スケーラブル符号化画像に対するアクセス制御のための効果的な暗号鍵生成方式

An Efficient Key Derivation Method for Access Control of Scalable Coded Images

今泉祥子 † Shoko IMAIZUMI　藤吉正明 ‡ Masaaki FUJIYOSHI　貴家仁志 ‡ Hitoshi KIYA　青木直和 † Naokazu AOKI　小林裕幸 † Hiroyuki KOBAYASHI

千葉大学大学院　融合科学研究科 †
Graduate School of Advanced Integration Science, Chiba University
首都大学東京　システムデザイン学部 ‡
Faculty of System Design, Tokyo Metropolitan University

1　まえがき

本稿では，スケーラブル符号化を施された画像を対象に，アクセス制御のための効率的な暗号鍵生成法を提案する．提案法は，鍵管理の安全性と煩雑性の観点から，サービス事業者が管理する鍵（管理鍵）をただ一つとする．この管理鍵は，いずれのユーザに対しても配送されることはない．また，ユーザがコンテンツ再生のために受信する鍵（配送鍵）の個数は，従来法 [1] 以下とする．暗号鍵生成には，ハッシュ連鎖および巡回シフトを用いることで, 演算量の効率性を考慮している．

2　スケーラブル符号化画像に対するアクセス制御

スケーラブル符号化として JPEG 2000 符号化 [2]（以降，JP2 と略）を施された画像を用いて，そのアクセス制御について説明する．JP2 符号化画像のアクセス制御では，SNR，解像度，色数が制御対象となる．ここで，レイヤ数を 5（$N_1 = 5$），解像度レベル数を 3（$N_2 = 3$）とすると，JP2 符号化画像の復号パターンは図 1 にまとめられる．D_{n_1,n_2} は暗号化処理を施す単位データであり，n_1 はレイヤ，n_2 は解像度レベルの番号を示す．単位データ D_{n_1,n_2} は同図に示す矢印の順序で復号される．また，Q_{n_1,n_2} は復号される JP2 符号化画像の再生品質を示しており，アクセス制御は品質 Q_{n_1,n_2} に基づいて施される．

3　提案法

一つの管理鍵から従属的に暗号鍵を生成する効率的な提案手法について説明する．図 1 の例に対応した暗号鍵生成法を図 2 に示す．図 2 において，K_{n_1,n_2} は単位データ D_{n_1,n_2} に対する暗号鍵である．ここで，K_m が提案法における唯一の管理鍵であり，いずれの単位データに対する暗号鍵にもならない．まず，管理鍵 K_m に対して，ある一定の巡回シフトを行った後，ハッシュ演算を施したものを単位データ $D_{4,2}$ に対する暗号鍵 $K_{4,2}$ とする．次に $K_{4,2}$ に同様の処理を施したものを $K_{4,1}$，さらに $K_{4,1}$ にこの処理を施したものを $K_{4,0}$ とする．巡回シフトとハッシュ演算の組合せ処理を $f()$ とすると，上述の関係は，

$$K_{4,n_2} = f^{3-n_2}(K_m), \quad n_2 = 2,1,0 \tag{1}$$

と表される．ここで，$f^b(a)$ は，a に対して組合せ処理を b 回施すことを意味している．この組合せ処理は，図 2 において，白矢印で示されている．その他の暗号鍵 K_{n_1,n_2} $(n_1 = 3,2,1,0, \quad n_2 = 2,1,0)$ は，式 (1) より生成された

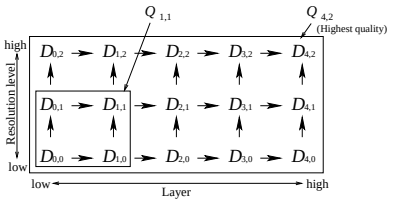

図 1　JP2 符号化画像の復号パターンの例

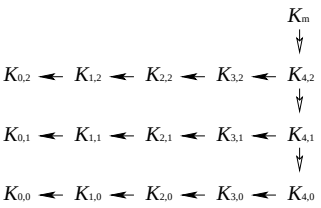

図 2　ハッシュ連鎖および巡回シフトを用いた提案手法

表 1　提案法と従来法 [1] の比較.

	提案法	従来法 [1]
管理鍵	1	$\min N_1, N_2$
配送鍵	1〜$\min N_1, N_2$	$\min N_1, N_2$
管理鍵の配送	無	有

K_{4,n_2} $(n_2 = 2,1,0)$ から，ハッシュ連鎖 $h()$ を用いて，

$$K_{n_1,n_2} = H^{4-n_1}(K_{4,n_2}), \quad n_1 = 3,2,1,0, \quad n_2 = 2,1,0 \tag{2}$$

により従属的に生成される．$h^b(a)$ は，a に対してハッシュ演算を b 回施すことを意味している．このハッシュ連鎖は，図 2 において，黒矢印で示されている．

このように，提案法は，巡回シフトとハッシュ連鎖のみを利用して，一つの管理鍵から各単位データに対する暗号鍵を生成できる．管理鍵は，いずれの単位データの暗号鍵にもならない．また，図 2 に示す提案法の暗号鍵生成順序では，原理的に結託攻撃が生じない．なお，演算量の観点から巡回シフトを用いているが，本アルゴリズムの実現はこれに限定されるものではない．

4　評価

提案法の効果を，管理鍵・配送鍵の個数と管理鍵の配送について，従来法 [1] と比較した結果を表 1 に示す．結託攻撃耐性については，提案法，従来法 [1] ともに考慮されている．同表より，提案法の有効性が示された．

5　あとがき

本稿では，スケーラブル符号化を施された画像を対象に，アクセス制御のため効率的な暗号鍵生成法を提案した．提案法は，ハッシュ連鎖と巡回シフトから構成され，管理鍵の個数をただ一つ，配送鍵の個数を従来法以下としている．さらに，提案法は，結託攻撃耐性を有する．

今後の課題として，電子透かしや改ざん検出への応用を検討する．

参考文献

[1] 今泉祥子, 阿部淑人, 藤吉正明, 貴家仁志, “一方向性ハッシュ関数を用いたディジタル動画像の効果的アクセス制御方式,” 映情学誌, vol.64, no.11, pp.1621–1627, Nov. 2010.

[2] *Information technology — JPEG 2000 image coding system – Part 1: Core coding system.* ISO/IEC IS–15444–1, 2004.