

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4680892号
(P4680892)

(45) 発行日 平成23年5月11日 (2011.5.11)

(24) 登録日 平成23年2月10日 (2011.2.10)

(51) Int. Cl.	F I	
G 1 1 B 20/10 (2006.01)	G 1 1 B 20/10	H
H O 4 N 5/92 (2006.01)	G 1 1 B 20/10	3 1 1
H O 4 N 5/93 (2006.01)	H O 4 N 5/92	H
H O 4 N 5/76 (2006.01)	H O 4 N 5/93	Z
	H O 4 N 5/76	Z

請求項の数 29 (全 33 頁) 最終頁に続く

(21) 出願番号	特願2006-508396 (P2006-508396)	(73) 特許権者	504031469
(86) (22) 出願日	平成16年6月7日 (2004.6.7)		ズー デジタル リミテッド
(65) 公表番号	特表2007-527588 (P2007-527588A)		ZOO DIGITAL LTD.
(43) 公表日	平成19年9月27日 (2007.9.27)		イギリス国 エス1 4キューエル シェ
(86) 国際出願番号	PCT/GB2004/002388		フィールド ファーニバル スクエア 2
(87) 国際公開番号	W02004/109678		ザ タワー
(87) 国際公開日	平成16年12月16日 (2004.12.16)	(74) 代理人	100068755
審査請求日	平成19年6月6日 (2007.6.6)		弁理士 恩田 博宣
(31) 優先権主張番号	0312874.1	(74) 代理人	100105957
(32) 優先日	平成15年6月5日 (2003.6.5)		弁理士 恩田 誠
(33) 優先権主張国	英国 (GB)	(72) 発明者	グリーン、スチュアート
(31) 優先権主張番号	60/480,322		イギリス国 エス1 4エフエス シェフ
(32) 優先日	平成15年6月20日 (2003.6.20)		ールド カーバー ストリート 26
(33) 優先権主張国	米国 (US)		パークヘッド ハウス ズーテック リミ
			テッド

最終頁に続く

(54) 【発明の名称】 オーディオビジュアル製品におけるデータの隠蔽

(57) 【特許請求の範囲】

【請求項1】

オーディオビジュアル製品(400)の生成に使用する方法であって、

元のコンテンツシーケンスに従って再生される元のオーディオビジュアルデータ(700)を受信するステップであって、前記元のオーディオビジュアルデータは、複数のセルを含む、前記受信するステップと、

前記元のコンテンツシーケンスに適切でない一つ以上の誤りセルを前記複数のセルに挿入するステップと、

複数のシーケンス命令(410)を生成するステップであって、各シーケンス命令が前記複数のセルを指定された順番に再生するための再生シーケンスを表わし、各シーケンス命令が前記複数のセルの一つ以上を参照するプログラムチェーン(PGC)を含む、複数のシーケンス命令を生成するステップとを備え、複数のシーケンス命令は、

前記再生シーケンスによって前記元のコンテンツシーケンスが再生される少なくとも一つの正しいシーケンス命令(410a)と、

前記再生シーケンスによって前記元のコンテンツシーケンスが再生されない複数の不正なシーケンス命令(410b)とを含み、各不正なシーケンス命令が前記一つ以上の誤りセルの少なくとも一つを参照するPGCを含む、方法。

【請求項2】

前記複数のセルを雑混に並べて前記元のコンテンツシーケンスをスクランブルするステップを備える、請求項1記載の方法。

【請求項 3】

前記正しいシーケンス命令 (410a) よりも多数の前記不正なシーケンス命令 (410b) を生成して、前記正しいシーケンス命令 (410a) が前記不正なシーケンス命令 (410b) の中に隠蔽されるようにするステップを備える、請求項 1 又は 2 に記載の方法。

【請求項 4】

前記不正なシーケンス命令 (410b) の各々によって、前記複数のセルのオーディオビジュアルデータ (700) の再生を無事に行なうことができなくなる、請求項 1 乃至 3 のいずれか一項に記載の方法。

【請求項 5】

前記一つの以上の誤りセル (421) の各々は、前記元のオーディオビジュアルデータ (700) のセクションを含む、請求項 1 記載の方法。

【請求項 6】

前記一つ以上の誤りセル (421) における前記元のオーディオビジュアルデータ (700) を改ざんするステップを備える、請求項 5 記載の方法。

【請求項 7】

前記複数のシーケンス命令 (410) は、前記セルのオーディオビジュアルデータ (700) が再生されている途中で、オーディオビジュアルデータ (700) 自体を複製することなく、異なる変更を実行する、請求項 1 乃至 6 のいずれか一項に記載の方法。

【請求項 8】

前記不正なシーケンス命令 (410b) が前記正しいシーケンス命令 (410a) の順序入れ替えとなるように前記複数のシーケンス命令 (410) は順序入れ替えシーケンスとして形成される、請求項 1 乃至 7 のいずれか一項に記載の方法。

【請求項 9】

複数の構造ロケーションをオーディオビジュアル製品 (400) 内に設定するステップと、

前記複数のシーケンス命令 (410) を前記複数の構造ロケーションに割り当てるステップと、を備える、請求項 1 乃至 8 のいずれか一項に記載の方法。

【請求項 10】

前記少なくとも一つの正しいシーケンス命令 (410a) 又は各少なくとも一つの正しいシーケンス命令に割り当てられる構造ロケーションは、アクセスコード (80) から生成することができる、請求項 9 記載の方法。

【請求項 11】

宛先関数を定義するステップであって、宛先関数をアクセスコード (80) に適用すると、宛先関数によって正しいシーケンス命令 (410a) の構造ロケーションが生成される、宛先関数を定義するステップを備える、請求項 10 記載の方法。

【請求項 12】

前記アクセスコード (80) は所定範囲内の数値を含み、これにより、前記宛先関数を前記アクセスコード (80) の数値に適用すると、前記宛先関数によって、前記正しいシーケンス命令 (410a) の前記構造ロケーションが計算される、請求項 11 記載の方法。

【請求項 13】

前記宛先関数を不正な数値に適用すると、前記宛先関数によって、複数の不正なシーケンス命令 (410b) のうちの一つの不正なシーケンス命令の構造ロケーションが計算される、請求項 12 記載の方法。

【請求項 14】

前記宛先関数は一方向性ハッシュ関数を含む、請求項 11 乃至 13 のいずれか一項に記載の方法。

【請求項 15】

前記宛先関数は、各々が複数の数値を有する少なくとも 2 つのアクセスコードで動作する、請求項 11 乃至 14 のいずれか一項に記載の方法。

10

20

30

40

50

【請求項 16】

前記宛先関数を適用してユーザに対して表示される第1アクセスコードを生成し、かつ前記宛先関数は、返信として提供される第2アクセスコードで動作する、請求項11乃至15のいずれか一項に記載の方法。

【請求項 17】

前記宛先関数によってシードを生成し、変換を適用して第1アクセスコードを生成して、第1アクセスコードのシードがユーザには見えないようにするステップを備える、請求項16記載の方法。

【請求項 18】

複数のセル(420)を少なくとも第1ビデオストリーム(1901)及び第2ビデオストリーム(1902)に割り当てるステップと、

前記第1及び第2ビデオストリーム(1901、1902)の間の切り替えを行なうことにより、前記複数のセル(420)を元のコンテンツシーケンスに従って再生するビデオストリーム切り替え命令(2011, 2021)を生成するステップと、を更に備える、請求項1乃至17のいずれか一項に記載の方法。

【請求項 19】

オーディオビジュアル製品(400)はDVDビデオ規格に従って再生することができる、請求項1乃至18のいずれか一項に記載の方法。

【請求項 20】

オーディオビジュアル製品(400)を携帯型ランダムアクセスストレージ媒体(40)に記録するステップを含む、請求項1乃至19のいずれか一項に記載の方法。

【請求項 21】

オーディオビジュアル製品(400)を光ディスク(40)にDVDビデオ規格に従って記録するステップを含む、請求項1乃至20のいずれか一項に記載の方法。

【請求項 22】

請求項1乃至21のいずれか一項に記載の方法を実行する命令であって、コンピュータが実行可能な命令が記録された記録媒体。

【請求項 23】

請求項1乃至21のいずれか一項に記載の方法を実行するように適合させたオーサリング装置。

【請求項 24】

再生装置を用いて再生するためのオーディオビジュアルデータからなる複数のセルを含む表示データが記録されるとともに、前記再生装置にオーディオビジュアルデータシーケンスの再生を制御させるための複数のプログラムチェーン(PGC)が記録された記録媒体であって、前記PGCは、前記セルへの参照を含み、一つ以上のPGCは、再生時において、前記再生装置に連続して再生するためのセルを選択させ、

前記複数のセルは、

複数の正しいセルであって、各正しいセルは、前記オーディオビジュアルデータシーケンスの一部を形成するデータを含む、前記複数の正しいセルと、

前記オーディオビジュアルデータシーケンスに適切でない誤りセルとを含み、

前記PGCは、

前記正しいセルを参照する正しいPGCであって、前記正しいPGCの制御によりセルを再生する場合、前記正しいPGCは、前記再生装置に前記オーディオビジュアルデータシーケンスに従って再生のために前記正しいセルを選択させる、前記正しいPGCと、

前記誤りセルへの参照を含む不正なPGCであって、前記不正なPGCの制御によりセルを再生する場合、前記不正なPGCは、前記再生装置に再生のために誤りセルを選択させる、前記不正なPGCとを含む、記録媒体。

【請求項 25】

前記複数のセルは、前記複数の正しいセル内に散在された複数の誤りセルを含む、請求項24に記載の記録媒体。

10

20

30

40

50

【請求項 26】

前記不正な PGC は、複数の不正な PGC のうちの一つであり、前記正しい PGC は、前記複数の不正な PGC の中に隠蔽される、請求項 24 又は 25 に記載の記録媒体。

【請求項 27】

前記不正な PGC は、前記正しい PGC と類似するように配置されている、請求項 24 乃至 26 のいずれか一項に記載の記録媒体。

【請求項 28】

少なくとも一つの前記 PGC は、一つ以上のプログラム (PG) を含み、各 PG は前記セルを参照する、請求項 24 乃至 27 のいずれか一項に記載の記録媒体。

【請求項 29】

記録媒体は、DVD ビデオディスクを含む、請求項 24 乃至 28 のいずれか一項に記載の記録媒体。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は概して、オーディオビジュアル製品の生成または再生に使用する方法及び装置に関する。特に、本発明は、オーディオビジュアル製品内のデータを隠蔽することによるオーディオビジュアル製品へのアクセスの制御に使用する方法及び装置に関する。

【背景技術】**【0002】**

オーディオビジュアル製品へのアクセスは制御することが望ましい。特に、現時点において存在する機会であって、認証を受けることなくオーディオビジュアルコンテンツを閲覧するか、またはオーディオビジュアルコンテンツにアクセスする機会を制限することが望ましい。

【0003】

一般的に、映画または他の表示のようなオーディオビジュアルコンテンツは、生のオーディオ及びビジュアルコンテンツの多くの小セクションまたは小クリップを収集することにより形成される。このことは通常、「オーサリング」プロセスと呼ばれ、このプロセスでは、生のサウンドクリップ及びビデオクリップを徐々に組み立て、そして纏めて編集して完成版のオーディオビジュアル製品を形成する。次に、オーディオビジュアル製品を或る形式の記録媒体に記録する。従来、この媒体はセルロイドフィルムまたはアナログビデオテープ（例えば VHS フォーマットビデオテープ）のようなアナログ媒体である。ごく最近では、オーディオビジュアルコンテンツを、特に DVD のような光ディスク媒体を含むランダムアクセス媒体、または磁気ハードドライブのような他の形式のランダムストレージに記録することが可能になっている。これらのランダムアクセス媒体は、サイズ、データ容量、再生スピード、画質などの点で多くの利点を有する。しかしながら、認証を受けることなく、保存されるオーディオビジュアル製品を閲覧するか、またはオーディオビジュアル製品にアクセスすることが比較的容易であるという不具合があることも認識されている。

【0004】

光ディスクは多くの異なる目的に関して利便性の良い記録媒体である。デジタル多用途ディスク (digital versatile disc: DVD) は、片面 1 層 (シングルレイヤ) ディスクに最大 4.7 Gb、そして両面 2 層 (デュアルレイヤ) ディスクに最大 17 Gb の容量を有するように開発されている。とりわけ DVD ビデオディスク、DVD オーディオディスク、及び DVD RAM ディスクを含む DVD ディスクにデータを記録するために、現在、幾つかの異なるフォーマットがある。これらのディスクの内、DVD ビデオは特に、動画のような予め記録されたビデオコンテンツに使用することができるように設計されている。記録容量が大きく、使用が容易であるということから、DVD ディスクが広く使用されるようになり、かつ商業的に重要になっている。便利なことに、DVD ビデオディスクは、比較的簡単なユーザ制御が行われる専用再生機器を使用して再

