研究論文

暗号鍵の生成・管理を考慮したディジタル動画像のアクセス制御

今泉　祥子*　阿部　淑人**

An Access Control Method for Digital Videos Based on Generation and Management of Encryption Keys

IMAIZUMI Shoko* and ABE Yoshito**

抄　録

ディジタル動画像を対象に，鍵管理および配送において効果的な暗号鍵生成法を用いたアクセス制御方式の研究を行った。静止画像に対する既存のアクセス制御方式を応用することで，フレームレートなど時間軸の階層に対応する動画像のための新しいアクセス制御方式を考案した。

1. 緒　言

ディジタル画像通信の一般化に伴い，画像の保護に関して様々な側面から研究がなされている。本研究では，階層構造を有する符号化動画像を対象に，鍵管理・配送および演算処理において効果的な暗号鍵生成方法を用いたアクセス制御方式を考案した。

通信路や通信端末の多様化により，様々な品質での画像配信が求められている。例えば，テレビジョン放送におけるフレームレートは，ワンセグ放送で 15 fps，高精細度テレビジョン放送で 30 fps，60 fps などのように，用途によって異なる。有料配信において，課金の額は再生品質により決定されるため，アクセス制御が要求されている。

一方，階層構造を有する符号化静止画像に対し，文献[1)2)3)]は，SNR，解像度，色数などを制御対象として，ユーザが許諾された品質でのみ再生するためのアクセス制御を実現している。これらの研究は，ある静止画像へのアクセス制御において，符号化列および管理鍵の個数に冗長がないよう検討されている。

動画像においては，静止画像で制御すべき対象に加えて，時間軸についても考慮することが不可欠となる。本研究は，静止画像に対するアクセス制御[1)2)3)]を応用することで，フレームレートなどの階層に対応する，動画像のための新しいアクセス制御方式を考案した。まず，制御対象が 1 つの場合に有効な手法を述べる。次に，制御対象を 2 つに拡張した手法について説明する。本手法は，2 つの制御対象に対して同時にアクセス制御を施すことが可能である。さらに，このとき必要となる管理鍵の個数についても議論する。

2. 静止画像に対するアクセス制御の従来法

本節では，本手法の基礎となる，階層構造を有する符号化静止画像のためのアクセス制御方式[1)]を説明する。また，アクセス制御の対象ごとに互いに独立な鍵を割り当てる最も簡易的なアクセス制御方式を，本論文では独立制御型方式と呼び，この方式において必要な管理鍵の個数を提示する。

2.1 Hash-Chain 型アクセス制御方式[1)]

2.1.1 暗号処理

文献[1)]の手法は，符号化列のパケット単位に暗号処理を施す。ある符号化列のパケット数を N とし，各パケットを P_i（$i = 0, 1, ..., N - 1$），

*　研究開発センター
**　下越技術支援センター

各パケットに対する暗号鍵を K_i（$i = 0, 1, ..., N-1$）とする。ここで，P_0 は最下位パケット，P_{N-1} は最上位パケットを表す。各暗号鍵 K_i は，

$$K_i = H^i(K_0), \quad i = 1, 2, \ldots, N-1 \qquad (1)$$

によって，最下位パケット P_0 に対応する鍵 K_0 を管理鍵として，下位パケットに対応する鍵から順に生成される。ここで，$H(\cdot)$ は一方向性ハッシュ関数であり，$H^y(x)$は x のハッシュ値を y 回求めることを意味する。したがって，あるパケット P_i に対する鍵 K_i は，式(1) を用いて，1 つ下位のパケット P_{i-1} に対する鍵 K_{i-1} のハッシュ値として求められる。以上のように，管理鍵 K_0 から従属的に生成された鍵 K_i を用いて，パケット P_i が順次暗号化される。

