コンピュータセキュリティ　10－2
（2000．　7．25）

MPEG-4　IPMPシステムへの暗号技術の実装

若尾聡　岩村恵市　安藤勉

キヤノン（株）画像技術研究所
〒211-8501 川崎市中原区今井上町53
{wakao,iwamura,ando}@cts.canon.co.jp

あらまし　現在ISO/IECにてマルチメディア対応の符号化方式としてMPEG-4が標準化作業中である。このMPEG-4は、ビデオデータ、オーディオデータ、CGデータ等の様々なデータをオブジェクトとして取り扱えるという特徴のため、従来のMPEGにはなかった知的財産の保護/管理機構（IPMPシステム：Intellectual Property Management and Protection）がシステムに標準で搭載されている。
本論文では、インターネット上において、このIPMPシステム上に暗号化技術を用いることで知的財産の保護/管理を高いレベルで行うことのできるデータ配信システムを提案すると共に、簡易化した該システムに対して実際に暗号化による実装を行いその機能の検証を行った。

キーワード　MPEG、IPMPシステム、著作権保護、画像セキュリティー

An Implementation of Cryptography on MPEG-4 IPMP System

Satoru Wakao　Keiichi Iwamura　Tsutomu Ando

Visual Information Technology Development Laboratory
53, Imaikami-cho,Nakahara-ku,Kawasaki 211-8501,Japan
{wakao,iwamura,ando}@cts.canon.co.jp

Abstract　ISO/IEC has standerdized MPEG-4 specification,which includes IPMP(Intellectual Property Management and Protection) System in Systems part(ISO/IEC 14496-1).Because recently intellectual property management is becoming a important issue and MPEG-4 has object based coding scheme which can process video,audio,CG,etc.
In this paper,we propose data distribution system which is able to protect and manage intellectual property rights using cryptography on MPEG-4 IPMP System on internet,and make an implementation of cryptography for simplify above system to verify the function.

key words　MPEG、IPMP System、Intellectual Property Protection、Image Security

1. はじめに

現在 ISO において、MPEG-2(Moving Picture Experts Group phase2)に続く次世代のビデオ・オーディオの規格としてMPEG-4の標準化作業が進められている[1]。MPEG-4は、従来のMPEG-1,-2とは異なりビデオデータ、オーディオデータ、CGデータ、テキストデータ等のマルチメディアデータはオブジェクトとして個別に取り扱われ、各オブジェクト毎に符号化された後にシーン記述情報に基づいて合成・表示が行われる。このため、各データをオブジェクトとして個別に操作/加工することが可能になった。

一方で、近年のディジタルメディアの普及に伴い、コンテンツを所有する映画業界や音楽業界を中心に、著作権保護の重要性が叫ばれている。これは、ディジタルメディアが従来のアナログメディアと異なり、劣化のない全く同一のデータが短時間のうちに大量に複製できるためであり、従って十分な保護が為されていない規格に対しては優良なコンテンツが提供されない恐れがある。

このような状況のもとで、各データをオブジェクトとして個別に操作/加工することが可能であるという特徴を有するMPEG-4において、著作権を有するビデオデータ、オーディオデータ等をいかにして管理/保護するかという問題が議論され、この著作権管理/保護を行うための仕組みとしてIPMPが標準として取り入れられた。このIPMPシステムは、データ保護のためのポインタ情報のみを定義しているだけであり、具体的な保護の仕組みは規定していない。従って確実なオブジェクトの保護/管理を行うためにはオブジェクトデータを暗号化により保護すると共に、システム全体でどのように安全性を保証するかということを考えることが必要であると考えられる。そこで今回、暗号技術をIPMPシステム上に組み入れると共に保護/管理システム全体を構築することで、MPEG-4における著作権管理/保護の機能を向上させることを目的とした。以下では、その提案モデル及び実装方法/結果について述べる。

2. MPEG-4

2.1 MPEG-4 ビデオ

MPEG-4ビデオ[2][3]では、ビットストリーム構造は図1に示すような階層構造が採用されている。画像のシーケンスにVideo Sessionが対応し、その下に1つ以上のVideo Objectが存在する。Video Objectの下位にはVideo Object Layerという階層がある。これは、Video Objectに対して複数の時間的、空間的解像度を与えるためのものである。Video Object Layerの下のGroup of VOPはランダムアクセスを行うためのものであり、そのVideo Object Plane（VOP）は、フレームに対応する階層であり、ある瞬間のデータを意味する。

