

[招待講演] 安心な映像サーベイランスのための プライバシー保護処理

馬場口 登†

†大阪大学 大学院工学研究科 電気電子情報工学専攻
〒565-0871 大阪府吹田市山田丘2-1
babaguchi@comm.eng.osaka-u.ac.jp

概要 本報告では安心な映像サーベイランスのためのプライバシー保護処理について議論する。まず、映像サーベイランスが安心安全な社会システムとして定着するために解決すべき課題を考察する。ついで、プライバシー保護機能を有する映像サーベイランスシステム PriSurv について述べる。PriSurv は、観察者と被写体の間でどのレベルまで視覚情報を開示するかを定めるプライバシーポリシーを取り決めて、開示情報を動的に変化させつつ映像を生成表示する。視覚的抽象化と呼ぶ画像処理オペレータを利用して視覚情報の開示制御を行い、被写体のプライバシー保護を図る。抽象化を実現するための画像の層状表現についても述べる。

Privacy Protected Visual Processing for Secure Video Surveillance

Noboru Babaguchi†

†Graduate School of Engineering, Osaka University
2-1 Yamadaoka, Suita, Osaka 565-0871, Japan
babaguchi@comm.eng.osaka-u.ac.jp

Abstract This report discusses privacy protected processing for secure video surveillance. The problems to be solved for realization as a secure social system are pointed out. A video surveillance system, named PriSurv, with privacy protecting mechanism is presented. To protect the privacy of subjects to be imaged, PriSurv is able to produce an image sequence that can be adaptively changed according to the privacy policy between the viewer and subject. To control disclosure of the subject's visual information, visual abstraction is introduced in PriSurv. The stratified representation of images for visual abstraction is also described.

1 はじめに

安全・安心な社会に直接結びつく情報通信 (ICT) 技術の一つに、視覚センサーネットワークによる映像サーベイランス (video surveillance) がある。映像サーベイランスとは、カメラ等の視覚センサーが多数、ネットワークで結合されたものから得られる画像・映像情報を基に、コンピュータビジョンや画像解析の技術を駆使し、自動的に環境やオブジェクト (人や車など) を監視するシステムに関する総合的な技術を指し、その社会的重要性が早くから指摘されてきた。

映像サーベイランスの研究は、図 1 に示す 3 つの

軸に展開できると考えられる。第 1 は、人物追跡、イベント検出、個人識別などの映像サーベイランスに不可欠な要素技術の高精度化である。これらは、パターン認識やコンピュータビジョンの応用事例として多くの研究者の関心を集めてきた。第 2 は、サーベイランスシステムの広域化・ユビキタス化の軸である。このためには、センサーネットのインフラ整備や大量カメラの連携法などが主要な課題となる。第 3 は、ヒューマンファクタである。これに関して、大量のサーベイランスカメラからの映像・画像をどのように見やすく表示するかなどが課題として挙げられる。

ここで、第 3 の軸に配されるプライバシー保護に

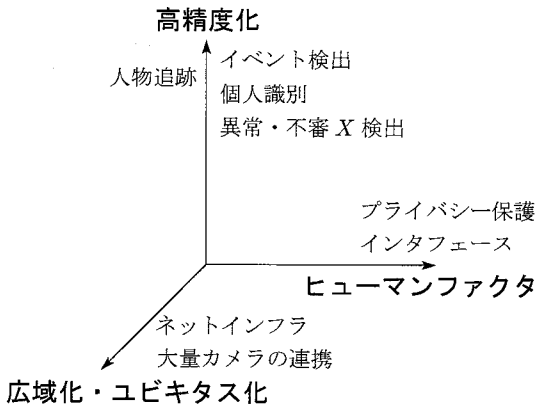


図 1: 映像サーベイランスの展開軸

関して考えよう。映像サーベイランスについては、実写映像を撮ることによる被写体へのプライバシー侵害の問題が背後にあるため、ややもするとその実現に懐疑的ないしは否定的な見方をされることもある。2005年4月の個人情報保護法の成立が証しているように、個人情報の保護・管理は益々厳しくなる傾向にある。犯罪とは無関係の場所、コンテキストにおいて、知らぬ間に自分の実写映像が撮影される可能性のある映像サーベイランスへの不安感はある意味で納得できるものである。また元来、CCTV(Closed-Circuit TV)と呼ばれていたサーベイランス(監視)カメラの映像が仮にインターネットのようにオープンなネットワークを流通するようになれば、映像に含まれるプライバシー情報の保護は一層重要となる。従って、映像サーベイランスが国民的コンセンサスを得、安心安全な社会システムとして普及定着するには、プライバシーやセキュリティを可能な限り尊重するシステムに変貌させることが急務である。

