

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-518294

(P2007-518294A)

(43) 公表日 平成19年7月5日(2007.7.5)

(51) Int. Cl.		F I				テーマコード (参考)
H04N	7/167	(2006.01)	H04N	7/167	Z	5C164
H04L	9/14	(2006.01)	H04L	9/00	641	5J104

審査請求 未請求 予備審査請求 未請求 (全 18 頁)

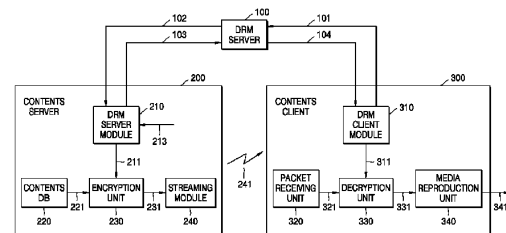
(21) 出願番号	特願2006-542508 (P2006-542508)	(71) 出願人	506193671
(86) (22) 出願日	平成16年12月8日 (2004. 12. 8)		デヤン・ファンデーション
(85) 翻訳文提出日	平成18年6月6日 (2006. 6. 6)		大韓民国・ソウル・143-747・クワンジンギョ・クンジャードン・98
(86) 国際出願番号	PCT/KR2004/003213	(71) 出願人	503447036
(87) 国際公開番号	W02005/055075		サムスン エレクトロニクス カンパニー リミテッド
(87) 国際公開日	平成17年6月16日 (2005. 6. 16)		大韓民国キョンギド、スウォンシ、ヨントンク、マエタンードン 416
(31) 優先権主張番号	10-2003-0088795	(74) 代理人	100064908
(32) 優先日	平成15年12月8日 (2003. 12. 8)		弁理士 志賀 正武
(33) 優先権主張国	韓国 (KR)	(74) 代理人	100089037
			弁理士 渡邊 隆
		(74) 代理人	100108453
			弁理士 村山 靖彦

最終頁に続く

(54) 【発明の名称】 動画ファイルの暗号化方法及びそれを利用したデジタル著作権の管理方法

(57) 【要約】

本発明は、動画ファイルの暗号化方法及びそれを利用したデジタル著作権の管理方法を提供する。本発明は、動画ファイルのメタデータからリアルタイムストリーミングの単位となるビデオサンプルの位置情報を抽出し、各ビデオサンプルの位置情報に基づいてビデオサンプルを抽出し、抽出された各ビデオサンプルのビデオサンプルヘッダ内のスタートコードを除いた残りの部分に対して、あらかじめ決定された暗号化情報に基づいて暗号化し、暗号化したビデオサンプルを再度組み合わせることによって、復号化した動画ファイルを生成する。これにより、MPEG4ファイルのフォーマットを維持しつつVOP単位でファイルを暗号化するため、完成した形態のファイルフォーマットに容易に適用可能であると共にストリーミングサービスが可能である。



【特許請求の範囲】

【請求項 1】

複数のビデオサンプルを含む動画ファイルの暗号化方法において、
前記複数のビデオサンプルのうち少なくとも一つのビデオサンプルの位置情報を抽出するステップと、
前記抽出された位置情報に基づいて、対応するビデオサンプルを抽出するステップと、
前記抽出されたビデオサンプルのうち、前記抽出されたビデオサンプルを表すビデオサンプルの識別情報を除いた残りの部分に対して、あらかじめ決定された暗号化情報に基づいて暗号化するステップと、
前記暗号化したビデオサンプルを前記動画ファイルに再挿入することによって、暗号化した動画ファイルを生成するステップと、
を含むことを特徴とする暗号化方法。 10

【請求項 2】

前記暗号化情報は、暗号化キー及び暗号化方式を含むことを特徴とする請求項 1 に記載の暗号化方法。

【請求項 3】

前記暗号化キーは、デジタル著作権管理サービスを利用して伝送されることを特徴とする請求項 2 に記載の暗号化方法。

【請求項 4】

前記暗号化方式は、暗号化以前のメッセージワードと暗号化後のコードワードとのビット数が同じになるように暗号化する方式であることを特徴とする請求項 2 に記載の暗号化方法。 20

【請求項 5】

前記暗号化方式は、データ暗号化標準及び韓国標準暗号化アルゴリズムのうち何れか一つであることを特徴とする請求項 4 に記載の暗号化方法。

【請求項 6】

前記動画ファイルは、MPEG規格によるファイルであることを特徴とする請求項 1 に記載の暗号化方法。

【請求項 7】

前記動画ファイルは、MPEG4規格によるファイルであり、前記ビデオサンプルは、ストリーミング単位を表すチャンクに含まれたVOPであることを特徴とする請求項 1 に記載の暗号化方法。 30

【請求項 8】

前記ビデオサンプルの位置情報を抽出するステップは、
VOPのメタデータを保存するムーブアトム内の下位アトムのうち、サンプルテーブルアトム内のメタデータからチャンクサイズ、チャンクオフセット、及びサンプルサイズを抽出するステップと、
前記抽出されたチャンクサイズ、チャンクオフセット、及びサンプルサイズに基づいて各VOPの位置を計算するステップと、
を含むことを特徴とする請求項 7 に記載の暗号化方法。 40

【請求項 9】

前記暗号化情報は、暗号化モードをさらに備え、
前記暗号化モードは、VOPのうちI-VOPのみを暗号化する第1モード、VOPのうちB-VOP及びP-VOPのみを暗号化する第2モード、及びVOPのうちI、B、P-VOPを何れも暗号化する第3モードのうち何れか一つであることを特徴とする請求項 8 に記載の暗号化方法。

【請求項 10】

前記暗号化情報は、暗号化されるVOPを識別するためのVOP IDをさらに含むことを特徴とする請求項 8 に記載の暗号化方法。

【請求項 11】

前記ムーブアトムは、デジタル著作権管理アトムを含み、前記デジタル著作権管理アトムは、前記暗号化情報をメタデータとして含むことを特徴とする請求項 8 に記載の暗号化方法。