10

20

30

40

50

生まれ、そしてDVDビデオディスクを再生するDVD再生装置は比較的広い範囲に渡って普及しつつある。DVDビデオ規格に関する更に詳細なバックグラウンド情報は、www.dvdforum.orgまたは他のいずれかのサイトのDVDフォーラムから入手することができる。

【0005】

DVDビデオ規格は、ディスクのオーディオビジュアルデータコンテンツを保護するために多くの内蔵コピー防止機能を含む。これらのコピー防止機能にはコンテンツスクランブリングシステム(Content Scrambling System: CSS)及びマクロビジョンコピープロテクト(Macrovision Copy Protection)があり、コンテンツスクランブリングシステムを使用してオーディオビデオデータブロックを暗号化し、このようなデータがDVDビデオ表示とは別に再生されることを防止し、そしてマクロビジョンコピープロテクトを使用して記録機器を使用してのビデオのコピーを防止する。これらのシステムは共に、再生中に適切な機能を実行するDVDビデオ再生装置によって解釈される。これらのアプローチは平均的なコンシューマに関するデータコンテンツを保護するために効果的であるが、ディスクのコピーまたはディスクの一部を生成する技術に長け、かつ生成することを生業とする「リバースエンジニア(reverse engineer)」であれば容易に両方のシステムを破ることができる。

10

【0006】

DVDビデオ規格には、非常に優秀なリバースエンジニアの手が届かないようにしながらコンテンツをディスクにセキュアに保持することを可能にする内蔵機能が含まれない、という問題が認識されている。この問題を示すための一例として、DVDビデオディスクが、特定のキー組合せを入力するなどの操作(例えば、或るメニューが現われてから5秒以内に「左矢印(left arrow)」キーを押下する)によりアクセスされる、ディスクの不可視データである所謂「イースターエッグ(Easter Eggs)」を含む場合がある。リバースエンジニアはこのようなコンテンツにキー組合せの知識が無くても、単に関連オーディオビデオオブジェクトをディスクから直接抽出することにより容易にアクセスすることができる。多くのオーディオビデオ調査ソフトウェアパッケージを入手することができ、これらのソフトウェアパッケージを使用してディスクの個々のビデオ表示の各々を「リップ(rip)する」ことができる。例えば、これについては、とりわけwww.dvd-ripper.comを参照されたい。

20

30

【0007】

米国特許第6,161,179号(ダブリューイーエー マニュファクチャリング インコーポレイテッド(WEA Manufacturing, Inc))は、光で読み取り可能なディスクをキーを用いて保護する方法を開示しており、この方法では、ディスク再生装置がディスクの再生の度に固有キーを供給する。ユーザは固有キーをトランザクションサービスに送信し、そしてアンロックキーを返信として受け取る。ユーザはアンロックキーをディスク再生装置に送信する。すると、ディスク再生装置はディスク再生の前に、アンロックキー及び固有キーが所定の関係を有することを確認する。この公知の保護方法によって、DVDビデオフォーマットにおけるように、光で読み取り可能なディスクに配信されるオーディオビジュアル製品のビデオペーパービュー(pay-per-view)または他のペーパーユース(pay-per-use)の商用化が可能になる。

40

【発明の開示】

【発明が解決しようとする課題】

【0008】

セキュリティ及び保護のレベルが、公知のコピー防止プロテクトアプローチによって実現するレベルを超え、かつ当該レベルよりも高いことが必要とされる広い範囲のアプリケーションがある。これらの問題は、DVDビデオフォーマット光ディスクに関連して生じるだけでなく、特にオーディオビジュアルコンテンツがランダムアクセス記録媒体に記録される他の多くの環境において生じる。

50

【課題を解決するための手段】

【0009】

本発明の一つの目的は、少なくとも本発明の或る好適な実施形態において、オーディオビジュアル製品の生成及び/又は再生に使用する方法及び装置を提供することにある。これらの方法及び装置によって、オーディオビジュアル製品へのユーザアクセスが制限される。特に、本発明の一つの目的は、オーディオビジュアル製品のコピー、閲覧、またはオーディオビジュアル製品への他の権限の無いアクセスを制限することにある。

【0010】

本発明の少なくとも幾つかの実施形態の一つの目的は、オーディオビジュアル製品の生成及び/又は再生に使用する方法及び装置を提供することにある。これらの方法及び装置によって、技術に精通したりバースエンジニアであっても、オーディオビジュアル製品への自由かつ無制限なアクセスを防止する相当に大きな障害に遭遇する。

【0011】

本発明によれば、添付の特許請求の範囲に示される装置及び方法が提供される。本発明の好適な特徴は、添付の特許請求の範囲及び以下に記載する説明から明らかになる。

一般的に、本発明に適するオーディオビジュアル製品は、オーディオビジュアルデータから成る複数のセルを有し、オーディオビジュアルデータの再生は一つ以上のシーケンス命令によって制御される。好適には、これらのセルの各々及びこれらのシーケンス命令の各々は、オーディオビジュアル製品内に所定の構造ロケーションを有し、この構造ロケーションによって、セルからセル、または一つのシーケンス命令から別のシーケンス命令のような、オーディオビジュアル製品内でのナビゲーションを用いた移動が可能になる。

【0012】

本発明の一つの態様は、オーディオビジュアル製品へのアクセスを制御するアクセスコードを或る形式のアンロックプロセスとして使用する方法に関連する。

本発明の一つの例示としての態様では、オーディオビジュアル製品の生成に使用する方法が提供され、この方法は、元のコンテンツシーケンスに従って再生される元のオーディオビジュアルデータを受信するステップと、元のオーディオビジュアルデータを複数のセルに分割するステップと、複数のシーケンス命令を生成するステップであって、各シーケンス命令がこれらのセルを指定された順番で再生する再生シーケンスを表す、生成ステップと、複数のシーケンス命令をそれぞれ、オーディオビジュアル製品内の複数の構造ロケーションのうちの一つの構造ロケーションに割り当てるステップと、アクセスコードに基づいて動作して、複数の構造ロケーションの中から宛先構造ロケーションを計算することにより、複数のシーケンス命令の中から一つのシーケンス命令を選択する宛先関数を生成するステップと、を含む。

【0013】

本発明の別の例示としての態様では、オーディオビジュアル製品の再生に使用する方法が提供され、この方法は、アクセスコードを受信するステップと、オーディオビジュアル製品内の宛先構造ロケーションを、宛先関数をアクセスコードに適用することにより計算するステップと、計算済み宛先構造ロケーションにジャンプすることにより当該ロケーションに対応するシーケンス命令を選択するステップと、を含む。

【0014】

使用状態では、オーディオビジュアル製品内の宛先構造ロケーションは、宛先関数を受信済みアクセスコードに適用することにより計算される。計算済み宛先構造ロケーションにジャンプすることにより、当該ロケーションに対応するシーケンス命令が選択される。その結果、選択されたシーケンス命令によって、オーディオビジュアル製品内のオーディオビジュアルデータのセルのシーケンスの再生が開始される。

【0015】

好適には、アクセスコードはオーディオビジュアル製品の再生中に入力する。最も好ましくは、アクセスコードはユーザが、キーボードまたはリモートコントロールユニット、或いは他の通信機器のような入力デバイスを使用して入力する。一例として、アクセスコ

10

20

30

40

50

ードは、数字キーパッドの画像表示を通して入力する数字コード（例えば1 2 3 4）である。

【0016】

好適には、アクセスコードに適用される宛先関数は、宛先構造ロケーションを表す数値を、受信済みアクセスコードで返す数学関数である。アクセスコードは適切であればどのような形式をとることもできるが、好ましくは、所定範囲内の数値を含み、宛先関数をアクセスコードの数値に適用した場合に、宛先関数によって正しいシーケンス命令の構造ロケーションが計算されるので、「イースターエッグ」機能または映画のセクションのような保護対象のオーディオビジュアルデータを入手することができる。これとは異なり、宛先関数を不正な数値に適用すると、他の或る構造ロケーションが生成される。例えば、宛先関数によって構造ロケーションが生成され、この構造ロケーションにより、例えば「アクセスが拒否されました」というメッセージが表示されるか、またはこの構造ロケーションにより不正なシーケンス命令が生成され、不正なシーケンス命令によってオーディオビジュアルデータを無事に再生することができなくなる。

10

【0017】

宛先関数は一方向性ハッシュ関数を含むことが好ましい。好適には、宛先関数は、各々が数値を有する少なくとも2つのアクセスコードで動作する。好適には、宛先関数を適用して第1アクセスコードを生成してユーザに対して表示し、かつ返信として送信される第2アクセスコードで動作する。宛先関数によってシードが生成され、そして変換が適用されて第1アクセスコードが生成され、第1アクセスコードのシードがユーザに明らかにならないようにする。

20

【0018】

本発明の本態様は、多くの異なる特定の構成で具体化することができ、この具体化は、アクセスコードが宛先関数に関連付けられることにより、オーディオビジュアルコンテンツがアンロックされてユーザがコンテンツを楽しむことができるという方法に従って行なわれる。このアンロック方法は、通常のコンシューマによるオーディオビジュアル製品への自由かつ無制限なアクセスを防止するために特に有用である。すなわち、ほとんどの通常のコンシューマは、一旦、正しいアンロックアクセスコードを保有すると、オーディオビジュアル製品、またはオーディオビジュアル製品の選択的にロックされたセクションへのアクセスのみを行なう。

30

【0019】

本発明の別の態様は、オーディオビジュアル製品内のデータを隠蔽することに関する。一つの例示としての実施形態では、本発明は、オーディオビジュアル製品の生成に使用する方法を提供し、本方法は、元のコンテンツシーケンスに従って再生される元のオーディオビジュアルデータを受信するステップと、元のオーディオビジュアルデータを複数のセルに分割するステップと、複数のシーケンス命令を生成するステップであって、各シーケンス命令がこれらのセルを指定された順番で再生する再生シーケンスを表す、生成ステップと、を含み、複数のシーケンス命令は、再生シーケンスによって、元のコンテンツシーケンスが再生される少なくとも一つの正しいシーケンス命令と、再生シーケンスによって、元のコンテンツシーケンスが再生されない複数の不正なシーケンス命令とを含む。

40

【0020】

別の例示としての実施形態では、本発明は、オーディオビジュアル製品の再生に使用する方法を提供し、本方法は、オーディオビジュアル製品を受信するステップであって、複数のシーケンス命令が、オーディオビジュアル製品を元の再生シーケンスに従って再生するための少なくとも一つの正しいシーケンス命令と、オーディオビジュアル製品を元の再生シーケンスに従って再生しない複数の不正なシーケンス命令とを含む、オーディオビジュアル製品を受信するステップと、複数のシーケンス命令の中から一つのシーケンス命令を選択するステップと、セルのオーディオビジュアルデータを、選択されたシーケンス命令に従って再生するステップとを含む。

【0021】

50

本発明の本態様は、オーディオビジュアル製品に含まれる元のオーディオビジュアルデータへのアクセスを制御する簡単であるが有効なメカニズムを提供する。元のコンテンツは複数のセルに分割し、これらのセルは、再生シーケンス命令に従って順番に再生されることになる。複数のセルからの元のコンテンツシーケンスの再構築を可能にする一つ以上の正しいシーケンス命令は、これらの命令自体が、複数の不正なシーケンス命令の中に埋もれて隠れてしまう。有利なことに、比較的多い数のシーケンス命令が生成され、この場合、比較的少ない数（例えば、1または2）のシーケンス命令によってセル群が正しく再生されて元のコンテンツシーケンスが再構築される。好適には、残りの多い数の不正なシーケンス命令の各々によって、オーディオビジュアル製品がセル群から無事に再生することができなくなる。正しいシーケンス命令をこのように難読化することによって、元のオーディオビジュアルデータへのアクセスを安全に、かつ信頼性よく制御することができる。正しいシーケンス命令を選択することができるユーザのみが元のオーディオビジュアルデータを入手できる。

10

【0022】

好適には、複数のシーケンス命令は複数の順序入れ替えシーケンスとして形成され、この場合、一つのこのような順序入れ替えシーケンスのみが元のコンテンツシーケンスに対応する。他の複数の順序入れ替えシーケンスの各々によってセルのオーディオビジュアルデータが再生されるが、元のコンテンツシーケンスに従った再生は行なわれない。従って、複数のシーケンス命令の各々は互いに適度に類似するので、リバースエンジニアがどのシーケンス命令が正しいのかを判断することが比較的難しい。その結果、正しいシーケンス命令が複数の順序が入れ替わった不正なシーケンス命令の中に埋もれてしまって正しいシーケンス命令の読み出しが難しくなる。

