3L4-OS-06c-1

プライバシを考慮した防犯カメラ映像処理

Privacy-aware processing for surveillance video

舩冨 卓哉 *1 Takuya Funatomi
川西 康友*1 Yasutomo Kawanishi
美濃 導彦*1 Michihiko Minoh
森村 吉貴*2 Yoshitaka Morimura
満上 育久*3 Ikuhisa Mitsugami

*1京都大学 学術情報メディアセンター
Academic Center for Computing and Media Studies, Kyoto University

*2京都大学 物質-細胞統合システム拠点
Institute for Integrated Cell-Material Sciences, Kyoto University

*3大阪大学 産業科学研究所
The Institute of Scientific and Industrial Research, Osaka University

A number of surveillance cameras are installed in public places. Their video will be very useful; browsing the video via internet will enable us to know how crowded, or face recognition technique will help us to search for a lost person or a crime suspect. However, such utilization is limited due to privacy issues. In this paper, we briefly present some techniques dealing with privacy issues for public use of the surveillance cameras.

1. はじめに

近年，観光地や商業施設，駅など至る所に解像度の高いカメラが設置されるようになってきた．こうしたカメラは，観光地のライブ映像をインターネットで公開しているものから，防犯目的で設置されているものなど，さまざまである．観光地に設置されたライブカメラからは，天候や混雑度などその地点の様子を，誰もがどこからでもリアルタイムで知ることができるように公開されている．このようなカメラはプライバシに配慮して，例えば人を大きく写さないように設置されていることが多い．一方，防犯目的で設置されたカメラは，そこに写る人の顔が判別できるよう設置されており，被撮影者のプライバシに配慮すると，公開することは不適切である．このように，現状では目的に応じてカメラが設置されており，一般に公開されているカメラ映像はほんの一部である．

これに対し我々は，多数設置されているカメラの利用価値を向上させることを目的として，カメラの設置目的によらず，それらが取得した情報を公開することができるよう，映像に対してプライバシに配慮した処理を施す技術の研究を行なっている．本稿では，これまでの我々の取り組みから 2 つの技術について紹介する．1 つめは，混雑状況等が一目で分かるよう，カメラ映像をインターネットへ公開するにあたり，被撮影者のプライバシを侵害しない映像を出力する「変身カメラ」である．2 つめは，防犯カメラ映像に対する人物検索システムを，迷子の捜索や見守りなどへ幅広く活用することを想定し，プライバシへの配慮として導入する利用制限についての技術である．

2. 変身カメラ - 背景画像生成を用いたリアルタイム映像変換

公共の場所を撮影した画像を公開しているサービスの一つに，Google ストリートビューがある*1．ここでは公道から撮影した画像が公開されており，プライバシを保護するための対策が行われている*2．具体的には，歩行者の顔がはっきりわかる場合やナンバープレートが読み取れる場合，これらを検出する技術により自動的にぼかし処理が行われ，個人や車両を特定できないようにしている．パターン認識技術の発展により，ナンバープレートや顔の検出はかなり進歩しているといえるが，それでも 100%の精度を保証するものではないのが現実である．実際，Google も自動ぼかし処理に加えて，この処理が施されていない画像の報告やユーザからの追加ぼかし処理・削除の依頼を受け付けている．

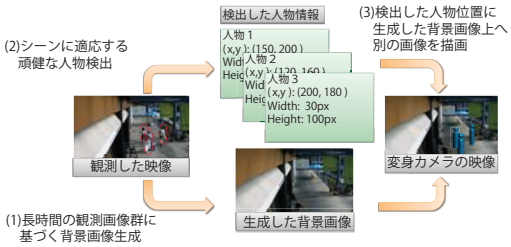


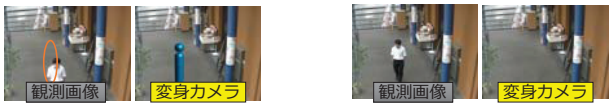
図 1: 「変身カメラ」処理の概要

しかし，カメラ映像をリアルタイムで公開する場合，後からぼかし処理を追加するだけでは不十分であり，確実に漏れのないプライバシ保護処理が必要である．変身カメラ [1] では，(1) 観測した映像から人の写っていない背景画像を生成し，(2) 映像中から検出した人の位置に (3) プライバシ情報を含まない別の画像を重畳した画像を出力する (図 1) という処理を行う．このアプローチであれば，仮に人物を検出できなかった場合，何も描画されずに背景画像だけが出力される (図 2(a))．また，人物が誤った位置に検出された場合，誤った位置に描画される (図 2(b)) だけである．これにより検出処理の失敗にプライバシ対策が影響されない．確実にプライバシ保護が実現できれば，混雑状況などプライバシに直結しない情報をリアルタイムで提供するサービスの実現に資すると考えられる．

連絡先: 舩冨卓哉，京都大学学術情報メディアセンター，京都市左京区吉田本町，funatomi@media.kyoto-u.ac.jp

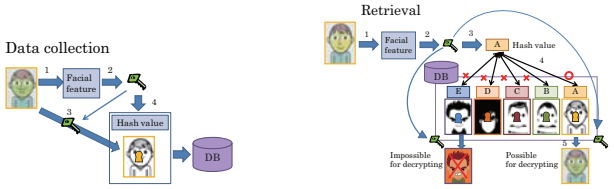
*1 http://www.google.co.jp/help/maps/streetview/ (平成 25 年 4 月 2 日取得)

*2 http://www.google.co.jp/intl/ja/help/maps/streetview/privacy.html (平成 25 年 4 月 2 日取得)



(a) 検出に失敗した場合　　(b) 検出を誤った場合

図 2: 人物検出に失敗した場合の変身カメラの出力



(a) 登録処理　　(b) 検索処理

図 3: 人物画像検索システムにおける暗号化の仕組み

背景画像の生成では，確実に人物を含まないようにするため，人物を検出して塗りつぶすのではなく，人物検出処理に依存しないアプローチをとる．防犯カメラ映像では，背景は同様のパターンが繰り返し観測されるが，人物が写った場合には人ごとに異なるパターンが観測される．このことに着目し，統計的な処理によって人物領域を含まない背景画像を生成する．単純な統計処理では，背景中の日照変化など，リアルタイムに状況を伝えるための情報を再現できないため，我々は背景の何度も観測される変化を保ちつつ，人物を確実に含まない背景画像を生成する技術を提案している [2].

