N-035

プライバシー保護のための閲覧者権限に応じた画像フィルタリング手法の提案

A proposal of image masking method with hierarchical access control for privacy protection

本多　隼也† Toshiya HONDA　村上　佑馬‡ Yuma MURAKAMI　熊木　武志† Takeshi KUMAKI　藤野　毅† Takeshi FUJINO

1. 背　　景

近年，人が多く集まる場所や，金銭のやり取りが行われる場所において，犯罪防止を目的とした，監視カメラの設置が進んでいる．撮影された画像は，犯罪発生時の証拠物件として利用され，特に，人物の顔は個人を特定することができる重要な情報となる．しかし一方では，監視カメラにより不特定多数の人が，本人が了知しえないまま撮影される事があり，その画像の取り扱い次第ではプライバシー侵害につながる恐れがある[1].

本稿では，監視カメラによる悪意を持った人物への犯罪抑止力と，その他の被撮影者のプライバシー保護を両立させるために，顔等個人の特定につながる箇所をリアルタイムにマスク処理しつつ，画像を閲覧する権限を有する者に対しては任意のタイミングでマスクを解除して犯罪捜査等の目的に応じて撮影画像を復元可能な，HMF(Hierarchical-Masked image Filtering)法を提案する．

2. 従来の画像マスク手法とその問題点

市場に流通している監視カメラの一部には，プライバシー保護機能を有する物がある．最も一般的な方式として，事前に使用者がマスク範囲を指定し，画像を塗りつぶす方式がある．この方式は，定点撮影が主用途であり，マスク対象が移動しない場合には有効であるが，車載カメラ等カメラが移動する場合や，マスク対象が移動する場合は有効とは言えない．また，犯罪捜査等で画像を利用する際に，塗りつぶしによるマスク箇所は復元できない．これを解決するために，撮影画像からマスク箇所の原画像を分離して別に保存する手法[2]が提案されているが，この手法は元画像を復元する際に，別途保存領域を必要とする上，復元作業に時間を要する．また，ネットワークカメラシステムに適用した場合，リアルタイム性が損なわれる恐れがある．

これらの従来手法に対し，図 1 に示す HMF 法は物体検出により動的にマスク箇所を判定し，その画素値と乱数の排他的論理和を適用することで，マスク機能及びその解除機能を実現するシステムである．

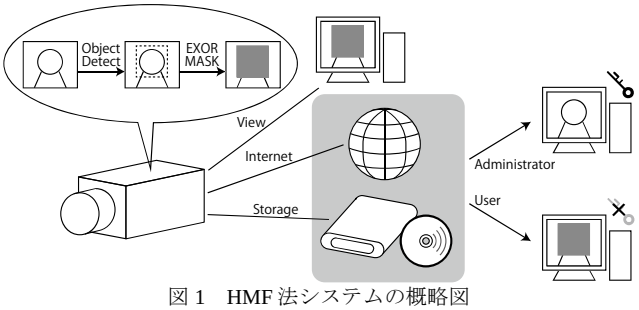


図 1　HMF 法システムの概略図

†立命館大学理工学部

‡立命館大学理工学研究科

マスクされた画像データ(または動画内の 1 フレーム)及び乱数シードのみを与えることで，排他的論理和により高速に元画像が復元できる．その結果，ネットワークカメラシステム等でも，乱数シードを持つ閲覧者はリアルタイムに画像を確認できる．また，複数の物体検出器を用いて階層的にマスク処理を行い，閲覧者の権限に応じてマスク解除の範囲を柔軟に変更することも可能である．

3. HMF(Hierarchical-Masked Image Filtering)法

3.1　マスク処理の方法

可逆圧縮である画像データの場合，画素毎に RGB 成分の値が格納されている．マスク対象画素の i 番目を a_i，生成した乱数の i 番目を r_i とすると，マスク後の画素値 a'_i は排他的論理和を用いて

$$a'_i = a_i \oplus r_i \quad (1)$$

で表現される．マスク解除は，逆変換

$$a_i = a'_i \oplus r_i \quad (2)$$

で実現される．

図 2 は，画像の一部を指定し，その画素値に乱数との排他的論理和を適用した結果である．マスクした箇所は元画像が識別不能となる．この画像に同じ乱数との排他的論理和を再度適用すると，画像は復元される．

