様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　5 月　21 日現在

機関番号：１２５０１
研究種目：研究活動スタート支援
研究期間：2011～2012
課題番号：２３８０００１０
研究課題名（和文）　視覚情報に基づくカラー画像のアクセス制御に関する研究

研究課題名（英文）　A Study on Access Control for Color Images Using Visual Information

研究代表者
今泉　祥子（IMAIZUMI SHOKO）
千葉大学・大学院融合科学研究科・助教
研究者番号：80535013

研究成果の概要（和文）：本研究では、再生環境の多様化に伴い、一つのコンテンツを様々な品質で再生可能とする要求に対応して､安全性および柔軟性が高いアクセス制御手法を開発した。また、表示色が限定された限定色画像に用いられる色、すなわち、インデックスカラーに着目し、視覚情報に基づいた表示色数によるアクセス制御手法について検討した。さらに、開発手法を用いて、限定色画像に対する著作権保護のための情報埋込技術に対する応用を行った。

研究成果の概要（英文）：With the rapid growth in communication channels and terminals, scalable transmission has become popular. First, we have developed a secure and flexible access control scheme for scalable media. Next, we have also proposed a color-based access control scheme by sorting indexed colors in palette-based images. Furthermore, our proposed sorting scheme for indexed colors has applied to information hiding for palette-based images.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１１年度	1,200,000	360,000	1,560,000
２０１２年度	1,100,000	330,000	1,430,000
年度			
年度			
年度			
総　計	2,300,000	690,000	2,990,000

研究分野：工学
科研費の分科・細目：メディア情報学・データベース
キーワード：アクセス制御、著作権保護、鍵管理、ハッシュ関数、限定色画像、インデックスカラー、ユークリッド距離、情報埋込

１．研究開始当初の背景

近年、ネットワークや DVD などの記憶媒体を介した、商品としての画像の流通が増加しており、その著作権保護、プライバシー保護が問題となっている。電子透かしは、画像に著作権情報を埋め込むことにより、不正利用を抑止する方式である。しかし、この方式では、画像の不正利用や不正コピーを未然に防ぐことが困難である。また、画像に含まれるプライバシー情報を保護することもできない。一方、画像情報全体を暗号化する手法は、暗号化した情報を完全に復号しなければ画像の内容を確認することができず、正規ユーザであっても内容の閲覧や検索に大きな制約が伴う。さらに、通信路や通信端末など再生環境の多様化により、一つの画像をユーザ権限に応じて様々な品質で提供することが求められているが、この要求に対応するこ

とも困難である。
　一つの画像を解像度や色数などの品質に応じて、複数の単位データに分け、それらの単位データを優先順位付け（階層化）し、単位データごとに暗号処理を施す手法がある。これにより、画像情報の一部のみの暗号解除および再生が可能となり利便性が向上する。その結果、正規ユーザに対してその権利に応じた品質で画像を提供するアクセス制御が実現する。アクセス制御では、単位データごとに異なる鍵を割り当てるため、階層が複雑になり単位データが増加すると鍵の個数も増加する。このことは、鍵管理・配送にかかる安全性・容易性の観点から問題となる。
　これまで、上述の問題を解決するため、効率的な暗号鍵生成法を用いたアクセス制御に関して様々な研究がなされてきた。これらの研究における暗号鍵生成にはハッシュ関数が用いられている。ハッシュ関数は、出力値から入力値を算出することが極めて困難な一方向性関数である。ハッシュ関数の導入により、各単位データに対する暗号鍵を従属的に生成し、暗号鍵の増加を抑止している。しかしながら、これらの研究は、単位データの階層構造が真部分集合の階層構造であることが条件となる。これまでに申請者は、ハッシュ関数を用いたアクセス制御について、検討してきた。

２．研究の目的

(1)　従来のアクセス制御技術では、鍵管理・配送にかかる安全性と容易性を高めるために、画像の階層構造は真部分集合の関係であることが条件となり、別の階層構造に対応するためには、鍵の個数が著しく増加する。そこで、本研究では、複雑な階層構造をもつ画像に対しても、鍵の増加を従来方式より削減し、効率的なアクセス制御方式を構築する。また、すでにハッシュ関数の応用や論理演算の導入などによる考察を行っているところであるが、リアルタイム処理や配信サービスへの実用性の観点から、具体的な演算量および処理速度を解析し、従来方式より演算量を削減する手法について検討する。