20

【0023】

本発明の一つの好適な実施形態では、複数のセルが元のコンテンツシーケンス以外のシーケンスで並べられる。すなわち、これらのセルを並べ替えて、新規の、雑混のセルシーケンスを提供し、このセルシーケンスによって元のオーディオビジュアルデータを隠蔽する。これらのセルを雑混のシーケンスで記録するということは、リバースエンジニアが元のオーディオビジュアルデータをセルから容易に再生するということができないことを意味する。元のコンテンツシーケンスを正しく再生するためには、正しいシーケンス命令を認識することも必要である。

30

【0024】

本発明の一つの態様は、元のコンテンツシーケンスに元々含まれているという訳ではない一つ以上の誤り「偽装」セルを加えることに関する。

一つの例示としての実施形態では、本発明は、オーディオビジュアル製品の生成に使用する方法を提供し、本方法は、元のコンテンツシーケンスに従って再生される元のオーディオビジュアルデータを受信するステップと、元のオーディオビジュアルデータを正しいオーディオビジュアルデータから成る複数のセルに分割するステップと、誤りのオーディオビジュアルデータを含む少なくとも一つの誤りセルを複数のセルに加えるステップと、複数のセルのうちの選択されたセルを指定された順番で再生する再生シーケンスを表す少なくとも一つのシーケンス命令を形成するステップと、を含む。

40

【0025】

別の例示としての実施形態では、本発明は、オーディオビジュアル製品の再生に使用する方法を提供し、本方法は、複数のセルに分割されたオーディオビジュアルデータを有するオーディオビジュアル製品を受信するステップであって、複数のセルが、元のコンテンツシーケンスに固有の正しいオーディオビジュアルデータを含む少なくとも一つの正しいセルと、誤りのオーディオビジュアルデータを含む少なくとも一つの誤りセルと、複数のセルのうちの選択されたセルを指定された順番で再生する再生シーケンスを表す少なくとも一つのシーケンス命令とを含む、オーディオビジュアル製品を受信するステップと、セルのオーディオビジュアルデータをシーケンス命令に従って再生するステップとを含む。

【0026】

50

好適には、誤り偽装セル (erroneous red herring cell) は、元のオーディオビジュアルデータの短いセクションを含み、かつ最初は元のコンテンツシーケンスに元々含まれていたものとして現われるが、オーディオビジュアルデータは、例えばビデオデータを逆方向に再生することにより変質する。従って、誤り偽装セルを再生すると、元のコンテンツシーケンスを正しく見るができない。誤りセルの他の例として、とりわけ、反転画像、高コントラストまたは低コントラスト画像、スノー (snow)、フェージング (fading)、ジッタ (jitter)、及び過剰音 (overly loud)、ソフトオーディオまたは歪みオーディオのような攪乱ビジュアルまたはオーディオ効果を挙げることができる。

【0027】

本発明の更に別の態様は、スクランブルされたビデオストリームをオーディオビジュアル製品内で使用する方法に関する。

本発明の一つの例示としての実施形態では、オーディオビジュアル製品の生成に使用する方法が提供され、本方法は、元のコンテンツシーケンスに従って再生される元のオーディオビジュアルデータを受信するステップと、元のオーディオビジュアルデータを複数のセルに分割するステップと、複数のセルが少なくとも第1ビデオストリーム及び第2ビデオストリームに含まれるようにこれらのセルをこれらのビデオストリームに割り当てるステップと、第1ビデオストリームと第2ビデオストリームとの間の切り替えを行って、これらのセルを元のコンテンツシーケンスに従って再生するビデオストリーム切り替え命令を生成するステップと、を含む。

【0028】

本発明の別の例示としての実施形態では、オーディオビジュアル製品の再生に使用する方法が提供され、本方法は、オーディオビジュアルデータから成り、かつ共になって元のコンテンツシーケンスを表す複数のセルを有するオーディオビジュアル製品を受信するステップであって、これらのセルが少なくとも第1及び第2ビデオストリームに分割される、オーディオビジュアル製品を受信するステップと、一つ以上のビデオストリーム切り替え命令を実行して、セルの再生中に少なくとも第1ビデオストリームと第2ビデオストリームとの間の切り替えを自動的に行って、オーディオビジュアルデータを元のコンテンツシーケンスに従って再生するステップと、を含む。

【0029】

元のコンテンツシーケンスに従って再生される元のオーディオビジュアルデータを複数のセルに分割し、これらのセルが少なくとも第1及び第2ビデオストリームに含まれるようにこれらのセルをこれらのビデオストリームに分割する。ビデオストリーム切り替え命令を使用して、第1ビデオストリームと第2ビデオストリームとの間の切り替えを自動的に行って、これらのセルを元のコンテンツシーケンスに従って再生する。

【0030】

好適には、ビデオオブジェクトは各セルを保持し、ビデオストリーム切り替え命令によって、ビデオオブジェクトから第1ビデオストリームまたは第2ビデオストリームのいずれかとして再生されるビデオストリームを決定する。誤りデータは理想的には他のストリームに記録される。少なくとも一つの予備ビデオオブジェクト (preliminary video object) は、ビデオ切り替え命令を実行して第1ビデオストリームまたは第2ビデオストリームのいずれかをそれぞれ選択するプログラム命令を有するので、マルチアングルビデオオブジェクトはセルを該当するビデオストリームに保持する。予備ビデオオブジェクト及びマルチアングルビデオオブジェクトは適切に交互に配置される。すなわち、一つ以上の予備ビデオオブジェクトが順番に再生され、続いて一つ以上のマルチアングルビデオオブジェクトが再生され、次にこの手順を繰り返す。ビデオストリーム切り替え命令は、隠れメニューボタンに接続される強制起動ボタン命令を使用して実行することが好ましい。ボタン命令はDVDビデオバーチャルコマンドセットから適切に選択してビデオストリームの特殊パラメータ (すなわちSPRM3) を、次のマルチアングルビデオオブジェクトに適する所望のビデオストリームに設定する。

10

20

30

40

50

【0031】

好適には、シーケンス発生器を使用してビデオストリームシーケンスを順番に生成する。シーケンス発生器は、一つ以上の初期パラメータをシードとして生成される決定的アルゴリズムであることが好ましい。一つの好適な実施形態では、複数の初期パラメータのうちの一つ以上の初期パラメータは一形式のキーとして再生時に再度供給される。

【0032】

本発明の好適な実施形態は、特にDVDビデオ規格に従って再生することができるオーディオビジュアル製品に関する。好適には、シーケンス命令はプログラムチェーン(PGC)として実行する。DVDビデオ製品に含まれるオーディオビジュアルデータへのアクセスを効果的に制御するだけでなく、光ディスクのような記録媒体の利用可能な記憶容量の効率的な使用を維持することが望ましい。通常DVDビデオディスクのデータの大部分は、セル及びビデオオブジェクト(video objects:VOBs)の内部に含まれるオーディオビデオ表示データによって占有される。これとは異なり、プログラム(programs:PGs)及びプログラムチェーン(program chains:PGCs)のようなナビゲーションデータが占有する記憶容量は比較的小さい。

10

【0033】

本明細書において説明する本発明の複数の態様の各々は単独で用いることができる。好適には、本発明の複数の態様のうちの2つ以上の態様は全て、組み合わせる形で用いることができる。最も好適には、本明細書において説明するロック形態、難読化形態、及びコンテンツスクランブル形態は全て、組み合わせる形で用いることができる。

20

【0034】

本発明の一つの特に好適な実施形態では、元のコンテンツシーケンスを複数のセルに分割し、そしてこれらのセル及び/又はビデオストリームをスクランブルする。従って、元のコンテンツシーケンスを、単にオーディオビジュアル製品のオーディオビジュアルオブジェクトを読み取るだけで再構築することは困難である。更に、正しいシーケンス命令は、多くの類似の不正なシーケンス命令の中に埋もれて隠れてしまう。更には、正しいシーケンス命令へのアクセスは宛先関数及びアクセスコードによって制御される。その結果、非常に高いレベルのセキュリティが、オーディオビジュアル製品に含まれる元のオーディオビジュアルデータに関して得られる。

【0035】

本発明はまた、本発明の複数の態様のうちのいずれかの態様によって形成されるか、またはいずれかの態様において使用されるように適合させたオーディオビジュアル製品を本明細書に定義するように拡張することができる。オーディオビジュアル製品は、DVDビデオ製品、特にオーディオビジュアルコンテンツをDVDビデオ規格に準拠して記録した光ディスクであることが好ましい。

30

【0036】

便利なことに、少なくとも幾つかの好適な実施形態においては、本発明は、コンピュータプログラム、または一連のコンピュータプログラムとして実行される。プログラムまたは複数のプログラムは、磁気ディスク、ハードディスク、または固体メモ리카ードのような消去可能なストレージ媒体を含む適切な記録媒体のいずれにも記録されるか、または搬送波に乗せた変調信号として記録してローカルエリアネットワーク(LAN)またはインターネットのようなワイドエリアネットワーク(WAN)のような適切なデータネットワークのいずれかを通して伝送される。

40

【0037】

少なくとも幾つかの好適な実施形態では、本発明はコンピューティングプラットフォーム、理想的にはパーソナルコンピュータのような汎用コンピューティングプラットフォームで、またはクライアントサーバコンピューティングネットワークにおいて適切に実行される。別の構成として、本発明は全体が、または少なくとも一部が専用ハードウェアによって実行される。例えば、本発明は光ディスク再生装置またはレコーダーのような娯楽家電製品の中で実行される。少なくとも幾つかの好適な実施形態では、本発明は、DVDビ

50

デオフォーマットの光ディスクを再生するDVDビデオ再生装置の中で、またはDVDビデオフォーマットデータを光ディスクに記録するDVDレコーダーの中で実行される。

【発明を実施するための最良の形態】

【0038】

本発明を更に深く理解するために、かつ本発明の実施形態をどのようにして実施することができるかについて示すために、一つの例として添付の概略図を参照することとする。

本発明の好適な実施形態について、オーディオビジュアルコンテンツを含むDVDビデオフォーマット光ディスクの特定の例を参照しながら記載する。しかしながら、本発明は、特にオーディオビジュアルコンテンツが或る形態のランダムアクセスストレージ媒体に格納される広い範囲の他の環境に適用することができることを理解されたい。また、DVDビデオフォーマットはそれ自体がやがて新規のフォーマット定義に取って代われ、置き換えられると考えられる。すなわち、本発明はかなり先の将来において、かつ未だに実現していない環境においても適用することができると考えられる。

【0039】

図1は、本発明の好適な実施形態において用いることができるオーサリング装置(authoring apparatus)の例を示している。本実施形態では、オーサリング装置は、クライアントサーバコンピュータシステムのようなコンピューティングプラットフォームまたはスタンドアロンパーソナルコンピュータ30を含む。任意選択の構成として、生のオーディオ及びビデオデータがカメラ10及びマイクロホン20などを通して受信されるか、またはファイルストレージデバイス25のような他のソースから供給される、或いは画像及びサウンド生成ソフトウェアなどによってオーサリング装置の内部で生成される。生のコンテンツデータは、ビデオクリップ、オーディオクリップ、スチル撮影画像、アイコン、ボタン画像、及びオンスクリーンに表示される他のビジュアルコンテンツを含むことができる。コンテンツは、適切にはMPEGまたはJPEGエンコードファイル形式であるが、いずれのフォーマットとすることもできる。

【0040】

この元のオーディオビジュアルデータは、他の多くの考え得る形態の中でも、映画またはカンパニープレゼンテーション、或いはクイズゲームのような、いずれかの形式とすることができる。オーサリング装置として機能するパーソナルコンピュータ30は、以下に更に詳細に説明するように所望のオーディオビジュアル製品を生成する。オーサリング装置30はオーディオビジュアル製品400を、パーソナルコンピュータ30内部のハードディスクのようなストレージ媒体に、または光ディスク40に書き込む。

【0041】

図2は、本発明の好適な実施形態において用いることができる、オーディオビジュアル製品400を再生する装置の全体概略図である。光ディスク40のオーディオビジュアル製品400は、本例では、DVD再生装置50及びテレビジョン画面60を含む再生装置に入力される。ユーザによるコントロールは、リモートコントロールハンドセット70などを通して行われる。以下に更に詳細に説明するように、一つの例示としての実施形態では、オーディオビジュアル製品400はアクセスコードまたはPINコード80をユーザが入力することにより制御される。図2に示すように、アクセスコード80は、ユーザがリモートコントロール装置70を通して入力することに対応してテレビジョン画面60に表示される。