2.1.2 暗号解除

暗号化された符号化列に対して，パケット P_J（J は $N-1$ 以下の任意の非負整数）以上の上位パケットの暗号解除を許諾されたユーザは，P_J に対する鍵 K_J を受信する。以降，この鍵 K_J を配送鍵と呼ぶ。ユーザは，

$$K_{J+i} = H^i(K_J), \quad i = 1, 2, \ldots, N-1 \qquad (2)$$

によって，P_J より上位のパケットに対する鍵 K_i（$i = J+1, J+2, ..., N-1$）を K_J から順に生成し，暗号を解除する。したがって，K_0 を配送されたユーザは最高品質で，K_{N-1} を配送されたユーザは最低品質で，それぞれ画像を再生することとなる。

2.2 独立離散型アクセス制御方式

単純なアクセス制御方式として，各パケットに対して互いに独立な鍵を与える方式（独立離散型方式と呼ぶ）を考える。したがって，この方式では，N 個のパケットに対して，必要な管理鍵の個数は N 個となる。また，S 個（S は N 以下の任意の正の整数）のパケットの暗号解除を許諾されたユーザは，各パケットに対応する S 個の鍵を受信する。

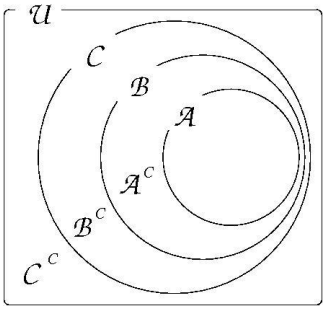


図 1　アクセス制御対象の相互関係

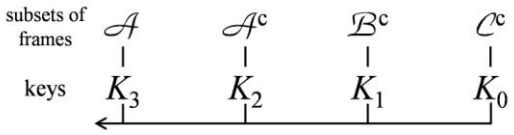


図 2　鍵生成順序

3. 単一アクセス制御方式

本研究で考案したアクセス制御方式のうち，まず，制御対象の個数が 1 つ（$T = 1$）の場合（単一アクセス制御方式と呼ぶ）について説明する。

3.1 階層条件

ディジタル動画像のアクセス制御は，コンテンツ単位，フレーム単位，解像度単位など様々であり，単一アクセス制御方式はその 1 つを制御対象とする。なお，制御対象は図 1 に示す階層関係を有する必要がある。同図において，$\mathcal{A}$ の $\mathcal{B}$ に関する補集合を $\mathcal{A}^c$，$\mathcal{B}$ の $\mathcal{C}$ に関する補集合を $\mathcal{B}^c$，$\mathcal{C}$ の $\mathcal{U}$ に関する補集合を $\mathcal{C}^c$ と表している。

3.2 暗号処理および暗号解除の手法

単一アクセス制御方式において，必要となる管理鍵および配送鍵の個数は，ともにただ 1 つである。本手法では，図 2 に示すように，図 1 における集合 $\mathcal{C}^c$ に対する鍵が管理鍵 K_0 となる。同様に，集合 $\mathcal{B}^c$ に対する鍵が K_1，集合

$\mathcal{A}^c$ に対する鍵が K_2，集合 $\mathcal{A}$ に対する鍵が K_3 となり，これらの鍵は次式によって従属的に生成される。

$$K_i = H^i(K_0), \quad i = 1, 2, 3 \qquad (3)$$

各集合に属するすべての要素は，その集合に割り当てられた同一の鍵で暗号化される。

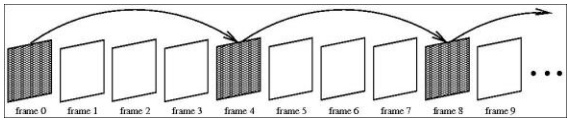
一方，暗号解除および再生について，全体集合 $\mathcal{U}$ を許諾されたユーザには，管理鍵 K_0 を配送する。K_0 を受信したユーザは式(3) により，鍵 K_1，K_2，K_3 を生成し，すべての集合に属する要素の暗号を解除し，再生することが可能となる。また，集合 $\mathcal{B}$ を許諾されたユーザには，鍵 K_2 を配送する。このユーザは，式(3) を用いて K_3 を生成し，集合 $\mathcal{B}$ に属する要素の暗号解除と再生が可能である。しかし，$H(\cdot)$ の一方向性によって，鍵 K_2 から鍵 K_0 および K_1 は生成できず，このユーザは許諾されていない集合に属する要素に対して，暗号解除および再生することはできない。同様のことが，集合 $\mathcal{A}$ または $\mathcal{C}$ を許諾されたユーザに対しても成り立つ。