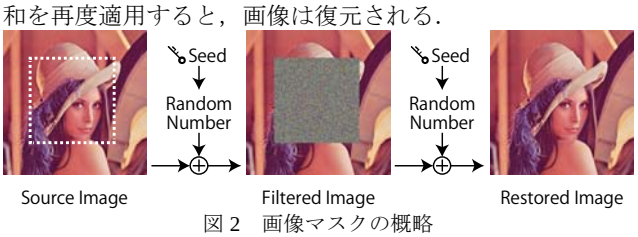


図 2　画像マスクの概略

本方式は排他的論理和により画像マスクを実現しているため，異なる乱数シードにより生成された乱数列を用いることで，階層的なマスク画像を生成できる．マスク を適用したい画素列の k 番目の値を a_k，乱数シード s1 から生成された乱数列 r1 の k 番目の値を $r1_k$，乱数シード s2 から生成された乱数列 r2 の k 番目の値を $r2_k$ とすると，マスク適用後の画素値 a'_k は，

$$a'_k = a_k \oplus r1_k \oplus r2_k \quad (3)$$

となる．乱数列 r1 のみが適用された箇所は，マスク後の画素値と乱数列 r1 との排他的論理和により復元できるが，乱数列 r1 及び r2 でマスクされた画素値と乱数列 r1 の排他的論理和をとっても，

$$a''_k = a'_k \oplus r1_k = a_k \oplus r2_k \quad (4)$$

となり，復号はできない．a''_k は，さらに乱数列 r2 と排他的論理和をとることで，

$$a_k = a''_k \oplus r2_k \quad (5)$$

となり，元画像に復元できる．このことを利用して，複数箇所に異なる乱数列との排他的論理和を適用することで，権限に応じて閲覧可能な範囲を制限できる．

例として，画像の複数箇所(顔全体と目)に別々の乱数を適用した結果を，図 3 に示す．まず，原画像(a)の目と顔の部分に乱数シード seed1 及び seed2 を施すことで，(b)のマスク画像が生成される． この画像に seed1 から生成された乱数との排他的論理和を適用すると，目を除く顔全体のマスクが外れる．さらに， seed2 との排他的論理和を適用すると，完全に元の画像を復元できる．したがって，全部閲覧する権限を持つ者には seed1 および seed2 を渡し，目以外を閲覧する権限を持つ者には seed1 のみを渡すことで，権限に基づいて階層的に閲覧範囲を制限できる．

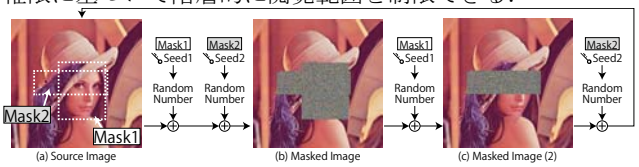


図 3　階層型マスクの概略

3.2　擬似乱数生成アルゴリズム

被撮影者のプライバシー保護のためには，不特定多数の人物に撮影画像を見られないことが重要となる．従って，マスク処理に用いる乱数は，十分な安全性を確保するために以下の特徴を持つ必要がある．

- 攻撃に対する耐性を持つ
- 予測不可能性を持つ
- マスク解除のための再現性を持つ
- 乱数生成速度が高速である

擬似乱数生成アルゴリズムは多数存在するが，以上の条件を満たすものとして本稿では，1997 年に松本眞により発表された[3]，Mersenne Twister MT19937 を用いる．実装では予測不可能性を向上させるために生成した乱数の一部を切り捨てて使用したが，有効性については今後詳細な検証を行っていく．

4. JPEG 方式における画像マスク

4.1　概要

JPEG (Joint Photographic Experts Group)方式は，画像圧縮フォーマットとして幅広く用いられている．また，動画圧縮フォーマットである Motion JPEG や MPEG (Moving Picture Experts Group)も，フレームの画像圧縮に JPEG と同様の処理を行っている．