【請求項 12】

前記デジタル著作権管理アトムは、ムーブアトムの最下位アトムとして保存されることを特徴とする請求項 11 に記載の暗号化方法。

【請求項 13】

前記デジタル著作権管理アトムは、暗号化フラッグ及びエントリーテーブルを備え、前記暗号化するステップは、前記暗号化フラッグが第 1 類型に設定されれば、あらゆる VOP を暗号化し、第 2 類型に設定されれば、前記エントリーテーブル内に含まれた VOP ID に該当する VOP のみを暗号化することを特徴とする請求項 11 に記載の暗号化方法。

10

【請求項 14】

所定の暗号化情報に基づいて、ビデオサンプル単位で選択的に暗号化された動画ファイルを復号化する方法であって、

前記動画ファイル内の各ビデオサンプルの開始を識別するビデオサンプル識別情報を検出するステップと、

前記ビデオサンプル識別情報に基づいて各ビデオサンプルを抽出するステップと、

前記暗号化情報に基づいて、前記抽出されたビデオサンプルのうち暗号化されたビデオサンプルを抽出するステップと、

20

前記暗号化情報に対応する復号化情報に基づいて、前記暗号化されたビデオサンプルを復号化するステップと、

前記復号化されたビデオサンプルを再挿入することによって、復号化された動画ファイルを再生するステップと、を含み、

前記暗号化されたビデオサンプルは、前記ビデオサンプル識別情報を除いた残りの部分のみが暗号化されたことを特徴とする復号化方法。

【請求項 15】

前記暗号化情報は、暗号化キー及び暗号化方式を含むことを特徴とする請求項 14 に記載の復号化方法。

【請求項 16】

30

前記復号化情報は、デジタル著作権管理サービスを利用して伝送されることを特徴とする請求項 14 に記載の暗号化方法。

【請求項 17】

前記暗号化方式は、暗号化以前のメッセージワードと暗号化以後のコードワードとのビット数が同じになるように暗号化する方式であることを特徴とする請求項 15 に記載の暗号化方法。

【請求項 18】

前記暗号化方式は、データ暗号化標準及び韓国標準暗号化アルゴリズムのうち何れか一つであることを特徴とする請求項 17 に記載の暗号化方法。

【請求項 19】

40

前記暗号化情報は、暗号化モードをさらに含み、

前記暗号化モードは、VOP のうち I-VOP のみを暗号化する第 1 モード、VOP のうち B-VOP 及び P-VOP のみを暗号化する第 2 モード、及び VOP のうち I、B、P-VOP を何れも暗号化する第 3 モードのうち何れか一つであることを特徴とする請求項 15 に記載の暗号化方法。

【請求項 20】

前記暗号化情報は、暗号化される VOP ID を識別する VOP ID をさらに含むことを特徴とする請求項 15 に記載の暗号化方法。

【請求項 21】

コンテンツサーバ及びコンテンツクライアントを利用するデジタル著作権の管理方法で

50

あって、

コンテンツサーバ及びコンテンツクライアントを通じて所定の動画ファイルに対するユーザ認証過程を行うことによって、暗号化情報及び復号化情報を受信するステップと、

前記受信された暗号化情報に基づいて、該当動画ファイルをビデオサンプル単位で選択的に暗号化するステップと、

前記暗号化された動画ファイルをストリーミングサーバを通じて伝送するステップと、

前記伝送された動画ファイルから暗号化されたビデオサンプルを抽出するステップと、

前記受信された復号化情報を利用して、前記ビデオサンプルを識別するビデオサンプル識別情報を除いた前記ビデオサンプルの残りの部分を復号化するステップと、

前記復号化されたビデオサンプルを再挿入することによって、復号化された動画ファイルをリアルタイムで再生するステップと、

を含むことを特徴とする方法。

【請求項 2 2】

前記暗号化情報及び復号化情報を受信するステップは、

前記コンテンツクライアントが所定の動画ファイルに対するユーザ認証要請を D R M サーバに伝送するステップと、

前記 D R M サーバは、ユーザ認証を行い、ユーザの認証に関する情報を含む D R M 認証情報を前記コンテンツサーバに伝送するステップと、

前記コンテンツサーバは、前記 D R M 認証情報に基づいて暗号化キーを生成し、前記暗号化キー及びユーザ入力による暗号化オプション情報に基づいて前記暗号化情報を生成するステップと、

前記コンテンツサーバが前記暗号化情報を前記 D R M サーバに伝送するステップと、

前記 D R M サーバは、前記暗号化情報に対応する前記復号化情報を前記コンテンツクライアントに伝送するステップと、

を含むことを特徴とする請求項 2 1 に記載の方法。

【請求項 2 3】

前記動画ファイルは、M P E G 規格によるファイルを含むことを特徴とする請求項 2 2 に記載の方法。

【請求項 2 4】

前記動画ファイルは、M P E G 4 規格によるファイルを含み、前記ビデオサンプルは、ストリーミング単位のチャンク内の V O P であり、

前記暗号化するステップは、

該当 M P E G 4 ファイルのムーブアトムをパースングすることによって各 V O P の位置情報を生成するステップと、

前記各 V O P の位置情報に基づいて、前記 M P E G 4 ファイルのメディアデータアトム内の各 V O P を抽出するステップと、

前記抽出された各 V O P を、V O P ヘッダ内のスタートコードを除いた残りの部分に対して、あらかじめ決定された暗号化情報に基づいて暗号化するステップと、

前記暗号化した V O P を再度組合わせることによって、復号化した M P E G 4 ファイルを生成するステップと、

を含むことを特徴とする請求項 2 2 に記載の方法。

【請求項 2 5】

前記位置情報を生成するステップは、

前記ムーブアトム内の下位アトムのうち、サンプルテーブルアトムからチャンクサイズ、チャンクオフセット及びサンプルサイズを抽出するステップと、

前記抽出されたチャンクサイズ、チャンクオフセット及びサンプルサイズに基づいて、各 V O P の位置情報を計算するステップと、

を含むことを特徴とする請求項 2 4 に記載の方法。

【請求項 2 6】

前記暗号化情報は、暗号化キー及び暗号化方式を含むことを特徴とする請求項 2 1 に記

10

20

30

40

50

載の暗号化方法。

【請求項 27】

前記暗号化方式は、暗号化以前のメッセージワードと暗号化以後コードワードとのビット数が同じになるように暗号化する方式であることを特徴とする請求項 26 に記載の暗号化方法。