(2)　カラー画像における表示色数に対してアクセス制御を施すことを考える。例えば、フルカラー画像（図 1）に減色処理を施して生成される限定色画像（図 2）は、カラーマップと呼ばれる色定義テーブルの中から各画素の色が参照番号として指定される。カラーマップの生成方法は、表示速度、圧縮効率などの様々な観点から研究されている。本研究では、解像度などの品質に応じた限定色画像のためのカラーマップの生成方法について、人間の視覚に基づいた評価手法で調査・


図 1. フルカラー画像


図 2. 限定色画像

実験し、(1)で構築したアクセス制御方式の安全性と効率性を保持した手法を確立する。

３．研究の方法

(1)　本研究では、複数の画像品質に対して細分化された階層構造が設定された場合に、この階層構造に適したアクセス制御方式を構築するとともに、暗号鍵の個数を従来方式より 50 %以上抑制する暗号鍵生成手法を確立する。この技術は、従来方式と同様にハッシュ関数の利用に基づく。しかしながら、単純な一次元的な利用ではなく、多次元的な利用により、実現を見込んでいる。ハッシュ関数のみの利用で実現困難な場合には、他の演算を追加しながら検討を行う。

(2) 暗号鍵の個数を抑えるため、ハッシュ関数を多次元方向に対して単純に再帰利用することは、暗号鍵生成にかかる処理動作を重くする。本研究では、リアルタイム処理を考慮し、ハッシュ関数のみの利用に限らず、比較的処理が軽いビットシフト演算を組み合わせて用いることで、暗号鍵生成にかかる全体の処理量を削減した。ただし、このとき追加されるパラメータ（ビットシフトにおけるシフト量など）は、ユーザが受信する鍵情報の一部となるため、安全性の観点から、パラメータについても著しい増加を回避するよう考慮している。

(3) 表示色に基づくアクセス制御方式への展開を図るため、少ない色数で画像を表示するための表示色選択アルゴリズムを構築した。また、この過程において、限定色表示に適した色のソート手法を検討した。ソートの方法は、画素上で隣り合う頻度に応じたソート法、輝度値の近さに応じたソート法など様々な研究がなされておりこれらの手法を参考とした。

４．研究成果

(1)　本研究では、管理鍵を 1 個のみとし、かつ、結託攻撃耐性を有する暗号鍵派生法を提案し、コンテンツを構成する個々のメディアに、複数の品質尺度に階層構造を設定可能

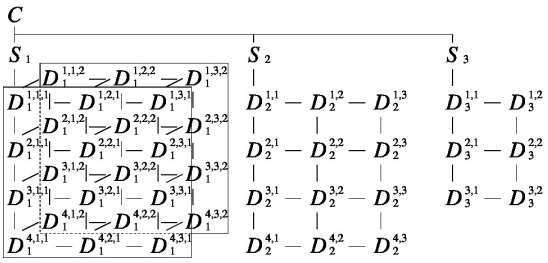

図 3. コンテンツの構成例

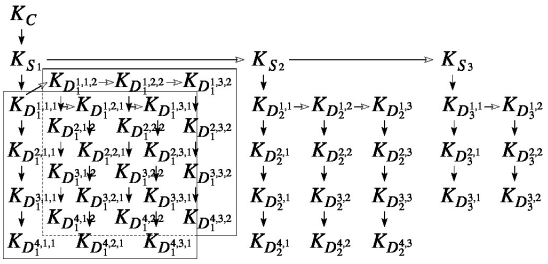

図 4. 暗号鍵生成アルゴリズム

とするアクセス制御方式を開発した。図 3 に示すコンテンツを例に、図 4 に暗号鍵生成アルゴリズムを示す。まず、次式に示すように、管理鍵 K_C に対してハッシュ演算を施したものを、メディア S_1 に対する初期鍵 K_{S1} とする。