以下では、筆者らが研究推進しているプライバシー保護機能を有する映像サーベイランスシステム PriSurv (Privacy Protected Video Surveillance System) [1, 2, 3] を中心に述べる。2章では、安心な映像サーベイランスを実現するための課題を指摘し、続く3章ではプライバシーと映像サーベイランスの関連研究を述べる。4章以降は PriSurv のシステム構成とコア機能である視覚的抽象化について述べていく。

2 安心な映像サーベイランスへの課題

本章では、映像サーベイランスを安心な社会システムとして定着させるにはどのようにすればよいか考えよう。そのために克服すべき問題には

- 社会的問題
- 法的問題

- 心理学的問題
- 工学的問題

が挙げられる。以下、順を追って考察しよう。

第1は社会的問題であるが、これはセキュリティとプライバシーのバランスを如何に取るかという一番の原点に還元される。このバランスをどこに置くかについては、各国で微妙に異なり、いわば文化的な背景も関係している。まず英国や韓国では、特殊な歴史的経緯、すなわち英国ではIRA、韓国では北朝鮮と長い間緊張関係にあったという背景があった。よって、サーベイランス(監視)カメラが積極的に公共スペースに設置され、市民も重大犯罪を減らすという目的において、設置へのコンセンサスが得られているといわれている。

一方、アメリカでは市民のプライバシー意識が格別が高く、G.OrwellのSF作品「1984年」の“Big Brother”に支配されるような監視社会を嫌悪する傾向がとりわけ強かった。そのため公共スペースでの監視カメラが自由自在に配備できる状況には従来なかった。ところが、2001年9月11日のニューヨーク同時多発テロを契機に、セキュリティ重視へ大きく天秤が振れ、現在は監視カメラの配備が街レベルに拡大されつつある。

我が国では以前は、銀行やコンビニにおける監視カメラが目立つ程度であった。ところが、治安の悪化に伴い、2002年の新宿歌舞伎町での監視カメラ設置を契機に、マンションなどのプライベートスペースのみならず、公共スペースへの進出は著しい。また、近年では、監視カメラ映像の解析が凶悪事件の犯人検挙の一翼を担うことも多く、その有用性も認知されつつある。いずれにせよ、プライバシーを取るか、セキュリティ(監視カメラ)を取るかは、社会的背景に依存することに疑いはないが、監視カメラを許容する社会的コンセンサスが徐々に醸成されつつあるとも筆者には思える。

第2は法的問題である。結論から言うと、監視カメラの設置、設置基準、運用法などに関する法的整備はまったくなされていない[4]。例えば、監視カメラの設置自体についても違法、適法の見解が分かれているのが現状である。公共スペースにおいて、無許可で人間を撮影、録画することは、これまでの判例に照らすと違法性が高いようである。しかしながら、セキュリティへの希求の増大から今後は変わる可能性もあろう。

第3は心理学的問題である。プライバシーとは、そもそも個人が個人の領分と考える範囲に依存する概念[5]であるため、個人性や主観性が強い。自分の容姿が映ったサーベイランス映像を他者に見せる場合に、どこまで自分の画像を開示すればプライバシーを侵されたと感じるかは、個人によりまちまちということである。つまり、ある人は実写で見せても良いが、別の人は存在すらも隠したいという場合が想定し得る。さらに、同じ人でも、場所、時間など状況依存的に自分の姿の開示範囲は異なることもある。

これらの点は後で論じる映像サーベイランスシステム的设计に大きな波紋を投げかけることになる。

最後は工学的問題である。プライバシー侵害を防ぎ、個人情報を守る技術の重要性については、近年のセキュリティ技術への注目度からも論を待たないところである。先に述べたようにプライバシーは個人性、主観性が特徴であり、これを工学的に扱うのは容易ではない。さらにユーザの安心感を向上させる技術の重要性は示唆されるものの確立されたものではなく、プライバシーに関連する技術には暗号、情報ハイディング、DBアクセス制御、映像・画像・音声などのメディア処理などが中心となろう。

3 関連研究

映像サーベイランスが注目される契機は、1990年代後半にアメリカで実施された VSAM (Video Surveillance and Monitoring) プロジェクトである。このプロジェクトは米国防総省高等研究計画局 DARPA がスポンサーで、軍事目的が主と見なすことができよう。これを通してオブジェクト(人や車など)の検出、追跡などサーベイランスの要素技術の高度化、及び新型視覚センサーの発明について大きな進歩が印された。一方、我が国においても VSAM プロジェクトと相前後して、サーベイランス応用の画像解析研究が活発化し、統計的背景画像推定や全方位視覚センサーによるサーベイランス、ITS (Intelligent Transportation System) 関連の画像解析などに目立った研究がなされた。しかしながら、歩行者や車などサーベイランス目標へのプライバシーの考慮は当時の研究にはほとんど見られない。

