化し、結果として部分的に暗号化されたウォーターマーク信号c_wを生じる。以下に詳細に説明されるように、サーバ２０２は、前記コンテンツ及び前記ペイロード情報を暗号化するのに様々な方法を使用することができる。例えば、２つの暗号化モジュールを使用する代わりに、サーバ２０２は、少なくとも２つの暗号化鍵と共に単一の暗号化デバイスを使用してもよい。サーバ２０２は、この場合、少なくとも部分的に暗号化された形式で、すなわち安全な方法で、少なくとも部分的に暗号化されたコン

テンツc_x及び少なくとも部分的に暗号化されたウォーターマーク情報信号c_wをクライアント２１８までネットワーク２１６上で送信する。

【００２２】

信号c_x及びc_wは受信器２１９により受信され、次いで、ウォーターマークエンジン２２０において結合される。この２つの少なくとも部分的に暗号化された信号c_x及びc_wは、暗号化された領域においてウォーターマーク入りコンテンツを生成するために結合される。換言すると、クライアント側のウォーターマークエンジン２２０は、演算$c_y = combine(c_x, c_w)$を実行する。

【００２３】

ウォーターマーク入りコンテンツc_yは、この場合、第３の復号鍵k_3を使用して復号デバイス２２２において復号される。復号デバイス２２２からの復号されたデータyはウォーターマーク入りコンテンツのみであり、すなわち、復号されたウォーターマーク入りメディア信号yは、第３の復号鍵k3を使用して、暗号化された結合メディア信号c_yを復号することにより生成される。送信された信号成分x 及びwは、第３の復号鍵k_3を使用して前記クライアントによりアクセスされることができない。前記ユーザのみが鍵k3を自由に使うことができ、成分x及びwがk3とは異なるk1及びk2でそれぞれ暗号化されているので、前記ユーザは、前記ウォーターマークを操作することができない。しかしながら、復号された信号yは、ウォーターマーク入りである正規のメディア信号であり、例えばユーザプレイヤユニット２２４において従来の方法で処理されることができる。

【００２４】

本発明の他の実施例によって、Paillier法を使用する準同型暗号を使用する前記コンテンツ及びペイロード情報の暗号化及び復号が、ここに記載される。図３は、本発明のこの実施例による準同型暗号を図示するフローチャートである。信用されているサーバ２０２において、管理プロセッサ２０３は、例えば、ステップ３０２において２つの素数p及びqを選択し、ステップ３０４においてK = pq、N = LCM(p-1,q-1)を算出し、ここでLCMは、最小公倍数である。K及びNは、クライアント３１８に供給される。管理プロセッサ２０３は、この場合、任意に、ステップ３０６においてKをK = k1+k2に分割する。正の整数r < Kに対して、暗号化デバイス２１２は、ここで、ステップ３０８において少なくとも部分的に暗号化されたコンテンツ信号c_xを計算し、ここで

$c_x = (1+K)^x r^{k1} \bmod K^2$　（１）又は

$c_x = (1+K)^x r^{N \cdot k1} \bmod K^2$　（２）

である。暗号化デバイス２１４は、ステップ３１０において暗号化されたペイロード情報信号c_wをも計算し、ここで$c_w = (1+N)^w r^{k2} \bmod K^2$又は$c_w = (1+N)^w r^{N \cdot k2} \bmod K^2$である。

【００２５】

c_x及びc_wがネットワーク２１６上でクライアント２１８に送信された後に、クライアント２１８は、ステップ３１２においてc_x及びc_wを結合し、ここで$c = c_w \cdot c_x = (1+N)^{w+x} r^{k1+k2} \bmod K^2$である。クライアント２１８は、次いで、ステップ３１４において、

$y = ((c^N-1) \bmod k3^2)/Nk3 \bmod k3$又は$y = ((c-1) \bmod k3^2)/k3 \bmod k3$　（３）

を使用して前記クライアントに供給された復号鍵k3 = Kを使用して前記ウォーターマーク入りコンテンツを抽出する。

【００２６】

（３）において与えられた関係が、以下の離散的な数学的恒等式の結果であることに注意する。k3 = p.q及びN = LCM(p-1,q-1)であるような素数p及びqを仮定すると、