3.3 節では，本方式の応用例を示す。ただし，3.1 節で述べた条件を満たせば，以下に示す例に限らず，本手法は利用可能である。

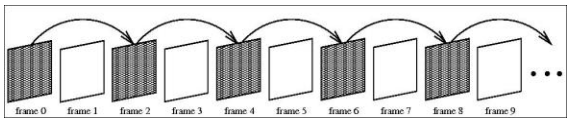
3.3 フレームレートに基づく応用例

図 3 に，15 fps（同図(a)），30 fps（同図(b)）および 60 fps（同図(c)）の 3 種類のフレームレートの例を示す。同図において，影部フレームが再生されるフレームである。ここからは，各フレーム集合を図 1 に示す集合に対応づけて説明する。ただし，この例では，3 段階のアクセス制御となるため，集合 $\mathcal{C}$ および $\mathcal{C}^c$ は用いない。

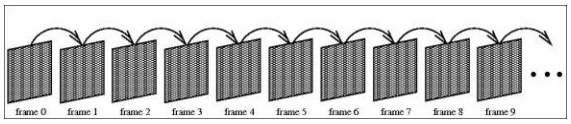
同図において，全体集合 $\mathcal{U}$ はフレームレートが最も高い 60 fps のフレーム集合である。続いて，30 fps のフレーム集合が $\mathcal{B}$，15 fps のフレーム集合が $\mathcal{A}$ となる。したがって，3.1 節の階層条件を満たしている。また，60 fps のフレーム集合 $\mathcal{U}$ のうち，15 fps および 30 fps では再生されないフレーム，すなわち，2x−1（x は正の整数）番目のフレーム集合が $\mathcal{B}^c$，30 fps で再生されるフレーム集合 $\mathcal{B}$ のうち，15 fps では再生されないフレーム，すなわち，4x − 2（x は正の整数）番目のフレーム集合が $\mathcal{A}^c$ となる。



(a) 15 fps



(b) 30 fps



(c) 60 fps

図 3　各フレームレートにおける動画像再生（影部フレームを再生）

この例では，集合 $\mathcal{B}^c$ に対する暗号鍵が管理鍵 K_0 となり，フレーム集合 $\mathcal{A}^c$ に対する鍵が K_1，集合 $\mathcal{A}$ に対する鍵が K_2 となる。これらの鍵は，式(3) によって従属的に生成される。

暗号解除および再生のため，60 fps を許諾されたユーザには，管理鍵 K_0 を配送する。ユーザは式(3) によって，鍵 K_1，K_2 を生成し，すべてのフレームの暗号を解除し，再生する。また，15 fps を許諾されたユーザには，鍵 K_2 を配送する。鍵 K_2 からは，鍵 K_0 および K_1 は生成できないため，このユーザは許諾されたフレームレート以上の品質で再生することはできない。同様のことが，30 fps を許諾されたユーザに対しても成立する。

4. 同時アクセス制御方式

3 章では，アクセス制御の対象が 1 つ（T = 1）の場合について説明した。ここでは，T = 2,

レベル 0　　レベル 1　　レベル 2

図 4　解像度レベルの例

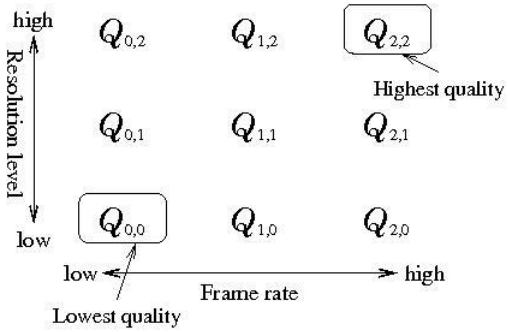


図 5　フレームレートと解像度の関係

すなわち 2 つの対象に対して同時にアクセス制御可能な同時アクセス制御方式を説明する。本方式は，文献 [1] を基礎とした文献 [2) 3)] を動画像のアクセス制御に応用したものである。