【0042】

図3は、オーディオビジュアル製品400の構造の詳細を示している。オーディオビジュアル製品400は、本例では、セルAV1, AV2, . . . AVmにより表わされる複数のセル420を含む。各セル420はオーディオビジュアルデータの短いセクションを含む。これらのセルは、通常次から次に連続して再生されて所望のオーディオビジュアル表示を再生シーケンス命令410による制御を受けながら提供する。図3に示すシーケンス命令410はこれらのセル420とは別である。適切な形で、セル420及びシーケンス命令410がそれぞれ、オーディオビジュアル製品内部の構造ロケーションに割り当てら

10

20

30

40

50

れて、これらの命令 4 1 0 の間のナビゲーション及び命令 4 1 0 からセル 4 2 0 へのナビゲーションが可能になる。

【 0 0 4 3 】

DVDビデオフォーマットデータの好適な例では、セル群 4 2 0 は、これらのセルへの参照によってセル群を複数のプログラム (programs : P G s) に取り込むことにより連続して再生され、今度は、これらのプログラムがプログラムチェーン (program chains : P G C s) に体系化される。図 3 では、シーケンス命令 4 1 0 はプログラムチェーン P G C 1 , P G C 2 . . . P G C n により表わされる。好適には、各セル 4 2 0 は少なくとも一つのビデオストリーム、少なくとも一つのオーディオストリーム、及び / 又は少なくとも一つのサブピクチャストリームを含む。

10

【 0 0 4 4 】

DVDビデオフォーマットによって、プログラムチェーン群 (P G C s) からセル群への多数対 1 のマッピングが可能になり、このマッピングは最初に規格の中に盛り込まれて、複数のストーリーラインをサポートする。この例がDVDビデオディスクであり、このDVDビデオディスクは、プログラム (P G) バージョン及び一般 (G : General Audience : 一般オーディエンス) バージョンに対応する、同じ映画の 2 つの別々のレイトバージョンを含み、一般バージョンは或るシーンが除去されている。閲覧者がディスクを再生すると、彼または彼女は手始めに、プログラム (P G) バージョンまたは一般 (G) バージョンのいずれを再生すべきかを選択することができ、そしてDVDの「ペアレントコントロール (parental control) 」機能は確実にこの目的のために利用することができる。通常、映画コンテンツのほとんどの部分は、プログラム (P G) バージョンまたは一般 (G) バージョンの両方に共通であり、かつ 1 度しかディスクに記録されない。しかしながら、プログラム (P G) バージョンに関するプログラムチェーン (P G C) は、一般 (G) バージョンに関するプログラムチェーン (P G C) にも含まれる選択シーンを省略しているか、またはその逆である。

20

【 0 0 4 5 】

通常のDVDビデオディスクのデータの大部分は、セル群 4 2 0 に含まれるオーディオビデオ表示データにより占有され、かつプログラムチェーン (P G C) 4 1 0 を含む表示データに占有される記憶容量は比較的小さい。本発明は、これらのセル 4 2 0 を、オーディオビデオデータを複製することなく再生する方法の複数の変形例を用いる。

30

【 0 0 4 6 】

[シーケンス命令の難読化]

第 1 の態様では、本発明は、正しい再生シーケンス命令を多くの不正なシーケンス命令の中に紛れ込ませて隠蔽したオーディオビジュアル製品を提供する。

【 0 0 4 7 】

本発明の好適な実施形態は、複数のプログラムチェーン (P G C) 4 1 0 を使用して下位のセル群 4 2 0 を複数の異なるシーケンスで参照し、このようなシーケンスの内、一つのシーケンスのみが正しいように構成することにより難読化を実現する。

【 0 0 4 8 】

例えば、3 個のセル A , B , 及び C に関して、6 個のプログラムチェーン (P G C) 1 ~ 6 を図 4 に示すように定義することができる。この場合、6 個の使用可能なコンテンツ再生シーケンスがあり、これらのシーケンスの内、P G C 1 のみが正しいシーケンスを提供する。従って、P G C 1 が正しいシーケンス命令 4 1 0 a であり、他の P G C 2 ~ 6 は全て不正なシーケンス命令 4 1 0 b である。このアプローチは、正しいビデオシーケンスを隠すために採用することができる。この目的のために、セル群 4 2 0 の期間は非常に短くする必要があり (1 個のセルは 0 . 4 秒という短い期間のオーディオ / ビデオを含むことができる) 、かつビデオプログラムは多くのセル 4 2 0 に分割する必要がある。DVDビデオ規格においては、P G C は最大 2 5 6 個のセルを含むことができ、そして P G C の全体構造 (enclosing structure) であるビデオタイトルセット (Video Title Set : V T S) は、最大 3 2 7 6 7 個の P G C を含むことがで

40

50

きる。従って、1個のセルは、最大でも32767個のPGCによってしか共有することができない。上の例では、正しいシーケンスA, B, Cは順次再生される連続するセル群420から成る。

【0049】

図5は、オーディオビジュアル製品を生成する好適な方法の概要を示している。生のオーディオビジュアルデータはステップ510で受信する。ステップ520では、オーディオビジュアルデータは、図4を参照しながら上に概要を示し、かつ以下に更に詳細に説明するように、セル群420に分割される。ステップ520はステップ521を含むことができ、このステップ521で、誤りセルを元のオーディオビジュアルデータに加える。またステップ520は任意選択の形でステップ522を含むことができ、このステップ522で、セル群420をスクランブルして(配列し直す、または雑混にする)、これらのセルが元の所望の再生シーケンスに対応しないようにする。

10

【0050】

ステップ530では、複数のシーケンス命令410を生成し、この命令により、ステップ520で生成されたセル群420の再生シーケンスを制御する。ステップ530はステップ531を含み、このステップ531では、一つ以上の正しいシーケンス命令410aを生成して、正しいシーケンス命令を他の不正なシーケンス命令410bの中に紛れ込ませる。ステップ532では、任意選択の形で、正しいシーケンス命令410aの順番を入れ替えて、より多くの不正なシーケンス命令410bを生成し、一つ以上の正しいシーケンス命令410aが、このような処理により生成される多くの不正なシーケンス命令410bの中に隠れてしまうようにする。

20

【0051】

オーディオビジュアルデータから成るセル群、及び該当する複数のシーケンス命令410をステップ520及び530で生成してしまうと、ステップ540において、オーディオビジュアル製品をフォーマットし、そして適切なストレージ媒体に記録する。好適な実施形態では、オーディオビジュアル製品は、DVDビデオ規格に従ってフォーマットし、そしてハードディスクドライブまたは好適には光ディスクに記録する。このステップ540は必要に応じて、下流の処理ステップを含むことができ、これらの下流の処理ステップでは、例えば構造ロケーションをセル群410及びシーケンス命令420に割り当て、そして光ディスクに記録するか、または焼き付ける準備の整った明示的なディスク画像(すなわちビットストリーム画像)を生成する。

30

【0052】

図6は、オーディオビジュアル製品400を再生する好適な方法の概略模式図である。

ステップ610では、オーディオビジュアルデータから成るセル群420及び複数の再生シーケンス命令410を含む生成済みオーディオビジュアル製品400を受信する。

【0053】

ステップ620では、これらの再生シーケンス命令410のうちの一つを選択する。ステップ620は、認証プロセスを実行してユーザがオーディオビジュアル製品を再生する許可を有することを確認するステップを含むことが好ましい。一つの実施形態では、認証処理はステップ621を含み、このステップ621では、ユーザアクセスコードまたはPINのようなユーザ入力を受信し、ステップ622では、オーディオビジュアル製品内部の構造ロケーションを計算し、そしてステップ623では、計算して求めたロケーションにジャンプする。ステップ622におけるこのような計算によって、複数の再生シーケンス命令の中の一つに対応する一つの構造ロケーションが適切に得られる。ステップ622における計算が正しく行なわれた場合には、正しい再生シーケンス命令410aの位置が特定されることになる。計算が正しく行なわれなかった場合には、多くの不正な再生シーケンス命令410bのうちの一つが選択されることになる。

40

【0054】

ステップ630では、セル群420のオーディオビジュアルデータを、選択された再生シーケンス命令410に従って再生する。ステップ630では適切な形で、参照セル群4

50

20のオーディオビジュアルデータを光ディスクのようなストレージ媒体から取り出し、適切なデコードを実行し、そしてデコードされたデータを、例えば図2を参照しながら上に概要を説明したように、ディスプレイ画面を通して、かつオーディオスピーカを通して出力する。

【0055】

[PGCの難読化]

次に、本発明の特に好適な実施形態について、図の内、図7～17を参照しながら更に例を示すことにより説明する。

【0056】

図7は、例示としてのオーディオビデオ映像クリップ700を示している。保護する必要があるソースビデオコンテンツが60秒クリップから成り、このクリップ内には、クリップが4つの異なるシーンを含むように3つの「カット」が含まれると、仮定する。ここで、シーンのカットポイントは通常、4つの個別のサブクリップとして与えられるのではなく、クリップ内で暗示的に設けられることに留意されたい。

【0057】

シーケンスがセル群420に分割され、各セルが3秒の平均期間を有し、結果的に合計で20個のセルがシーケンスを構成することが望ましい。

提供されるビデオクリップは、シーンカットに関してサーチされる。この目的のためにビデオストリーム及び/又はオーディオストリームの不連続性に基づいて使用される公知の方法がある。例えば、多くの文献の中でも特に、ジー・アクリーバス、エヌ・ドゥラミス、エイ・ドゥラミス、エス・コリアス(G. Akriavas, N. Doulamis, A. Doulamis, 及びS. Kollias)による「MPEG符号化ビデオ信号のシーン検出方法」と題するProceedings of MELCON 2000 Mediterranean Electrotechnical Conference, Nicosia, Cyprus, May 2000を参照されたい。シーンカットは、図8に示すように、後で細分化を行なうためのアンカーポイントとなる。

【0058】

図9に示すように、本例では、クリップは、各々が約3秒の期間を有するセル群420に分割され、セル群420はカットシーンポイントに固定される。セル群420の期間を少しだけ変更することにより、結果として得られるセル群が均一な期間を持たないようにする。

【0059】

[誤り「偽装(red herring)」セル群]

図10によれば、参照されることがない誤り「偽装」セル群421を正しい再生シーケンス410aに取り入れると有利である。(「偽装(red herring)」とは文字通り、注意をそらすための攪乱であり、魚(薫製ニシン:red herring)を利用して猟犬に臭いの痕跡が判別できないように猟犬を攪乱させることに由来する。)このような誤りセル群421は、これらの誤りセルが正しいセル群420に非常に類似して見えて、明らかに不適當なセル群421を含む全てのシーケンス命令を容易に取り除くことができなくなるように適切に構成される。例えば、製品が、各セルが4秒の期間を有する一連のセル群を含むとすると、以下ようになる。

【0060】

セル1 - - 0秒から始まって4秒で終了する

セル2 - - 4秒から始まって8秒で終了する

セル3 - - 8秒から始まって12秒で終了する

この場合、幾つかの例示としての誤りセル群は、

偽装1 - - 2秒から始まって6秒で終了する

偽装2 - - 6秒から始まって10秒で終了する

実際に、各セルの期間は、例えばタイムコード検索法を使用して明らかに誤っているセ

10

20

30

40

50

ル群をパターンから廃棄することができるパターンが生成されないように変化させる。

【 0 0 6 1 】

図 1 0 に示すように、多くの誤り「偽装」セル群 4 2 1 が生成され、これらのセルは他のセル群 4 2 0 と同様の長さを有する。保護レベルは、誤り偽装セル群 4 2 1 の数と共に高くなり、そして通常、ディスクの利用可能な記憶容量によって制限される。本例では、20%の誤り偽装セル群を設けると仮定する。これらの誤り偽装セル 4 2 1 は理想的には、他の有効なセル群によって共有されることがないか、またはシーンカットのポイントではないポイントから始まり、そしてポイントで終了する。誤り偽装セル群 4 2 1 は図 1 0 の斜線付きボックスで示される。

【 0 0 6 2 】

誤り偽装セル群 4 2 1 は、図 1 1 に示すように、有効セル群 4 2 0 の再生順番に、セルの開始時間から始まる形で挿入する。

[セルのスクランプリング]