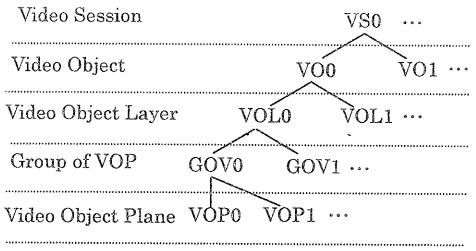

図1 ビットストリーム構造

2.2 MPEG-4 システム

図2に示すようにMPEG-4システム[4]では、ビデオデータやオーディオデータ、CGデータなどを個別に符号化し、夫々の符号化データをオブジェクトデータとして扱い、これらの所謂マルチメディアデータを多重化して単一のビットストリームとして伝送する。

受信機側においては、データがオブジェクトとして扱われるというMPEG-4の特性のため、受信したビットストリームを各オブジェクトに分離した後に個別に復号し、復号した各オブジェクトデータを時間的、空間的に合成することでシーン（画面構成）を作り、表示する。このオブジェクトデータを合成するための情報としてVRML2.0を修正したBIFS（BInary Format for Scenes：シーン記述情報）が存在する。

このBIFSはVRML記述をバイナリ化したもので、このBIFSに従って各オブジェクトデータが合成される。従ってこのシーン記述情報を変化させることで、同一のオブジェクトデータから異なるシーン（オブジェクトの位置や前後関係、視点）を表示させることも可能になる。さらに、シーン記述と各オブジェクトデータとの関連付けと、復号に必要な情報を格納するためのデータであるオブジェクトディスクリプタが規定されている。システムレイヤでは、上記シーン記述、ディスクリプタの他に従来のMPEGシステムと同様に同期、多重化を規定している。

次にMPEG-4のアーキテクチャを図3に示す。符号化されたデータは、伝送路であるDeliveryLayer

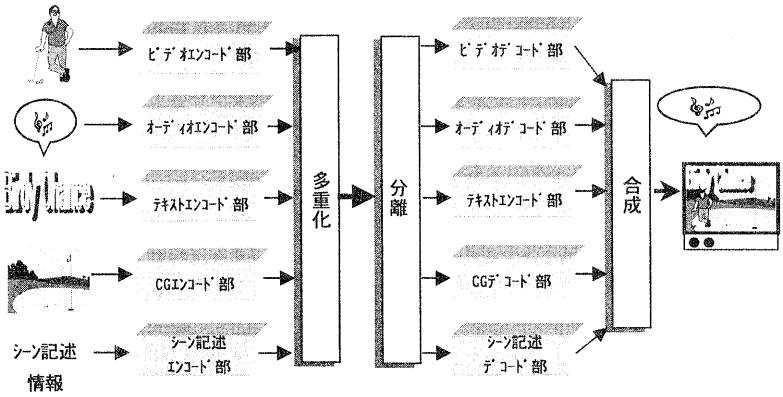

図2 MPEG-4システム

から SL と呼ばれる単位（パケット）毎に Sync Layer に渡される。ここでは、(i)該パケットがビデオ、オーディオ、テキスト、CG、シーン記述情報のうちどの属性のものであるか (ii) タイムスタンプ等による各オブジェクトの時刻の再生や各オブジェクト間の同期が行われる。その後 Compression Layer において各オブジェクトの復号が行われた後、シーン記述情報に従い、合成、表示が行われる。

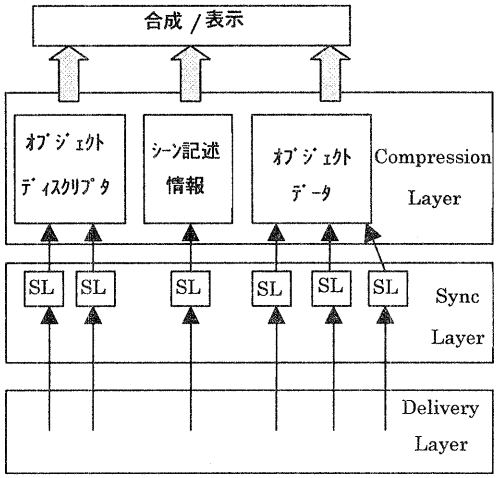

図3 MPEG-4 アーキテクチャ

2.3 MPEG-4 IPMP システム

MPEG-4 においては、オブジェクトデータ毎に符号化/復号するという特性のために従来の MPEG-2 等よりも著作権管理に配慮がなされている。その具体的な仕組みが IPMP システム[5]である。図4にその仕組みの一例を示す。