プライバシー保護のための画像・映像処理研究が報告されるようになったのはここ2、3年のことである。プライバシー上、不都合な部分(顔など)に自動的にモザイクやマスクを掛ける手法が検討されている。Newtonら[6]らは、顔部に対してマスクや平均顔を重畳する手法を提案した。Cavallaroら[7]

は、映像符号化の観点から適応的なコンテンツ配信法を開発し、映像サーベイランス応用において、人物像へのモザイク・マスク・位置表示処理を与えた。北原ら[8]は、移動型のカメラを対象に、顔部にモザイクを自動的に映像に重畳する方法を提案した。

一方、プライバシー保護を指向したサーベイランスシステムには以下のものがある。Wickramasuriyaら[9]はRFIDタグを援用してオブジェクト同定を行い、映像サーベイランスと結合させたシステムを報告した。SeniorらによるPrivacyCam[10]では、プライバシーを考慮した統一的なサーベイランス枠組が提唱されている。また、Zhangら[11]は、画像電子透かし技術を用いたプライバシー保護を提案した。このようにプライバシー保護を目的とする画像映像処理の問題は大きくクローズアップされつつある。

4 PriSurv

PriSurvは、プライバシー保護のための各種映像画像処理、プライバシーポリシー記述、コンテンツ流通におけるセキュリティなどの技術を確認することにより安心感のある映像サーベイランスの実現を図るシステムである。PriSurvでは、映像サーベイランスにおける情報獲得(センサー)、情報流通(ネットワーク)、情報表示(インタフェース)に対し、プライバシーとセキュリティをトータルに考えている点の特徴である。

特定の閉じたエリア(施設、地区、校区など)におけるサーベイランスを前提に、サーベイランスサービスを受けるメンバー(登録ユーザ、権限有ユーザ、匿名ユーザ、不正ユーザなど様々な種別を認める)を想定し、観察者(viewer)と被写体(subject)との間で、どのレベルまで視覚情報を開示するか(プライバシーポリシー)を取り決めて、開示情報を動的に変化させつつ映像を生成表示する。視覚情報の開示制御については、視覚的抽象化(visual abstraction)[1, 2]と呼ぶ画像処理オペレータを通じて状況依存的にプライ

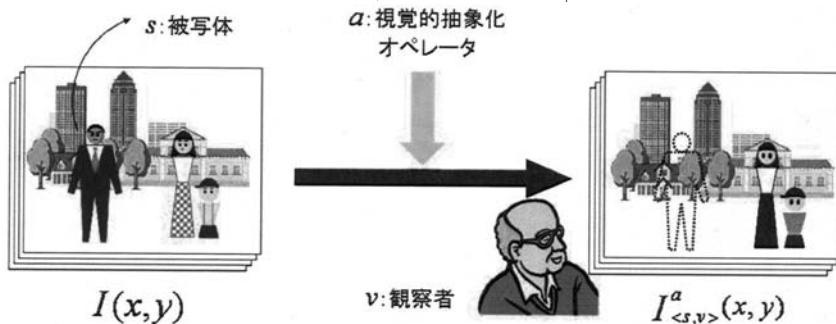


図 2: 視覚情報制御プロセス

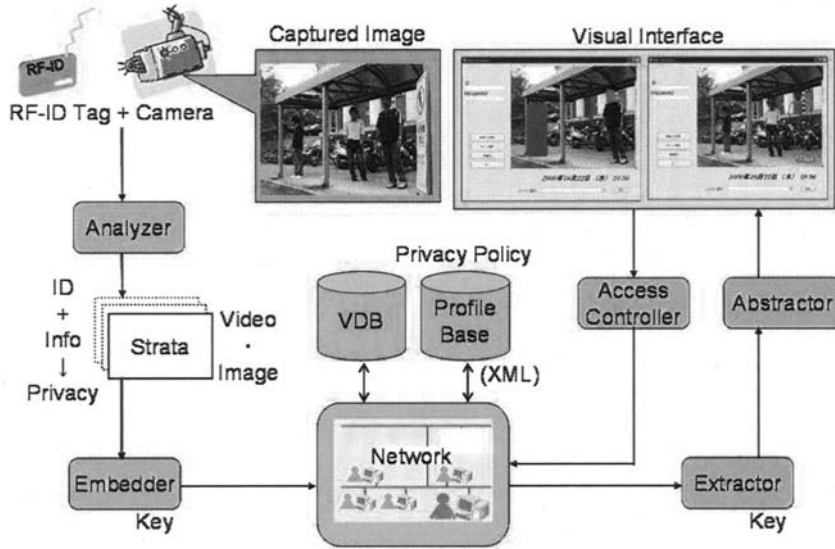


図 3: PriSurv の構成

プライバシーを保護した映像を生成表示する。図 2 に視覚情報制御プロセスを示すが、環境センシングして得られる画像 $I(x, y)$ が、被写体 s と観察者 v 、及び画像抽象化オペレータ a に従って加工され $I_{<s,v>}^a(x, y)$ を得る。被写体と観察者の関係を明示的に記述して、画像を生成することが先行研究 [6, 7, 8, 9] と異なる点である。