図 1 2 に示すように、セル群 4 2 0 (全ての誤りセル 4 2 1 を含む) は、他のセル群に対する各セルのロケーションを変えることにより雑混にするので、セル群 4 2 1 がディスクに表示される順番が決定される。セル群 4 2 0 は任意の形で雑混にすることができるが、この構成は、利用可能な各再生シーケンスがシームレス再生に関連する DVD ビデオ規格に詳細が記載される制約を満たす場合に、高いレベルの保護を実現することになる。すなわち、シームレスに再生を行なう - - 再生飛びがない - - セル 4 2 0 が 2 個ある場合、これらのセルに関連するデータはディスク上で比較的近接する必要がある。実際には、セル群 4 2 0 は、互いに離れた多くのセクターとした場合でもシームレスに再生を行なうことができるので、本例では、セル群 4 2 0 は任意に連続して配置することができるが、例示のために、いかなるセルも、当該セルの正しい位置から 3 個分のセル 4 2 0 の内側に位置する必要があると仮定している。

【 0 0 6 3 】

好適な DVD ビデオフォーマットでは、セル群 4 2 0 はこれらのセルがディスクに現われる順番に 1 から始まる番号が付けられる。従って、雑混になったセル群 4 2 0 は、再命名されたセル識別子を示す下線付き番号を使用して図 1 3 に示すように、これらのセルがディスクに現われる順番に連続して名前が付け直される。

【 0 0 6 4 】

図示の配列での、正しい再生シーケンスを図 1 4 に示す。

ここで、セル 4 , 8 , 15 , 及び 19 は誤り偽装セルであり、かつ正しい再生シーケンスには生じないことに留意されたい。

【 0 0 6 5 】

ディスクに 1 , 2 , . . . 24 , として設定されるセル群 4 2 0 のリストに基づいて、多くの不正な再生シーケンス 4 1 0 b を生成し、各再生シーケンスは、24 個のセルからいずれか 20 個のセルを選択し、そしてこれらのセルをランダムな順番に表示することにより決定される。ここでもまた、保護レベルは、このようなシーケンスが全て、シームレス再生の DVD ビデオ規格要件を満たす場合に高くなる。シーケンスを N 個のセル 4 2 0 に分解して R 個の誤り偽装セル 4 2 1 を加える場合、利用可能なシーケンスの数は (シームレス再生に関する制限を無視すると) $(N + R) ! / R !$ となる。本例では、この数は $24 ! / 4 !$ に等しい。この数は非常に大きく $(2 . 6 \times 10^{22})$ 、そして実際には、ディスクに表示される利用可能なシーケンスの数は、プログラムチェーン (PGC) の数に対する DVD ビデオ限界によって制限される。オーディオ / ビデオデータは、複数のプログラムチェーン (PGC) の間で共有されるので、実際には再生シーケンスは 32 , 767 個に制限される。各再生シーケンスは再生セル群 4 2 0 を参照して保存するので、これらのシーケンスの各々は DVD ディスクに非常に少ないデータを使用して表示することができる。

【 0 0 6 6 】

これらの再生シーケンス 4 1 0 (すなわち、複数の不正なシーケンス 4 1 0 b を合わせ

10

20

30

40

50

た正しいシーケンス 4 1 0 a) の各々は、プログラム (P G) D V D ビデオナビゲーション構造を使用して表示される。ナビゲーション構造はセルポイント群のリストから成る。複数のプログラムはプログラムチェーン構造の内部に格納される。この動作例における正しいシーケンス 4 1 0 a に対応するプログラムは、図 1 5 に示すように構造化することができる。

【 0 0 6 7 】

再生シーケンス 1 , 2 , . . . 2 0 から成る一つの不正なシーケンス 4 1 0 b の例を図 1 6 に示す。

プログラムチェーンは、1 個のビデオタイトルセット (V T S) の内部の再生シーケンス群の各々に関して生成される。合計で 1 , 0 0 0 個のシーケンスがディスクに関して生成され、これらのシーケンスのうち 1 個が正しいシーケンスであり、かつ 9 9 9 個が不正なシーケンスであると仮定する。複数のシーケンス命令 4 1 0 a のうちのひとつが、ビデオをアンロックするための宛先 (d e s t i n a t i o n) となるシーケンス命令、本例では、図 1 7 に示すように、正しく並べられたセル群 4 2 0 から成るシーケンスを有するプログラムを含む P G C 番号 3 2 1 として選択される。

【 0 0 6 8 】

次に、オーディオビジュアル製品を適切なストレージ媒体、本例では光ディスクに記録する準備が整う。しかしながら、更に別の中間オーサリングステップ (i n t e r m e d i a t e a u t h o r i n g s t e p s) を実行して編集済みオーディオビジュアル製品を特定バージョンに、すなわち空きの既に未記録になっている光ディスクに焼き込む準備の整っているディスク画像に変換する。

【 0 0 6 9 】

正しいシーケンスのセル群 4 2 0 を抽出するために、リバースエンジニアは全ての考えられる組合せを分析する必要がある。利用可能な最大数のセル群 4 2 0 が符号化されると仮定すると、1 時間のプログラムを再構築するためには、リバースエンジニアが最大 3 2 , 7 6 7 時間 (3 . 7 4 年分) のコンテンツを閲覧する必要があることになる。

【 0 0 7 0 】

ビデオの複数のセクションを用意する場合には、正しいシーケンスのセル群 4 2 0 に対する明確な手掛かりが確実に無いことが好ましい。例えば、M P E G エレメンタリストリームのタイムコードは全て消去して、この情報を使用して一連のセル 4 2 0 を必要な順番に並べることができないようにする。また、セル群 4 2 0 は複数のシーン境界で分割して、リバースエンジニアが簡単に一つのセルの最後のフレームを別のセルの最初のフレームと比較して正しい再生シーケンスを推測するということができないようにする必要がある。

【 0 0 7 1 】

ビデオタイトルセット (V T S) 当たりのプログラムチェーン (P G C) の数に対する制限の問題を解決するために、上に概要を記載した方法を拡張して複数のビデオタイトルセット (V T S) を用いることにより、調査する必要のある、宛先となるシーケンス命令 (d e s t i n a t i o n s) の数を増やして、再生シーケンスを見つけ出すことができる。この場合、ビデオプログラムを v 個のセクションの同等の期間に分割し、セクション 1 をビデオタイトルセット (V T S) 1 にマッピングし、最後のセクション v をビデオタイトルセット (V T S) v にマッピングする。各ビデオタイトルセット (V T S) の内部では、最大 3 2 7 6 7 個のプログラムチェーン (P G C) を使用してプログラムを難読化することができ、各 V T S の正しい P G C の無関係化を図り、そして正しい P G C に個別の計算を通して到達する。

【 0 0 7 2 】

オーディオビジュアル製品の再生では、多くの不正な再生シーケンス命令 4 1 0 の中から正しい再生シーケンス命令を求める。図 1 7 に示す上の例では、このことは、P G C 3 2 1 を正しい再生シーケンス命令 4 1 0 a として求めて、オーディオビジュアルコンテンツを満足の行く形で、すなわち図 1 4 に示すセルシーケンスに従って、セル 3 の次にセル

10

20

30

40

50

1、次にセル2などとセルを再生することにより再生することができることを意味する。当業者の読者には明らかなように、種々の選択肢を利用して、ユーザがオーディオビジュアルコンテンツに対するアクセスを認証されるかどうかを判断することができる。例えば、スマートカードのような物理トークンをカードリーダーに提示するか、または或る形式の生体認証（例えば指紋認証）を実行する。次に、再生装置に指示して正しい再生シーケンス命令に従って動作させるが、この動作は、正しい再生シーケンス命令に関連する構造ロケーションにジャンプすることにより適切に行われる。

【0073】

[ビデオストリームのスクランプリング]

本発明の更に別の態様は、オーディオビジュアル製品内のビデオオブジェクトをスクランブルしてオーディオビジュアル製品に対する権限のないアクセスまたは権限のないコピーを更に難しくすることに関する。

【0074】

好適な実施形態は、DVDビデオ規格に従って再生することができるオーディオビジュアル製品に関し、以下に詳細に説明する。

DVDビデオ規格は、オーディオビジュアルデータストリームを保持し、かつビデオオブジェクト（Video Object：VOB）として知られる構造を提供する。ビデオオブジェクト（VOB）は、これも図4を参照しながら上記で概略的に説明したように、セル群に内部的に分割される。オーディオビジュアルプログラムは、一連のビデオオブジェクト（VOB）を所定のシーケンスで、プログラム及びプログラムチェーン（PGC）を使用して再生することにより表示される。現行のDVDビデオ規格では、ビデオオブジェクト（VOB）は1～9個のビデオストリーム（「マルチアングル（multi-angle）」ストリームと呼ばれることが多い）、0～8個のマルチチャンネルオーディオストリーム、及び0～32個のサブピクチャストリームを含む。

【0075】

連続するビデオオブジェクト（VOB）が異なる数のストリームを含むようにこれらのオブジェクトに順番を付けることができる。例えば、第1VOBが1個のビデオストリームを含み、第2VOBが4個のビデオストリームを含むようにすることができる。複数のビデオストリームを含むVOBは多くの場合、「マルチアングルブロック」と呼ばれる。特定パラメータ（Special Parameter：SPRM）-番号3（SPRM3）-を使用して、どのビデオストリームを再生するかについて規定する。オーディオビジュアル製品を、値「4」に設定されるこの特定パラメータSPRM3で記録する場合、後のマルチアングルストリームが続くとアングル4が選択されて再生される。この機能は、閲覧者が最大9個の異なるカメラアングルの中から選択を行ない、次に、選択されたカメラアングルの記録ビデオストリームを閲覧することができるように構成される。しかしながら、本発明はこのカメラアングルビデオストリーム機能を用いてオーディオビジュアル製品を保護する機能を向上させ、オーディオビジュアル製品に対するコピーまたは権限のないアクセスが行われないようにする。

【0076】

図18は、オーディオビジュアル製品のコンテンツを、ビデオストリームを使用してスクランブルする好適な方法の概要である。MPEG符号化オーディオデータ及び/又はビデオデータのような元のオーディオビジュアルデータをステップ1810で受信する。元のオーディオビジュアルデータ401は、セル群420にステップ1820で分割する。セル群420はステップ1830で、複数のビデオストリームの中に分布させる。すなわち、セル群が全て1個のビデオストリームの内部に残るのではなく、セル群は少なくとも2個の異なるビデオストリームの内部に分布させる。また、少なくとも一つのビデオストリーム切り替え命令（video stream switch instruction）が生成され、この命令によって、オーディオビジュアル製品の再生中に自動的に第1ビデオストリームから第2ビデオストリームへの切り替えが行われる。ステップ1830ではシーケンス命令410を生成し、この命令によってセル群420の再生シーケンスを

10

20

30

40

50

制御する。次に、ステップ1840において、オーディオビジュアル製品をフォーマットし、そして適切なストレージ媒体に記録する。

【0077】

次に本方法について、図19～23を参照しながら更に詳細に説明する。

図19に示すように、所望の再生シーケンス（例えば、ほぼリニアなストーリーライン）を有する元のオーディオビジュアルデータ401を、図7、8、及び9を参照しながら上に説明した処理と同様にして複数のセル420に分割する。本例では、A、B、C、及びDの記号を付した4個のセルがある。これらのセルを分割して異なるビデオストリームに含ませる。すなわち、セル群の幾つか（A、B、及びD）を第1ビデオストリーム1901に割り当て、少なくとも一つのセル（C）を異なる第2ビデオストリーム1902に割り当てる。セル群402を所望のシーケンス（ABCD）で再生するためには、ビデオストリームスイッチが第1ビデオストリーム1901と第2ビデオストリーム1902との間に必要になる。単純に第1ビデオストリーム1901を続けると、所望の再生シーケンスが得られない。本例では、単純に第1ビデオストリーム1901を続けると、セルCの再生が行なわれないことになる。セルCを取り込むためのビデオストリームスイッチは図19の太線矢印で表わされる。

10

【0078】

図20はビデオストリームをビデオオブジェクト（VOB）の内部で使用する様子を詳細に示している。都合の良いことに、セル群420はビデオオブジェクト（VOB）の内部に含まれる。セル群のうちの幾つか（A、B、D）は、ビデオストリームを一つしか持たない単純な構成のビデオオブジェクト（VOB）2010の内部に保持される。しかしながら、少なくとも一つのビデオオブジェクト2020は、複数のビデオストリーム1901、1902を有するものとして定義される。第2ビデオストリーム1902は、このようなマルチストリームビデオオブジェクト（マルチアングルブロック）を形成することにより設定される。セルCは、マルチアングルブロック1920の内部の第2ビデオストリーム1902に保持される。