如何なるr < k3に対しても、$r^{NK} \bmod k3^2 = 1 \bmod k3^2$であり、

如何なる整数a < k3に対しても、$(1+k3)^a \bmod k3^2 = (1+k3a) \bmod k3^2$である。

【００２７】

したがって、（１）及び（２）におけるc_xの定義に依存して、$c^N-1 \bmod k3^2 = (1+N)^{N(x+x)} r^{Nk3} \bmod k3^2 = (1+Nk3(x+w)) \bmod k3^2$又は$c-1 \bmod k3^2 = (1+N)^{(x+x)} r^{Nk3} \bmod k3^2 = (1+k3(x+w)) \bmod k3^2$である。これを（３）に入れると、

$y = ((c^N-1) \bmod k3^2)/Nk3 \bmod k3 = (x+w) \bmod k3$　又は

$y = ((c-1) \bmod k3^2)/k3 \bmod k3 = (x+w) \bmod k3$ （４）
を得る。
【００２８】
x+w < k3である場合、(x+w) mod k3 = x+2である。したがって、前記クライアントは、前記ウォーターマーク入りコンテンツを復号することができる。クライアント２１８は、どのようにk3がk1及びk2に分割されるかを知らないので、クライアント２１８は、前記暗号化されたコンテンツ信号及び前記暗号化されたペイロード情報信号を復号することができない。加えて、前記暗号化されたコンテンツ信号は、放送されることができる。各クライアント(i)は、この場合、一意的なk2（すなわち一意的なk3）を割り当てられる。前記暗号化されたペイロード情報信号は、したがって、この一意的なk2で暗号化され、これにより、前記ウォーターマークが対象とするクライアントのみがx+wを復号することができる。
【００２９】
本発明の他の実施例によって、El Gamal法を使用する準同型暗号を使用する前記コンテンツ及びペイロード情報の暗号化及び復号が、ここに記載される。図４は、本発明のこの実施例による準同型暗号を図示するフローチャートである。信用されているサーバ２０２において、管理プロセッサ２０３は、例えば、ステップ４０２においてランダムな数r及びk1及びgを選択し、ステップ４０４においてg^r及び$h_1 = g^{k1}$を算出する。暗号化デバイス２１２は、次いで、ステップ４０６において暗号化されたコンテンツ信号c_xを計算し、ここで$c_x = h_1{}^r g^x$であり、暗号化デバイス２１２は、前記クライアントに対(g^r, c_x)を提供する。暗号化デバイス２１４は、次いで、ステップ４０８において暗号化されたペイロード情報信号c_wを計算し、ここで$c_w = h_2(i)^r g^w$であり、各クライアント(i)に対して、前記サーバは、k2(i)及びk(i) = k1+k2(i)及び$h_2(i) = g^{k2(i)}$を選択し、ここでk(i)は前記クライアントに既知である。
【００３０】
(g^r, c_x)及びc_wがネットワーク２１６上でクライアント２１８に送信された後に、クライアント２１８は、ステップ４１０においてc_x及びc_wを結合し、ここで$c = c_w \cdot c_x = (h_1{}^r g^x) \cdot (h_2(i)^r g^w) = h(i)^r \cdot g^{x+w}$であり、$h(i)^r = h_1{}^r \cdot h_2(i)^r$である。前記クライアントは、この場合、ステップ４１２において$h(i)^r = (g^r)^{k(i)}$を計算し、x+wを復号する。
【００３１】
前記復号に対して、前記クライアントは、演算
$g^{x+w} = c/(h(i)^r) = (h(i)^r g^{x+w})/(h(i)^r)$ （５）
を実行し、ここでx+wは、離散的な指数関数g^{x+w}を反転することにより得られる。x+wが小さな語長（例えば８－１６ビットのオーダ）を持つと仮定すると、前記反転は、ルックアップテーブル（ＬＵＴ）により計算される。
【００３２】
図５による本発明の他の実施例において、コンピュータ読み取り可能媒体が概略的に図示される。コンピュータ読み取り可能媒体５００は、コンピュータ５１３により処理する、デバイスにおいてメディア信号にウォーターマークを埋め込むコンピュータプログラム５１０を包含している。コンピュータプログラム５１０は、暗号化が第１の暗号化鍵k1を使用して実行される、前記メディア信号xの少なくとも部分的に暗号化されたメディア信号c_xを提供する第１のコードセグメント５１４と、暗号化が第２の暗号化鍵k2を使用して実行される、少なくとも部分的に暗号化されたウォーターマーク信号c_wを提供する第２のコードセグメント５１５と、暗号化された結合メディア信号c_yを得るように結合器において少なくとも部分的に暗号化されたメディア信号c_x及び少なくとも部分的に暗号化されたウォーターマーク信号c_wを結合する第３のコードセグメント５１６と、第３の復号鍵k3を使用して前記暗号化された結合メディア信号c_yを復号することにより復号されたウォーターマーク入りメディア信号yを得る第４のコードセグメント５１７とを有する。
【００３３】
本発明は、ハードウェア、ソフトウェア、ファームウェア又はこれらの組み合わせを含