【請求項 28】

前記暗号化方式は、データ暗号化標準及び韓国標準暗号化アルゴリズムのうち何れか一つであることを特徴とする請求項 27 に記載の暗号化方法。

【請求項 29】

前記暗号化された VOP を抽出するステップは、
前記伝送されたパケットの伝送プロトコルヘッダをデカプセル化することによって、パケットのデータ部分のみを抽出するステップと、
前記パケットのデータ部分を組合わせることによって、前記 VOP が結合されたデータストリームを生成するステップと、
前記結合されたデータストリーム内で各 VOP を識別する VOP 識別情報を検出するステップと、
前記 VOP 識別情報に基づいて各 VOP を抽出するステップと、
前記暗号化情報に基づいて、前記抽出された VOP のうち暗号化された VOP を抽出するステップと、
を含むことを特徴とする請求項 21 に記載の復号化方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、動画ファイルの暗号化方法及びそれを利用したデジタル著作権の管理方法に係り、さらに詳細には、動画ファイルのフォーマットを維持しつつファイルを暗号化することによって、デジタル著作権の管理下でストリーミングサービスを可能にする暗号化方法及びデジタル著作権の管理方法に関する。

【背景技術】

【0002】

現在、マルチメディアデータは、ダウンロードサービスまたはストリーミングサービスの形態でサービスの提供者からユーザに提供されている。ダウンロードサービスは、再生の単位となる完全なマルチメディアファイルをサービス提供者のコンピュータからユーザのコンピュータに完全にダウンロードした後に再生することであり、ストリーミングサービスは、サービス提供者が、再生の単位となるファイルをリアルタイムで再生可能な部分に分割してユーザに伝送した後、ユーザは、前記伝送された部分をリアルタイムで再生するサービスをいう。

【0003】

サービス提供者が、このうちいかなる形態を使用しても、ユーザは、該当マルチメディアデータに対する適法な権利を取得する過程が先行されねばならない。このための先行条件として、正当な権利を取得していないユーザの該当ファイルに対するアクセスを防止せねばならず、このためにマルチメディアファイルは暗号化される。

【0004】

デジタル著作権管理 (Digital Right Management : DRM) は、正当な権利を有するユーザのみを暗号化されたデータにアクセスさせるあらゆる構造のソリューションとして定義される。一般的に、このようなデジタル著作権管理システムは、コンテンツ提供者、ユーザ及びデジタル著作権管理サーバなどを含み、電子支払い手続き、ユーザ認証手続き及び共用キー構造 (Public Key Infrastructure : PKI) を含む。

【0005】

最も一般的に使用されるデジタル著作権管理の方法は、MPEG ファイル自体を暗号化

してユーザに伝送した後、暗号化したファイルを復号できるキーを、ユーザ認証手続を通じて正当な権利を有するユーザに提供することである。ユーザ認証手続は、電子支払い手続を含み、キーの伝送には、共用キー構造が使用されうる。

【0006】

しかし、このような暗号化方法は、ストリーミングサービスでは使用されえない。なぜなら、復号化は、ファイル全体をダウンロードした後になって初めて可能であるためである。すなわち、ユーザキーは、DRMサーバから伝送されても、暗号化の対象となるファイル全体をダウンロードされる以前には、該当映像を再生できない。

【0007】

また、暗号化方法の他の方法として、動画ファイルのコーディング過程で離散コサイン変換の係数、すなわち、AC値またはDC値を暗号化する方法がある。 10

【0008】

しかし、この方法は、完成した動画ファイルを暗号化するものではなく、動画ファイルのエンコーディング過程に暗号化過程を追加せねばならないので、完成したMPEGファイルに対しては容易に適用できない。また、コンテンツ提供者が、動画ファイルの生成過程に自身に特定された暗号化アルゴリズムを適用する必要がある場合、コンテンツ提供者は、動画ファイルの提供者に従属されてサービスを提供しなければならないので、事業過程で不利益をもたらす。これは、オンラインコンテンツ事業を妨げる。

【発明の開示】

【発明が解決しようとする課題】

20

【0009】

したがって、本発明は、前記課題を解決するためになされたものであって、ストリーミングサービスに適用可能であると共に、動画ファイルの生成過程に関係なく完成した動画ファイルに容易に適用可能な暗号化方法及びそれを利用したデジタル著作権の管理方法を提供することを目的とする。

【課題を解決するための手段】

【0010】

前記課題を解決するための本発明は、メディアデータ領域及びメタデータ領域を含む動画ファイルの暗号化方法であって、動画ファイルのメタデータからリアルタイムストリーミングの単位となるビデオサンプルの位置情報を抽出するステップと、前記各ビデオサンプルの位置情報に基づいて前記ビデオサンプルを抽出するステップと、前記抽出された各ビデオサンプルのビデオサンプルヘッダ内のスタートコードを除いた残りの部分に対して、あらかじめ決定された暗号化情報に基づいて暗号化するステップと、前記暗号化したビデオサンプルを再度組合わせることによって、復号化した動画ファイルを生成するステップと、を含む。 30

【0011】

また、本発明において、前記オフセットを抽出するステップは、前記ムーブアトム内の下位アトムのうち、ビデオメディア情報アトムの存否を検査するステップと、前記ビデオメディア情報アトムが存在する場合に、前記ムーブアトム内の下位アトムのうちサンプルテーブルアトム内のチャンクサイズのアトム、チャンクオフセットアトム及びサンプルサイズアトムからチャンクサイズ、チャンクオフセット及びサンプルサイズを抽出するステップと、前記抽出されたチャンクサイズ、チャンクオフセット及びサンプルサイズに基づいて、各VOPのオフセットを計算するステップと、を含む。 40

【0012】

また、本発明は、所定の暗号化情報に基づいてVOP単位で暗号化されたMPG4ファイルを復号化する方法であって、前記MPG4ファイル内の各VOPのスタートコードを検出するステップと、前記スタートコードを基準に各VOPを抽出するステップと、前記暗号化情報に基づいて、前記抽出されたVOPのうち暗号化されたVOPを抽出するステップと、前記暗号化情報に対応する復号化情報に基づいて、前記暗号化されたVOPを復号化するステップと、前記復号化されたVOPを再度組合わせることによって、復号 50