20

【0079】

図20では、セルCは、ビデオストリーム1901及び1902の両方にC1及びC2として挿入される。これによりコピーが更に困難になる。その理由は、ストリーム1901及び1902の両方が明らかに有効なデータを含むからである。セルC2は、変質した、または欠陥のあるビデオデータを含む誤り「偽装」セルであることが好ましい。セルC2を再生する（すなわち、第1ビデオストリーム1901を継続する）と、元のオーディオビジュアルデータ401が無事に再生されない。最大9個の別のビデオストリームを、正しいセルC1を含む各マルチアングルブロックの内部に設定することができる。

30

【0080】

シーケンス命令（PGC）を生成してビデオオブジェクト（VOB）1910、1920を順番に再生するので、セル420 ABCDが再生される。再生シーケンスは更に、ビデオストリーム切り替え命令2011、2021によって制御され、シーケンスの適切なポイントにおいて、ビデオストリーム1901と1902との間の切り替えが行われる。正しいビデオストリーム1901、1902は、各マルチアングルブロック2020に関して、決定的アルゴリズムを使用して計算される。同じ決定的アルゴリズムを再生中に用いると、再生は記録されている複数のビデオストリームの中の同じ経路に従って行われる。

40

【0081】

好適な実施形態では、ビデオストリーム切り替え命令2011、2021は、マルチアングルブロック群2020のうちの一つのブロックに先行するビデオオブジェクト2010の隠れメニューボタンに対応する強制起動ボタン命令を使用して実行する。本例では、セルBのビデオオブジェクト（VOB）は、SPRM3の特定パラメータを「2」に設定するための切り替え命令2011を含む。セルCに関するマルチアングルブロックとしての次のビデオオブジェクト（VOB）を入ると、特定パラメータSPRM3の設定値によ

50

って、ストリーム「2」を再生する必要があることが決定され、これによりこの場合においてはセルC1が再生される。また本例では、セルCのビデオオブジェクト(VOB)2020によって同じようにしてSPRM3を値「1」に設定し、次のセルを再生する準備が整う。

【0082】

好適な実施形態では、シーケンス発生器を使用して正しいビデオストリーム再生シーケンスを決定する。一つの適切なシーケンス発生器は、一つ以上の初期パラメータが組み込まれた決定的アルゴリズムに基づき、かつこの決定的アルゴリズムから連続値が、発生器に一連のパラメータを適用することにより生成される。このようなシーケンス発生器の例は、線形合同発生器(Linear Congruential Generator)であり、A及びBを素数とする場合に、次の数を現在の数から $r_{n+1} = (A * r_n + B) \text{ mod } M$ によって生成する方法として定義される。

10

【0083】

図21は、値A=7、B=3、M=17によって提供される短いシーケンスの例としての表である。各マルチアングルブロックが(例えば)4つのビデオストリームを含む場合、(4を法とする値 r_n)+1(1~4の範囲の値を返す)を連続アングルを選択する際の基礎として使用する。

【0084】

従って、第1マルチアングルブロック2020では、アングルストリーム1が再生され、次に第2ブロックのアングル4が再生される、などが行なわれる。

20

元のオーディオビジュアルデータは、元のセルがマルチアングルブロック群の各々に關して再生される場合にのみ正しく再生され、このことを行なうには、シーケンス発生器に関するパラメータ(本例ではA、B及びM)の値を認識する必要がある。これらのパラメータに関して多くの使用可能な値があるため、これらのパラメータのうちの一つ以上をコンテンツをアンロックする「キー(key)」として使用することができる。不正なパラメータを選択して再生を行なうと、不正なビデオシーケンスがマルチアングルブロックの再生中に再生され、これによってコンテンツを再生することができなくなる(すなわち、非常に不満の残る形の再生となる)。

【0085】

すなわち、本方法では、初期パラメータによって変わる繰り返し出力シーケンスを有する決定的アルゴリズムを生成し、そしてビデオアングルストリームをシーケンスに従って決定する。また、本方法では、一つ以上のパラメータをオーディオビジュアル製品の再生中に受信し、決定的アルゴリズムをこれらのパラメータに適用して出力シーケンスを生成し、そして複数のビデオストリームの中からの選択を生成されたシーケンスに従って行なう。

30

【0086】

図22は、説明したLCGアルゴリズムを繰り返し実行するための例示としてのDVDビデオナビゲーション命令を示している。現行版のDVDビデオ規格の下では、1つの命令しかメニューボタンに關連付けることができない。従って、必要な命令シーケンスをシーケンス発生器を繰り返し用いる度に実行するために、マルチアングルブロックに入る前に、多くの連続セルの強制起動ボタンを用いることが好ましい。すなわち、プログラムは実際には、各マルチアングルブロックの間に挟まれる、順番に並んだ幾つかの予備ビデオオブジェクト(VOB)の各々の最後に実行される命令を使用して実行する。このシーケンスに従って、再生用のビデオアングルの番号を記録する特定パラメータSPRM3を適切な値に設定する。

40

【0087】

図23は、好適なスクランブル方法の基本的な特徴を示すための簡易例である。セルC1及びC2が完全な誤りセルであり、かつ図10を参照しながら上に記載した実施形態におけるように元のコンテンツシーケンスに「偽装」セルとして付加されている。同様に、セルB1、B2、B4、D2、D3及びD4は全て誤りセルである。元のオーディオ

50

ビジュアルデータは、セル A , B 3 及び D 1 を接続する太線で示す経路に従うことによつてのみ再生される。この経路を採るには、正しいシーケンス命令 (P G C) によつてこれらのビデオオブジェクト (V O B) を順番に選択することが必要であり、更には正しいビデオストリーム切り替え命令によつて、各マルチアングルビデオオブジェクト (V O B) 内部の適切なストリームを選択することが必要である。この相乗効果的な組合せによつて、オーディオビジュアル製品がコピーまたは閲覧のような権限のないアクセスに対する非常に強力な防止手段を有することになる。

【 0 0 8 8 】

[ロック / アンロック]

本発明の別の態様はオーディオビジュアル製品の「ロック」に関するものであり、このロックには、ユーザがオーディオビジュアル製品へのアクセスを許可される前に「アンロック」が必要となる。

【 0 0 8 9 】

本発明の好適な実施形態では、ユーザはアクセスコードをキーボードまたは携帯リモートコントロールユニットのような入力デバイスを通して提供する。便利なことに、オーディオビジュアル製品には、ユーザによるアクセスコードの入力を催促するスタートアップシーケンス (例えば第 1 再生プログラムチェーン (P G C)) が設定される。従つて、アクセスコードによつて、直接的または間接的にプログラムチェーン (P G C) 3 2 1 の正しいプログラムシーケンス命令が得られる。

【 0 0 9 0 】

本発明の更に別の実施形態は、ベンダーが D V D ビデオディスクのビデオコンテンツを発行して、全ての D V D ビデオプレーヤにおける再生を可能にするように開発され、この場合、コンテンツは、閲覧の前に「アンロックする」必要がある。これによつて、とりわけ、次のシナリオに示すようにプレイアプリケーション (p l a y - t o - p l a y a p p l i c a t i o n s) が可能になる。

【 0 0 9 1 】

1 . エンドユーザは、雑誌の表紙カバーのような重要なコンテンツを含む D V D ビデオディスクを受け取る。

2 . ユーザがディスクを再生する場合、彼 / 彼女は、コンテンツまたはコンテンツの一部を再生することができるようになる前に、「アンロックコード」の入力を催促される。

【 0 0 9 2 】

3 . アンロックコードを入手するためには、ユーザは、例えば高額な電話番号 (p r e m i u m - r a t e n u m b e r) を呼び出すか、またはクレジットカード決済を実行する必要がある。

【 0 0 9 3 】

4 . アンロックコードを画面にディスクが再生されているときに入力すると、保護対象コンテンツを再生することができる。

多くの変形例を、以下に概要を説明するように、必要なセキュリティレベル及び機能レベルに従つて用いることができる。

【 0 0 9 4 】

例 1 :

例示としての第 1 の方法では、1 個の固定アンロックコードを使用してディスクコンテンツをアンロックする。このことは、例えば 4 桁の P I N とすることができる。画面の上では、ユーザには数字キーパッドの画像が提示され、そしてリモートコントロールナビゲーションボタン (例えば、U p , D o w n , L e f t , R i g h t , 及び E n t e r) を使用することにより、4 桁で鍵をかけることができる。好適には、各桁が入力されると、当該桁が画面に表示され、これをユーザが確認する。勿論、他の多くの入力選択肢も利用することができる。

【 0 0 9 5 】

例 2 :

10

20

30

40

50

例示としての第1の方法の特徴は、全てのユーザが同じアンロックコードを受け取るので、セキュリティの弱点は、アンロックコードを一人の人間によって他の多くの人に渡すことができ、これらの人がアクセス制御のレベルを下げてしまうことである。コードペアを使用することによってセキュリティを次のように強化することができる。

【0096】

1. アンロックコードの催促を行うとき、ディスクは「識別コード (i d e n t i f i c a t i o n c o d e) 」を表示し、このコードは、例えば再生装置によって再生時にランダムに選択される4桁コードとすることができる。

【0097】

2. ユーザがアンロックコードを購入すると、彼/彼女はまず、識別コードを引用する必要があり、この場合、使用可能な各識別コードには該当するアンロックコードが設定される。

10

【0098】

3. ユーザはアンロックコードを入力してディスクコンテンツにアクセスする。

多くのアルゴリズムが、公開/秘密キーペアのようなセキュリティコードの一致ペア (m a t c h i n g p a i r s o f s e c u r i t y c o d e s) を生成するために利用することができる。

【0099】

例示としての第2の方法の特徴は、新規の識別コードがDVDディスクの再生の各セッションに関して生成され、かつアンロックコードが各識別コードに固有である、ということである。これは、ユーザがアンロックコードを購入すると、このコードはコンテンツを1回だけアンロックするためにのみ使用することができる(1回支払い、1回再生)ということである。この構成は、幾つかのアプリケーション(例えば、競技への参加であり、彼/彼女が競技への参加を希望する度にユーザは支払いを再度行なう必要がある)に関して望ましいが、他のアプリケーションにおいては望ましくない。或るアプリケーションに関しては、1回支払い、多機能再生が可能であることが望ましい。

20

【0100】

例3:

例示としての第2の方法に変更を加えて、ユーザによる識別コードの入力を、当該ユーザに固有であるか、または少数のユーザに制限される情報を使用して可能にする。例として次のような項目を挙げることができる。

30

【0101】

1. ユーザに割り当てられる追跡可能な「カスタマー番号」(例えば企業が使用するのに適する)。

2. カスタマーのクレジットカード番号(カスタマーが他人に渡す可能性のない)。

【0102】

必要とするセキュリティレベルによって変わる形で、アクセスコードまたはアンロックコードを受け取るためのこれらの種々の選択肢は単独で用いることができるか、またはどのような組合せでも用いることができる。本発明が提供するアクセス制御及びコンテンツセキュリティによって、オーディオビジュアル製品を定義し、かつ現時点ではまだ使用することができない多くの画期的な商業的に価値のある形態で生成することができる。幾つかの例を次の表に示す。

40

【0103】

【表 1】

アプリケーション	例	必要なセキュリティ
ドリップフィード (D r i p F e e d) - ディスクがユーザに配布され、そしてコンテンツが或る時間間隔でアンロックされる。	新聞社が、多くの出来事を含む月曜日の記事を書いたディスクを提供する。アクセスコードは週の各日に発行され、このコードで閲覧対象の出来事をアンロックする。	セキュリティレベルは比較的低い-読者が、未だ公表されていない出来事をどのようにすれば閲覧することができるかについて早期に分かるはずの場合には重要ではない。
見返り (R e w a r d) - コンテンツは、ユーザが或るタスクを実行するとアンロックされる。	ディスクが或る種のパズルを含む。パズルの解読に成功すると、見返りとしてビデオシーケンスが得られる。	低い。
ペイツープレイ (P a y t o P l a y) - コンテンツは、ユーザがトランザクション (恐らく料金を支払う) を実行するとアンロックされる。	ディスクが特典内容 (b o n u s e p i s o d e) を含む。ユーザはクレジットカードによる支払いを行ってコンテンツにアクセスするコードを取得する。	中程度。権限のないアクセスを行なうと、損失を被ることになるが、発行元に更に別のコストが生じることはない。
スキルウィズプライズ (S k i l l w i t h P r i z e) - ユーザが或るタスクを実行すると懸賞金が支払われる。	ディスクがクイズのような競技を含み、そしてユーザ回答に基づいて、懸賞金をユーザが請求することができる。	中程度/高い。懸賞金の支払いによって発行元に追加のコスト及びリスクが生じる。