JPEG は圧縮過程で高周波成分を切り捨てる，非可逆のアルゴリズムであるため，HMF 法を適用する場合， JPEG 圧縮・展開処理のうち，可逆の過程で排他的論理和をとらなければならない．

4.2　JPEGマスク画像の生成

JPEG の圧縮過程のうち，量子化後のエントロピー符号化は可逆処理である．そこで本稿では図 4 に示すように，指定したビット長の乱数との排他的論理和を，量子化後の画像データのうち画像の特徴を最も表している DC 成分（可変長）の下位ビットからとることにより，高速に復元可能な JPEG マスク画像の生成を行う．

MPEG 方式についても，I フレームについては JPEG と同様の処理を行う．一方，P/B フレームは，復号された I フレーム，または I フレームを参照した P フレームを参照するため，I フレームにこの処理を施すことにより，復元可能な MPEG マスク映像を生成できる[4].

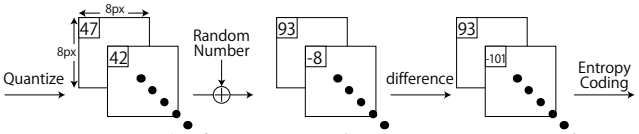
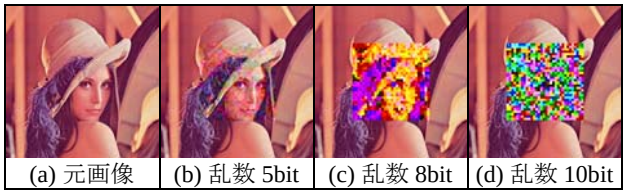


図 4　JPEG 画像ブロックの DC 成分に対する HMF 法の適用

4.3　実装と評価

本節では，JPEG 処理ライブラリである Independent JPEG Group’s JPEG software release 8c[5]を用い，HMF 法によるマスク処理を行った JPEG 画像を生成した．

乱数ビット幅の変化による，マスク結果の変化について図 5 にまとめた．JPEG では 8 x 8 ピクセル単位で圧縮が行われるため，マスクも 8 x 8 ピクセル単位で行われていることがわかる．



(a) 元画像　(b) 乱数 5bit　(c) 乱数 8bit　(d) 乱数 10bit

図 5　乱数ビット幅の変化によるマスク結果の比較

マスク処理に使用する乱数ビット幅を大きくすると，DC 成分値の変化量も大きくなるため，マスクの影響は大きく変化する．従って，用途に合わせて使用する乱数ビット幅を変化させることで，マスクの強度を変化させることが可能である．例えば，図 5(c)に示した程度のマスク強度であれば，顔の存在や向きは識別できる．一方で，図 5(d)の場合は，マスク対象が識別できない．図 5(b)程度であれば，画像は劣化しているもののマスク対象がおおよそ判別できるため，デジタルコンテンツの保護にも利用できる．

5. まとめ

本論文では，プライバシー保護のための閲覧者権限に応じた画像マスク手法として，HMF 法を提案した．HMF 法では被撮影者のプライバシーを保護しつつ，監視カメラによる防犯効果を実現できる．この手法は，ネットワークカメラの撮影画像に対するセキュリティの維持，支払いに応じたデジタルコンテンツ配信等への応用が考えられる．

参　考　文　献

[1] 柳井　啓司, "人物を認識することの法的問題点～監視カメラシステムの設置運用基準～," IPSJ Magazine, Vol.48, No.1, Jan. 2007.

[2] 井上　学, "監視カメラシステム," 特開 2008-288744 , 2008-11-27.

[3] M. Matsumoto and T. Nishimura, “Mersenne Twister: A 623-dimentionally equidistributed uniform pseudo-random number generator,” ACM Trans. On Modeling and Computer Simulation, Vol. 8, No1, pp.3-30, Jan.1998

[4] Y. Nemoto, Y. Toyota, S. Sakazawa, L. Zhao, and H. Yamamoto, “A Study on Video Scrambling Considering Inter-Frame Prediction,” IWAIT2006, pp.192-197, 2006

[5] http://www.ijg.org/