図4の IPMP システムでは保護/管理対象のオブジェクトデータに対して、該オブジェクトデータを処理するデコード部の前後においてデータの流れを制御することで、再生の停止及び再開を行っている。

この制御のために必要となるのが IPMP データであり、この IPMP データは制御対象のオブジェクトデータに関連づけられて IPMP 制御部に伝送される。

しかし、IPMP システムは、保護の方式そのものについては何の規定もしていない。従って悪意を持った第三者によってデータが取得され、不正に使用される可能性があった。そこでオブジェクトデータの暗号化を行うことがこの問題に対処するための有効な手段の一つになると考えられる。

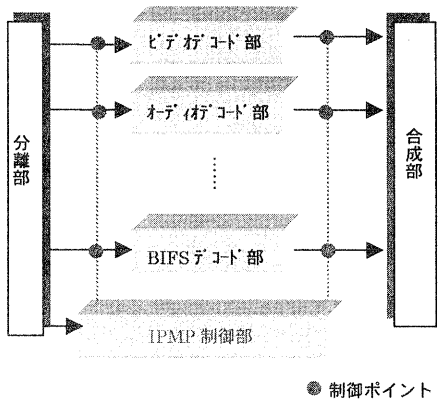

図4 IPMP システムの例

3. 提案モデル

3.1 システム概要

ここでは、インターネット上での MPEG-4 を用いたコンテンツ配信システムを仮想的に考え、該配信システム対して暗号化システムモデルを適用する。その形態は、受信機（ユーザ）が要求を出した時に、送信機側から蓄積されたデータが受信機へ送られる On-Demand 型とする。図 5 を用いて、仮定したコンテンツ配信システムと受信機がコンテンツを得るまでの手順を説明する。

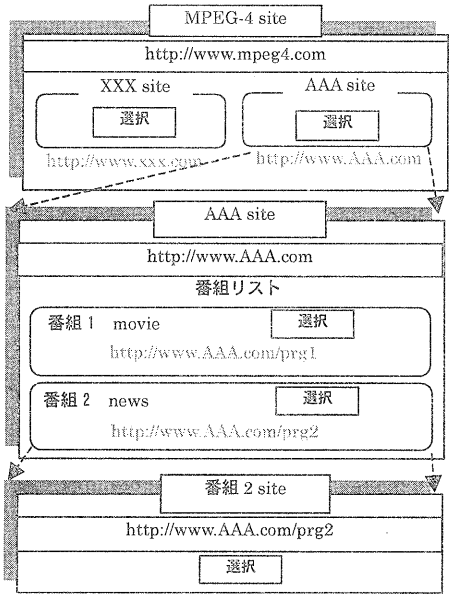

図 5　コンテンツ選択の流れ

コンテンツの受信を希望する受信機は最初に、MPEG-4 サイトにアクセスする。この MPEG-4 サイトは、図 5 のように各メーカ別になっているサイトのアドレス（リンクが貼られている）の集合で構成されいる。受信機はそのサイトから好みのメーカを選択することで、メーカのサイトにアクセスする。さらに、メーカのサイト内にある好みの番組を選択する。ここで上記において、MPEG-4 サイトにアクセスする際にはユーザ登録/認証を行うものとする。

一方で、送信機は、番組を作成するために各オブジェクトデータを編集して MPEG-4 ストリームを生成するとともに視聴制御を行うデータストリームに対しては暗号化による視聴制御に関する設定を行う。そして作成した番組である MPEG-4 ストリームをサイト（サーバ）に送信する。