化されたMPEG4ファイルを生成するステップと、を含み、前記暗号化情報は、復号化キー、暗号化方式、暗号化モード及びVOPIDを含む。

【0013】

また、本発明は、デジタル著作権の管理方法であって、コンテンツサーバ及びコンテンツクライアントが、DRMサーバを通じて所定のMPEG4ファイルに対するユーザ認証過程を行うことによって暗号化情報及び復号化情報を受信するステップと、前記コンテンツサーバが、前記暗号化情報に基づいて該当MPEG4ファイルをVOPI単位で暗号化するステップと、前記暗号化されたMPEG4ファイルのVOPIを含むパケットを、ストリーミングサーバを通じて前記コンテンツクライアントに伝送するステップと、前記コンテンツクライアントが、前記パケットから暗号化されたVOPIを抽出するステップと、前記抽出されたVOPIを、前記復号化情報を利用して復号化するステップと、前記復号化されたVOPIを再度組合わせることによって、復号化されたMPEG4ファイルをリアルタイムで再生するステップと、を含む。

10

【発明を実施するための最良の形態】

【0014】

以下、添付された図面を参照して、本発明に係る望ましい一実施例を詳細に説明する。

図1は、動画ファイルフォーマットを示す図面である。動画ファイルは、MPEG1、MPEG2及びMPEG4ファイルフォーマットを含む。各動画ファイルは、ユーザデータが含まれるメディアデータ領域と、ユーザデータに関する位置及び大きさ、その他の再生に必要なメタデータを保存するメタデータ領域とに分けられる。以下では、MPEG4ファイルフォーマットについて本発明を適用する概念を説明する。

20

【0015】

MPEG4ファイル10は、複数のアトム20、21、22、30、31、32を含む。各アトムは、下位のアトムを有することによって階層的な構造を形成する。このとき、上位アトムをコンテナアトム、下位アトムをリーフアトムという。最も上位のアトムは、2個のアトムであり、ムーブアトム及びメディアデータアトムアトムである。メディアデータアトム30は、MPEG4ファイル内に保存されるユーザメディアデータ、すなわち、オーディオまたはビデオデータなどが保存される空間であり、ムーブアトム20は、メディアデータに関する情報、すなわち、メタデータが保存される空間である。メディアデータアトム30は、複数のビデオオブジェクトプレーン31、32、・・・及び複数のオーディオデータを備える。

30

【0016】

図2は、本発明に係るデジタル著作権管理の概要図である。デジタル著作権管理のための解決策は、コンテンツサーバ200、コンテンツクライアント300及びDRMサーバ100を備える。コンテンツサーバ200は、メディアデータをユーザに提供し、DRMサーバモジュール210、コンテンツデータベース220、コンテンツ暗号化部230及びストリーミングモジュール240を備える。コンテンツクライアント300は、コンテンツサーバからコンテンツを伝送されて再生し、DRMクライアントモジュール310、パケット受信部320、コンテンツ復号化部330及びメディア再生部340を備える。

【0017】

DRMサーバ100は、コンテンツサーバ200とクライアント300との間のユーザ認証を通じたキー伝送を行う。コンテンツクライアント300内のDRMクライアントモジュール310が、ユーザ認証要請101をDRMサーバ100に送れば、DRMサーバ100は、電子支払システム（図示せず）を利用してユーザ認証を行う。ユーザ認証が完了すれば、DRMサーバ100は、ユーザ認証と関連したユーザ情報などを利用してDRM認証情報102を生成し、生成されたDRM認証情報をコンテンツサーバ200に伝送する。

40

【0018】

コンテンツサーバ200内のDRMサーバモジュール210は、コンテンツサーバ200から伝送されたDRM認証情報102から暗号化キーを生成し、生成された暗号化キー

50

及びユーザ入力による暗号化オプション情報 213 を、暗号化情報 211 として暗号化部 230 に伝送する。暗号化オプション情報 213 は、暗号化方式の種類、暗号化対象 VOP ID 及び暗号化モードの種類に関する情報などを含む。

【0019】

コンテンツサーバ 200 内の DRM サーバモジュール 210 及びコンテンツクライアント 300 内の DRM クライアントモジュール 310 は、DRM サーバ 100 とユーザ認証動作を行う。DRM サーバモジュール 210 は、DRM サーバ 100 から DRM 認証情報 102 を受信し、これを利用して暗号化キーを生成する。また、DRM サーバモジュール 210 は、暗号化キー及びユーザ入力による暗号化オプション情報 213 を含む暗号化情報 211 を暗号化部 230 に伝送する。また、DRM サーバモジュール 210 は、暗号化情報 211 及び DRM サービスに必要なその他の情報などを利用して DRM 暗号化情報 103 を生成し、DRM サーバ 100 に伝送する。

10

【0020】

DRM サーバ 100 は、DRM サーバモジュール 210 から DRM 暗号化情報 103 を受信して、ユーザ認証を通じた多様な情報を含めて DRM 復号化情報 104 を生成し、これを DRM クライアントモジュール 310 に伝送する。もし、DRM サービスが対称キーの構造を使用すれば、DRM 暗号化情報 103 に含まれた暗号化キーと DRM 復号化情報 104 内に含まれた復号化キーとが同じであるが、DRM サービスが非対称キーの構造を使用すれば、暗号化キーと復号化キーとは相異なるので、DRM 暗号化情報 103 と DRM 復号化情報 104 とが有する内容は相異なる。

20

【0021】

DRM クライアントモジュール 310 は、DRM サーバ 100 から DRM 復号化情報 104 を受信して復号化情報 311 を抽出し、DRM 復号化 330 は、復号化情報 311 を利用して、受信した動画ファイルを復号化する。

【0022】

図 2 で、コンテンツサーバ 200 内の暗号化部 230 は、コンテンツデータベース 220 からコンテンツ 221 を伝送されて、これを暗号化することによって暗号化したコンテンツ 231 を生成する。本発明の特徴によって、コンテンツ 221 及び暗号化したコンテンツ 231 は、図 1 に示すものと同じ MPEG 4 ファイルのフォーマットを有する。

