

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4666302号
(P4666302)

(45) 発行日 平成23年4月6日 (2011.4.6)

(24) 登録日 平成23年1月21日 (2011.1.21)

(51) Int.Cl.

F I

H04L 9/08 (2006.01)
G06F 21/24 (2006.01)

H04L 9/00 601B
H04L 9/00 601E
G06F 12/14 520A
G06F 12/14 540B
G06F 12/14 540C

請求項の数 25 外国語出願 (全 35 頁)

(21) 出願番号 特願2004-226125 (P2004-226125)
(22) 出願日 平成16年8月2日 (2004.8.2)
(65) 公開番号 特開2005-124150 (P2005-124150A)
(43) 公開日 平成17年5月12日 (2005.5.12)
審査請求日 平成19年6月14日 (2007.6.14)
(31) 優先権主張番号 0317964.5
(32) 優先日 平成15年7月31日 (2003.7.31)
(33) 優先権主張国 英国 (GB)

(73) 特許権者 593081408
ソニー ヨーロッパ リミテッド
イギリス国 サリー、ウェーブブリッジ、ブ
ルックランズ、ザ ハイッ (番地なし)
(74) 代理人 100104215
弁理士 大森 純一
(74) 代理人 100117330
弁理士 折居 章
(72) 発明者 ペリー ジェイソン チャールズ
イギリス国 KT13 0XW、ウエイ
ブリッジ、ブルックランズ、ザ ハイ
ッ (番地無し) ソニー ユナイテッド
キングダム リミテッド内

最終頁に続く

(54) 【発明の名称】 デジタルコンテンツのためのアクセス制御

(57) 【特許請求の範囲】

【請求項 1】

データコンテンツを、読出専用媒体識別子が記録されたコンテンツ記録媒体に記録する
ために、当該データコンテンツを入力可能な記録装置であって、

コンテンツ鍵の組に含まれる各コンテンツ鍵により、上記データコンテンツの、上記各
コンテンツ鍵に対応する各一部を暗号化する暗号化器と、

複数のユーザのそれぞれの公開鍵を記憶するアクセス制御メモリ装置と、

上記データコンテンツの各一部を復号するための上記各コンテンツ鍵を導出するには、
上記読出専用媒体識別子へのアクセス及び上記アクセス制御メモリ装置に記憶された各公
開鍵に対応する各秘密鍵へのアクセスが必要となるように、上記複数のユーザのそれぞれ
に上記データコンテンツの各一部へのアクセス許可を与えるためのコンテンツアクセス制
御データを生成するデータ生成器と、

上記暗号化されたデータコンテンツ及び上記コンテンツアクセス制御データを上記コン
テンツ記録媒体に記録するレコーダと
を備える記録装置。

【請求項 2】

上記データ生成器は、セッション鍵を用いて上記読出専用媒体識別子を対称的に暗号化
することを特徴とする請求項 1 記載の記録装置。

【請求項 3】

上記データ生成器は、セッション鍵を用いて、上記各コンテンツ鍵のうち少なくとも 1

つのコンテンツ鍵を対称的に暗号化し、上記セッション鍵を上記読出専用媒体識別子に結合することによって結合データを生成し、上記各ユーザのそれぞれの公開鍵／秘密鍵の対のうち少なくとも1つの公開鍵を用いて、上記結合データを暗号化することで上記アクセス制御データを生成することを特徴とする請求項1記載の記録装置。

【請求項4】

上記データ生成器は、コンテンツアクセスセッション鍵を用いて、上記各コンテンツ鍵のうち少なくとも1つのコンテンツ鍵を対称的に暗号化し、上記各ユーザのそれぞれの公開鍵／秘密鍵の対のうち少なくとも1つの公開鍵を用いて、上記コンテンツアクセスセッション鍵を非対称的に暗号化し、読出専用媒体識別子セッション鍵を用いて、上記媒体識別子を暗号化して実効媒体識別子を導出し、上記実効媒体識別子を用いて、上記非対称的に暗号化されたコンテンツアクセスセッション鍵を暗号化し、上記各ユーザのそれぞれの公開鍵／秘密鍵の対のうち少なくとも1つの公開鍵を用いて、上記媒体識別子セッション鍵を非対称的に暗号化することで上記アクセス制御データを生成することを特徴とする請求項1記載の記録装置。

10

【請求項5】

上記データ生成器は、上記各ユーザのそれぞれの公開鍵／秘密鍵の対のうち少なくとも1つの公開鍵を用いて、上記各コンテンツ鍵のうち少なくとも1つのコンテンツ鍵を非対称的に暗号化することで上記アクセス制御データを生成することを特徴とする請求項1記載の記録装置。

【請求項6】

上記読出専用媒体識別子は、ユニーク媒体識別子であることを特徴とする請求項1記載の記録装置。

20

【請求項7】

上記コンテンツ記録媒体は、光ディスク媒体であることを特徴とする請求項1記載の記録装置。

【請求項8】

上記アクセス制御メモリ装置は、上記複数のユーザのうち、当該アクセス制御メモリ装置を所有するユーザの公開鍵／秘密鍵の対のうち秘密鍵を導出可能な情報を安全に記憶し

、当該記録装置は、上記暗号化器と、上記アクセス制御メモリ装置との間の安全なデータ接続を提供するインタフェースを備える請求項1記載の記録装置。

30

【請求項9】

上記アクセス制御メモリ装置は、リムーバブルメモリ装置であることを特徴とする請求項8記載の記録装置。

【請求項10】

上記リムーバブルメモリ装置は、上記データコンテンツの暗号化を実行し及び／又は上記コンテンツアクセス制御データの生成に関連する暗号化を実行するデータ処理モジュールを備えることを特徴とする請求項9記載の記録装置。

【請求項11】

上記リムーバブルメモリ装置は、スマートカードであることを特徴とする請求項9記載の記録装置。

40

【請求項12】

上記リムーバブルメモリ装置は、マジックゲート（商標）メモリースティック（商標）装置であることを特徴とする請求項9記載の記録装置。

【請求項13】

上記リムーバブルメモリ装置は、セキュアデジタルカードであることを特徴とする請求項9記載の記録装置。

【請求項14】

上記データコンテンツは、ビデオ画像を含み、上記ビデオ画像の少なくとも幾つかについて、第1の暗号化方式が上記ビデオ画像の全てではない一部のそれぞれに適用され、第

50

2の暗号化方式が上記ビデオ画像の残りのそれぞれに適用されることを特徴とする請求項1記載の記録装置。

【請求項15】

上記第1の暗号化方式は、可視ウォーターマークの付与であり、上記第2の暗号化方式は、対称又は非対称の暗号化であることを特徴とする請求項14記載の記録装置。

【請求項16】

読出専用媒体識別子及びコンテンツアクセス制御データと共にコンテンツ記録媒体に記録された暗号化されたデータコンテンツを再生する再生装置であって、

上記データコンテンツの各一部は、コンテンツ鍵の組に含まれる、当該各一部に対応する各コンテンツ鍵によって暗号化されており、

10

上記コンテンツアクセス制御データは、複数のユーザのそれぞれに上記データコンテンツの各一部へのアクセス許可を与えるためのものであって、かつ、上記データコンテンツの各一部を復号するための上記各コンテンツ鍵を導出するには、上記読出専用媒体識別子へのアクセス及び上記各ユーザの各秘密鍵へのアクセスが必要となるように生成されており、

当該再生装置は、

上記各ユーザの各秘密鍵に対応する公開鍵を記憶するアクセス制御メモリ装置と、

上記コンテンツ記録媒体から、上記読出専用媒体識別子、上記暗号化されたデータコンテンツ及び上記コンテンツアクセス制御データを再生する再生器と、

上記読出専用媒体識別子及び上記各ユーザの秘密鍵を用いて、上記コンテンツアクセス制御データから、上記データコンテンツの各一部を復号するための上記各コンテンツ鍵を導出するプロセッサと、

20

上記復号された各コンテンツ鍵を用いて、上記暗号化されたデータコンテンツの各一部を復号する復号器と

を備える再生装置。

【請求項17】

上記コンテンツアクセス制御データは、暗号化された媒体識別子セッション鍵を含み、

上記コンテンツ鍵の組に含まれる各コンテンツ鍵は、上記媒体識別子セッション鍵に基づいて暗号化されており、

上記プロセッサは、上記各ユーザの各秘密鍵を用いて、上記暗号化された媒体識別子セッション鍵を復号し、上記媒体識別子セッション鍵を用いて上記読出専用媒体識別子を暗号化することによって実効媒体識別子を生成し、上記実効媒体識別子を用いて、上記暗号化された各コンテンツ鍵を復号し、当該復号された各コンテンツ鍵を用いて、上記暗号化されたデータコンテンツの各一部を復号することを特徴とする請求項16記載の再生装置。

30

【請求項18】

請求項1記載の記録装置及び請求項16記載の再生装置を備える記録／再生装置。

【請求項19】

当該記録装置は、オーディオ記録装置、ビデオ記録装置、ビデオ処理装置又はビデオ出力装置のうちの少なくとも1つを含むことを特徴とする請求項1記載の記録装置。

40

【請求項20】

データコンテンツを、読出専用媒体識別子が記録されたコンテンツ記録媒体に記録する記録方法であって、

暗号化器において、コンテンツ鍵の組に含まれる各コンテンツ鍵により、上記データコンテンツの、上記各コンテンツ鍵に対応する各一部を暗号化するステップと、

インタフェースを介して、複数のユーザのそれぞれの公開鍵を記憶するアクセス制御メモリ装置と、上記暗号化器とを接続するステップと、

上記データコンテンツの各一部を復号するための上記各コンテンツ鍵を導出するには、上記読出専用媒体識別子へのアクセス及び上記アクセス制御メモリ装置に記憶された各公開鍵に対応する各秘密鍵へのアクセスが必要となるように、上記複数のユーザのそれぞれ

50

に上記データコンテンツの各一部へのアクセス許可を与えるためのコンテンツアクセス制御データをデータ生成器により生成するステップと、

レコーダにより、上記暗号化されたデータコンテンツ及び上記コンテンツアクセス制御データを上記コンテンツ記録媒体に記録するステップと
を有する記録方法。

【請求項 2 1】

読出専用媒体識別子及びコンテンツアクセス制御データと共にコンテンツ記録媒体に記録された暗号化されたデータコンテンツを再生する再生方法であって、

上記データコンテンツの各一部は、コンテンツ鍵の組に含まれる、当該各一部に対応する各コンテンツ鍵によって暗号化されており、

上記コンテンツアクセス制御データは、複数のユーザのそれぞれに上記データコンテンツの各一部へのアクセス許可を与えるためのものであって、かつ、上記データコンテンツの各一部を復号するための上記各コンテンツ鍵を導出するには、上記読出専用媒体識別子へのアクセス及び上記各ユーザの各秘密鍵へのアクセスが必要となるように生成されており、

当該再生方法は、

再生器により、上記コンテンツ記録媒体から、上記読出専用媒体識別子、上記暗号化されたデータコンテンツ及び上記コンテンツアクセス制御データを再生するステップと、

インタフェースを介して、上記各ユーザの各秘密鍵に対応する公開鍵を記憶するアクセス制御メモリ装置と、プロセッサとを接続するステップと、

上記プロセッサにより、上記読出専用媒体識別子及び上記各ユーザの秘密鍵を用いて、上記コンテンツアクセス制御データから、上記データコンテンツの各一部を復号するための上記各コンテンツ鍵を導出するステップと、

復号器により、上記復号された各コンテンツ鍵を用いて、上記暗号化されたデータコンテンツの各一部を復号するステップと

を有する再生方法。

【請求項 2 2】

コンピュータに、請求項 2 0 記載の記録方法を実行させるプログラム。

【請求項 2 3】

請求項 2 2 記載のプログラムを記録した記録媒体。

【請求項 2 4】

コンピュータに、請求項 2 1 記載の再生方法を実行させるプログラム。

【請求項 2 5】

請求項 2 4 記載のプログラムを記録した記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、デジタルコンテンツのためのアクセス制御に関する。このようなコンテンツとしては、例えばオーディオビジュアルコンテンツ等、ビデオコンテンツ、オーディオコンテンツ、メタデータコンテンツ、テキストコンテンツ、画像コンテンツの1つ以上が含まれる。

【背景技術】

【0002】

プロセッサパワーの強化と相まって、デジタル機器及び高速ネットワークを始めとする新たなデジタルインフラストラクチャの成長により、コンテンツの作成、処理及び配布が簡単で高速に行えるようになった。このことは、コンテンツの合法的な使用を大いに促進するが、このようなコンテンツ（特に、著作権コンテンツ）の権限なき不正使用、例えば権限のない再生又は配布もより容易に行うことができるようになり、コンテンツの所有者の被害も大きくなっている。

【0003】

10

20

30

40

50

ユーザがコンテンツを使用する権利を所有者から購入する前に、商業的理由から、コンテンツの所有者が潜在的ユーザにコンテンツの視聴又は使用を試させる場合があり、このことが状況をより複雑にしている。

【0004】

これらの問題を解決するために、所謂デジタル著作権管理 (digital rights management: 以下、DRMという。) システムが提案されている。周知のDRMシステムは、通常、コンテンツを配信するために、データ暗号化技術を用いてコンテンツを暗号化する。認証された受信者 (recipient) は、復号鍵を受け取り、受信者は、暗号化されたコンテンツを復号することができる。これは、コンテンツへのアクセス制御を実現する極めて基本的な手法であるが、この手法は煩雑であり、柔軟性に欠ける。アクセスを提供するために用いられる全てのデータ (この場合、復号鍵及び関連するアクセス許可データを含む) は、それが関係する記録された情報コンテンツとは別に保存されている。この手法では、コンテンツと関連するアクセスデータとの関係を把握するためのある種のデータベースを維持しなくてはならないという問題が生じる。これらの短所の全ては、職場の生産性を低下することになる。

10

【発明の開示】

【課題を解決するための手段】

【0005】

ツにアクセス制御処理を適用し、及び読出専用媒体識別子が記録されているコンテンツストレージ媒体にアクセス制御されたデータコンテンツを記録する記録装置において、コンテンツ鍵の組に基づいて、データコンテンツの一部を暗号化する暗号化手段と、情報コンテンツを復号するには、読出専用媒体識別子へのアクセスが必要となるように、コンテンツ鍵の組のそれぞれのサブセットの少なくとも1つの暗号化されたバージョンを含むコンテンツアクセス制御データを生成するデータ生成手段と、暗号化されたデータコンテンツ及びコンテンツアクセス制御データをコンテンツストレージ媒体に記録する記録手段とを備える。

20

【0006】

本発明は、コンテンツに対する選択的なアクセス及び個別のアクセスの必要性及びコンテンツの認証されていない (海賊版) コピーへの同等なアクセスを許すことなく特定の記録媒体に記録されたコンテンツへのアクセスを提供する必要性を見出し、これを実現する。