本手法において，必要となる管理鍵および配送鍵の個数は，各制御対象の階層数を X および Y とすると，$\min\{X, Y\}$個である。これは，文献 [2) 3)] の結論と一致しており，時間軸を対象とする場合においても成立する。

例として，1 つの動画像において，フレームレートと解像度の 2 つの対象を同時に制御することを考える。フレームレートは 3.3 節で挙げた 15，30，60 fps，解像度は図 4 に示す解像度レベル 0，1，2 の 3 種類とする。

上述の例を図 5 にまとめる。$Q_{f,r}$ において，f はフレームレート，r は解像度レベルの番号を示している。同図において，$Q_{2,2}$ がフレームレートが 60 fps，かつ，解像度レベルが 2 である最高品質を，$Q_{0,0}$ がフレームレートが 15 fps，

表 1　管理鍵の個数の比較

	本手法	独立離散型方式
T=1	1	X
T=2	$\min\{X, Y\}$	$X \times Y$

かつ，解像度レベルが 0 である最低品質を，それぞれ示している。この例では，どちらの階層数も 3 であることから，$\min\{3, 3\} = 3$ となる。階層数が異なる例として，例えば，フレームレート，解像度レベルの階層数が，それぞれ 5 および 2 の場合，必要な管理鍵の個数は，$\min\{5, 2\} = 2$ となる。

5. 評　　価

本手法の効果を，必要となる管理鍵の個数について，2.2 節で述べた独立離散型方式と比較することにより評価する。ここで，1 つの動画コンテンツにおいて，符号化列は 1 つであり，制御対象は 3.1 節の階層条件を有することを前提とする。

制御対象が 1 つ（$T = 1$） の場合は，表 1 に示すように，本手法で必要となる管理鍵の個数は，制御対象の階層数に関わらず，常に 1 つである。一方，独立離散型方式は，制御対象の階層数と同数の管理鍵が必要となる。すなわち，階層数を X とすると X 個の管理鍵を要する。

制御対象を 2 つ（$T = 2$） に拡張した場合，表 1 に示すとおり，各制御対象の階層数を X および Y とすると，本手法では，$\min\{X, Y\}$個の管理鍵を必要とする。一方，独立離散型方式では，$X \times Y$ 個の管理鍵が必要となる。

以上より，本手法は，独立離散型方式と比較した場合，$T = 1$ の場合は $1/X$ 倍，$T = 2$ の場合は $1/\max\{X, Y\}$倍に削減される。したがって，階層数が大きいほど，本手法の効果が大きいことがわかる。

6. 結　　言

本研究では，鍵管理および配送において効果

的な暗号鍵生成法を，時間軸を考慮したディジタル動画像に応用することで，新しいアクセス制御方式を考案した。

(1) 制御対象が 1 つの場合，必要な管理鍵および配送鍵はどちらもただ 1 つである。

(2) 制御対象が 2 つの場合，対象の階層数 X および Y とすると，管理鍵および配送鍵は $\min\{X, Y\}$個である。

(3) 独立離散型方式との比較により本手法の有効性を評価した。

なお，本研究は，平成 21 年度（独）科学技術振興機構のシーズ発掘試験「暗号鍵の生成・管理を考慮したディジタル動画像のアクセス制御」において実施したものである。

参考文献

1）Y. Wu，D. Ma，and R.H. Deng，“Progressive Protection of JPEG 2000 Code-streams”，Proc. IEEE Int. Conf. Image Process.，2004，p3447‐3450.

2）須賀祐治，岩村恵一，“一方向性ハッシュ関数を用いた階層構造を持つアクセス制御方式”，（社）情報処理学会 コンピュータセキュリティシンポジウム，2003，p295–300.

3）S. Imaizumi，M. Fujiyoshi，and H. Kiya，“Efficient Collusion Attack-free Access Control for Multidimensionally Hierarchical Scalability Content”，Proc. IEEE Int. Sympo. Circuits and Sys.，2009，p505-508.