む如何なる適切な形式でも実施されることができる。しかしながら、好ましくは、本発明は、１以上のデータプロセッサ及び／又はデジタル信号プロセッサ上で実行されるコンピュータソフトウェアとして実施される。本発明の実施例の要素及び構成要素は、物理的に、機能的に及び論理的に如何なる適切な方法でも実施されることができる。実際に、機能は、単一のユニット、複数のユニット又は他の機能ユニットの一部として実施されてもよい。このように、本発明は、単一のユニットにおいて実施されてもよく、又は異なるユニット及びプロセッサ間で物理的に及び機能的に分散されてもよい。

【００３４】

本発明は、特定の実施例を参照して上に記載されているが、ここに記載された特定の形式に限定されることは意図していない。むしろ、本発明は、添付の請求項によってのみ限定され、特定の上記実施例とは別の実施例、例えば上に記載されたものとは異なる配信システムは、これらの添付の請求項の範囲内で同等に可能である。

【００３５】

請求項において、用語"有する"は、他の要素又はステップの存在を除外しない。更に、個別にリストされるが、複数の手段、要素又は方法ステップは、例えば単一のユニット又はプロセッサにより実施されてもよい。加えて、個別の特徴が異なる請求項に含まれうるが、これらはあるいは有利に組み合わされることができ、異なる請求項内への包含は、特徴の組み合わせが可能及び／又は有利ではないことを意味しない。加えて、単数形表示は、複数を除外しない。用語"１つの"、"第１の"、"第２の"等は、複数を除外しない。請求項内の参照符号は、単に明確化する例として提供され、請求項の範囲をいかなる形にも限定すると解釈されるべきでない。