30

【0007】

例示的な状況として、コンテンツは、例えば、コンパクトディスク、DVDディスク、又は所謂ブルーレイ (商標) ディスク等の高密度ストレージデバイスを介して配付してもよい。各ユーザに容認されたアクセスのレベルは、各ユーザのRMDに保存されている秘密鍵及び情報コンテンツを復号するためには、読出専用媒体識別子へのアクセスが必要となるように生成されたコンテンツアクセス制御データによって制限される。すなわち、コンテンツアクセス制御データは、読出専用媒体識別子が関連付けられた特定の記録媒体のみに対して有効である。コンテンツ及び鍵データが異なる記録媒体識別を有する別のディスクにコピーされた場合、コンテンツを復号することはできない。

40

【0008】

認証されていないコピーでは、情報コンテンツ及び鍵データのみではなく、媒体識別子もコピーされてしまう。記録媒体のデータのビット毎の不正なコピーが作成された場合、ビット毎の記録が作成された記録媒体の媒体識別子は、コンテンツアクセスデータが関連付けられている媒体識別子とは異なるものとなり、これにより、如何なるユーザ又は装置も、不正にコピーされた情報コンテンツにアクセスできなくすることができる。

【0009】

本発明の更なる側面及び特徴は、添付の請求の範囲において定義されている。

【発明を実施するための最良の形態】

【0010】

50

図1は、本発明に基づくデジタルデータコンテンツのためのアクセス制御システムを図式的に示している。このアクセス制御システムは、画像を撮像し、ディスクやビデオテープ等の記録媒体にデジタル画像データを記録するカメラ110と、記録された画像データを再生する再生装置120と、デジタル的に記録された画像データをコピーすることによって、複製及び再生を可能にする記録装置124と、アクセス制御メモリ装置（この実施例ではリムーバブルメモリ装置）130と、ディスク状記録媒体140とを備える。カメラ110及び再生装置120は、いずれもリムーバブルメモリ装置130に接続するためのインタフェースを有する。カメラ110は、静止画及び／又は動画を撮影することができる。このアクセス制御システムは、ディスク状記録媒体140に記録された暗号化されたコンテンツへの選択的なアクセスを提供し、復号された情報コンテンツの異なる部分へのアクセスを異なるユーザ及び／又はユーザグループに選択的に許可することができる。

10

【0011】

情報コンテンツを暗号化／復号するための暗号方式には、対称鍵暗号（symmetric key cryptography）と非対称鍵暗号（asymmetric key cryptography）といった2つの主要な暗号方式がある。対称鍵暗号では、情報を復号するために用いられる鍵は、情報を暗号化するために用いられる鍵と同じ（又は容易に導出可能）である。一方、非対称鍵暗号では、復号に用いられる鍵は、暗号化に用いられる鍵とは異なり、ある鍵から他の鍵を演算によって推定することが不可能である必要がある。非対称鍵暗号では、一对の公開鍵／秘密鍵が生成され、情報の暗号化には、公開鍵（秘密にされる必要はない。）が使用され、情報の復号には、秘密鍵（秘密にする必要がある。）が使用される。使用できる非対称鍵暗号アルゴリズムの具体例としては、RSAアルゴリズムがある。RSAアルゴリズムは、一方向性関数に基づいている。公開鍵 X は、共に秘密鍵を構成する2つの大きな素数 p と q の積である。公開鍵 X は、暗号化処理において、一方向性関数に挿入され、これにより、受信者の公開鍵に適合する特定の一方方向性関数が得られる。特定の一方方向性関数は、メッセージを暗号化するために使用される。受信者は秘密鍵（ p と q ）のみに関する知識に基づいて、特定の一方方向性関数の逆関数を求めることができる。なお、公開鍵 X に関する知識のみからは、 p と q を推定することが不可能となるように、公開鍵 X は、十分大きくなければならない。

20

【0012】

RSAの代替となる非対称暗号方式としては、楕円曲線暗号（elliptical curve cryptography：以下、ECCという。）がある。RSAの場合のように、非常に大きい素数の積として鍵を生成するのではなく、ECCでは、楕円曲線方程式の性質によって鍵を生成する。ECCは、鍵をRSAよりも高速に生成でき、したがって、本発明に基づく構成においては、より好ましい非対称暗号技術である。ディスク状記録媒体140に記録された情報コンテンツは、1つ以上のコンテンツ暗号化鍵（content encryption key：以下、CEKという。）を用いて対称的に暗号化され、CEKは、公開鍵／秘密鍵の対を用いて非対称的に暗号化される。本発明の他の実施例では、情報コンテンツを非対称的に暗号化してもよい。CEKは、図8を用いて以下に詳細に説明するように、バイナリツリー暗号化方式（binary tree encryption）に基づいて生成され、暗号化された情報コンテンツの異なった部分がCEKの異なるサブセットに対応するように、例えば10秒毎等、定期的に更新される。これにより、復号された情報コンテンツへの選択的なアクセスが実現する。対称暗号方式は、演算負荷が小さく、したがって非対称暗号方式より高速に実行できるため、ここでは、情報コンテンツの暗号化には対称暗号方式を使用する。

30

40

【0013】

この実施例では、各ユーザ及び／又はユーザグループに対し、複数のユーザのそれぞれと、CEKのサブセットを暗号化するために用いることができる公開鍵とのリストであるユーザディレクトリを保存する安全なリムーバブルメモリ装置130を提供する。他の実施例では、公開鍵及び／又は秘密鍵が保存されるメモリ装置は、リムーバブルではなく、固定メモリ（例えば、カメラ内に設けられる）であってもよい。これにより、ユーザは、CEKのサブセットに対応する情報コンテンツの一部にアクセスすることができる。また

50

、リムーバブルメモリ装置（removable memory device：以下、RMDとも呼ぶ。）は、そのRMDを所有するユーザ又はユーザグループに対する秘密鍵も保存する。

【0014】

記録情報コンテンツへのアクセス許可は、必要に応じて新しいユーザにRMDを発行し、及び既存のユーザから認証を奪う権限が与えられた管理者（administrator）が集中的に管理することができる。それぞれの新しい認可されたユーザに対して、公開鍵／秘密鍵の対を生成する必要がある、そのユーザのための秘密鍵は、そのユーザに対応するRMDに保存される。また、新しいユーザは、そのユーザのRMDに保存されているユーザディレクトリにも追加される。ユーザディレクトリには、バージョン番号を示すタグがあり、新しいユーザが追加され又は削除される毎にバージョン番号を増やすことができる。

10

【0015】

RMDに保存されている情報に対する権限のないコピーを防ぐために、RMDには、情報を安全に格納する必要がある。秘密鍵に対する権限のないアクセスを防止することは特に重要である。この装置に適切に用いられる安全なメモリ装置の具体例としては、スマートカード、ソニー株式会社（商標）のマジックゲートメモリースティック（Magic Gate Memory Stick、商標）記憶装置、セキュアデジタルカード（Secure Digital Card：SDカード）等があり、この場合、インタフェースは、RMDが挿入される、RMDの形状に対応するスロットであることが望ましい。マジックゲートシステムの動作については、図18～図20を用いて後に詳細に説明する。

【0016】

20

RMDは、ユーザディレクトリとRMD所有者データとを含むデータの保存のみに使用してもよい。なお、他の実施例として、RMDは、暗号化及び／又は復号の処理を実行可能なオンボードデータ処理モジュールを有していてもよい。この場合、データコンテンツの暗号化及び／又はコンテンツアクセス制御データを生成するための暗号化処理の少なくとも一部は、RMD上のデータ処理モジュールによって実行することができる。同様に、データコンテンツ又はコンテンツアクセス制御データの復号の少なくとも一部をRMDのデータ処理モジュールによって実行することもできる。更に、リムーバブルメモリ装置と機器との間の接続は、物理接続で行ってもよく無線インタフェースを介して行ってもよい。リムーバブルメモリ装置は、入力データコンテンツを暗号化し、コンテンツアクセス制御データを生成するデータ処理モジュールを備えていてもよい。

30

【0017】

ディスク状記録媒体140には、対称的に暗号化された情報コンテンツと非対称的に暗号化されたCEKが記録される。この実施例では、ディスク状記録媒体140は、コンパクトディスク（CD）、デジタルバーサタイルディスク（DVD）、光ディスク、又はブルーレイ技術を用いた高密度ディスク等のディスク状記録媒体である。なお、これに代えて、テープ状記録媒体等の他の種類の記録媒体を用いてもよい。情報コンテンツの復号された部分へのアクセスは、それらの部分に関連しているCEKを復号する能力に依存するので、異なる権限を有するユーザは、情報コンテンツのそれぞれ異なる復号された部分へのアクセス権を有していることとなる。

【0018】

40

カメラ110によって情報コンテンツを撮影する場合、カメラ操作者は、RMD130をカメラRMDインタフェース112に挿入する。撮影された画像データの対照的な暗号化に用いるCEKは、その画像データへのアクセス権を与えられた認証されたユーザの個々の公開鍵を用いて、非対称的にエンコードされる。公開鍵は、カメラの撮影者のメモリーカードに登録されたユーザディレクトリから入手される。この実施例では、メモリーカード内に公開鍵自体を保存しているが、これに代えて、公開鍵は、例えばハッシュ値（このハッシュ値を逆にすることによって鍵が復元される）として保存してもよく、又はルックアップテーブルとして保存してもよい。データセットのハッシュは、データから擬似ランダム的に得られる固定長ビット列である。また、秘密鍵も、そのままルックアップテーブル内に又はハッシュ値として保存してもよい。再生時には、認証されたユーザのRMD

50

130は、再生装置120のRMDインタフェース122に挿入され、ディスク状記録媒体140にそのユーザに対応する公開鍵を用いて格納されたユーザの秘密鍵を用いてCEKが復号される。適切なCEKが復号されると、それらのCEKを用いて、対応する情報コンテンツを復号することができるようになる。記録装置124を用いて、再生装置120内のディスク状記録媒体140をコピーする操作が行われることがある。記録装置124と再生装置120は、共通のRMDインタフェース122を有する。RMDは、記録媒体上のコンテンツに関するアクセスを制御するが、記録装置（実際には如何なる記録装置でもよい）を用いて、復号された情報コンテンツをコピーすることができる。これは、復号された情報コンテンツが安全な環境で操作されることを仮定している。これにより、アクセス制御システムがビデオ編集者による仕事の流れの障害となることを比較的少なくすることができる。例えば、新たにコピーされたバージョンは、そのバージョンをコピーしたユーザのみがアクセスできるようにしてもよい。これに代えて、新たにコピーされたバージョンには、（このバージョンとともに保存された、暗号化されたCEKの異なるバージョンによって）、アクセス権限を記録してもよく、これにより、元のコピーへアクセス権を有する全てのユーザが、このコピーされた新たなバージョンにもアクセスできるようにしてもよい。

10

【0019】

図2は、本発明に基づくカメラ110内における録画処理を説明するための図である。この構成のカメラ110では、捕捉されたオーディオビジュアル（audio-visual：以下、AVという。）情報は、圧縮エンジン210によって圧縮され、圧縮されたAVデータは、暗号化エンジン220に供給され、暗号化エンジン220は、次世代暗号化規格（Advanced Encryption Standard：以下、AESという。）アルゴリズムを用いて、圧縮されたAVデータを暗号化する。暗号化エンジン220は、一般的な圧縮データレート（例えば、DVCAm圧縮のための25Mbps又はIMX圧縮のための50Mbps）を容易に取り扱うことができる。また、圧縮データには、可視ウォーターマーク法として知られる暗号化の手法も適用でき、この処理は、AES対称暗号化に加えて行ってもよく、AES対称暗号化に代えて行ってもよい。

20

【0020】

可視ウォーターマーク法とは、可逆的なアルゴリズムを用いて画像マテリアルに目に見える変更を施し、これによって画像マテリアルの品質を低減する処理である。目に見える変更は、画像／ビデオデータの選択された部分に適用され、例えば、コンテンツにおいて「ロゴ」が見えるようにする。変更される画像の部分は、ビットマップ又は変更テンプレートによって定義される。この変更処理は、変換画像の離散コサイン変換（Discrete Cosine Transform：以下、DCTという。）係数の一部を変更する処理を含んでもよい。この可視ウォーターマークにより、安全な形式で（すなわち、品質が損なわれていないコンテンツへの直接のアクセスを許可することなく）ユーザにコンテンツをプレビューさせることができる。画像の変更は、暗号的に安全な手法（cryptographically secure manner）で完全に可逆的に行われ、元のコンテンツは、「ウォッシング鍵（washing key）」として知られている復号鍵にアクセスすることにより、ビット毎に復元することができる。可視のウォーターマーク付与と、対称／非対称の暗号化の両方を画像に適用することができる。アクセス許可の第1のレベルではユーザに画像の復号を許可するが、ウォーターマークの除去（wash）は許可せず、更なる第2のレベルでは、ユーザにウォッシング鍵を提供し、これにより画像から可視ウォーターマークを取り除くことを許可する。このウォッシング鍵は、例えば、ユーザによる料金の支払いに応じて提供してもよい。

30

40

【0021】

暗号化エンジン220は、バイナリツリー暗号化方式により、CEKを生成する。対称CEKは、認証された複数のユーザのそれぞれの公開鍵によって非対称的に暗号化される。公開鍵は、カメラ110に現在接続されているRMD130に保存されている公開鍵のユーザディレクトリから得られる。暗号化されたAVデータの異なる部分に対応するCEKの異なるサブセットは、認証された各ユーザに対し、それぞれのアクセス許可に応じて

50

、非対称的に暗号化することができる。複数のユーザのそれぞれに対する非対称的に暗号化されたC E Kは、対称的に暗号化されたA V情報コンテンツの単一のコピーとともにディスク状記録媒体140に記録される。非対称の暗号化は、RMD130自体の回路（例えば、スマートカードプロセッサ）で行ってもよく、カメラ110自体の暗号化エンジン220で行ってもよい。