3.2 処理概要

以下では図 6 に従い暗号化処理の説明を行う。

1. 受信機毎に異なる Kp は、あらかじめ送信機と受信機とで共有しておく。

2.「送信機」…(ⅰ)メーカ毎に異なる Km を Kp で暗号化して E(Kp,Km)を生成し、サイト選択時に受信機に送信する。(ⅱ)次に番組毎に異なる Kw と許可情報とを Km で暗号化して E(Km,Kw)を生成し、番組選択時に受信機に送信する。すなわち送信機はメーカ、番組選択時に、それらに固有な階層化した鍵データを送信する。(ⅲ)一定時間毎に異なる Ks を Kw で暗号化して E(Kw,Ks)を生成し、該 E(Kw,Ks)で IPMP ストリームを生成するとともに、(ⅳ)符号化されたデータを Ks で暗号化して E(Ks,Data)を生成し、該 E(Ks,Data)で暗号化ストリームを生成する。(ⅴ)最後に IPMP ストリームと暗号化ストリームとを多重化して MPEG-4 ストリームを生成する。

「受信機」…(ⅵ)サイト選択時に受信した E(Kp,Km)を、共有している Kp で復号して Km を得る。(ⅶ)次に番組選択時に受信した E(Km,Kw)を、前記で得た Km で復号して Kw を得る。(ⅷ)さらに受信した MPEG-4 ストリームを IPMP ストリームと暗号化ストリームとに分離し、(ⅸ)IPMP ストリーム中の E(Kw,Ks)を、前記で得た Kw で復号して Ks を得て、この Ks を用いて E(Ks,Data)を復号する。(ⅹ)最後に符号化データをデコードすることで映像/音声等が再現される。

3.3 システムの特徴

◎階層的な暗号化を行う

オブジェクトデータに対して使用する鍵(Ks)を番組毎に異なる鍵(Kw)で暗号化を行い、該番組毎に異なる鍵をメーカ毎に異なる鍵(Km)で暗号化を行い、さらに該メーカ毎に異なる鍵をユーザ毎に異なる鍵(Kp)で暗号化を行う　といった階層的な暗号化を行う。これにより Kw による番組毎の制御を、Km によるメーカ毎の制御を、Kp による受信者毎の制御を、行うことができる。

◎階層化した鍵データが異なるルート、タイミングで伝送される

Kp は一連のシーケンスを開始する前に IC カード等の耐タンパーな記憶媒体や安全な配送手段で配布され、E(Kp,Km)、E(Km,Kw)はメーカ、番組選択時に SSL といった保護された伝送路で伝送される。

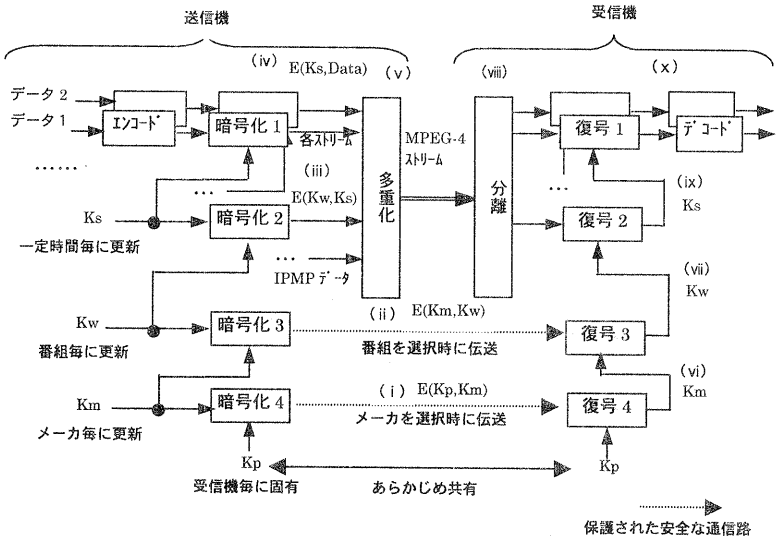

図6　提案モデル

また、E(Kw,Ks)は MPEG-4 ストリーム受信時に MPEG-4 ストリームの構成要素である IPMP ストリームで伝送される。鍵データに関するデータ全てを IPMP ストリームで伝送することも考えられる。しかし Kw、Km といった中間的な鍵を導入して鍵データを階層化することで、必要な時に必要なデータのみが伝送されるので効率が良くなると共に伝送ルート、タイミングを分散できるので状況に応じて鍵データのルート、タイミングを変更可能であり、システムに柔軟性を持たすことができる。