$$K_{S1} = H(K_c) \quad (1)$$

ハッシュ演算およびハッシュ連鎖は、図 4 において黒矢印で示されている。次に、K_C と式(1)より算出された K_{S1} を用いて、

$$K_{S2} = H(F(K_c, K_{S1}) \quad (2)$$

より、メディア S_2 に対する初期鍵 K_{S2} を算出する。ここで、関数 $F(\ )$は結合関数を表す。さらに、K_{S1} と K_{S2} を用いて、式(2) と同様、

$$K_{S3} = H(F(K_{S1}, K_{S2}) \quad (3)$$

により、メディア S_3 に対する初期鍵 K_{S3} を算出する。上式(2)、(3) に示すように、本手法では、算出されたハッシュ値を再度用いる再帰ハッシュ連鎖を導入することで、各メディアの初期鍵をそれぞれ派生している。図 4 において、再帰ハッシュ連鎖は白矢印で示されている。

さらに、各メディアの単位データに対する暗号鍵についても、ハッシュ連鎖と再帰ハッシュ連鎖を組合せて用いることで従属的に派生される。例えば、メディア S_1 の単位データ $D_1^{n_1^1,n_1^2,n_1^3}$ に対する暗号鍵 $K_{D1^{n_1^1,n_1^2,n_1^3}}$ は、階層数が少ない方向から順に以下の式を用いて順に生成される。

$$K_{D1^{1,1,n_1^3}} = H(F(K_{D1^{1,1,n_1^3-1}}, K_{D1^{1,2,n_1^3-1}}) \quad (4)$$

$$K_{D1^{1,n_1^2,n_1^3}} = H(F(K_{D1^{1,n_1^2-1,n_1^3}}, K_{D1^{2,n_1^2-1,n_1^3}}) \quad (5)$$

$$K_{D1^{n_1^1,n_1^2,n_1^3}} = H(K_{D1^{n_1^1-1,n_1^2,n_1^3}}) \quad (6)$$

以上のように、本手法では、再帰ハッシュ連鎖を導入することで、各メディアの複数の品質尺度に階層構造を設定しても、一つの管理鍵から各単位データに対する暗号鍵を派生可能である。また、本手法は、あらゆる結託攻撃に対して耐性を考慮している。図 4 に示すとおり、各メディアを関連付ける暗号鍵は、いずれの単位データにも割り当てられず、各メディアは、見かけ上、それぞれ独立な暗号鍵で暗号化される。また、いずれの品質尺度の階層についても、下位の階層から上位の階層に対する暗号鍵は派生できない。これにより、複数ユーザが互いの暗号鍵を共有し、組合せて用いても、許諾されていない単位データに対する暗号鍵は派生することはできない。このように、本手法は、許諾されていないメディア及び許諾されていない高品質での不正再生を防いでいる。

また、従来法においては、制御対象となるメディアの種類や各メディアの品質尺度の個数が増加するにつれて、管理鍵の個数も増加した。しかし、本手法では、これらのいずれの増加にも関わらず、管理鍵は 1 個のみであり、目標である 50 %以上の削減を達成した。さらに、本手法における再帰ハッシュ演算部に対して、ビットシフト演算に置き換えることで演算量の削減も達成している。

(2)　本研究では、まず、図 5 に示すように、カラーパレット内のインデックスカラーをユークリッド距離による類似度の順番にソートする手法を構築した。

index	R	G	B
0	r_0	g_0	b_0
1	r_1	g_1	b_1
2	r_2	g_2	b_2
3	r_3	g_3	b_3
4	r_4	g_4	b_4
⋮	⋮	⋮	⋮
255	r_{255}	g_{255}	b_{255}

index	
0	$argmin(255^2r + 255g + b)$
1	$argmin(\delta_{0,I_h})$
2	$argmin(\delta_{1,I_h})$
3	$argmin(\delta_{2,I_h})$
4	$argmin(\delta_{3,I_h})$
⋮	⋮
255	$argmin(\delta_{254,I_h})$

図 5. インデックスカラーのソート手法

[Step 1] 代表色 C_i に対して、

$$a_i = 256^2 r_i + 256^1 g_i + 256^0 b_i, \quad i = 0, 1, 2, \ldots \quad (7)$$

より、2 色間の色差 a_i を計算し、$\arg\min a_i$ となる代表色 C_i を C'_0 とする。

[Step 2] 直前にインデックスが割り当てられた色を $C'_{I_{h-1}}$ とする。インデックスが割り当てられていない代表色の中から、$\arg\min \delta_{I_{h-1},I_h}$ となる代表色 C'_{I_h} を $I_{h-1} + 1$