【0023】

図 3 は、本発明に係る MPEG 4 ファイルの暗号化方法を示すフローチャートである。本発明は、MPEG 4 ファイルをファイル全体ではなく、VOP 単位で暗号化することの特徴とする。暗号化される VOP は、暗号化オプション情報 213 により選択可能である。暗号化方式は、データ暗号化標準 (Data Encryption Standard: DES) または 128 ビット方式の韓国標準暗号化アルゴリズム (SEED) のようなブロック暗号化方式を使用する。このような暗号化方式は、ブロック暗号化方式であるので、既存の MPEG 4 ファイルの大きさ及び形式を変化させない。したがって、暗号化以後の MPEG 4 ファイルと暗号化以前の MPEG 4 ファイルとは、大きさ及びフォーマットが変わらないので、既存の MPEG 4 ファイルの再生アルゴリズムの修正なしに適用可能である。また、暗号化は、VOP 単位で行われるが、各 VOP の最初の 4 バイトは暗号化しない。最初の 4 バイトは、スタートコードであって、コンテンツクライアント側から VOP の抽出に使用されるためである。

30

40

【0024】

コンテンツ DB から受信された MPEG 4 ファイルのムーブアトムから各 VOP のオフセットを抽出する (ステップ 301)。VOP のオフセットとは、MPEG 4 ファイル内の各 VOP の位置情報をいう。各 VOP のオフセットに基づいて、暗号化オプション情報 213 により選択された VOP を抽出する (ステップ 302)。抽出された VOP を、DES または SEED を利用して暗号化する (ステップ 303)。暗号化した VOP を暗号化していない VOP と再度組み合わせることによって、暗号化された MPEG 4 ファイルを生成する (ステップ 304)。

50

【0025】

以下、図4ないし図6を参照して、MPEG4ファイルの各VOPのオフセットを抽出する過程を説明する。

【0026】

図4は、MPEG4ファイルのメディアデータアトムの構成を示す図面である。MPEG4ファイルフォーマットによって、メディアデータアトムは、実際のメディアデータが存在する部分であるチャンクと、メディアデータが存在していない部分である未使用部分と、を含む。チャンクは、ビデオチャンク及びオーディオチャンクを含み、各チャンクは、複数のサンプルに分けられる。チャンクの内部に含まれたメディアデータがビデオデータである場合、サンプルは、VOPである。

10

【0027】

図5Aは、MPEG4ファイルのムーブアトムの構成を示す図面である。ムーブアトム510は、下位アトムとして複数のトラックアトム(track1)520を含み、各トラックアトム520は、下位アトムとしてメディアアトム530を含み、メディアアトム530は、下位アトムとしてメディア情報アトム540を含み、メディア情報アトム540は、下位アトムとしてサンプルテーブルアトム550を含む。

【0028】

各アトムの最初の4バイトは、アトムのサイズ情報を有し、その次の4バイトは、アトムの類型情報を有し、残りの領域は、各アトムが表すメタデータ情報を有する。メディア情報アトム540は、下位アトムとしてビデオ情報アトム541を有する。ビデオ情報アトム541は、該当メディアデータがビデオデータであることを表す。サンプルテーブルアトム550は、下位アトムとしてチャンクサイズのアトム551、サンプル数アトム552及びサンプルサイズアトム553を有する。

20

【0029】

図5Bは、チャンクサイズのアトム、サンプル数アトム及びサンプルサイズアトムの内部構成を示す図面である。

【0030】

図5Bの最初の図面で、チャンクサイズのアトム551は、メタデータ領域に各チャンクが有するサンプルの数に関する情報を含む。第1チャンク611及び第4のチャンク612は、14個のビデオサンプルを有し、第10のチャンク613は、13個のビデオサンプルを有するということが分かる。図5Bの二番目の図面で、チャンク位置アトム552は、メタデータ領域に各チャンクの位置情報を含む。1番目のチャンク614は、40番目のビットから表され、10番目のチャンク615は、607848ビットから表されるということが分かる。図5Bの三番目の図面で、サンプルサイズアトム553は、各サンプルの大きさに関する情報を表す。1番目のサンプル617は、12604ビットの大きさを有するということが分かる。

30

【0031】

MPEG4ファイル内の各VOPのオフセットを抽出する過程は、各メタデータのパーシングを通じて行われる。まず、メディア情報アトム540内にビデオメディア情報アトム541が存在しているかを検査することによって、該当メディアデータがビデオデータであるか否かを確認する。もし、ビデオデータであれば、次の下位アトムであるサンプルテーブルアトム550にパーシングしてメタデータを抽出する。

40

【0032】

前記三つのアトムに保存された情報の組合わせからサンプル、すなわち、VOPのオフセットに関する情報を抽出できる。図5Bの1番目の図面で、1番目のチャンクの大きさ、すなわち1番目のチャンクに含まれたサンプル数は14個であり、二番目の図面で、1番目のチャンクのオフセットは40ビットであり、1番目のサンプルの大きさは、12604ビットである。したがって、二番目のサンプルのオフセットは、 $40 + 12604 = 12644$ ビットである。このような方式で、あらゆるサンプル、すなわち、VOPのオフセットを抽出できる。

50

【0033】

図6Aないし図6Cは、多様な方式で暗号化した暗号化されたMPEGファイルの再生画面を示す。

【0034】

暗号化されるVOPは、暗号化オプション情報により選択可能である。暗号化オプション情報は、ユーザによりDRMサーバモジュールに入力され、暗号化キーと共に暗号化部に伝送されて暗号化に使用される。

【0035】

暗号化されるVOPの選択は、暗号化モードの選択または暗号化IDの選択により行われる。暗号化モードは、あらゆるI-VOPを暗号化する第1モード、あらゆるB-VOP及びP-VOPを暗号化する第2モード、及びあらゆるI、B、P-VOPを暗号化する第3モードに分けられる。暗号化IDの選択は、暗号化オプション情報として入力された暗号化番号に該当するVOPのみを暗号化する。この時、暗号化されるVOPは、種類に関係なく選択される。