●鍵データの送信手段に IPMP ストリームを、受信機の制御に IPMP システムを用いる
オブジェクトデータに対して使用する鍵を番組毎に異なる鍵で暗号化した鍵データ E(Kw,Ks)は、該オブジェクトデータと関連付ける必要があるので IPMP ストリームを用いて送る。このようにオブジェクトデータと IPMP ストリーム（データ）を関連付けることでオブジェクトデータ毎に IPMP システムによる制御が可能になる。また、IPMP ストリームの処理、受信機の制御を行うためには IPMP システムを用いた処理が必要になる。

●きめ細かいオブジェクトデータの制御が可能
一定時間毎にオブジェクトデータに対して使用する鍵を更新できるので、きめ細かい制御が可能であり、ビデオデータの場合には 1 フレーム毎の制御が可能となる（4.2.2 IPMP データ　参照）。

4．簡易化したシステムの暗号処理

4.1 暗号化および復号処理概要

今回は、上記提案モデルを簡易化したシステムに対して暗号処理を実装した。簡易化したシステムおよび実装した暗号処理の説明を以下で行う。

簡易化システムを図 7 に示す。暗号化対象は 1 つのメーカの 1 つの番組の 1 つのビデオデータとする。従って鍵はビデオデータの暗号化に使用する Ks と Kp の 2 つを使用し、提案モデルでの Km や Kw といった中間的な鍵は存在しない。従って、送信機と受信機との間で E(Km,Kw)や E(Kp,Km)といった鍵情報が伝送されることもない。

図 7 に従い暗号化および復号処理の概要説明を行う。

1.Kp を、送信機と受信機とであらかじめ共有しておく。

2.「送信機」…(ｉ) ビデオデータに暗号化を行う Ks を Kp で暗号化して、暗号化鍵データ E(Kp,Ks)を生成し、この E(Kp,Ks)を基に IPMP データを生成する。(ii)ビデオエンコーダで符号化されたビデオデータを Ks で暗号化して暗号化ビデオデータ E(Ks,Video_Data)を生成する。(iii)IPMP データと、E(Ks,Video_Data)、BIFS ストリーム等を多重化して MPEG-4 ストリームを生成して送信する。

「受信機」…(iv) MPEG-4 ストリームを受信した後に各オブジェクトデータに分離し、IPMP データ中の E(Kp,Ks)を、共有している Kp で復号して Ks を得る。