番目の色とする。
[Step 3] すべての代表色にインデックスが割り当てられるまで、[Step 2] を繰り返す。
以上の手順により、インデックスの隣同士は類似色が配置される。本研究では、これを利用して、限定色画像における使用色の選択を可能とした。

(3) さらに、(2)で考案したインデックスカラーのソート手法を用いて、大容量かつ低劣化な情報埋込法を開発した。256×256 画素の 12 枚の画像に対して、21,000 ビットまたは 45,000 ビットを埋め込むシミュレーションを行った。図 6 に、提案手法あるいは従来手法を用いて、それぞれ 21,000 ビットを埋め込んだ結果を示す。さらに、表 1 および表 2 に、21,000 ビットおよび 45,000 ビットの埋め込みを行った際の PSNR における比較を示す。以上より、従来手法と比較して、効果的な結果が得られていることがわかる。

(a) 原画像

(b) 提案手法による埋込画像

(c) 従来手法による埋込画像

図 6. 埋込画像の比較(埋込量: 21,000 ビット)

表 1. PSNR 評価（埋込量: 21,000 ビット）

	提案手法	従来手法
Aerial	41.34	37.97
Lenna	41.96	39.02
Parrots	38.13	35.34

表 2. PSNR 評価（埋込量: 45,000 ビット）

	提案手法	従来手法
Aerial	35.53	34.59
Lenna	36.00	35.68
Parrots	32.11	31.51

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）
① 今泉祥子，“コンテンツ配信サービスにおけるアクセス制御と鍵管理，”日本印刷学会学会誌，vol. 49，no. 3，2012 年.

〔学会発表〕（計 8 件）
① Shoko IMAIZUMI, “A Collusion-Free Key Assignment Scheme for Hierarchical Access Control Using Recursive Hash Chains,” IEEE International Symposium on Circuits and Systems, Beijing, China, 20th May, 2013.

② 小澤慶，“限定色画像に対する多ビットステガノグラフィ，” 電子情報通信学会総合大会，岐阜大学（岐阜市），2013 年 3 月 20 日.

③ Kei OZAWA, “A High-Capacity Data Embedding Scheme for Palette-Based Images with High Image Quality,” International Workshop on Advanced Image Technology, Nagoya, Japan, 8th January, 2013.

④ Shoko IMAIZUMI, “Multi-dimensional Key Assignment for Hierarchical Media Access Control with Collusion Resilience,” IARIA International Conference on Systems and Networks Communications, Lisbon, Portugal, 20th November, 2012.

⑤ 小澤慶，“限定色画像に対する多ビット情報埋込法の画質改善，” 電子情報通信学会マルチメディア情報ハイディング・エンリッチメント研究会，山口大学（山口市），2012 年 8 月 28 日.

⑥ Shoko IMAIZUMI, “Hierarchical Key Assignment Scheme for Multimedia Access

Control with Modified Hash Chain," IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Piraeus, Greece, 20th July, 2012.

⑦ Shoko IMAIZUMI, "Key Derivation Scheme for Hierarchical Access Control to Multimedia Content," International Workshop on Advanced Image Technology, Ho Chi Minh City, Vietnam, 10th January, 2012.

⑧ 今泉祥子, "メディアアクセス制御のための再帰ハッシュ連鎖型多次元鍵派生方式," 電子情報通信学会暗号と情報セキュリティシンポジウム, 金沢エクセルホテル東急（金沢市), 2012 年 2 月 2 日.

〔図書〕（計 1 件）

① Shoko Imaizumi, Masaaki Fujiyoshi, and Hitoshi Kiya, "A Novel Access Control Scheme for Multimedia Content with Modified Hash Chain," in Multimedia - A Multidisciplinary Approach to Complex Issues (edited by Ioannis Karydis), pp.85–98, Intech, 2012.

６．研究組織

(1)研究代表者

今泉　祥子（IMAIZUMI SHOKO）

千葉大学・融合科学研究科・助教

研究者番号：80535013

(2)研究分担者

なし

(3)連携研究者

なし