10

【0036】

図6Aで、左側映像は、暗号化以前の映像であり、右側映像は、第1モードで暗号化した後のMPEG映像である。I-VOPは、イントラコーディングされたVOPであるので、マクロブロック内にあらゆる映像情報が含まれている。したがって、イントラブロック情報が完全に喪失されたということが分かる。また、I、P、B-VOPの参照位置が変わるので、原本ファイルとは全く異なる映像を再生する。

20

【0037】

図6Bで、左側映像は、暗号化以前の原本映像であり、右側映像は、第2モードで暗号化したMPEG映像である。B-VOP及びP-VOPは、イントラコーディングされたマクロブロック及びモーションベクトルに関する情報が共存する。したがって、第1モードに比べて映像客体の確認がさらに可能になるということが分かる。これは、P-VOP内部のモーションベクトルは暗号化されたが、I-VOP内部のイントラブロックの影響によって、連続するフレームの中間画面に時々完全な画面が発生可能である。但し、モーションベクトルが暗号化されるので、各客体の移動経路は不規則になるということが分かる。

30

【0038】

図6Cで、右側映像は、第3モードで暗号化したMPEG映像を表す。第3モードは、あらゆるVOPを暗号化するので、最も完全に暗号化された映像を生成する。暗号化するVOPの数が多くなるほど、暗号化の性能は向上するが、復号化にさらに多くの資源を使用する。

【0039】

暗号化が行われれば、暗号化されたVOPを再度組合わせることによって、暗号化された新たなMPEGファイルが生成される。生成された暗号化MPEG4ファイルは、ストリーミングモジュールによりコンデンツクライアント300にストリーミングされる。ストリーミングのためにMPEG4ファイルはパケット化されねばならない。

【0040】

図7は、ストリーミングモジュールによりパケット化された伝送パケットの内部構造を示す図面である。また、図2で、ストリーミングモジュール240は、暗号化されたMPEG4ファイルを伝送されて、パケット化することによって伝送パケット241を生成する。図7で、経時的に伝送される4個の伝送パケットが表されている。各伝送パケット710、720、730、740は、伝送プロトコルヘッダ711、712、721、722、731、732、741、742及び伝送データ713、724、733、743、744を含む。伝送プロトコルヘッダは、伝送経路によって異なり、一般的に、リアルタイム伝送プロトコル712及びユーザデータグラムプロトコル711が使用される。

40

【0041】

1番目の伝送パケット710は、伝送データとして1番目のVOPの一部713を含み

50

、二番目の伝送パケット 720 は、伝送データとして 1 番目の VOP の残りの一部 723 及び二番目の VOP の一部 724 を含む。三番目の伝送パケット 730 は、二番目 VOP の他の一部 733 を含む、四番目の伝送パケット 740 は、二番目の VOP の残りの一部 743 及び三番目の VOP の一部 744 を含む。各伝送パケットが VOP の一部を伝送データとして有する理由は、VOP の大きさが相異なり、伝送パケットの長さで伝送される VOP の大きさが一致していないためである。図 7 で、斜線の VOP の一部 724、733、743 は、暗号化された VOP を表す。

【0042】

ストリーミングモジュール 240 は、コンテンツサーバ内になく、独立的なサーバとしても具現可能である。この場合には、暗号化部 230 からストリーミングサーバ 234 への MPEG4 ファイルの伝送は、インターネットのような通信網を通じて行われる。 10

【0043】

図 8 は、コンテンツクライアント 300 が伝送パケット 241 を受信して MPEG4 ファイルを再生する方法を表すフローチャートである。

【0044】

コンテンツクライアント 300 内のパケット受信部 320 は、コンテンツサーバ 200 から伝送パケット 241 を受信して VOP を抽出する。VOP 抽出過程は、パケット受信部 320 内のバッファに入るパケットを監視することによって行われる。まず、パケット受信部 320 は、伝送パケット 241 を伝送されて、パケットの伝送プロトコルヘッダ 711、712 など除去することによってデカプセル化を行う（ステップ 801）。その後、各 VOP の VOP ヘッダ内に存在するスタートコードが受信されるか否かを検出する（ステップ 802）。 20

【0045】

図 9 は、伝送された VOP の内部構造を示す図面である。各 VOP 910、920、・・・は、VOP ヘッダ 911 及び VOP データ 912 を含む、各 VOP ヘッダ 911 の最初の 4 バイトとしてスタートコード 913 を有する。

【0046】

スタートコードは、各 VOP の最初の 4 バイトであって、あらかじめ決定された値を有する。後続する VOP のスタートコードが発見されれば、現在の VOP は抽出されて、復号化部 330 に伝送される（ステップ 803）。 30

【0047】

復号化部 330 は、コンテンツサーバ 200 から DRM サーバ 100 を通じて伝送された DRM 復号化情報 311 を利用して、該当 VOP を復号化する（ステップ 804）。DRM 暗号化情報 311 は、暗号化方式、暗号化した VOP ID、暗号化モードに関する情報及び暗号化キーを含み、DRM サーバモジュール 210、DRM サーバ 100、DRM クライアントモジュール 310 を通じて復号化部 330 に伝送される。

【0048】

メディア再生部 340 は、復号化部 330 から復号化された VOP を受信して、それらを組み合わせることによって復号化された MPEG4 ファイルを生成し、これを再生する（ステップ 805）。 40

【0049】

図 10 は、本発明の他の実施例に係るデジタル著作権管理アトム 1000 の内部構成を示す図面である。本発明の他の実施例で、既存の MPEG4 ファイルのメタデータとして新たなアトムが追加される。図 2 で、暗号化情報 211 は、DRM 暗号化情報 103 に含まれて DRM サーバ 100 を通じて伝送されたが、本実施例では、DRM アトム 1000 の内部に暗号化情報 211 が含まれる。暗号化情報 211 は、暗号化キー、暗号化方式、暗号化モード及び暗号化された VOP ID を含む。

【0050】

図 10 に示す DRM アトムは、アトム大きさ 1010 及びアトム種類 1020 以外に、暗号化モード 1030、暗号化フラグ 1040、エントリー数 1050 及びエントリー 50