【0022】

図3は、本発明に基づく再生装置120において行われる再生処理を説明するための図である。圧縮され、対称的に暗号化された情報コンテンツと、非対称的に暗号化されたC E Kは、ディスク状記録媒体140から読み出され、復号エンジン310に供給される。認証されたユーザは、再生装置120のRMDインタフェース122にRMD130を挿入し、復号エンジン310は、RMDインタフェース122に保存されている秘密鍵にアクセスし、A Vコンテンツの少なくとも一部を復号する。認証されたユーザがアクセス可能なA Vコンテンツの一部（例えば、フレーム、ショット又はシーンのあるサブセット）は、ユーザの公開鍵を用いて暗号化され、ディスク状記録媒体140に記録されているC E Kに依存する。ユーザが再生装置120を用いて保護されたコンテンツを復号すると、ユーザは、「保護が解除された（de-protected）」情報コンテンツをディスク状記録媒体140に戻すか、或いは新たなディスク記録媒体に記録するかを選択することができる。この実施例では、再生装置120は、記録処理も行うことができると仮定している。データパッケージ328は、復号された情報コンテンツとともに、ディスク状記録媒体140に記録される。データパッケージ328は、ソースデータパッケージ内に、ユーザの保有するアクセス権の詳細を示している。復号されたコンテンツをディスク状記録媒体140に記録したユーザ、又はこれ以外のユーザが、ディスク状記録媒体140に記録されている情報コンテンツにアクセスしようとする場合、そのユーザは、保護が解除され、その保護が解除されたフォーマットで記録されたコンテンツの少なくとも一部にアクセスすることが許可される場合がある。ここで、再生装置120が、単に、ユーザが視聴することを選択した（ユーザがアクセス権を有するフレームのサブセットから選択された）フレームを復号するのであれば、その選択されたフレームの組が既に保護が解除され、記録された所定のフレームを含んでいる場合、これらの所定のフレームは、スクランブされている情報コンテンツを残して、再び復号することができてしまう。このような問題は、データパッケージ328に、保護が解除されたフォーマットで記録された個々のフレーム又はフレームの範囲の詳細を示す保護解除情報リスト（de-protection information list）を含めることによって回避することができる。保護解除情報リストを用いることにより、認証されたユーザから所定のフレームの視聴が要求された際に、第2の復号は実行されないことを確実にすることができる。保護解除情報リストは、ユーザが保護が解除されたフレームをディスク状記録媒体140に記録する毎に更新される。

【0023】

図4は、RMD130に保存されている代表的な情報の組を示している。情報は、1つ以上のXMLファイルとして、RMD130に保存される。MXLは、マークアップ言語である。広く知られているマークアップ言語であるハイパーテキストマークアップ言語（Hypertext Markup Language：以下、HTMLという。）は、ヘッディング及びタイトルによりドキュメント構造を定義し、及び例えばキャプション及びフォントによってその表現を定義することによってウェブページテキスト及び画像をどのように表示するかに関する指示をウェブブラウザに提供する。一方、XMLは、共通の情報フォーマットを定義する手法並びにこれらのフォーマット及び関連するデータをウェブ及びイントラネット上で共有する手法を提供する。HTMLの用途は、テキストと情報とをどのように表示し、インタラクトさせるかを定義することに制限されるが、XMLでは、アプリケーション開発者は、特定のデータカテゴリに属するように文書内のセクション又は単語をマークするカスタムタグを定義することができ、これにより、ドキュメントのコンテンツに関するコンテキスト情報を与えることができる。例えば、RMD130上のユーザディレクトリについて、タグ<NAME>及び<PUBLIC KEY>を定義することができる。カスタ

ムタグを利用して、情報を特定し及び選択的に抽出することによって、データ処理タスクをXMLドキュメント上で実行することができる。

【0024】

図4に示すように、RMD130に保存された情報は、パスワードデータ、RMD所有者データ410、ユーザディレクトリ420及び一組のデフォルトユーザデータ430を含んでいる。RMD所有者データ410は、認証されたユーザの氏名、そのユーザが所属する会社名、ユーザが任命されたプロジェクト名及び秘密鍵／公開鍵の対を含む。なお、ここでは、例えば認証されたユーザの氏名と、非対称鍵とを最低限保存する必要がある、会社名やプロジェクト名等の他のデータは任意の項目である。ユーザディレクトリ420は、N人のユーザのそれぞれについて、一組のデータを含んでいる。ユーザに割り当てられたアクセス権に応じて、ユーザディレクトリ内の1つ以上のユーザリストに復号された情報へのアクセスに関する情報を含めてもよい。この場合、ユーザディレクトリ内の各エントリには、認証されたユーザの氏名、会社名及びプロジェクト名とともに、そのユーザの公開鍵の値が含まれる。公開鍵は、そのユーザがアクセスすることを許可された情報コンテンツを復号するために必要であるCEKを暗号化するために用いられる。ユーザディレクトリは、認証されたユーザが追加及び／又は削除される毎に定期的に更新されるので、ユーザディレクトリの比較と更新を容易にするために、ユーザディレクトリバージョンIDタグも保存される。この更新は、カメラ110及び／又は再生装置120に保存されているユーザディレクトリのローカルなコピーと、RMD130に保存されているユーザディレクトリの外部のコピーとを比較し、ローカルの又は外部のユーザディレクトリが最近更新されているか否かを判定し、一方が更新されている場合、最近更新されていない方のユーザディレクトリのユーザ識別情報、公開鍵、バージョンIDタグを更新することによって実行される。

10

20

【0025】

デフォルトユーザデータ430の組は、D人のデフォルトユーザそれぞれの氏名と関連する公開鍵とを含む。特定のRMD130の所有者については、デフォルトユーザは何人いてもよく、又はデフォルトユーザが一人もいなくてもよい。デフォルトユーザは、所定の組の情報コンテンツの全てに対するアクセス権を有している（図11Bを用いて後に説明する）。如何なるユーザをデフォルトユーザとして選択してもよい。デフォルトユーザデータ430の組は、RMD所有者に固有のデフォルトユーザのリストを含んでおり、例えば、RMD所有者のマネージャ又はスーパーバイザをRMD所有者のデフォルトユーザとしてリストに登録してもよい。管理者は、どのユーザをデフォルトユーザ状態に割り当てるかを決定する権限を有している。情報コンテンツが作成されると、その情報コンテンツに関連する全てのCEKの組は、常にデフォルトのユーザの公開鍵を用いて暗号化され、記録媒体に記録され、これにより、デフォルトユーザによる全てのコンテンツへのアクセスが保証される。復号された情報コンテンツへのアクセスがデフォルトユーザに保証されるので、デフォルトユーザは、RMDの不注意による紛失に対するセーフガードを提供する。

30

【0026】

RMD所有者には、パスワードデータが関連付けられ、パスワードデータは、CEKの符号化における安全性の追加的なレベルとして用いてもよく、例えば、CEKを非対称的に暗号化する前にパスワードに結合してもよい。この特定の実施例では、ユーザは、それらのRMD130上のパスワードデータに保存されているパスワードに対応するパスワードを用いてシステムにログインしなければならない。図4の実施例では、ユーザディレクトリはRMD130に保存されるが、他の実施例では、カメラ110又は再生装置120が備える固定メモリ（すなわち、リムーバブルではないメモリ）にユーザディレクトリ全体又は少なくともユーザディレクトリの公開鍵のリストを保存する。ユーザディレクトリの公開鍵がカメラ110又は再生装置120の固定メモリに保存される場合、ユーザ又はユーザグループの秘密鍵を保存するRMDは、そのRMDと、カメラ110又は再生装置120に保存されている各公開鍵とを関連付ける識別データを保存できる。更なる他の実

40

50

施例として、記録／再生装置とRMDの両方にユーザディレクトリのコピーを保存してもよい。

【0027】

ここでRMDを用いず、秘密鍵が機器内のメモリに保存される実施例について説明する。この実施例では、5個のリモートカメラと、制作設備（production facility）とを用いるとする。この場合、制作設備機器の全てが共通の公開鍵／秘密鍵の対を共有し、共通の秘密鍵は、制作設備機器のそれぞれが備える固定メモリ内に保存されている。5個のカメラのそれぞれは、それぞれの公開鍵／秘密鍵の組（各カメラには、異なる鍵の組が関連付けられている。）を保存する固定アクセス制御メモリ装置を備える。この実施例では、各カメラが「ユーザ」であるとみなされる。撮影されたデータコンテンツは、共通の公開鍵と、データコンテンツを撮影するために用いられているカメラの公開鍵の両方に基づいて暗号化される。これにより、「フィールド」すなわち撮影が行われる場所では、撮影されたデータコンテンツにアクセスすることができるが、制作設備にコンテンツを送信する際には、認証されていないアクセスからコンテンツを保護することができる。制作設備においては、共通の秘密鍵を用いて、データコンテンツにアクセスすることができ、これを編集することができる。

10

【0028】

図5は、本発明に基づく第1の暗号化方式を図式的に示している。この方式では、情報コンテンツは、ステージ510において、1つ以上のコンテンツ暗号化鍵520を用いて対称的に暗号化される。対称的に暗号化された情報コンテンツは、ディスク状記録媒体140に記録される。ステージ530では、コンテンツ暗号化鍵520は、複数のユーザのそれぞれに対応する複数の公開鍵540のそれぞれを用いて非対称的に暗号化される。公開鍵540は、RMD130のユーザディレクトリ420から読み出される。非対称暗号化ステージ530の出力は、一組の暗号化されたコンテンツ暗号化鍵550である。各ユーザは、ユーザディレクトリ420からのそれぞれの公開鍵540に関連付けられているので、各ユーザについて、暗号化されたコンテンツ暗号化鍵550のバージョンがそれぞれ1つある。暗号化されたコンテンツ暗号化鍵550は、対称的に暗号化された情報とともに、ディスク状記録媒体140に記録される。

20

【0029】

図6は、図5に示す暗号化方式に対応する第1の復号方式を図式的に示している。復号の最初のステージでは、ディスク状記録媒体140から暗号化されたコンテンツ暗号化鍵550（図5参照）を読み出す。RMD130の所有者に関連する秘密鍵620は、RMD所有者データ410から読み出され、ステージ610において、使用可能な秘密鍵に対応する公開鍵を用いて暗号化された暗号化されたコンテンツ暗号化鍵550のバージョンが非対称的に復号される。非対称復号ステージ610の出力は、RMD所有者のアクセス許可に適するコンテンツ暗号化／復号鍵630の組である。これらのコンテンツ暗号化鍵630は、ディスク状記録媒体140から読み出された暗号化されたコンテンツの少なくとも一部に対する対称復号のために用いられる。

30

【0030】

図7A～図7Dは、3人の異なるユーザに対する選択的なアクセス許可の具体例を示している。図7Aは、ディスク状記録媒体140に保存された情報コンテンツを表す8個の画像フレームを表している。8個の画像フレームのそれぞれは、暗号化されて、可視ウォーターマークが付されている（ここでは、影付きのフレームで示している）。図7Bは、コンテンツ所有者のアクセス許可を示しており、ここでは、全てのフレームが影付きではなく、これは、所有者が、全ての画像フレームの復号されたコンテンツを見ることが許可されていることを示している。図7Cは、コンテンツ保有者が個人Bに与えた許可を表している。「W」のマークが付されたフレーム（フレーム4、5）は、復号されているがウォーターマークは付されたままであるフレームを示し、影付きではないフレーム1、2、3、6は、復号され、ウォーターマークも除去されたフレームを示している。図7Dは、個人Bが個人Cに与えた許可のサブセットを示している。個人Bは、自らが許可されていないフ

40

50

フレーム7、8については、許可を与えることができないことは明らかである。個人Cには、フレーム2、3に対するフルアクセスと、復号されているがウォーターマークが付されたままであるフレーム4、5に対するアクセスが許可されている。但し、個人Bは、個人Cに対し、フレーム1、6へのアクセスを許可していない。アクセス許可は、ユーザがそのユーザの公開鍵を用いてアクセスすることができるコンテンツ暗号鍵のサブセットによって決定されるため、アクセス許可は、事実上、ディスク状記録媒体140に保存されていると言える。また、個人のユーザではなく、カメラマンのチーム又は編集者のグループ等のようなユーザグループに対してアクセス許可を割り当ててもよい。所定のフレームのサブセットへのアクセスは、暗号化技術によって実現することができ、この構成では、階層的バイナリツリー暗号化法(hierarchical binary tree cryptography scheme)を用いる。

10

【0031】

図8は、復号された情報コンテンツの一部に選択的にアクセスするための本発明に基づく階層的暗号化法を説明する図である。図8に示すように、暗号化方式は、複数のL個の階層レベルを有するバイナリツリーとして表すことができる。この具体例では、4つの階層レベルL0、L1、L2、L3を示している。レベルL3における8つのノードは、図7Dに示す8個のピクチャフレームに対応している。ルートノードであるL0を除くレベルLj(j=1, 2, 3)の各ノードは、上位の階層レベルL(j-1)のノードへの単一のブランチと、下位の階層レベル(L+1)の各ノードへの2つのブランチとを有し、各階層レベルは、2j個のノードを含んでいる。

20

【0032】

図8に示すバイナリツリーの各ノードには、親へのブランチに基づくラベルが付され、すなわち、左側のブランチには0が、右側のブランチには1が付されている。各ノードは、ルートからそのノードまでを辿るブランチラベルのシーケンスによって定義された2jビットのコードによって識別される。カメラ110内の暗号化エンジン220は、レベルL0から暗号化処理を開始する。レベルL0では、周知の手法により、鍵及び初期化ベクトルを含む暗号化コードが生成される。2つのL1暗号化コードは、L0暗号化コードに基づいて生成され、それぞれが個々の鍵及び初期化ベクトルを含む。レベルL2における暗号化コード00及び暗号化コード01は、レベルL1の親ノード0に基づいて生成される。同様に、レベルL2における暗号化コード10及び暗号化コード11は、レベルL1

30

【0033】

ここで、階層レベルL3において、(図7Dにおける個人Cのみに対する)フレーム2～5のみの選択的なアクセス許可をどのようにして実現するかを説明する。バイナリツリー技術では、暗号コードの全てをディスク状記録媒体に記録するのではなく、許可されたデータの一部の復号を行うために十分な復号データを提供しながら、ユーザに提供すべき復号コードの数を削減できる。この実施例では、フレーム1～8のうち、フレーム2～5のみが復号される。フレーム2を復号し、フレーム1を復号しなくてもよい場合は、ノード001のコードK1が必要である。フレーム3及びフレーム4を復号するためには、ノード01のコードK2が必要である。また、フレーム5を復号し、フレーム6を復号しなくてもよい場合は、ノード100のコード3が必要である。したがって、フレーム2～5を選択的に復号するためには、3つのノード001、100、01に対応する鍵及び初期化ベクトルが必要となる。包括的に言えば、ビデオシーケンスの特定の部分(フレーム/フィールドのサブセット)の復号に必要なコードの最小の組は、復号すべきビデオシーケンスの部分のみに接続されている(L0を最高のレベルとして)最低の階層レベルにおけるノードを判定することによって導出される。他のコードは、復号を実行するために必要ではない。このように、コンテンツ暗号化鍵の所定の組は、復号すべき情報シーケンスの各部分に関連付けられる。