3. 人物検索システムにおけるプライバシに配慮した利用制限法

防犯カメラで撮影された映像を後から分析し，容疑者の足取りを調査することで，事件解決に繋がるケースが増えている．このような分析が，警察だけでなく，一般にも利用できるようになれば，迷子の捜索や見守りにも活用することができると考えられる．利用者各自が分析をできるよう，防犯カメラ映像を一般公開することは，前述の通りプライバシ問題を引き起こす可能性がある．無用な映像の閲覧を制限できるよう，防犯カメラ映像から人物画像を検索できるシステムを構築することが有用であると考えられる．

システムの実現に向けて，防犯カメラの映像から人物画像を抽出し，保存しておくデータベースを導入することが考えられる．このデータベースには防犯カメラに写りうる全ての人物の画像がレコードとして含まれるため，データが流出すると重大なプライバシ問題を引き起こすと考えられる．プライバシへの配慮として，データベース中のレコードの閲覧を制限するため，我々はデータベース暗号化の枠組みを提案している．閲覧の制限として，何らかの人物画像をクエリとして検索を行った場合，その検索結果は復号して閲覧できるが，データベースに含まれる他のレコードは復号できず，閲覧できないようにする仕組みを提案している [3]．図 3 にこの手法の登録処理と，検索および復号を行う処理の流れを示す．

この制限は，データベース内のレコードをそれぞれ異なる鍵で暗号化することで実現する．この際，各レコードを暗号化する鍵は，それぞれの画像から抽出した人物の顔特徴を基に生成することにする．この処理により，同人物の画像からは同一の鍵，別人物の画像では別の鍵が生成できると考えられる．このような暗号鍵が生成できれば，クエリの画像と同じ人物の画像は，クエリから生成した暗号鍵で復号することができる．一方，それ以外の画像は暗号鍵が異なるため復号できず，閲覧不可能となると考えられる．また，データを復号する鍵は検索クエリから自動的に生成するため，データベースに画像を登録する際，その画像を暗号化した鍵はその場で破棄し，管理する必要がなくなるという利点がある．

ここで問題となるのは，カメラに写る人物に対し，画像から個別の鍵を生成できるかである．同一人物には同一の鍵を，異なる人物には異なる鍵を生成できるのが理想的であるが，これを 100%達成することは，即ち不特定多数の人物で画像による照合を完璧に行うことに相当し，これは困難である．実際には，同一人物に対して異なる鍵が生成されてしまうことによる検索精度低下と，異なる人物に対して同一の鍵が生成されてしまうことによるプライバシ脆弱性のトレードオフが発生する．我々は，顔特徴量を基にした鍵の生成法を検討し，公開顔画像 DB を用いた評価によって，これらの関係を数値的に示した [3]．これにより，完璧にプライバシを保護できないが，ある程度の検索精度低下を許せば，大多数の無関係なレコードへのアクセスを制限できることが示された．

しかし，データベースの暗号化だけでは，例えば Web などから入手できる特定人物の画像をクエリとして用いれば，その人物の行動を誰でも容易に把握することができることを示唆している．つまり，検索自体を制限しなければ，誰でも自由に他人の足取りを追うことができ，プライバシへの配慮が不十分であると考えられる．そこで我々は，人物画像の暗号化に非対称暗号化を導入することで，どんなカメラでも自由に暗号化できるようにする一方で，復号についてはクエリ画像から入手できる鍵に加え，検索について第三者からの承認を要求するような仕組みを導入することを検討している．

4. まとめ

本稿では，街中に多数設置されたカメラの開かれた活用を目指し，カメラ映像に対するプライバシに配慮した処理についての取り組みを紹介した．プライバシへの配慮には，パターン認識技術を利用して，映像から人に関する情報を抽出する必要があるが，現在の技術では 100%の精度での処理は保証できない．このようなパターン認識の誤りがプライバシ保護にできるだけ悪影響を与えないよう，技術の適用方法を工夫することが今後求められていくと考えられる．

謝辞　本研究の一部は，文科省「センサ情報の社会利用のためのコンテンツ化」，および「安全・安心な社会のための犯罪・テロ対策技術等を実用化するプログラム」の支援による．

参考文献

[1] I. Mitsugami, M. Mukunoki, Y. Kawanishi, H. Hattori, M. Minoh, “Privacy-Protected Camera for the Sensing Web”, Information Processing and Management of Uncertainty in Knowledge-Based Systems, 2010.

[2] 川西 康友, 椋木 雅之, 美濃 導彦, “隣接フレーム間の背景変化に着目した固有空間中での時系列フィルタに基づく背景画像推定”, 電子情報通信学会論文誌, Vol.J95-D No.9 PP.1759-1768, 2012.

[3] T. Fujita, T. Funatomi, Y. Morimura, M. Minoh, “Privacy-aware Database System for Retrieving Facial Images”, Information Processing and Management of Uncertainty in Knowledge-based Systems, 2012.