(v)このKsを用いてE(Ks, Video_Data)を復号してビデオデータを得る。(vi)最後にビデオデータをデコードすることで映像が再生される。

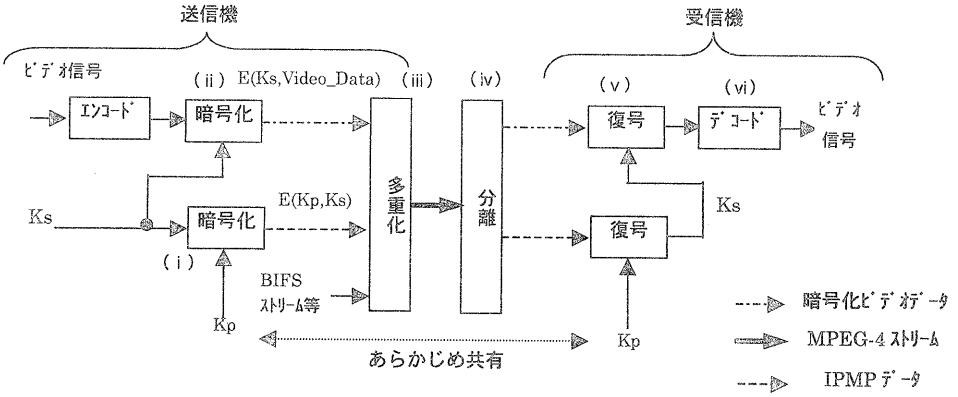

図7　簡易化システムの処理概要

4.2 暗号化および復号処理の詳細

4.2.1 暗号化ビデオデータ

送信機において、VOP（ビデオデータ1フレームに相当）が何番目のVOPであるかを調べ、図8に示す鍵データテーブルから対応するKsを参照してKsを特定する。特定したKsでVOPを暗号化して得られたデータが暗号化ビデオデータとなる。鍵データテーブルが図6のような場合、ビデオデータのVOPが1～１００番目までの時、KsとしてK1により暗号化される。図8では、１００フレーム毎に区切っているが、最小1フレーム毎に区切ることも可能であり、このフレーム数の設定は送信機側で行う。また、保護する必要のないVOP（鍵テーブルが図8のような場合、１０１から２００番目のフレーム）に対してはKsとしてK0(Ksのように秘密にする必要がなく公開してもかまわないデータ）により暗号化される。

ﾌﾟﾛﾃｸﾄ	ﾌﾚｰﾑ番号	Ks
ON	1~100	K1
off	101~200	*K0*
ON	201~300	K3
ON	301~400	K4
……	……	……

図8　鍵データテーブル

4.2.2 IPMP データ

IPMPデータの中には、図9に示すように、送信機においてビデオデータに暗号化を行う時に使用したKsをKpで暗号化したE(Kp,Ks)がフレーム番号と関連付けて記述されている暗号化鍵データテーブルがある。送信機におけるこの暗号化（Ksを鍵Kpで暗号化）の時、KsがK0のデータには暗号化を行わない。受信機ではこのE(Kp,Ks)をあらかじめ共有しているKpで復号して鍵データテーブルを生成する。ただし、E(Kp,Ks)がK0のデータは復号しない。

ﾌﾚｰﾑ番号	E(Kp,Ks)
1~100	K1
101~200	K0
201~300	K3
301~400	K4
……	……

□ はKpで暗号化されている部分

図9　暗号化鍵データテーブル

次に送信機と同様にVOPが何番目のVOPであるかを調べ、生成した鍵データテーブルから復号に使うKsを特定する。Kpが正しいデータであれば、送信機で暗号化に使用した鍵データテーブルと同一のテーブルが生成できるため暗号化ビデオデータの復

号には、暗号化に使用されたデータが使用される。従ってビデオデータが再生できることとなる。一方で Kp が正しいデータでない場合、暗号化に使用した Ks と異なるデータが復号に使用されることになるので、ビデオデータが再生されない。また、保護する必要のない VOP は Ks としてK0 が暗号化に使用され、K0 は Kp で暗号化を行っていないため Kp の値にかかわらず再生が可能である。

本方式では、ある時点での鍵が漏れたとしてもその影響はその鍵を用いて暗号化しているフレームのみに限定される。また更新周期を 1 フレームとすることができるので、I ピクチャのみで構成されるビデオデータの場合には、視聴制御がフレーム毎に可能となる。

4.4 暗号化処理

4.4.1 暗号アルゴリズム

暗号アルゴリズムは、現在一般的に使用されている DES[6]を採用した。

4.4.2 鍵の更新周期

同じ Ks を用いて長期間にわたり暗号化を行った場合、暗号文攻撃にさらされる可能性が高くなる。このため安全性を高めるためは Ks の更新周期を短くすることが必要となる。従って更新周期を最大 1 フレーム（例えば毎秒 20 フレームのビデオデータの場合、更新周期は 50ms）に行える仕様とした。一方で更新周期を短くした場合には、多くの鍵データを送信する必要があるためにより多くの伝送帯域が必要となる。従って、暗号化を行うデータの重要性に応じて更新周期を変化させることが必要になる。

4.4.3 暗号の処理モード

ビデオデータ等の暗号化対象データはバイトアラインされているが、必ずしも DES のブロック長である 64 ビットで割り切れるデータ長であるとは限らない。そのため CFB モードや OFB モードと比較して高速処理ができる CBC モードで 8 バイト単位の処理を行い、残りのバイトを OFB モードで処理する併用モードとした。これは、現在のディジタル放送において採用されている暗号化処理モードと同様のものである。

4.4.4 処理性能

1374Kbyte のビデオデータに対して、DES による暗号化（復号）に 328(ms)を要した。これは、ビデオデータから暗号化ビデオデータ E(Ks,Video_Data)を生成する処理に相当する。