40

【0034】

50

図7に示す異なるユーザに対するコンテンツのアクセス許可の階層について、図8に示すバイナリツリー暗号化方式とともに説明する。上述のように、コンテンツへの選択的なアクセスは、ユーザによってアクセスできるコンテンツ暗号鍵の適切なサブセットを作成することによって実現できる。ユーザがアクセス権を有するフレームに適切なコンテンツ暗号化鍵の所定の組は、暗号化された形式で、データアクセスパッケージ内の記録媒体に保存される。この暗号化は、ユーザの公開鍵を用いて行われる。各ユーザについて保存された、暗号化されたコンテンツ暗号化鍵のサブセットがあり、各ユーザは、そのユーザのコンテンツ暗号化鍵のサブセットを暗号化した各公開鍵を有している。但し、あるユーザに対して、重複する範囲のフレームに対してアクセスが許可される場合、又はユーザが隣り合うフレームの範囲についてアクセス権を有している場合、バイナリ鍵暗号化法から導出されるコンテンツ暗号化鍵間の関係を利用して、データパッケージ内に保存すべきデータの量を削減することができる。例えば、第1の具体例では、アクセス許可が重複しており、詳しくは、ユーザAがフレーム0～200へのアクセス権を有し、ユーザBがフレーム100～400へのアクセス権を有し、ユーザCは、ユーザAからフレーム150～190へのアクセス権を与えられ及びユーザBからフレーム180～300へのアクセス権を与えられているとする。更に、第2の具体例では、許可されたフレームが隣接しており、詳しくは、ユーザCは、ユーザAからフレーム190～200へのアクセス権を与えられ及びユーザBからフレーム201～210へのアクセス権を与えられているとする。これらの第1及び第2の具体例において、ユーザCの公開鍵によってそれぞれ暗号化されたコンテンツ暗号化鍵の2つの個々の組（ユーザAからユーザCに与えられたアクセス権に関するフレーム範囲に対応し、他方がユーザBからユーザCに与えられたアクセス権に関するフレーム範囲に対応する。）を保存するのではなく、2つの個々の鍵の組を結合することによって形成された、単一の暗号化されたコンテンツの暗号化鍵を保存する。結合された鍵の組は、2つの個々の組ではなく、結果的にアクセス可能なフレームの範囲を考慮して、基準ノード（principle node）のみを含んでいる。2組の鍵を結合することが自明である（trivial）場合もあるが、幾つかの場合、2つの兄弟ノード（sibling nodes）をその親ノードに置き換えることが適切な場合もある。この兄弟ノードを置き換える処理は、基準ノードの核となる組（core set of principal nodes）を導出するために、複数回行う必要がある場合もある。図8に示すようなバイナリツリーの構成では、兄弟の鍵を排他的論理和演算することによって親の鍵を導出することができる。2つの鍵の組を併合することにより、データパッケージのサイズを削減でき、更に、再生ステージにおいて、ユーザの秘密鍵を用いて、コンテンツ暗号化鍵を復元（復号）する際に必要とされる演算量を低減できる。

【0035】

図9は、本発明に基づく第2の暗号化方式を説明する図である。この場合、暗号化処理において、ディスク状記録媒体140から読み出されるユニークな又は準ユニークな読出専用ディスク識別子（ID）を利用する。これにより、認証されていないディスク状記録媒体のコピーに由来するデータの復号を効果的に阻止することができる。ここでは、図5に示す構成と同様、例えば、図8に示すバイナリツリー暗号化方式に基づいて一組のコンテンツ暗号化鍵が生成される。アクセスバンドル910として示すコンテンツ暗号化鍵の組は、ステージ920において、情報コンテンツの暗号化及び／又は可視ウォーターマーク付与に用いられ、暗号化された情報コンテンツは、ディスク状記録媒体140に記録される。なお、ここでは、記号E（暗号化すべきデータ、鍵）は、図9～図13及び図15に示す暗号化処理を表し、記号D（復号すべきデータ、鍵）は、復号処理を表すものとする。ステージ930では、アクセスバンドル910が、ランダムに生成されるセッション鍵 k_a を用いて、対称的に暗号化され、ステージ930の出力は、データ1としてディスク状記録媒体140に記録される。また、ランダムに生成されたセッション鍵 k_a は、結合器940にも供給され、結合器940は、2を法とする加算（すなわち、XOR論理ゲート）によってセッション鍵 k_a をディスクIDに結合し、セッション鍵及びディスクIDの組合せ（session key/ disc ID combination）Cを生成する。他の実施例として、2を

法とする加算以外の演算によってセッション鍵とディスクIDを結合してもよい。ステージ950では、 n 人の予定される受信者の各公開鍵 k_{w1} 、 k_{w2} 、 $k_{w3} \cdots k_{wn}$ を用いて、組合せCが非対称的にエンコードされる。公開鍵 k_{w1} 、 k_{w2} 、 $k_{w3} \cdots k_{wn}$ は、RMD130のユーザディレクトリ420から得られる。非対称的に暗号化された組合せCの複数のバージョンは、データ2として、対称的に暗号化されたコンテンツ暗号化鍵のバンドルと共にディスク状記録媒体140に記録される。

【0036】

図10は、図9に示す第2の暗号化法によって暗号化された情報を復元するための復号処理を説明する図である。復号処理の第1のステージ1010では、ディスク状記録媒体140からデータ2が読み出され、再生装置にインストールされているRMDに対応する受信者の秘密鍵を用いて、エンコードされた組合せCが非対称的に復号される。これにより、組合せCが復元される。次に、ステージ1020において、ディスク状記録媒体140から固有のディスクIDが読み出され、これを用いて、ディスクID及びセッション鍵の組合せのときと逆の処理を行い、セッション鍵 k_a が得られる。ステージ1030において、セッション鍵 k_a を用いてRMD所有者のアクセス許可に適切なコンテンツ暗号化鍵を含むアクセスバンドルが復号される。そして、ステージ1040において、アクセスバンドル鍵を用いて、ユーザに対してアクセスが許可された情報コンテンツの部分が復号される。

【0037】

図11Aは、図9に示すディスクIDを含む他の暗号化処理を説明する図である。ここでは、図9に示す処理と同様、情報コンテンツは、コンテンツ暗号化鍵のアクセスバンドルを用いて対称的に暗号化され、アクセスバンドルは、ランダムに生成されたセッション鍵 k_a を用いて対称的に暗号化され、データ1としてディスク状記録媒体に記録される。但し、この実施例では、セッション鍵 k_a をディスクIDに結合するのではなく、ディスクIDは、ステージ1110において、更なるセッション鍵 k_d を用いて対称的に暗号化され、「実効ディスクID (effective disc ID)」として示されるディスクIDに基づく暗号化鍵（対称鍵）が生成される。セッション鍵 k_a は、ステージ1120において、予定される受信者の各公開鍵 k_{w1} 、 k_{w2} 、 $k_{w3} \cdots k_{wn}$ を用いて非対称的に暗号化され、この非対称暗号化の結果は、ステージ1130において、実効ディスクIDを用いて対称的に暗号化され、データ2としてディスク状記録媒体に記録される。また、更なるセッション鍵 k_d は、ステージ1140において、予定される受信者の各公開鍵 k_{w1} 、 k_{w2} 、 $k_{w3} \cdots k_{wn}$ を用いて非対称的に暗号化され、この暗号化の結果は、データ3としてディスク状記録媒体に記録される。したがって、この場合、ディスク状記録媒体に記録されたアクセスデータパッケージは、CEKの対称的に暗号化されたバンドルと、受信者の公開鍵を用いて非対称的に暗号化された後、実行ディスクIDを用いて対称的に暗号化されたセッション鍵 k_a と、受信者の公開鍵を用いて非対称的に暗号化された第2のセッション鍵 k_d とを含む。

【0038】

図11Bは、ディスク状記録媒体に記録されているコンテンツアクセス制御データの組に含まれるデータアクセスパッケージ1150の具体例を示している。ディスク状記録媒体には、2つ以上のデータアクセスパッケージ1150を記録することができる。各データアクセスパッケージ1150は、データコンテンツの単一の断片 (single piece) (例えば与えられたカメラのオペレータによって撮影された一連のビデオ画像) に関連しており、そのデータコンテンツの断片へのアクセスに関する何らかのレベルが与えられた、認証された全てのユーザ又はユーザグループによって要求される全ての情報をリストアップしている。認証された各ユーザ又はユーザグループは、それぞれの秘密鍵によって利用可能なアクセスレベルに基づいて、コンテンツアクセス制御データと共に記録媒体に記録された、暗号化された情報コンテンツの部分にアクセスすることができる。また、データアクセスパッケージ1150は、データコンテンツの対応する断片について、バイナリツリー (図8参照) のレベルの数をリストアップしている (すなわち、最小数のレベルを用い

て、コンテンツの特定の断片の全体のフレーム範囲がカバーされる)。データアクセスパッケージ1150は、保護が解除されたセクション1152と、媒体識別子鍵セクション1154と、プライマリアクセスセクション1156と、第1のアクセスセクション1160と、第2のアクセスセクション1170とを含む。データアクセスパッケージ1150は、複数のアクセスセクションを含んでいてもよい、各アクセスセクション1160、1170は、ユーザセクション1162と、可視ウォーターマーク(visible watermarking: 以下、VWMという。)ウォッシュバンドルセクション1164と、復号バンドルセクション1166とを含む。

【0039】

保護が解除されたセクション1152は、復号され及び可視ウォーターマークが除去された画像フレームの範囲のリストを示す。これにより、復号処理が同じフレームに2回適用されないことが確実にされる。既に復号したフレームを再び復号すると、画像が歪む。媒体識別子鍵セクション1154は、データアクセスパッケージ1150によって何らかのアクセスが許可される全てのユーザのリストを示す。このリストでは、各ユーザについて、暗号化された媒体識別子セッション鍵 k_d がリストアップされている。媒体識別子セッション鍵 k_d の値は、特定のデータアクセスパッケージに固有である(一方、コンテンツアクセスセッション鍵 k_a は、各アクセスセクション1160、1170毎に異なっている)。各ユーザは、それぞれ自らの秘密鍵を用いて、 k_d を復号することができる。アクセスセクション1160、1170は、それぞれ情報コンテンツの断片のある一定のセクションへのアクセスを許可する情報を提供する。データアクセスパッケージ1150に更なるアクセスセクションを追加することにより、コンテンツの他の部分へのアクセス許可を追加することができる。第1のアクセスセクション1160は、情報コンテンツの全体へのアクセスを特定のユーザグループに提供する「プライマリアクセスセクション」である。このデータアクセスパッケージ1150は、コンテンツがディスク状記録媒体に記録された際に(通常、コンテンツが作成された際に)記録される。プライマリアクセスセクションは、通常、コンテンツの記録/作成時においては、唯一のアクセスセクションである。プライマリアクセスセクションに示される各ユーザは、「デフォルトユーザ」と呼ばれる。デフォルトユーザには、暗号化されたデータコンテンツを記録した(及び作成した場合もある)個人として、データアクセスパッケージ1150が関連する情報コンテンツの断片への同じアクセスレベルが与えられ、すなわち、データパッケージの全体のコンテンツへのアクセス権が与えられる。後に、更なるアクセスセクションをディスク状記録媒体に加えることができ、これにより、データアクセスパッケージ1150にリストとして登録された他の認証されたユーザに対して、コンテンツの全て又は一部へのアクセス権を与えることができる。

【0040】

図11に示す実施例において、対応するアクセスセクションが媒体識別子に関連付けられているか否かを示すフラグを設けてもよい。コンテンツセッション鍵 k_a は、媒体識別子に関連付けるのではなく、そのアクセスセクションにリストとして示されたユーザの公開鍵を用いて単に非対称的に暗号化してもよい。コンテンツセッション鍵 k_a の非対称的に暗号化されたバージョンは、記録媒体に記録される。この場合、媒体識別子セッション鍵 k_d は、復号に必要でなくなる。この暗号化方式は、図13に関して以下に説明するように、「マスタユーザ(master user)」に対して適用される。なお、マスタユーザに対しては、コンテンツの全てへのアクセスを提供する。これは、媒体識別子に関連付けられていないアクセスセクションに関連しているユーザグループの場合には不要である。

【0041】

各アクセスセクションは、ユーザセクション1162、VWMウォッシュバンドルセクション1164及び復号バンドルセクション1166を含む。ユーザセクション1162は、アクセスセクションに関連するコンテンツの断片へのアクセス権を有する各ユーザ又はユーザグループのリストを示す。各ユーザに対して、暗号化されたアクセスセッション鍵 k_a が関連付けられている。ユーザは、(アクセスセクションが媒体識別子に関連付けら

れていない場合) ユーザの秘密鍵のみを用いて、又は(アクセスセッションが媒体識別子に関連付けられている場合) ユーザの秘密鍵と媒体識別子セッション鍵 k_d の両方を用いて、アクセスセッション鍵 k_a を復号することができる。各アクセスセッションについて、異なるコンテンツアクセスセッション鍵 k_a が用いられる。VWMウォッシュバンドルセッション 1164 は、1つ以上のサブセッションを有する。各サブセッションは、サブセッションヘッダの特定のフレーム範囲に関連し、それらのフレームから可視ウォーターマークを除去するために必要な(バイナリツリー暗号化方式からの) 鍵の暗号化されたバージョンを保存する。アクセスセッション 1160 のユーザセッション 1162 のリストに示されるユーザのみがそれらを復号することができるように、VWM鍵は、コンテンツアクセスセッション鍵 k_a を用いて全て暗号化されている。また、復号バンドルセッション 1166 は、それぞれがサブセッションヘッダに示されたフレーム範囲をカバーする1つ以上のサブセッションを有し、これらのフレームを復号するために必要な(バイナリツリー暗号化方式からの) 鍵のリストを含んでいる。この場合、暗号化方式は、可視ウォーターマークではなく、対称又は非対称の暗号化である。ここでも、全ての鍵は、コンテンツアクセスセッション鍵 k_a を用いて暗号化され、したがって、これらは、アクセスセッション 1160 のユーザセッション 1162 のリストに示されているユーザによってのみ復号される。

10

【0042】

図12は、図11Aに示す暗号方式に基づいて暗号化されたデータを復元するための復号処理を示している。まず、ステージ1210において、受信者の秘密鍵 k_{s_i} を用いて、(データ3として) ディスクに記録されている非対称的に暗号化されたバージョンから、更なるセッション鍵 k_d が復号される。次に、ステージ1220において、ステージ1210で復元された更なるセッション鍵 k_d を用いて、ディスクIDから実効ディスクIDが再生される。対称鍵である実効ディスクIDは、非対称的に暗号化された第1のセッション鍵 $E(k_a, k_{w_i})$ を復元するために、ディスク状記録媒体からの数量データ(quantity Data) 2を復号する第1のステージに用いられる。次に、受信者の秘密鍵 k_{s_i} を用いて、次の復号のステージ1240が実行され、ここでは、非対称の暗号化の逆の処理を行うことにより、セッション鍵 k_a が復元される。次に、ステージ1250において、セッション鍵 k_a を用いて、アクセスバンドルCEKが復号される。そして、ステージ1260において、アクセスバンドルCEKを用いて、ディスク状記録媒体に記録されている、対称的に暗号化された及び/又は可視ウォーターマークが付された情報コンテンツが復号される。