テーブル1060を備える。暗号化フラッグ1040が1に設定されれば、あらゆるVOPを暗号化したことを意味し、暗号化フラッグ1040が0に設定されれば、一部のVOPのみが暗号化されたことを意味する。暗号化された一部のVOPのVOP IDは、エントリーテーブル1060に保存され、暗号化されたVOP数は、エントリー数1050に保存される。

【0051】

既存のMP EG 4ファイルのフォーマットに影響を与えないために、DRMアトム1000は、ムーブアトムの下位アトムのうち最上位アトムに位置する。もし、DRMアトム1000が他の下位アトムに位置すれば、DRMアトムの上位アトムの大きさは何れも修正されねばならないためである。

10

【0052】

本実施例で、暗号化情報211は、MP EG 4ファイルの内部に伝送されるため、コンテンツクライアント300は、暗号化情報に対応する復号化情報311に対する別途のファイルシステムを管理する必要がないという効果がある。

【0053】

図11は、アトムを生成する例示的なAPI (Application Program Interface) コードを表す。アップル社では、MP EG 4ファイルフォーマットのアトムを生成するためのAPIとして 'QuickTime' を提供しており、図10は、QuickTimeで作成したアトム生成の例である。図10によれば、アトムの名称は、'drma' と命名され、大きさは、'100' と定められているということが分かる。

20

【0054】

以上、本発明について、その望ましい実施例を中心に説明した。当業者ならば、本発明が本発明の本質的な特性から逸脱しない範囲で変形された形態で具現され得るということが理解できる。したがって、開示された実施例は、限定的な観点ではなく、説明的な観点で考慮されねばならない。本発明の範囲は、前述した説明ではなく、特許請求の範囲に記載されており、それと同等な範囲内にあるあらゆる差異点は、本発明に含まれたものと解釈されねばならない。

【0055】

本発明に係るMP EG 4ファイルの暗号化方法及びそれを利用したデジタル著作権の管理方法によれば、MP EG 4ファイルのフォーマットを維持しつつ、VOP単位でファイルを暗号化するため、完成した形態のファイルフォーマットに容易に適用可能であると共にストリーミングサービスが可能である。

30

【0056】

また、MP EG 4ファイルの生成過程に関係なくファイルを暗号化できるため、コンテンツ提供者の独立的な暗号化が可能であり、コンテンツ提供事業の活性化に役に立つ。

【図面の簡単な説明】

【0057】

【図1】 動画ファイルのフォーマットを示す図面である。

【図2】 本発明に係るデジタル著作権管理の概要図である。

40

【図3】 本発明に係るMP EG 4ファイルの暗号化方法を示すフローチャートである。

【図4】 MP EG 4ファイルのメディアデータアトムの構成を示す図面である。

【図5A】 MP EG 4ファイルのムーブアトムの構成を示す図面である。

【図5B】 チャンクサイズアトム、サンプル数アトム及びサンプルサイズアトムの内部構成を示す図面である。

【図6A】 多様な方式で暗号化した暗号化されたMP EGファイルの再生画面を示す図面である。

【図6B】 多様な方式で暗号化した暗号化されたMP EGファイルの再生画面を示す図面である。

【図6C】 多様な方式で暗号化した暗号化されたMP EGファイルの再生画面を示す図面

50

である。

【図 7】ストリーミングモジュールによりパケット化された伝送パケットの内部構造を示す図面である。

【図 8】コンテンツクライアントが伝送パケットを受信して M P E G 4 ファイルを再生する方法を示すフローチャートである。

【図 9】伝送された V O P の内部構造を示す図面である。

【図 10】本発明の他の実施例に係るデジタル著作権管理アトムの内部構成を示す図面である。

【図 11】アトムを生成する例示的な A P I コードを示す図面である。

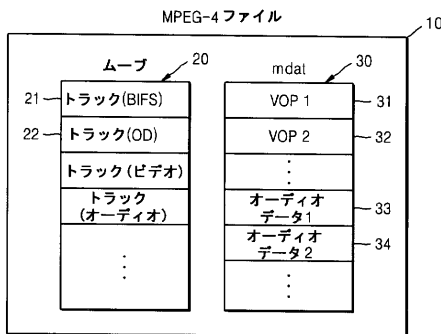
【符号の説明】

【0058】

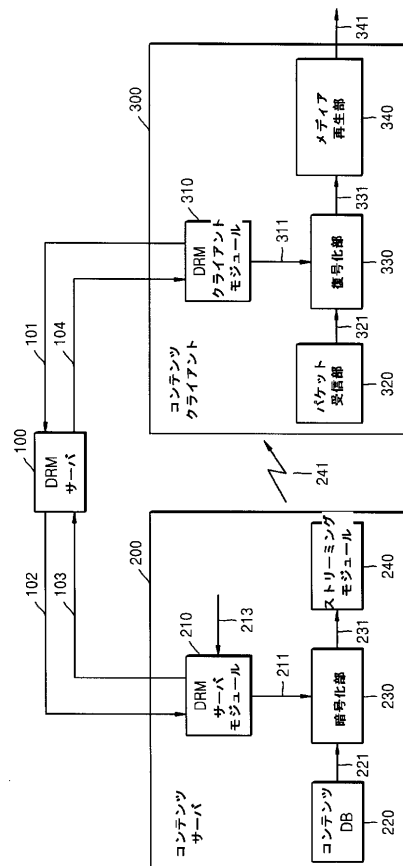
- 100 DRMサーバ
- 200 コンテンツサーバ
- 220 コンテンツデータベース
- 300 コンテンツクライアント
- 320 パケット受信部