以上から処理速度：33.5Mbps

計測環境：CPU Pentium II 300MHz, メモリ 128Mbyte

ストリームの分離、各オブジェクトデータの復号、合成、表示等の処理を行う必要のある受信機に対して多大な（暗号化データの）復号処理の負荷をかけることは、MPEG-4 データの再生に支障をきたす恐れがあるために避ける必要があるが、今回の MPEG-4 ビデオの伝送速度を考えると上記の処理速度であれば受信機に対する負荷に関しては問題ないと考えられる。

4.4.5 鍵の生成

C 言語の標準関数である rand 関数や srand 関数等を用いてデータの系列を発生させ、それらのデータを Ks として使用した。

5. 安全性の検討

本方式で採用した DES に対しては差分攻撃や線形攻撃といった攻撃による解析が進んでおり、さらには鍵の全数探索による攻撃方法により、約 1 日で鍵が解読されておりその安全性が急速に低下しつつある。そのため、ある時点の Ks が攻撃により露出した場合、露出した Ks の次に使用される Ks が、露出した Ks から簡単に予測されるものであってはならない。そのため、疑似乱数系列に基づいて Ks の発生を行うといった安全性が保証されている方式[7]を鍵生成に採用すること、または安全性の評価がなされていて、高速な処理が行える暗号アルゴリズムを用いることが考えられる。ただし、本方式では、最大 1 フレーム毎に鍵を更新することができ、保護するデータに機密性が厳格に求められるものではないことを考えると安全性を損なう重大な問題は存在しないと考えられる。

6. 今後の課題

●DES に替わる暗号アルゴリズムによる実装

上記にも述べたように DES に関しては、安全性に関する様々な問題が指摘されていてこのまま DES を暗号化アルゴリズムに採用することは、安全性の面から好ましくない。そのため現在標準化が行われている AES（Advanced Encryption Standard）[8]等の新しい暗号アルゴリズムを用いた実装を行う必要がある。

●鍵データ生成方法の改良

今回のシステムでは、rand 関数や srand 関数等を用いて鍵生成を行っているが、この方法では発生させ

た鍵データの間に周期性があることが多い。そのため鍵データが推定されやすくなり、安全性に問題が発生する可能性を否定できない。そのため、十分に長い周期をもった疑似乱数を発生させるような方式を鍵データ生成に用いるか、または疑似乱数系列に基づいて鍵データの生成を行うといった[7]のような方式を採用する必要がある。

◎ディジタル署名による認証

IPMP データは鍵データを含みデータの再生に関して重要なデータであるので、改竄がなされた場合には、それを検出する必要がある。そのために IPMP データに対する署名データを送信機において生成し、受信機で認証を行うことで、もしも改竄が行われていた場合には、受信機での再生停止やデータが改竄されていることの表示といった対策を行う必要がある。

7. まとめ

MPEG-4 の著作権を保護/管理する機構である IPMP システム上に、暗号技術を導入することにより従来よりもレベルの高い管理/保護を行うことの可能なシステムを提案した。

さらに、提案システムを簡略化したシステムに対して実際に MPEG-4 ビデオを暗号化のターゲットとして実装を行い、その機能を確認するとともにこの暗号処理による不具合も発生しないことを確認した。

「参考文献」

[1]「MPEG ホームページ」
http://drogo.cselt.stet.it/mpeg/standards/mpeg-4/mpeg-4.htm

[2]ISO/IEC 14496-2"Information technology-Coding of audio-visual objects Part2:Video"

[3]渡辺敏明："MPEG-4 最終版解説とデモンストレーション"、電子情報通信学会技術報告 IE97-177(1998-03)

[4]ISO/IEC 14496-1"Information technology-Coding of audio-visual objects Part1:Systems"

[5]金子格："MPEG-4 著作権管理・支援フィールドの特徴"、情報処理学会 研究報告 (99-EIP-3,pp.25-32)

[6]National Bureau of Standard,Federal Information Processing Standards Publications,81"Data Encryption Standard"

[7]山本他："2 乗型疑似乱数生成器とブロック暗号を用いた実用的暗号方式"、電子情報通信学会技術報告 ISEC93-29(1993-08)

[8]NIST : "Advanced Encryption Standard Development Effort"、http://www.nist.gov/aes