20

30

【0043】

図13は、情報コンテンツの全てに関するアクセスを「マスタユーザ」に許可するための暗号化方式を図式的に説明する図である。マスタユーザとは、媒体識別子にかかわらずデータアクセスパッケージ1150(図11B参照)が関連付けられているコンテンツ全体へのアクセス権を有するユーザ又はユーザグループと定義される。したがって、媒体識別子セッション鍵 k_d は、コンテンツの復号には不要である。また、データアクセスパッケージ1150のプライマリアクセスセッション1160にリストとして示されたデフォルトユーザは、全体のコンテンツへのアクセス権を有しているが、デフォルトユーザは、媒体識別子に関連付けてもよく、関連付けなくてもよい。データアクセスパッケージ1150内のデフォルトユーザのマスタユーザのグループには、何人のユーザ又はユーザグループを追加してもよい。この暗号化方式は、図11Aに示す暗号化方式に類似しているが、更なるステージ1310が追加されている点が異なり、このステージ1310においては、セッション鍵 k_a は、マスタ公開鍵 k_{w_master} を用いて非対称的に暗号化され、ディスク状記録媒体140に保存される。マスタ公開鍵 k_{w_master} は、全てのユーザのRMDに保存され、マスタユーザには、記録媒体に記録された情報コンテンツの全体に対するアクセスが許可される。各マスタユーザのそれぞれについて、異なるマスタ公開鍵を設けてもよい。マスタユーザの対応する秘密鍵は、マスタRMDに安全に保存される。マスタRMDを用いることにより、マスタではないRMDが不注意に紛失されて

40

50

も、暗号化されたデータへのアクセス権が失われないようにすることができる。図14のステージ1410に示すように、マスタユーザは、ディスクIDにアクセスすることなく、マスタ秘密鍵 k_{s_master} を含む単一の復号ステップによって、セッション鍵 k_a を復元できる。マスタユーザが、ディスクIDにかかわらず、データアクセスパッケージに関連する全体のコンテンツにアクセスするのを可能にするために、プライマリアクセスセクションのVWMウォッシュバンドルセクション1164及び復号バンドルセクション1166（図11B参照）の両方において、暗号化された鍵へのアクセス権をそれぞれのマスタユーザに与えなくてはならない。マスタユーザの公開鍵を用いてプライマリアクセスセクションのコンテンツアクセス鍵 k_a を直接暗号化し、データアクセスパッケージ内のどこかにこの暗号化された k_a を保存することによって、それぞれのマスタユーザにこのようなアクセスを提供することができる。

10

【0044】

図13の実施例では、セッション鍵 k_a の暗号化においてマスタユーザのディスクIDを用いない。なお、他の構成では、マスタユーザをディスクIDに関連付けてもよい。同様に、ある受信者の組をディスクIDに関連付け、他の受信者の組に対しては、図13におけるマスタユーザの場合と同様に、そのユーザの公開鍵でセッション鍵 k_a を直接暗号化することによって、より自由なアクセス許可を与えてもよい。

【0045】

図15は、図11及び図13に対応する暗号化シーケンスのフローチャートである。ステージ1510において、CEKのアクセスバンドルを用いて、情報コンテンツを暗号化し及び／又はウォーターマークを付与し、暗号化したコンテンツを記録媒体に保存する。この処理に続くステージには、暗号化コンテンツとともにディスクに記録するためのアクセスデータパッケージの作成が含まれる。ランダムに生成された第1のセッション鍵 k_a を用いて、ステージ1520では、アクセスバンドルのCEKを対称的に暗号化し、次に、ステージ1530において、アクセスデータパッケージの一部として、暗号化されたアクセスバンドルを記録媒体に記録する。ステージ1540において、ディスクIDを入手し、ステージ1550において、第2のセッション鍵 k_d を生成し、これを用いて、ディスクIDを対称的に暗号化する。この暗号化の結果は後に、「実効ディスクID」と呼ばれる暗号化鍵として用いられる。暗号化処理は1560に進み、 n 人の各受信者（すなわち、予定される認証ユーザ） $w_1, w_2 \dots w_n$ に対して暗号化シーケンスを実行する。詳しくは、ステージ1570において、ユーザの公開鍵を用いて第2のセッション鍵 k_d を暗号化し、この結果を記録媒体に保存する。ステージ1580では、各受信者について、まず、受信者の公開鍵を用いて、第1のセッション鍵 k_a を非対称的に暗号化し、次に、実効ディスクIDを用いて、非対称の暗号化の出力を対称的に暗号化して記録媒体に保存するといった、2段階の暗号化処理を実行する。図13に示す暗号化方式の場合、フローチャートには、マスタユーザの公開鍵を用いて第1のセッション鍵 k_a を暗号化し、結果をディスクに保存するための更なるステージ1590が追加される。

20

30

【0046】

図16は、図12及び14に対応する復号シーケンスのフローチャートである。復号は個々の受信者毎に行われ、各受信者は、そのユーザのRMD130に保存された秘密鍵を用いて、そのユーザがアクセスを許可された情報コンテンツの部分を復号する。復号処理はステージ1610において開始され、ここで、ユーザの秘密鍵 k_s を用いて、第2のセッション鍵 k_d を復号する。次に、ステージ1620において、第2のセッション鍵 k_d を用いて、（受信者が利用可能であると仮定される）ディスクIDを暗号化することによって実効ディスクIDを生成する。次に、ステージ1630において、実効ディスクIDとユーザの秘密鍵の両方を用いて、第1のセッション鍵 k_a を復号する。ステージ1640においては、第1のセッション鍵 k_a を用いて、CEKのアクセスバンドルを復号するこれにより、ステージ1650において、復号及び／又は可視ウォーターマークの除去が可能になる。図14の復号構成の場合、フローチャートには、マスタユーザの秘密鍵を用いて、第1のセッション鍵 k_a を復号するステージ1660、第1のセッション鍵 k_a を用

40

50

いることでアクセスバンドルを復号するステージ1670、復号されたアクセスバンドルを用いて、情報コンテンツを復号する及び／又は可視ウォーターマークを除去するステージ1680といった更なるステージが追加される。

【0047】

図17は、ディスクがコピーされる際に行われるアクセス許可を図式的に説明する図である。コピーに対して付与されるアクセス許可は、用いられている特定の暗号化方式に依存する。ここで、元のディスク1710がディスクID「A」を有しているとする。この元のディスクの直接的なバイナリコピー（すなわち、ビット毎のコピー）が作成された場合、ディスクIDを用いた暗号化処理を行ったとすると、ディスクID「B」を有する不正コピー1720のコンテンツには、如何なるユーザもアクセスすることができない。暗号化処理において、マスタユーザをディスクIDに関連付けなかったと仮定すると（すなわち、第1のセッション鍵 k_a がマスタ受信者の公開鍵だけを用いて暗号化されたと仮定すると）、この場合、マスタユーザは、コンテンツにアクセスすることができる。

10

【0048】

ディスクID「C」を有するディスク1730は、ディスクAに保存されたアクセスデータパッケージにおいて、第1のセッション鍵 k_a をディスクIDに結合し、この結果を受信者の公開鍵を用いて非対称的に暗号化することによって、暗号化とディスクIDとが結びつけられている場合における、ディスクAの正当なコピーを表している。これは、図9に示す暗号化処理に対応している。この場合、ID「C」を有するディスク1730を用いてユーザによって作成された正当なコピーは、コピーを作成した認証されたユーザだけがアクセス可能な情報コンテンツを含む。但し、この情報コンテンツには、元のディスク1710に記録された情報コンテンツに対するアクセス権を有する認証されたユーザは、アクセスできない。コピーの作成者は、元のアクセスデータパッケージで指定されている情報コンテンツの部分のみに対するアクセス権を有する。また、この場合も、暗号化処理においてマスタユーザとディスクIDとを関連付けていない場合、マスタユーザは、正当なコピー1730上の情報コンテンツへのアクセス権のみを有する。

20

【0049】

ディスクID「D」を有するディスク1740は、ディスクAに保存されたアクセスデータパッケージにおいて、第1のセッション鍵 k_a を非対称的に暗号化し、次に、実効ディスクIDによって第1のセッション鍵を対照的に暗号化することにより、暗号化とディスクIDとが結びつけられている場合におけるディスクAの正当なコピーを表している。これは、図11及び図13に示す暗号化処理に対応している。この暗号化方式は、正当なコピーが認証されたユーザによって作成された場合、元のユーザアクセス許可の組が引き継がれるという点で図9に示す暗号化方式より優れている。したがって、元のディスクAについて、情報コンテンツへのアクセス権を有する全てのユーザは、正当なコピーであるディスクDに記録された情報に対して同じアクセスレベルを有する。また、マスタユーザは、マスタユーザがディスクIDに関連付けられているか否かにかかわらず正当なコピー1740における情報コンテンツへのアクセス権を有している。

30

【0050】

更に、データをディスクEに保存する前に、ディスクIDへの依存性を取り除いて、元のディスク1710の正当なコピーを作成したとする。この場合、元のディスク1710のアクセス許可は、正当なコピー1750及びその正当なコピー1750の不正なバイナリコピー1760の両方に引き継がれる。また、この場合も、マスタユーザは、正当なコピー1750及び不正なバイナリコピー1760の両方に対してアクセス権を有する。

40

【0051】

図11及び図13に示す暗号化方式には、元のディスクの正当なコピーが作成された場合、アクセス許可をコピーにも引き継ぎ、元のディスクの不正なバイナリコピーにおいては、情報コンテンツへのアクセスを拒否することができるといった、明らかな利点がある。

【0052】

50

図18は、マジックゲートメモリスティック及びマジックゲートメモリスティック装置を図式的に示している。マジックゲートメモリスティックは、本発明に基づくユーザディレクトリと秘密鍵の安全なストレージに用いることができるRMDの1つの具体例である。マジックゲートシステムは、マジックゲート装置1810とマジックゲートメモリスティック1860とを備える。マジックゲート装置は、データ処理を実行する中央演算処理装置（central processing unit：以下、CPUという。）1830と、暗号化回路1842を含むマジックゲートモジュール1840と、メモリスティック1860とマジックゲート装置1850との接続を確立するためのインタフェース（IF）1850とを備える。メモリスティック1860は、データを保存するためのフラッシュメモリモジュール1880と、オフボード暗号化回路1872を含むマジックゲート（MG）モジュール1870とを備える。機器の暗号化回路1842は、MGセッション鍵 SeK_{MG} 及びMGコンテンツ鍵 CK_{MG} といった2つの関連する暗号鍵を有する。一方、メモリスティックのオフボード暗号化回路1870は、MGセッション鍵 SeK_{MG} とMGストレージ鍵 KST_{MG} を使用する。

【0053】

マジックゲート装置1810は、MGコンテンツ鍵 CK_{MG} を用いて情報コンテンツを暗号化／復号する。MGセッション鍵 SeK_{MG} は、マジックゲート装置1810とメモリスティック1860の両方によって用いられる。MGセッション鍵 SeK_{MG} は、各認証レベルにおいて生成され、一時的なデータの交換に利用される。メモリスティックは、MGストレージ鍵 KST_{MG} を用いて、MGコンテンツ鍵 CK_{MG} を暗号化／復号する。

【0054】

マジックゲートシステムは、メモリスティック1860とマジックゲート装置1810の間で、メモリスティック1860及びマジックゲート装置1810の双方がコピー保護をサポートし、暗号化／復号が認証されたメモリスティック1860を用いてマジックゲート装置1810において実行されることを確実にする。マジックゲートシステムは、情報コンテンツのためだけではなく、認証処理においても暗号化／復号（及び関連付けられた鍵）を用いる。メモリスティック1860がインタフェースを介してマジックゲート装置1810との接続を確立し、この後に記録を行い、コンテンツの再生を可能とする処理のそれぞれにおいて、毎回、最初のステップとして認証を行う必要がある。

【0055】

図19は、マジックゲートシステムにおける記録処理を説明するフローチャートである。記録処理はステージ1910において開始され、ここで、MG装置に供給された情報コンテンツは、暗号化回路1842において、MGコンテンツ鍵 CK_{MG} を用いて暗号化される。次に、ステージ1920において、MGセッション鍵 SeK_{MG} を用いてMGコンテンツ鍵 CK_{MG} を暗号化し、インタフェース1850を介して、メモリスティック1860に供給する。セッション鍵 SeK_{MG} を用いる暗号化により、メモリスティック1860とマジックゲート装置1810の間で安全なリンクが実現する。ステージ1930において、メモリスティック1860は、確立されたMGセッション鍵 SeK_{MG} を用いてMGコンテンツ鍵 CK_{MG} を復号し、次に、ステージ1940において、メモリスティック1860は、MGストレージ鍵 KST_{MG} を用いて CK_{MG} を暗号化した後、暗号化されたコンテンツ鍵をマジックゲート装置1810に渡す。そして、ステージ1950において、マジックゲート装置1810は、メモリスティック1860のフラッシュメモリ1880に暗号化されたコンテンツと暗号化されたコンテンツ鍵を書き込む。

【0056】

図20は、マジックゲートシステムにおける再生処理を説明するである。再生処理は、ステージ2010から開始され、ここで、MGマジックゲート装置1810は、メモリスティック1860から暗号化された情報コンテンツと暗号化されたコンテンツ鍵とを読み出し、データが不正コピーされているものではないことを確認する。次に、ステージ2020において、MGデバイス1860は、暗号化されたコンテンツ鍵をメモリスティッ

ク1860に供給する。次に、再生処理は、ステージ2030に進み、ここで、メモリースティックは、MGストレージ鍵 KST_{MG} を用いてコンテンツ鍵 CK_{MG} を復号する。ステージ2040において、メモリースティック1860は、MGセッション鍵 SeK_{MG} を用いてコンテンツ鍵 CK_{MG} を暗号化し、この結果をMGマジックゲート装置1810に供給する。そして、ステージ2050において、MGマジックゲート装置1810は、MGセッション鍵 SeK_{MG} を用いてMGコンテンツ鍵 CK_{MG} を復号し、続いてコンテンツを復号する。

【0057】

図21は、本発明に基づき、新たに認証されたユーザをどのようにシステムに追加し、及び、認証の期限が切れたユーザをどのようにシステムから削除するかを説明するフローチャートである。処理の最初のステージ2110は、管理用のステージであり、ここでは、認証された新たなユーザに対し、その認証されたユーザに固有の公開鍵／秘密鍵の対が保存された個人用のRMDが供給される。また、新たに割り当てられたRMDは、そこに保存されたユーザディレクトリの新たに更新されたバージョンを含んでいる。更新されたユーザディレクトリは、この新たに認証されたユーザの公開鍵を含んでいる。また、この実施例では、認証の期限が切れたユーザは、最も最近に更新されるユーザディレクトリから削除される。次に、ステージ2120において、新しいユーザは、新しいユーザは、そのユーザに新たに割り当てられたRMDを互換性がある記録装置に挿入し、ここで、RMD及び記録装置が互いに認証を確認する。