10

【図 1】

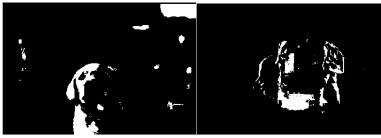


【図 2】



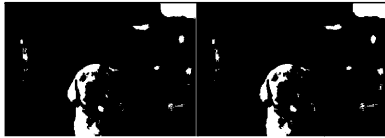
【図 6 A】

FIG. 6A



【図 6 B】

FIG. 6B

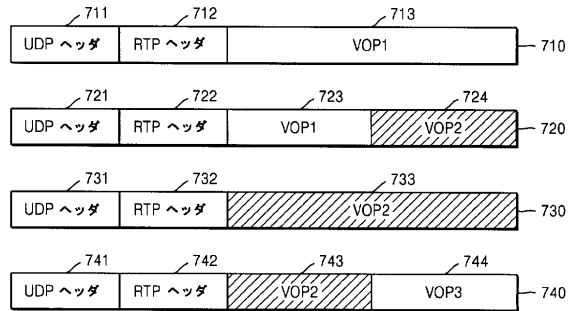


【図 6 C】

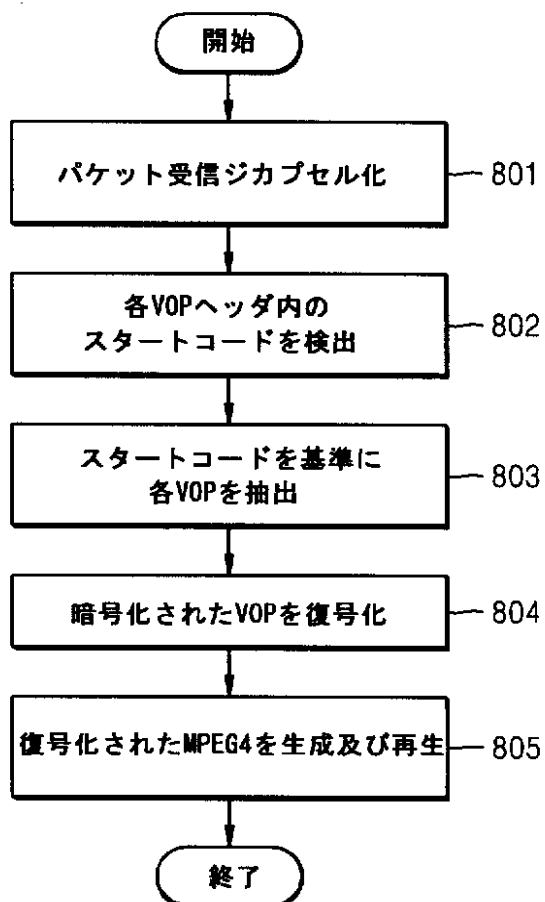
FIG. 6C



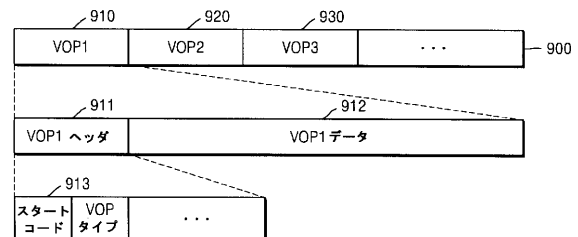
【図 7】



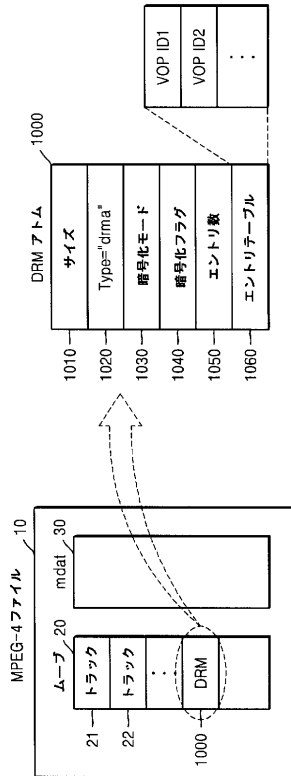
【図 8】



【図 9】



【図 10】



【図 11】

FIG. 11

```
QAtom firstAtom;  
QAtomContainer container;  
OSerr err;  
err = QTNewAtomContainer (&container);  
if(!err)  
err = QTInsertChild (container, kParentAtomIsContainer,  
                    drma', 1000, 1, 0, nil, &firstAtom);
```

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/KR2004/003213
A. CLASSIFICATION OF SUBJECT MATTER		
IPC7 G06F 17/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC7 G06F 17/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean patents and applications for inventions since 1975		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2000-4713 A (PHILIPS ELEC. INC.) 27 JAN. 2000 SEE THE WHOLE DOCUMENTS	1-29
A	KR 2001-74604 A (SILTRONIC TECH. INC.) 4 AUG. 2001 SEE THE WHOLE DOCUMENTS	1-29
A	KR99-44818 A (TRUSTTECK INC. et ETR.) 25 JUN. 1999 SEE THE WHOLE DOCUMENTS	1-29
A	KR 2002-75060 A (MARKTECH INC. et ETR.) 24 OCT. 2002 SEE THE WHOLE DOCUMENTS	1-29
☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 07 APRIL 2005 (07.04.2005)		Date of mailing of the international search report 13 APRIL 2005 (13.04.2005)
Name and mailing address of the ISA/KR  Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140		Authorized officer JEONG, Jae Hoon Telephone No. 82-42-481-5787 

フロントページの続き

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

(74)代理人 100110364

弁理士 実広 信哉

(72)発明者 ドンキー・シン

大韓民国・ソウル・156-724・ドンジャクグ・ノランジン・1ードン・(番地なし)・シ
ンドンガ・リバーパーク・アパート・705-1403

(72)発明者 ジュンイル・キム

大韓民国・キョンギド・482-709・ヤンジュシ・ヘチョンユプ・(番地なし)・クク
ドン・アパート・109-1003

(72)発明者 ドンイル・シン

大韓民国・ソウル・138-240・ソンパーク・シンチョンードン・(番地なし)・ジャンミ・
3ーチャ・アパート・2-401

(72)発明者 ヨンビン・キム

大韓民国・ソウル・139-224・ノウォング・ジュンギェ・4ードン・(番地なし)・サム
チャン・タワー・プラザ・1806

(72)発明者 スンヨン・チェ

大韓民国・ソウル・136-037・ソンブクグ・ドンソムンードン・7ーガ・32

Fターム(参考) 5C164 MB11P SA53P SB03P TB13P

5J104 AA01 AA16 AA32 BA03 EA01 EA04 EA15 EA16 JA03 MA05

NA02 NA27 NA37 PA05