【図面の簡単な説明】

【００３６】

【図１】既知の電子音楽配信システムの概略図である。

【図２】本発明の一実施例による電子音楽配信システムの概略図である。

【図３】本発明の他の態様によるPaillier法を使用する準同型暗号を図示するフローチャートである。

【図４】本発明の他の実施例によるEl Gamal法を使用する準同型暗号を図示するフローチャートである。

【図５】本発明の他の実施例によるコンピュータ読み取り可能媒体を図示する。

【図１】

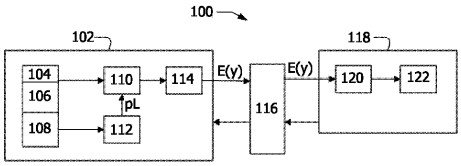


FIG.1

【図２】

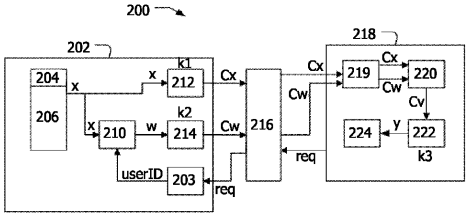


FIG.2

【図３】

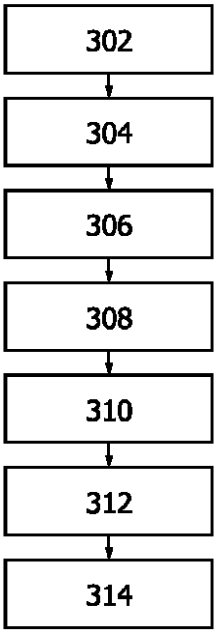


FIG.3

【図４】

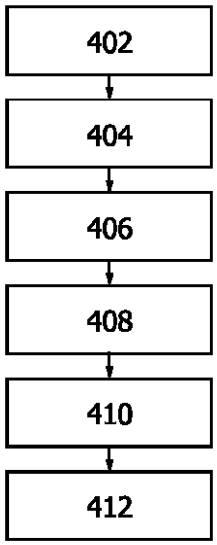


FIG.4

【国際調査報告】

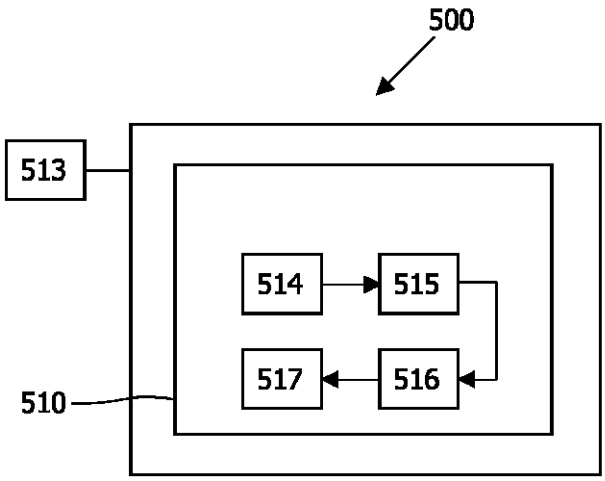


FIG.5

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/051773

A. CLASSIFICATION OF SUBJECT MATTER
INV. G10L19/00 G06T1/00 H04N7/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G10L G06T H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	S. KATZENBEISSER: "D.WVL.5 First summary report on hybrid systems" ECRYPT, 31 May 2005 (2005-05-31), XP002401346 Magdeburg, D	1-6, 10-18
Y	pages 11-16	19
Y	VEEN VAN DER M ET AL: "WATERMARKING AND FINGERPRINTING FOR ELECTRONIC MUSIC DELIVERY" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 5306, 2004, pages 200-211, XP008037770 ISSN: 0277-786X abstract	19

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance
'E' earlier document but published on or after the international filing date
'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
'O' document referring to an oral disclosure, use, exhibition or other means
'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 October 2006	16/10/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Quélavoine, Régis

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/051773

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HAK SOO JU, HYUN JEONG KIM, DONG HOON LEE, JONG IN LIM: "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control" ICISC 2002, , - 29 November 2002 (2002-11-29) pages 421-432, XP002401347 Seoul, Korea * section 2.1 Memon-Wong's scheme *	1-6, 13-19
P,X	EP 1 612 727 A (CANON RESEARCH CENTRE FRANCE; INRIA INSTITUT NATIONAL DE RECHERCHE EN) 4 January 2006 (2006-01-04) abstract paragraphs [0005], [0040]	1-6, 10-19
P,X	KATZENBEISSER, KALKER: "Structure preserving cryptography" BIRS 05W5505, 23 July 2005 (2005-07-23), - 28 July 2005 (2005-07-28) XP002401348 Calgary, Canada the whole document	1-6, 10-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/051773

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1612727 A	04-01-2006	FR 2872373 A1	30-12-2005

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ペンティアム

(72)発明者 ファン デル フェーン ミンネ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６
(72)発明者 トゥイルス ピム ティー
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６
(72)発明者 カルケル アントニウス エイ シー エム
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６

Ｆターム(参考) 5B057 CE08 CG07
5C076 AA14 BA06
5J104 AA14 AA32 JA03 NA02 NA27 NA37 PA14