【0058】

次に、ステージ2130において、記録装置のメモリにローカルに保存されているユーザディレクトリのコピーと、RMDに保存されているユーザディレクトリの外部のバージョンとを比較する。各ユーザディレクトリは、バージョン識別タグを有し、これにより、ユーザディレクトリのローカルのバージョンと、外部のバージョンとのどちらかがより最近に更新されているかを判定することができる。この実施例では、簡単なタイムスタンプタグを使用している。このステージでは、認証された新たなユーザがシステムに追加され、期限切れのユーザがシステムから削除されているため、RMDユーザディレクトリは、ローカルのユーザディレクトリより最近に更新されている。これに応じて、ステージ2140では、認証された新たなユーザの公開鍵を加え、期限切れのユーザに関連している公開鍵を除去するように、記録装置のローカルのユーザディレクトリを更新する。更に、ユーザディレクトリを更新するステージにおいて、デフォルトユーザの組430を検証し、これらのデフォルトユーザが新たなユーザディレクトリにおいて、有効なデフォルトユーザとしてリストに残っているかを確かめる必要がある。次に、ステージ2150において、記録装置において記録処理を実行する。例えば、記録装置がカメラである場合、そのRMDがカメラにインストールされている新たに認証されたユーザによって新しい場面が撮影される。コンテンツ鍵を暗号化するためのユーザの公開鍵の入手には、ユーザディレクトリの外部のバージョンとローカルのバージョンのどちらを用いてもよい。この時点では、更新処理が完了しているので、ユーザディレクトリの2つのバージョンは、現在、同一のものである。ステージ2150における記録処理の間に、記録媒体に保存されたアクセスデータパッケージは、新たに認証されたユーザの公開鍵を用いて暗号化を行い、これにより、新たに認証されたユーザは、記録された情報コンテンツの少なくとも一部へのアクセスが許可される。通常、カメラマンは、新たに撮影した情報コンテンツの全体に対するアクセス権を有する。新たなマテリアルが撮影されると、コンテンツアクセス許可の詳細を示す新たなアクセスデータパッケージが記録媒体に記録される。既存のユーザが、新たなユーザに対して、既存の情報コンテンツに関するアクセス許可を与える場合、その既存の情報コンテンツに関連するアクセスデータパッケージにその新たなユーザを加えることができる。これは、新しいユーザの公開鍵を用いて、新たなユーザにアクセス権が与えられる既存のコンテンツに関連するCEKのサブセットを暗号化し、これらの暗号化されたCEKを既存のアクセスデータパッケージに追加することによって実現される。ステージ2160において、新たに認証されたユーザは、記録セッションを終了させ、記録装置か

10

20

30

40

50

ら自らのRMDを取り出す。

【0059】

次に、ステージ2170では、既存のユーザが、新たな記録操作を開始するために自らのRMDを記録装置に挿入する。ステージ2180においては、ユーザディレクトリのローカル及び外部のバージョンが比較され、一方のバージョンがより最近に更新されているか否かが判定される。この時点では、ステージ2140において、新たに認証されたユーザが追加され、及び期限切れのユーザが削除されているユーザディレクトリのローカルのバージョンが、外部の、すなわち既存のユーザのRMDに記録されているユーザディレクトリより最近に更新されている。ここでも、デフォルトユーザの組430の検証が行われる。そして、ステージ2190において、既存のユーザのRMDのユーザディレクトリが更新され、新たに認証されたユーザが追加され、期限切れのユーザが削除される。このように、ユーザディレクトリに関する変更は、接続が確立される毎に、RMD及び互換機器のユーザディレクトリのバージョンを比較することによって伝播する。上述の実施例では、この比較は、機器にRMDを挿入した際、最初に実行されるが、この比較は、RMDと機器の間の通信シーケンスの他の段階で行ってもよい。

10

【0060】

なお、更新されたユーザディレクトリの伝播には、いくらかの時間がかかる場合がある。ここで、コンテンツの作成時に、新しいユーザがユーザディレクトリに追加されていない場合その新しいユーザに対し、記録ステージ後において、その記録されたデータに対するフルアクセスを許可してもよい。同様に、ユーザディレクトリの更新によって期限切れのユーザのアクセス権を取り消すには、一定の時間がかかるが、期限切れのユーザに対し、認証が取り消された時点で（例えば、退職時に）そのRMDを返却することを要求してもよい。

20

【0061】

更新処理におけるユーザディレクトリに対する不正行為を防ぐために、ユーザディレクトリの与えられたバージョンの真正性を確かめることができることは重要である。この目的で、デジタル署名を用いることができる。一実施例においては、デジタル署名は、バージョン識別タグを含むユーザディレクトリの全体のコンテンツに基づいていてもよい。これは、例えば、バージョン識別に用いられる日付タグの変更等、ユーザディレクトリに対する如何なる無許可の改竄はそのユーザディレクトリのデジタル署名によって検証されないもので、ユーザディレクトリを平文で保存できることを意味する。

30

【0062】

図22は、デジタル署名に関連するメッセージ署名及び検証手続を図式的に説明する図である。デジタル署名を含むユーザディレクトリの署名は、ステージ2210において、ユーザディレクトリの平文バージョンPから開始される。次に、ステージ2220において、平文Pのハッシュが生成される。ハッシュは、平文データから一義的に導出される短い固定長ビット列である。次に、ステージ2230において、デジタル署名の作成者が自らの秘密鍵を用いて、ハッシュ化された平文を暗号化し、ハッシュ化され、暗号化された平文、すなわち署名Qを生成する。そして、ステージ2240において、平文自体に、ハッシュ化され、暗号化された平文、すなわち署名Qを添付することによって、デジタル署名の処理が終了する。署名検証処理は、ステージ2250において開始され、ここでは、例えば、記録装置に平文Pと署名Qとが供給される。ステージ2260では、受信者は、署名の作成者の公開鍵を用いて、署名Qを復号し、数値h2 (quantity h2) を生成する。ここでは、ユーザディレクトリが完全且つ正しいことのみではなく、ユーザディレクトリのソースが、そのユーザディレクトリの更新を許可されていることを確かめる必要がある。具体的には、ユーザディレクトリに添付されたデジタル署名が、信頼できるパーティから発行されたものであることを確かめる必要がある。このため、ユーザディレクトリを検証する公開鍵（図22に示す発行者の公開鍵に対応する）を各機器に保存する。ユーザディレクトリは、検証を通過するために、対応する秘密鍵を用いて署名されている必要がある。ステージ2270では、平文のハッシュが生成され、出力値h1が出力される。そ

40

50

して、ステージ 2 2 8 0 では、 $h1 = h2$ であることを確認することによって、デジタル署名が検証される。比較されているバージョンより最近のものであると判定されたユーザディレクトリのデジタル署名が検証を通過しなかった場合、図 2 1 のフローチャートに示す更新のステージ 2 1 4 0 は実行されない。本発明に基づく手法では、認証されたユーザに対し、ストレージ媒体内の情報コンテンツへのアクセスを選択的に許可することができ、例えば、ユーザには、ビデオシーケンス内のフレームのあるサブセットのみに関するアクセス権を与えることができる。選択的なアクセスは、認証されたユーザにコンテンツ暗号化鍵のサブセットのみの復号を許可し、これにより、復号されたコンテンツ鍵を用いて復号できる画像フレームのみへのアクセスを可能とすることによって実現される。これを
10
実現するバイナリツリー暗号化方式については、図 8 を用いて上述した通りである。既知の暗号化方式では、情報コンテンツは、全体として暗号化又は復号され、したがって、復号されたデータストリームの処理は、単純である。一方、本発明に基づく選択的なアクセス方式では、再生されたデータストリームは、暗号化されたままのビデオフレーム及び復号された又は部分的に復号された（例えば、可視ウォーターマークが付された）フレームの両方を含んでいることが多い。そこで、再生装置は、連続したビデオフレームにおいて、そのビデオフレームが暗号化されたまま（所定のユーザによってはアクセス不可能）であるか、アクセスバンドルの利用可能な鍵を用いて復号されているかを区別できることが望ましい。更に、フレーム境界が暗号化されたデータストリームにおいて、認識可能であるならば、個別の配信のために、暗号化されたデータの個々のサブセットを分離することが可能となる。暗号化されたコンテンツは、特定のデータ形式に従っていることが多い。こ
20
こでは、フレーム境界を特定するのに役立つデータの部分をデータの「フォーマット識別部分（format identifying portion）」と呼び、残りのデータを「ペイロードデータ部分（payload data portion）」と呼ぶ。例えば、MPEG-2 フォーマットのビデオストリームデータについて検討する。MPEG-2 では、ビデオストリームは、ヘッダと、画像要素（画素）を復号して表示するために必要な情報を提供するデータとの階層的構造として組織化される。ビデオデータは、グループオブピクチャ（groups of pictures：GOP）を構成する所定の異なる種類のフレーム（I フレーム、P フレーム、B フレーム）を有するフレームを含む。各ヘッダは、3 バイトの開始コード接頭辞プレフィックスと、これに続く 1 バイトの開始コード ID からなる 4 バイトのコードを含む。開始コードプレフィックスは、2 3 個の（又はこれ以上の）バイナリ値 0 と、これに続く 1 つのバイナリ値 1
30
を含む。開始コード ID は、下記の表 1 に示すように、後に続くデータの種別を示す。ビデオストリームの様々な箇所において、幾つかの「拡張」を行うことも認められている。拡張は、拡張開始コードと、これに続く、所定の拡張 ID の 1 つによって表される。下記の表 2 は、所定の拡張 ID のリストを示している。

【0063】

【表 1】

開始コードタイプ	開始コード ID (8 ビット)
Picture_start_code	00
Slice_start_code	01 to AF
User_data_start_code	B2
Sequence_header_cod	B3
Sequence_error_code	B4
Extension_start_code	B5
Sequence_end_code	B7
Group_start_code	B8
予備	B0, B1, B6

【0064】

10

20

30

40

50

【表 2】

Extension_ID (4ビット)	名称
1	シーケンス拡張 Sequence extension
2	シーケンス表示拡張 Sequence display extension
3	Quant Matrix Extension
4	著作権拡張 Copyright Extension
5	シーケンススケーラブル拡張 Sequence Scalable Extension
7	ピクチャ表示拡張 Picture Display Extension
8	ピクチャ符号化拡張 Picture Coding Extension
9	ピクチャ空間スケーラブル拡張 Picture Spatial Scalable Extension
A	ピクチャ時間スケーラブル拡張 Picture Temporal Scalable Extension
0, 6, B to F	予備

10

【0065】

MPEG-2 ビデオストリームにおいて、フレーム境界を特定するために、暗号化されたデータストリームにおいて、フレーム境界が識別されるように、データを選択的に暗号化する。図 23 は、ビデオストリームの所定の部分に対する選択的な暗号化を説明する図である。データストリームは、「開始コード」2310、2312、2316、2318 と、これに続く、関連する可変長のヘッダとからなる複数の 4 バイトのヘッダ ID を含む。この実施例における 4 バイトの開始コードは 16 進ストリングであるが、これは、10 進ストリング又は 8 進ストリングであってもよい。MPEG では、開始コードストリング長は、4 バイト（すなわち、バイト整列された 32 バイト）でなくてはならない。

20

【0066】

ヘッダ ID 内の 1 バイトの開始コード ID は、表 1 に示すように、ヘッダの種類を特定する。ピクチャペイロードデータ部分 2360、2362 は、それぞれスライスヘッダ 2350、2352 の直後に続いている。各画像フレームは、複数のスライスを含む。ピクチャヘッダ 2320 とピクチャ拡張 2330 は、フレーム境界に関する情報を提供する。したがって、暗号化すべきビデオストリームの部分にはピクチャヘッダ 2320 とピクチャ拡張 2330 とは含まれないが、残りのヘッダ及びピクチャデータは、暗号化に割り当てられる。暗号化エンジンは、ピクチャヘッダ 2320 に先行するヘッダ ID 2310 を検出し、ヘッダ ID に続く所定数のデータビットを暗号化しない。すなわち、この特定の実施例では、ヘッダに続く所定数のデータビットを識別し、これらの識別されたデータビットに対しては暗号化を行わない。なお、他の実施例では、処理の時点で、例えば、ヘッダを解析してそのヘッダの正確な長さを判定することにより、ヘッダに続くデータビットの数を判定する。同様に、ピクチャ拡張 2330 に先行するヘッダ ID 2312 が暗号化エンジンによって検出された場合、暗号化処理では、そのヘッダに続く所定数のバイトを暗号化しない。ピクチャヘッダ 2320 とピクチャ拡張 2330 とは、可変長であり、所定数のビットはスキップされる（暗号化されない）ので、データストリームの暗号化されていない部分は、例えば、ピクチャデータの最初のスライス等、ピクチャデータ内に拡張することが可能である。データの部分を特定するフォーマット（この具体例では、フレーム境界データ）は、暗号化されていないピクチャヘッダ及びピクチャ拡張から導出されるため、ストリームにおける残りのデータ、すなわち、ヘッダ 2340、スライスヘッダ 2350、2352 及びピクチャペイロードデータ部 2360、2362 は、暗号化してもよい。フレーム境界データ以外のデータは、ペイロードデータとして分類できる。但し、関連するヘッダ ID 2314、2316、2318 は、いずれも暗号化されない。所定のヘッダ ID の 1 つに対応するビットシーケンスが誤って生成されないことを確実にするように行われる。このような誤生成は、フレーム境界の識別に悪影響を与え、すなわち、

30

40

50

デコーダにおいて、誤った境界が認識される虞があるため、避けなくてはならない。ヘッダIDシーケンスの生成を回避する暗号化ストリームは英国特許出願番号0128887.7号（公開番号GB2382753号）「全ての暗号化されたデータ値が正当な範囲となることを確実にするビデオデータ暗号化方法（Encrypting video data ensuring that all encrypted data values lie in a legal range）」に開示されている。データストリームの選択的な暗号化により、MPEG-2ビデオデコーダ/プレーヤーは、フレーム境界エラーを生じさせることなく、データストリームの暗号化され及び復号されたサブセクションの両方を再生することができる。

【0067】

選択的に暗号化されたデータストリームは、入力データのフォーマット識別部分（例えば、フレーム境界データ）と、暗号化されたペイロード部分とを弁別する弁別器（discriminator）を備える復号装置を用いて復号される。復号装置は、弁別器の出力に応じて、入力データを処理し、フォーマット識別部分は復号せず、暗号化されたペイロード部分の少なくとも一部を復号する。

【0068】

以上、主にデータ暗号化及び可視ウォーターマーク法と関連して、本発明に基づくデジタル権利管理システムについて説明したが、本発明は、脆弱ウォーターマーク法（fragile watermarking）、ユニークマテリアルID（Unique Material ID：UMID）ウォーターマーク法及びフィンガプリント法等のその他の画像処理形式にも同様に適用できる。

【0069】

上述の手法は、少なくとも部分的に、記録／再生装置内の又はRMD内のデータプロセッサ上で実行されるコンピュータプログラムによって実現でき、例えば、暗号化及び復号処理は、コンピュータプログラムによって実現してもよい。このソフトウェアは、CD-ROM又はフロッピディスク等のストレージ媒体によって提供してもよい。これに代えて、コンピュータネットワークを介して装置にソフトウェアを供給してもよい（例えば、インターネットからダウンロードしてもよい）。