10

20

再生が行なわれている間、DVDビデオディスクのコンテンツは、使用者に認証を受けさせるように作用し、そして認証に合格すると有効なビデオを再生させるか、または認証に失敗すると他の或るビデオを再生させるように作用することになる。

【0104】

例 4 :

本発明の好適な実施形態をサポートするために、或るステップをディスクのコンテンツを用意している間に実行し (すなわちオーサリング)、そして特定のステップを再生中に実行してコンテンツを認証済みユーザに対してアンロックする。

30

【0105】

オーサリングの間、ディスクコンテンツは次のようにして用意される。

1. 次の要件を満たすディスク上の宛先を決めて再生を行なうために使用する関数 D を定義する。

【0106】

a. D を n 個の値 C_1, C_2, \dots, C_n によってパラメータ化し、これらの値の各々は、別々のアクセスコード成分に対応し、これらのアクセスコード成分を共に使用してコンテンツをアンロックする。

【0107】

b. 全ての使用可能な値に関する見積もりを行なって得られる D の結果は、1 ~ m の範囲に含まれる必要がある。m の値が大きくなると通常、コンテンツの保護レベルが高くなる。

40

【0108】

c. 各コード C_i の範囲は、 C_1, C_2, \dots, C_n を組み合わせた場合に、D に対して非常に多くの数の入力値を使用することができるように設定される。

d. D の固有の出力、 $D_{unlock} = D(C_1', C_2', \dots, C_n')$ が理想的に得られる或る組合せの C_1', C_2', \dots, C_n' (アンロックコード) の値が存在する。 D_{unlock} が全ての値 C_1, C_2, \dots, C_n に関して一意的である訳ではない (すなわち、複数のアンロックコードが存在する) 場合、理想的には、 D_{unlock} が得られる使用可能なこのような値の組合せの数を出来る限り少なくする必要がある。

50

【0109】

2. m個の宛先を生成して次のプロパティでプログラムを実行する。
 - e. 宛先 $D_{u n l o c k}$ は、保護対象コンテンツのスムーズな再生に対応する。
 - f. 全ての他の宛先は別のコンテンツ、または偽コンテンツを再生することになる。

【0110】

ディスクを再生している間、次のステップを実行する。

1. アクセスコード C_1, C_2, \dots, C_n を取得する。
2. 宛先 $D(C_1, C_2, \dots, C_n)$ を決定する。

【0111】

3. 宛先にジャンプする。

コード C_1, C_2, \dots, C_n は、次のいずれかの組合せを含む、上に挙げた複数の例のいずれかから取り出すことができる。

【0112】

1. ユーザに提供される PIN 番号。この番号は、例えば簡易な 4 桁コードの形をとることができる。DVD ビデオディスクに設けられるユーザインターフェースは催促を行ない、これらの催促によって、今度はユーザが 4 桁の各々を入力する。催促は数字キーパッドを表示することによって行なうことができ、数字キーパッドを通して、ユーザは標準 DVD ビデオリモートコントロールボタン (`up, down, left, right, OK`) を使用して一連の桁を選択する。

【0113】

2. 現在の実行に特有の番号であり、この番号は DVD ビデオランダム番号発生器により生成することができる。

3. クレジットカード番号のようなユーザ私有の番号、またはカスタマーコード。この番号は上の項目 1 と同様な方法により入力される。

【0114】

例 5 :

種々のアプローチが宛先関数 D の定義に使用することができる。例えば、原始関数 (`crude function`) が合格 / 失敗結果を、例えば PIN 番号に基づいて単純に返す。次の擬似コードは、ユーザが有効な PIN コード "1234" を入力すると 1 を返し、他の全てのコードに対して 2 を返す。

【0115】

```
Function D(C)
{
    if C = 1234 then return 1 else return
2
}
```

ディスク上では、2つの宛先 (1 及び 2) を設定し、1 がアンロックされる正しいコンテンツに対応し、そして 2 が、「アクセスが拒否されました」というテキストを示す静止画像のような或る別のコンテンツに対応する。このアプローチでは非常に低いレベルの保護しか行なわれない - リバースエンジニアにとっては、正しいアンロックコード及び保護対象コンテンツのディスク上の宛先も共に識別することは非常に容易である。このアプローチの利点は、実行するのが非常に簡単であり、簡単なオーサリング方法及び再生方法を必要とするだけであるということである。従って、このアプローチは、コンテンツのセキュリティが重要な要件ではない場合には十分である。

【0116】

例 6 :

少しだけよりセキュアなアプローチは、一方向性 `hash` (ハッシュ) 関数を使用することであり、このハッシュ関数は、メッセージ M (通常は任意の長さを有する) を固定長の「メッセージダイジェスト」にマッピングする関数 H であり、この場合、

1. $H(M)$ は計算が簡単であり、

2. どのようなメッセージダイジェスト MD が与えられても、 $MD = H(M)$ の構成を有する該当するメッセージ M を検出するのが難しい、すなわち H は実際には反転させることができず、かつ

3. M 及び $H(M)$ が与えられると、 $H(M') = H(M)$ となるようなメッセージ M' M を検出することが難しい。

【0117】

従って、一方向性ハッシュ関数は、任意長のメッセージを指定長の或る値 - 多くの場合「フィンガープリント (finger print)」と呼ばれる - に圧縮して、同じフィンガープリントを有する 2 つの異なるメッセージの検出を不可能にする決定的アルゴリズムである。このような関数は暗号化において広く使用され、広く使用される方法としては、MD5, SHA, 及び S n e f r u を挙げることができる。

10

【0118】

一方向性ハッシュ関数が重要であるのは、リバースエンジニアは関数を評価して必要な結果を求めることができるが、当該結果をもたらすことになる入力値を求める容易な方法が無いということである。

【0119】

ハッシュ関数 H に基づく簡単な宛先関数 D は、次のように表わされる。

Function D (C)

{

if H (C) = MD then return 1 else return

2

}

20

上の表現において、MD は予め決まっている一定のメッセージダイジェスト値であり、この値は、 $H(C)$ を正しいアンロックコードに関して評価した結果として定義される。H は反転させることができないので、リバースエンジニアにとって、宛先関数をロック対象コンテンツにジャンプさせる C の値を求めることが容易ではない。しかしながら、リバースエンジニアにとっては、上記ハッシュ関数を置き換えるか、または取り除くことは依然として比較的容易である。その理由は、所望の宛先 (すなわち「1」) はコードから容易に求めることができるからである。

【0120】

例 7 :

更にセキュアな宛先関数は、比較的多くの外見上有効な利用可能な宛先を有するかどうか依存する。例えば、関数 D (C) は入力として 4 桁の PIN コードを用いるとする。10,000 個の利用可能な宛先を有し、その内 9,999 個が「アクセスが拒否されました」という応答を出し、1 個が保護対象のコンテンツになるディスクを編集することができる。このことは、次の非常に簡単な宛先関数によって実行することができる。

30

【0121】

Function D (C)

{

return C

}

40

従って、ここでのセキュリティとは、リバースエンジニアにとって、多くの収集物の中から保護対象のコンテンツを識別することがどのくらい容易であるかに関連する。

【0122】

従って、セキュリティの弱さは、正しい宛先をアンロックするために使用するコードを求めるために使用されるテクニックになる。

1 回のみ支払い、1 回のみ再生というシナリオを考察する際においては、リバースエンジニアが、アンロックコードを購入し、そしてこれらのコードを使用して多くの回数に渡って再生を行なうことにより、保護対象コンテンツを抽出して、認証を必要としないディスクに転送するということが容易に行なうことができなくなることを保証すること

50

が重要である。

【 0 1 2 3 】

例 8 :

例示としての別の技術では、キーペアを宛先関数のパラメータとして使用し、一方のキーを競技者が生成し、そしてコンテンツをアンロックするための第 2 の一致キーをベンダーが供給する。このアプローチの一つの実施形態は次のように動作することができる。

【 0 1 2 4 】

1 . ユーザはディスクを再生し、このことによってランダムアクセスコード C_1 が、例えば 4 桁 P I N の形で生成される。コードは画面に表示される。

2 . ユーザはベンダーにコンタクトし、そして C_1 の値を供給する。

10

【 0 1 2 5 】

3 . ベンダーは、ここでも例えば 4 桁 P I N の一致コード C_2 を供給する。

4 . ユーザは C_2 を DVD ビデオ再生装置に入力すると、再生装置が内部で宛先を $D (C_1, C_2)$ として評価する。

【 0 1 2 6 】

5 . DVD は計算された宛先にジャンプする。

ここで、例示としての宛先関数は次のように表わされる。

`Function D (C1 , C2)`

{

`return (C1 + C2) mod 10000`

20

}

この場合、ベンダーから供給され、上のステップ 3 で計算されたコードは、正しい宛先が $D_{u n l o c k}$ とすると次のようにして評価される。

【 0 1 2 7 】

$C_2 = (D_{u n l o c k} - C_1) \text{ mod } 10000$ (注記: $0 \leq C_2 < 10000$)

例えば、正しい宛先が 1 2 3 4 であり、かつ DVD 再生装置が 5 6 7 8 のコードを提示する場合、コンテンツをアンロックするために必要な該当するコードは $(1 2 3 4 - 5 6 7 8) \text{ mod } 10000 = 5556$ となる。

【 0 1 2 8 】

30

例 9 :

宛先をアンロックする手段としての別の例は、次の擬似コードによって表現される。

`Ref = RND (10 , 000)` # ランダム番号 0 . . . 9 , 999 を生成する

【 0 1 2 9 】

`Ref` を表示する

`Key` を催促する

' `Key` ' はユーザが入力する 4 桁アンロックキーである

【 0 1 3 0 】

`Destination = (Ref XOR Key) mod 1000 + 1` # 1 . . . 1000 個の範囲の目標 PGC

40

PGC の宛先にジャンプする

上の表現においては、ランダムな参照番号が表示される。ユーザは、ディスクの発行者にコンタクトして一致キーを取得する必要がある。発行者はこのキーを次式により計算する。

【 0 1 3 1 】

`Key = D XOR Ref`

上の式において、' `D` ' は正しい宛先 - 本例では 3 2 1 - である。ユーザはこのキーを入力し、そして宛先を計算し、更に実行が該当する PGC にジャンプする。

【 0 1 3 2 】

50

ここで、上のPINコードは例示のために使用しているものであり、実際には、これよりも長いコードが高いセキュリティレベルを実現するために適切である。例示の宛先関数は非常に簡単であり、かつ安全ではない。実際には、一方向性ハッシュ関数は容易には反転させることができないので好ましい。

【0133】

本方法の利点は以下のとおりである。

1. 宛先コードは、ディスク上の命令を分析しても容易には求めることができない。
2. ディスク再生の度に、異なるコードが、異なるアンロックコードを要求する形で生成される。

【0134】

不利な点は、ディスクをアンロックする一致コードペアを認識しているリバースエンジニアが、ディスクのコピーを生成し、そしてランダム番号を生成する命令を、既知の生成キーを必ず生成する命令で置き換えることができることである。従って、この新規のディスクは必ず、一致ペアの既知のアンロックキーを使用してアンロックすることができる。

【0135】

例10:

本方法を別の形で強化した方法では、非可逆変換を真の原コード C_1 に適用してコードを「見えなくする」。すなわち、真の原コード C_1 は、ユーザに対して表示される第1アクセスコード C_1' を生成するためのシードとして作用する。この場合、変形実施形態は次のようになる。

【0136】

1. ユーザがディスクを再生すると、ランダムアクセスコード C_1 が、例えば4桁PINの形式で生成される。
2. (非可逆)変換 T を C_1 に適用して $C_1' = T(C_1)$ を生成し、そしてこの変換済みコードを画面に表示する。

【0137】

3. ユーザはベンダーにコンタクトし、そして C_1' の値を供給する。
4. 全ての利用可能なコード及びこれらのコードの該当する変換済み値を含む大きな予め計算されたルックアップテーブルを使用して、ベンダーはテーブルルックアップを実行して C_1 を、供給された C_1' から生成する。

【0138】

5. 生成された C_1 値を使用して、ベンダーは、ここでもまた例えば4桁PIN形式の一致コード C_2 を取得し、そして供給する。
6. ユーザが C_2 を入力すると、内部的に宛先が $D(C_1, C_2)$ として評価される。(注記: 値 C_1' はもはや必要ではない)
7. DVDは計算された宛先にジャンプする。

【0139】

本方法が前の例よりも優れる点は、明らかになる値 C_1' 及び C_2 は、ディスクコンテンツをアンロックするには十分ではないが、明らかになる値から容易に生成することができない予め変換された値 C_1 を必要とすることである。これは、リバースエンジニアが変換 T において使用される方法を求めることができたとしても、この変換は可逆ではないからである。逆変換は、ベンダーオフィスにおいて実行する必要がある。逆変換はこのオフィスにおいてテーブルルックアップを使用して行われる。通常、このテーブルは規模が非常に大きいので、高いセキュリティを提供することになる。

【0140】

幾つかの好適な実施形態について示し、そして記載してきたが、この技術分野の当業者であれば、種々の変更及び変形を、添付の請求項に規定される本発明の技術範囲から逸脱しない範囲において加え得ることが分かるであろう。

【0141】

本明細書と同時に、または本明細書よりも前に本出願に関連して申請され、かつ本明細

10

20

30

40

50

書を利用する公の調査に対して開示される全ての論文及び文書に注目が置かれ、かつ全てのこのような論文及び文書の内容は、これらの論文及び文書を参照することにより本発明の開示に含まれる。

【0142】

本明細書に開示される特徴の全て（全ての添付の請求項、要約、及び図を含む）、及び／又は上のように開示された全ての方法またはプロセスのステップの全てはどのような組合せにでも組み合わせることができるが、このような特徴及び／又はステップのうちの少なくとも幾つかが互いに相容れない組合せは除く。

【0143】

本明細書に開示される各特徴（全ての添付の請求項、要約、及び図を含む）は特に断らない限り、同じ、等価な、または同様の目的を実現する別の特徴に置き換えることができる。従って、特に断らない限り、開示する各特徴は、一般的な一連の等価な、または同様の特徴を示す一例に過ぎない。

10

【0144】

本発明はこれまでの実施形態（群）の詳細に限定されない。本発明は、本明細書に開示する複数の特徴のうちのいずれか一つの新規の特徴、またはこれらの特徴のあらゆる新規な組合せ（全ての添付の請求項、要約、及び図を含む）、或いは上のように開示した全ての方法またはプロセスの複数のステップのうちのいずれか一つの新規のステップ、またはこれらのステップのあらゆる新規な組合せに拡張することができる。

【図面の簡単な説明】

20

【0145】

【図1】本発明の好適な実施形態に用いる、オーディオビジュアル製品を生成する装置の模式図である。

【図2】本発明の好適な実施形態に用いる、オーディオビジュアル製品を再生する再生装置の模式図である。

【図3】本発明の好適な実施形態による、光ディスク記録媒体及びこの記録媒体に記録されるデータの模式図である。

【図4】本発明の好適な実施形態に使用するPGCの順序入れ替えの様子を示す模式図である。

【図5】オーディオビジュアル製品を生成する好適な方法のフロー模式図である。

30

【図6】オーディオビジュアル製品を再生する好適な方法のフロー模式図である。

【図7】例示としての元のオーディオビジュアルクリップの模式図である。

【図8】オーディオビジュアルクリップ内のシーンカットの識別情報を示す。

【図9】各シーンに細分されたオーディオビジュアルクリップを示す。

【図10】各セルに分割されたオーディオビジュアルクリップを示す。

【図11】複数のセルに挿入される偽装セルを示す。

【図12】雑混にした複数のセルを示す。

【図13】参照番号の複数のセルへの再割り当てを示す。

【図14】例示としての正しい再生シーケンス命令を示す。

【図15】正しい再生シーケンス命令のナビゲーションプログラムを示す。

40

【図16】不正な再生シーケンス命令のナビゲーションプログラムを示す。

【図17】多くの不正な再生シーケンス命令の中に埋もれた一つの正しい再生シーケンス命令を示す。

【図18】ビデオストリームを使用する好適なコンテンツスクランブル方法の概要模式図である。

【図19】複数のセルに分割され、かつ複数のビデオストリームに割り当てられるコンテンツデータの模式図である。

【図20】好適なコンテンツスクランブル方法に用いるビデオオブジェクトの模式図である。

【図21】例示としてのシーケンス生成関数の表である。

50

【図 2 2】ビデオストリーム切り替えを実行するために使用するDVDバーチャルコマンドの例である。

【図 2 3】複数のセルに分割され、かつ複数のビデオストリームに割り当てられるコンテンツデータの別の模式図である。

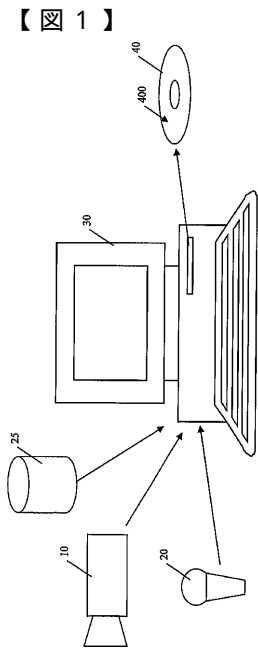


Fig. 1

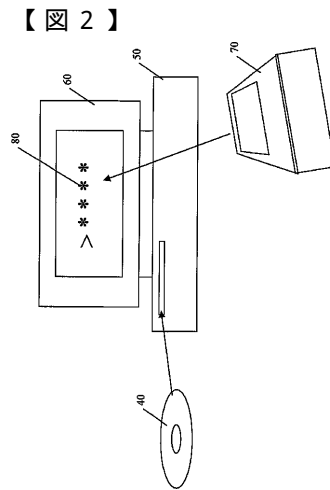


Fig. 2

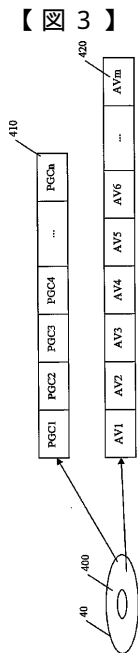


Fig. 3

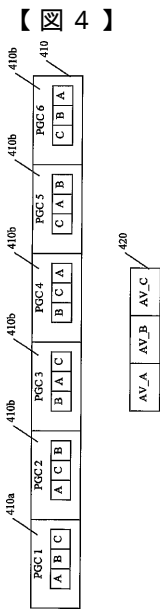
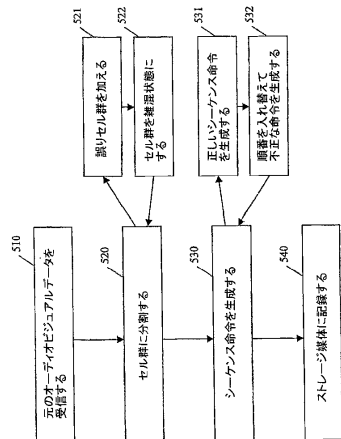
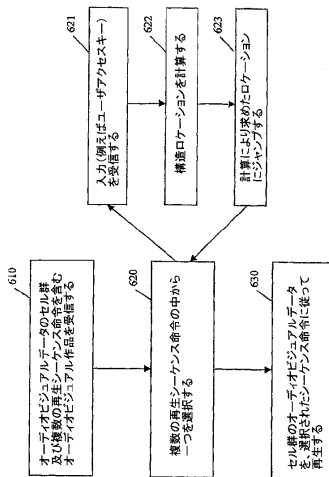


Fig. 4

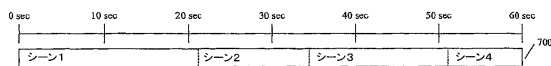
【 図 5 】



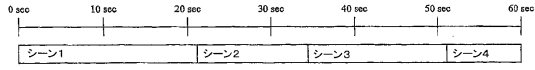
【 図 6 】



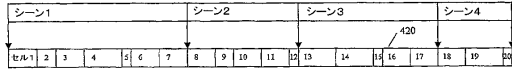
【 図 7 】



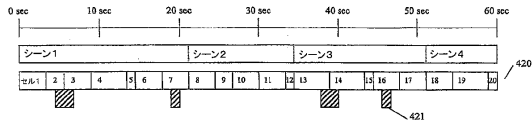
【 図 8 】



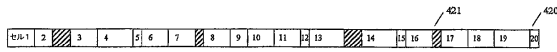
【 図 9 】



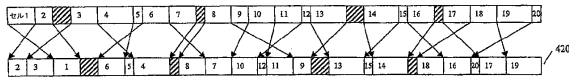
【 図 10 】



【 図 11 】



【 図 12 】



【 図 13 】

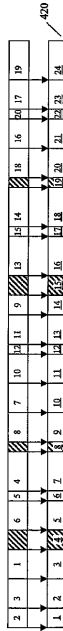


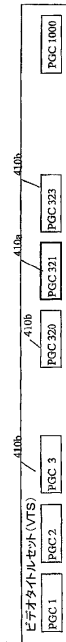
Fig. 13

【 図 14 】

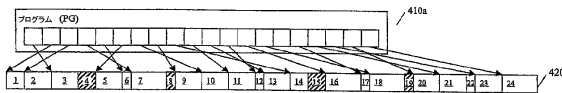
3 1 2 7 6 5 10 9 14 11 13 12 16 18 17 21 23 20 24 22

Fig. 14

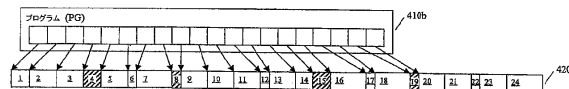
【 図 17 】



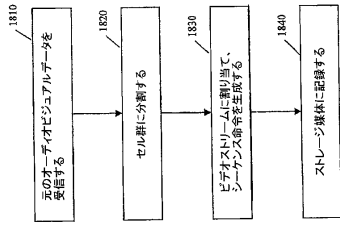
【 図 15 】



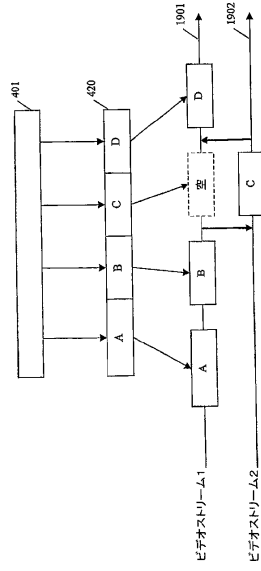
【 図 16 】



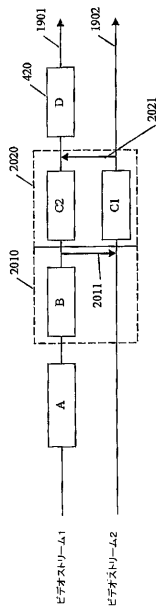
【 図 18 】



【 図 19 】



【 図 20 】



【 図 21 】

n	r_n	$r_n \bmod 4 + 1$
0	0	1
1	3	4
2	7	4
3	10	3
4	5	2
5	4	1
6	14	3
7	15	1
8	13	2
9	6	4
10	15	4
11	6	3
12	11	4
13	12	1
14	11	4
15	2	3

Fig. 21

【 図 2 2 】

命令	コメント
GPRM0 = A	# 設定初期値
GPRM1 = B	
GPRM2 = C	
GPRM5 = m	
SPRM3 = アングルスโตรム番号	
MUL GPRM5 GPRM0	# m = m * A
ADD GPRM5 GPRM1	# m = m * A + B
MOD GPRM5 GPRM2	# m = (m * A + B) mod C
MOV SPRM3 GPRM5	# angle = m
MOD SPRM3 4	# angle = m mod 4
ADD SPRM3 1	# angle = (m mod 4) + 1

【 図 2 3 】

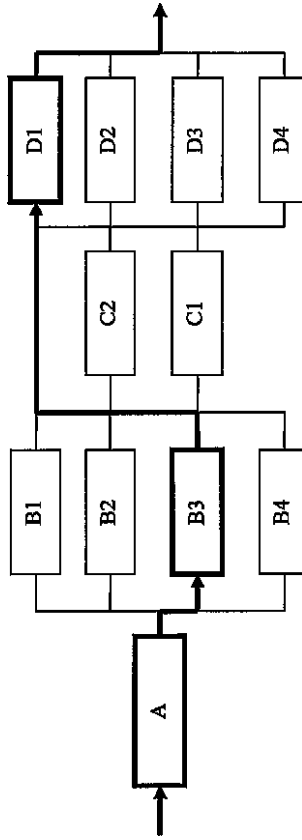


Fig. 23

フロントページの続き

(51)Int.Cl.

F I

G 1 1 B 20/10 3 2 1 Z

審査官 金子 秀彦

(56)参考文献 特開2002-314929(JP,A)
米国特許第06430360(US,B1)
国際公開第02/073617(WO,A1)
特開2001-167517(JP,A)

(58)調査した分野(Int.Cl., DB名)

G11B 20/10

H04N 5/76

H04N 5/92

H04N 5/93