【0070】

図24は、記録／再生装置の概略を示している。この記録／再生装置は、記録のための信号を受け取り、この信号を処理し、記録に適するフォーマットにフォーマット化する記録ロジック2510と、ロータリヘッド（ヘリカルスキャン方式）構成体等の記録ヘッド構成体2520と、磁気テープ媒体等の線形アクセス記録媒体2530と、ヘッド構成体2520から信号を受け取り、この信号を処理し、出力信号にフォーマット化する再生ロジック2540とを備える。

【0071】

以下、この記録／再生装置を用いて、暗号化されたコンテンツを処理する手法について説明する。

【0072】

上述したアクセス制御装置では、圧縮されたオーディオ／映像信号は、コンテンツ鍵を用いて暗号化される。暗号化は、MPGデータストリーム内の現在のヘッダ情報が無くならないような手法で行われる。これにより、暗号化されたデータストリームにおいて、データの各フレームを特定できる。この具体例では、この記録／再生装置において、同様の構成を用いているが、もちろん、これに代えて他の構成を用いてもよい。

【0073】

ここで、上述の構成においては、（例えば）暗号化されたコンテンツ鍵を含む「アクセスパッケージ」がセットアップされる。このアクセスパッケージは、ユーザが記録媒体からの再生時にビデオコンテンツの復号を望む場合に必要となる。

【0074】

暗号化されたビデオコンテンツとアクセスパッケージは、例えばディスク等のランダムアクセスストレージ媒体に記録するのではなく、図24に示すような線形アクセス記録媒体2530にこれらのアイテムを記録してもよい。以下では、これを実現するための様々

な手法について説明する。

【0075】

図25、図26及び図27は、それぞれ線形アクセス記録媒体2530に記録された一連のビデオフレームを図式的に示している。

【0076】

図25に示す実施例では、暗号化されたコンテンツ鍵（及び他の情報）を含むアクセスパッケージは、「ダミー」フレーム2610として記録されている。このダミーフレームは、図25では、影付きの領域として示している。アクセスパッケージは先に記録され、次に、ビデオデータの連続したフレーム2620が記録される。少なくとも幾つかのフレーム2620は、フレームのシーケンスにおけるアクセスパッケージ2610の位置を示すポインタ2630を含んでいる。図25に示す構成では、ポインタ2630は相対的位置を、ポインタ2630を含むフレームとアクセスパッケージとの間のフレームの数として表現している。この相対的なアドレス指示法には、アドレスをシーケンスが記録されているテープ上の位置から独立して取り扱えるという利点がある。

【0077】

各フレーム又はビデオデータに、アクセスパッケージを示す関連するポインタを設けてもよく、或いは、これに代えて、フレームの1つ以上のサブセットにこのようなポインタを設けてもよい。もちろん、例えば、フレーム単位の分解能を有するタイムコード（frame-resolution time code）によって、テープが「予め区分されている（pre-striped）」場合、絶対アドレスを用いてもよい。ユニークな又は準ユニークであるSMPTE UID等の物理的な識別子（ウォーターマークとして、コンテンツに任意に組み込まれる）を用いて適切な絶対アドレスを提供してもよい。

【0078】

先に（暗号化されたコンテンツデータより先に）アクセスパッケージを記録する構成は、例えば、カメラレコーダ（カムコーダ）等のオーディオ／ビデオデータが事実上リアルタイムに捕捉され、記録される記録構成において特に有益である。カムコーダを用いる場合、記録処理の特定のいずれの時刻においても、記録処理がいつ終了するかは未知である。したがって、シーケンスの始めに記録されたアクセスパッケージを含んでいるダミーのフレームを遡って示すポインタを用いることが好適であり、シーケンスの途中のフレーム又はシーケンスの最後に設けられたダミーフレームを指示する順方向ポインタ（forward pointer）を実現することは、困難であり、これを実現するには、記録処理後に記録されたフレームを変更する必要がある。

【0079】

一方、編集装置又はマスタリング装置等の他の記録構成では、現在の記録シーケンスの長さを事前に知ることができる場合がある。このような場合、アクセスパッケージは、シーケンスの途中又はシーケンスの最後に設けてもよく、ポインタは、各フレームにおいて、後ろにあるアクセスパッケージを指示することもできる。図26は、記録されたフレームのシーケンス2720の最後に設けられたアクセスパッケージ2710を示している。少なくとも幾つか（全てでもよい）の記録フレームに添付されたポインタ2730は、順方向にあるアクセスパッケージ2710の位置を示している。

【0080】

図27は、記録されたフレームのシーケンス2820の最初に「メイン」アクセスパッケージ2810を記録した更なる構成を図式的に示している。ポインタ2830は、逆方向にあるメインアクセスパッケージ2810を指示している。シーケンスの最後には、「予備」アクセスパッケージ2840を設けている。この予備アクセスパッケージ2840を設けることにより、メインアクセスパッケージ2810が記録されたテープ位置が破損した場合であっても、記録されたマテリアルにアクセスすることができる。

【0081】

また、図27は、各フレームが先行するフレームを指示し、メインアクセスパッケージ2810に戻る連鎖的アドレスリンク（address chain of links）2830を形成する相

10

20

30

40

50

対アドレスの更なる可能性も示している。

【0082】

図28は、アクセス記録媒体2530に記録されたビデオフレームを図式的に示している。多くのビデオテープ記録フォーマットは、各フレームに、ユーザデータを記録するために、メタデータ「ユーザビット」を含んでいる。ポインタ2630、2730、2830は、これらのユーザビットに設けることが理想的である。そこで、図28に示す実施例では、ビデオデータとオプションのオーディオデータは、テープ上のフレームのペイロードセクション2910に記録され、ポインタは、フレームのユーザビットセクション2920に格納されている。

【0083】

図29及び図30は、データアクセスパッケージのフォーマットを図式的に示している。データアクセスパッケージは、1個以上の「ダミー」フレームに保存され、すなわち、ビデオフレームの1つと同じ総合的なデータフォーマットで保存され、暗号化されたコンテンツ鍵は、ビデオフレームのペイロードセクション内に保存される。これにより、ビデオフレームに適用される記録処理と同じ記録処理をアクセスパッケージにも適用できるため、この手法は特に有益である。換言すれば、これにより、ビデオテープ記録／再生装置において必要となる変更を減らすことができる。また、図27に示す構成において、そのシーケンスに関するアクセスパッケージが「メイン」アクセスパッケージであるか否かを示すフラグをユーザビット3020に格納してもよい。

【0084】

図31は、ダミーのビデオフレーム3210を図式的に示している。

【0085】

この実施例におけるビデオフレームは、一連の画像領域3220として画像の空間周波数成分に関連する圧縮映像データを保存する。この領域は、所謂マクロブロックであってもよく、所謂スライスであってもよく、他の領域であってもよい。このような領域のそれぞれにおいて、圧縮データの最も低い空間周波数（所謂「DC」）部分に格納される。この実施例では、この領域に暗号化されたコンテンツ鍵及びアクセスパッケージの他の部分を保存する。この手法の有益な点は、DCデータは、従来のビデオ画像の再生をうまく行うために重要な部分であるので、多くのテープフォーマットにおいて、DCデータに対してはより慎重な処理が行われるという点である。より慎重な処理とは、より高度なエラー検出及びエラー訂正処理及び／又は例えば、テープの中央領域等、エラーが生じにくい領域へのDCデータの保存を含む。

【0086】

アクセスパッケージは、単一のフレームのためのDC係数によって提供されるストレージ容量より大きいストレージ容量を必要とする場合がある。したがって、データアクセスパッケージは、複数のダミーフレームに亘って格納してもよい。このような場合、ポインタにより、例えば、アクセスパッケージを表す最初のダミーフレームのアドレスを指示してもよい。

【0087】

添付の図面を参照して本発明を詳細に説明したが、本発明は上述の実施の形態の詳細に限定されるものではなく、当業者は、添付の請求の範囲に定義された本発明の思想及び範囲から逸脱することなく、上述の実施の形態を様々に変更及び修正することができる。

【図面の簡単な説明】

【0088】

【図1】本発明に基づくデジタルコンテンツのためのアクセス制御システムの構成を示す図である。

【図2】図1に示すカメラの記録処理を説明する図である。

【図3】図1に示す再生装置における再生処理を説明する図である。

【図4】図1に示すリムーバブルメモリ装置に保存される情報の組を示す図である。

【図5】本発明に基づく第1の暗号化方式を説明する図である。

【図 6】図 5 に示す暗号化方式に対応する復号方式を説明する図である。

【図 7】3 人の異なるユーザに対する選択的なアクセス許可の一例を説明する図である。

【図 8】異なる鍵が異なる情報部分に関連付けられたバイナリツリー暗号方式を説明する図である。

【図 9】ディスク I D を暗号化処理に用いる暗号化方式を説明する図である。

【図 10】図 9 に示す暗号化方式に対応する復号方式を説明する図である。

【図 11 A】ディスク I D を含む代替的な暗号化方式を説明する図である。

【図 11 B】記録媒体に保存されるコンテンツアクセス制御データを示す図である。

【図 12】図 11 A に示す暗号化方式に対応する復号方式を説明する図である。

【図 13】マスタユーザに対するデータの暗号化を含む暗号化方式を説明する図である。

10

【図 14】図 13 に示す暗号化方式に対応する復号方式を説明する図である。

【図 15】図 11 及び図 13 の暗号化方式で実行される処理シーケンスのフローチャートである。

【図 16】図 12 及び図 14 の復号方式で実行される処理シーケンスのフローチャートである。

【図 17】ディスクがコピーされたときに実行されるアクセス許可を説明する図である。

【図 18】マジックゲート（商標）装置とメモリースティックからなるシステムを示す図である。

【図 19】マジックゲート（商標）システムにおける記録処理のフローチャートである。

【図 20】マジックゲート（商標）システムにおける再生処理のフローチャートである。

20

【図 21】ユーザディレクトリの更新によって、どのようにユーザがシステムに追加され、及びシステムから削除されるかを説明する図である。

【図 22】デジタル署名に関連するメッセージ署名及び検証手続を説明する図である。

【図 23】ビデオストリームの所定の部分の選択的な暗号化を説明する図である。

【図 24】テープ記録／再生装置を示す図である。

【図 25】テープに記録される一連のビデオフレームを示す図である。

【図 26】テープに記録される一連のビデオフレームを示す図である。

【図 27】テープに記録される一連のビデオフレームを示す図である。

【図 28】ビデオフレームを示す図である。

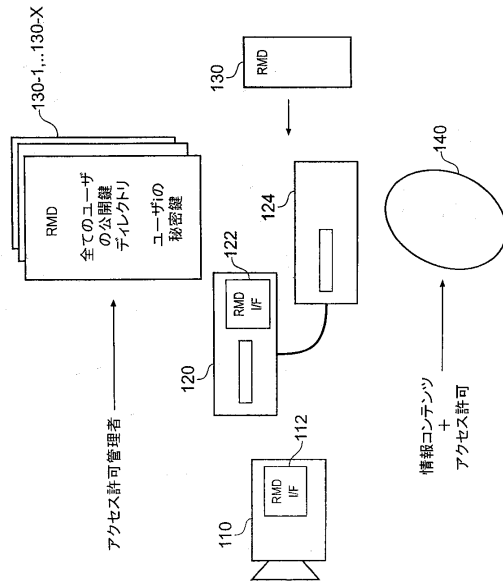
【図 29】データアクセスパッケージのフォーマットを示す図である。

30

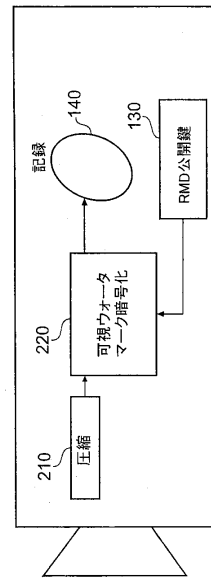
【図 30】データアクセスパッケージのフォーマットを示す図である。

【図 31】ダミービデオフレームを示す図である。

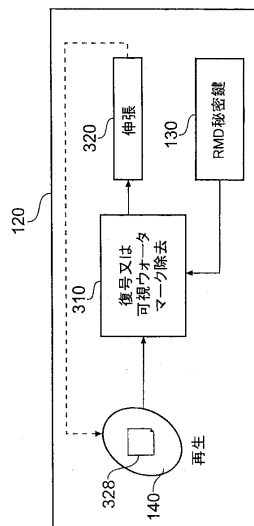
【図 1】



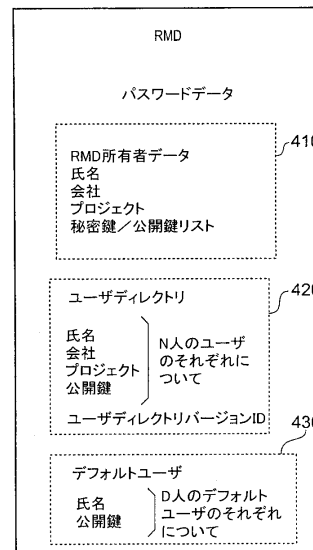
【図 2】



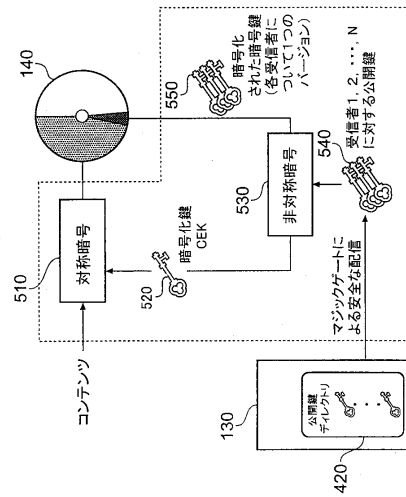
【図 3】



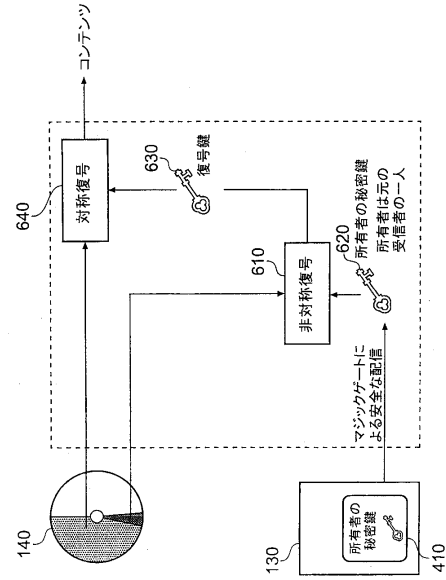
【図 4】



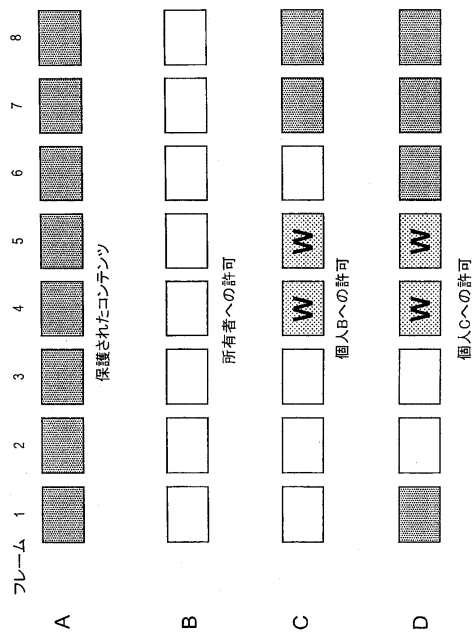
【図 5】



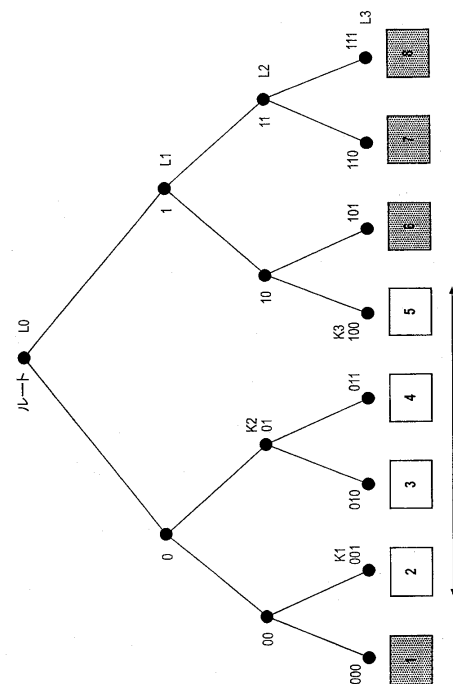
【図 6】



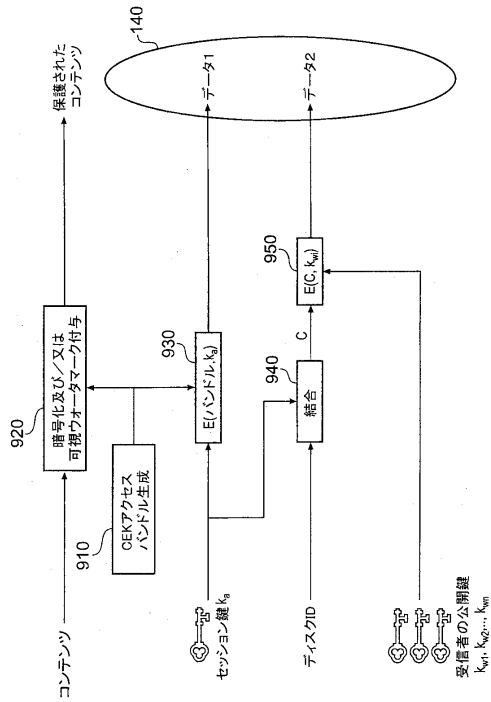
【図 7】



【図 8】



【図 9】



【図 10】

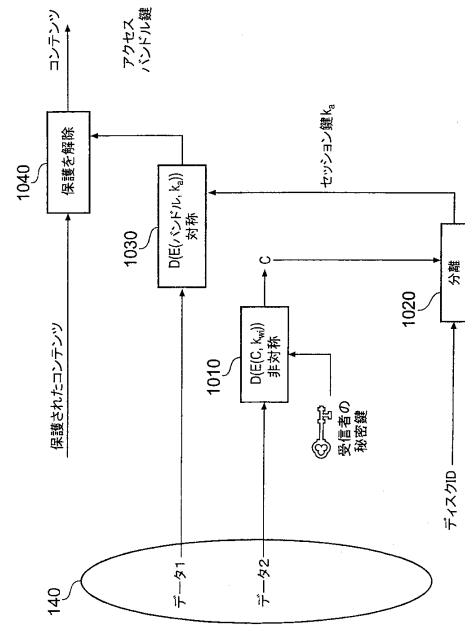
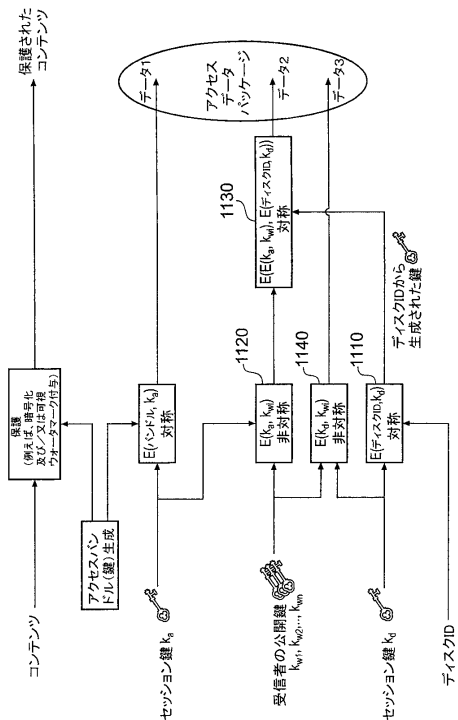
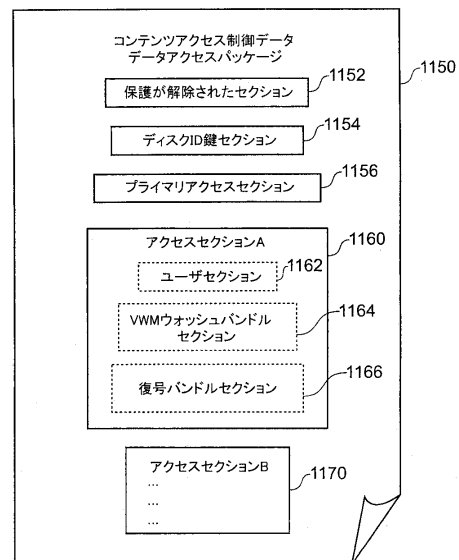


Fig. 10

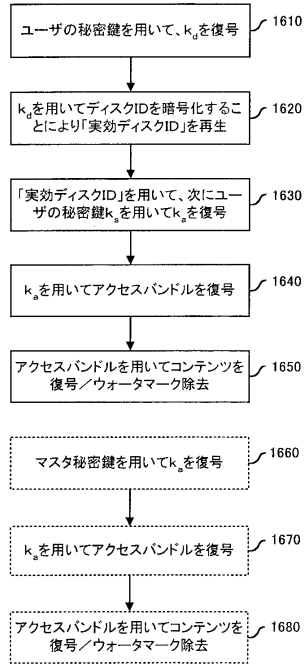
【図 11 A】



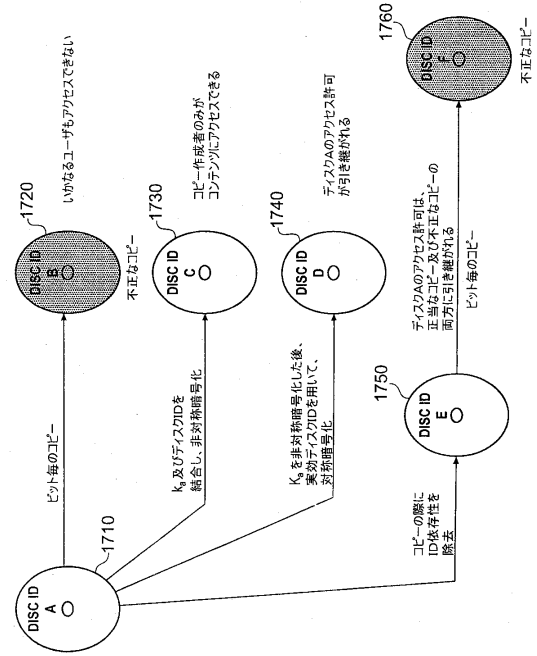
【図 11 B】



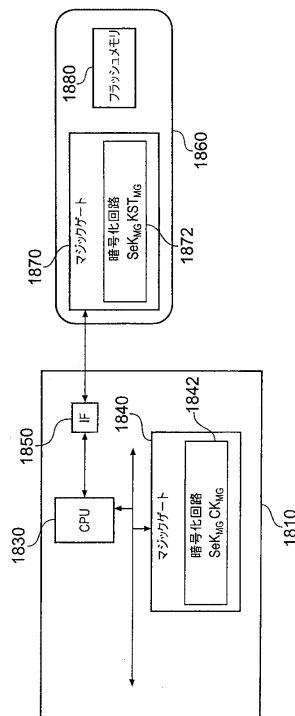
【図 16】



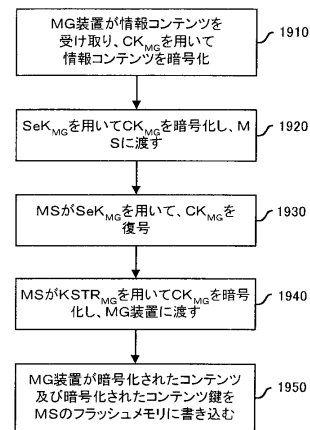
【図 17】



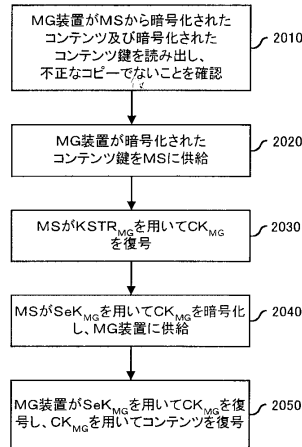
【図 18】



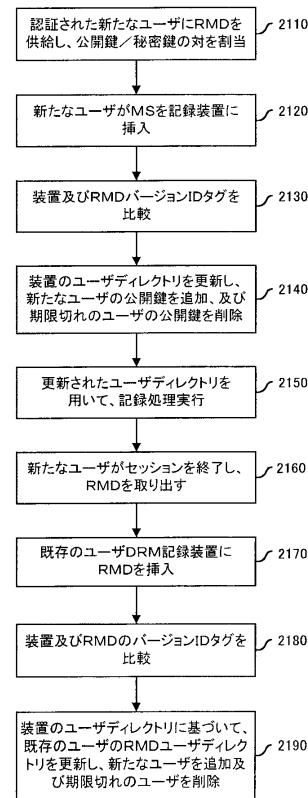
【図 19】



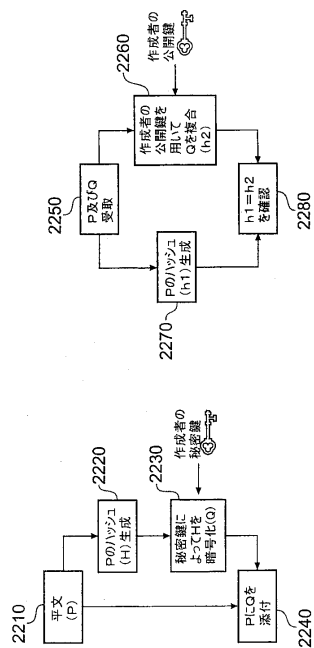
【図 20】



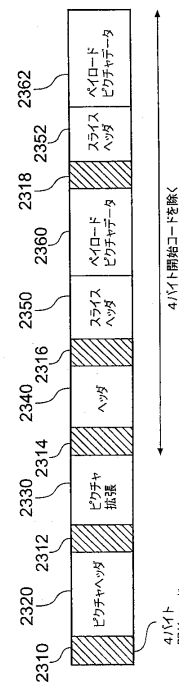
【図 21】



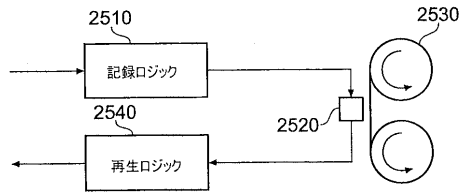
【図 22】



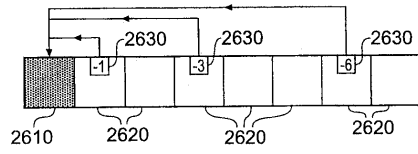
【図 23】



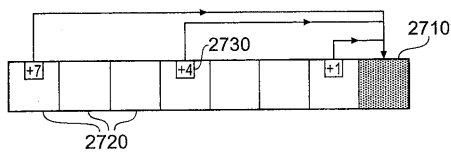
【図 24】



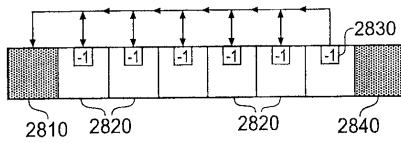
【図 25】



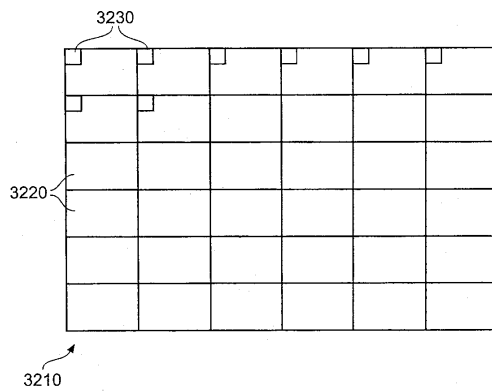
【図 26】



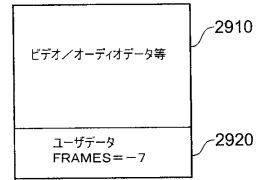
【図 27】



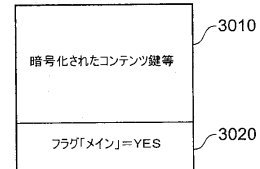
【図 31】



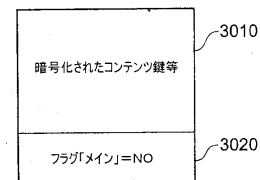
【図 28】



【図 29】



【図 30】



フロントページの続き

- (72)発明者 テイラー、 アンドリュー ロバート
イギリス国 KT13 OXW、 ウェブリッジ、 ブルックランズ、 ザ ハイッ (番地無し) ソニー ユナイテッド キングダム リミテッド内
- (72)発明者 タブソン、 ダニエル ワレン
イギリス国 KT13 OXW、 ウェブリッジ、 ブルックランズ、 ザ ハイッ (番地無し) ソニー ユナイテッド キングダム リミテッド内
- (72)発明者 フーパー、 ダニエル ルーク
イギリス国 KT13 OXW、 ウェブリッジ、 ブルックランズ、 ザ ハイッ (番地無し) ソニー ユナイテッド キングダム リミテッド内
- (72)発明者 エマニエル、 アルベスーモーリア
イギリス国 KT13 OXW、 ウェブリッジ、 ブルックランズ、 ザ ハイッ (番地無し) ソニー ユナイテッド キングダム リミテッド内

審査官 石田 信行

- (56)参考文献 特開2003-122637 (JP, A)
特開2000-298974 (JP, A)
特開2000-196582 (JP, A)
特開2001-331106 (JP, A)
特開2004-362238 (JP, A)
特開2003-132625 (JP, A)
特開2001-176189 (JP, A)
特開2000-231760 (JP, A)
特開平11-224456 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| H04L | 9/08 |
| G09C | 1/00 |
| G06F | 21/24 |
| G11B | 20/10 |