また、実写映像や被写体情報というプライバシー情報がオープンなネットワークに流れることを前提とすると、悪意の第三者（不正ユーザ）の盗み見 (eavesdropping) や改ざん (tempering) にも対処できる機能が必須となる。PriSurv では、鍵暗号、情報ハイディング（電子透かし、ステガノグラフィ）、コンテンツ認証、プライバシーポリシーに基づくアクセス制御により上記の機能を実現する。

図 3 に PriSurv の構成を示す。PriSurv は、大きく 5 つのモジュールと 2 つの DB を有する。以下にモジュール群の機能を簡単に述べる。

Analyzer : サーベイランスカメラと ID タグにより、環境センシングを行い、メンバーと非メンバーとの分類、メンバーについては個人同定を行う。個人同定されると被写体に関する属性（年齢、性別など）がタグを通して得られるが、これらはカメラから得られる実写情報とともにプライバシー情報ともなる。一方、画像処理については、背景差分処理に基づき、背景と前景（オブジェクト）に分け、オブジェクト（人物）を人物ごとに分離して、画像の層状表現 (stratified representation) を行う。

Abstractor : 層状表現された人物あるいは背景に視覚的抽象化を施し、視覚情報の開示を制限し、プ

ライバシー保護した画像映像を生成する。

Access Controller: メンバーの視覚情報開示範囲（どの人にどこまで見せて良いか）を記述したプライバシーポリシーに従い、映像情報や被写体関連情報へのアクセスを制御する。プライバシーポリシー、およびメンバーの ID や属性情報の集合がプロフィールベース (Profile Base) である。プロフィールは個人情報であるため、機密性には十分な注意を要する。プロフィールはその所有者である登録メンバーのみが内容の削除、更新、追加などの管理を行うことができ、他者は直接参照できない。また、プライバシーポリシーはプロフィールに記述された情報の利用法を規定するものとして位置付けられる。PriSurv では、プライバシーポリシーは XML で記述され、アクセス制御は XACML (eXtensible Access Control Markup Language) を用いて実現する。

Embedder : 実写コンテンツが流通するネットワークにおけるプライバシー情報の保護のために、情報ハイディング技術を利用する。例えば、背景映像に前景映像を埋め込んだり、前景映像にオブジェクト関連情報を埋め込む。

Extractor : 情報ハイディングされた情報から鍵を用いて、埋め込まれた情報を抽出して、もとの映像情報を再構成する。

PriSurv は心理学的考察 [3] に基づく概念設計段階を終え、画像・映像処理の機能である Analyzer と Abstractor、さらには視覚的インタフェースについては中核部分の実装を完了している。プライバシーを保護した上で、有用なセキュリティシステムの開発という思想を掲げ、上記以外の部分の詳細設計、実

表 1: 抽象化オペレータによる視覚情報の開示と隠蔽 (○: 開示 △: 一部 ×: 隠蔽)

	存在	位置	縦幅(身長)	横幅	視形	所持品の有無	姿勢向き	顔の向き	髪型	服装(色・形)	表情
実写	○	○	○	○	○	○	○	○	○	○	○
シースルー	○	○	○	○	○	○	○	○	○	○	○
モーション	○	○	○	○	○	○	○	○	○	△(色は×)	○
ぼかし	○	○	○	○	○	○	○	○	△	△	×
モザイク	○	○	○	○	○	○	○	○	△	△	×
エッジ	○	○	○	○	○	○	△	△	△	△	×
輪郭	○	○	○	○	○	△	△	×	×	×	×
シルエット	○	○	○	○	○	△	△	×	×	×	×
ボックス	○	○	○	○	×	×	×	×	×	×	×
バー	○	○	○	×	×	×	×	×	×	×	×
ドット	○	○	×	×	×	×	×	×	×	×	×
透明	×	×	×	×	×	×	×	×	×	×	×

装を進めている。次章では, Analyzer と Abstractor が関与するプライバシー保護画像の生成を示す。

5 視覚的抽象化によるプライバシー保護画像の生成

プライバシー保護のための画像生成は, 画像の層状表現, ID 獲得, 視覚的抽象化, 画像表示を経て実現される。まず, 画像の層状表現では, 背景差分 (background subtraction) により, 前景 (foreground) と背景 (background) に分割する。ここでは, 固定の

サーベイランスカメラを前提とし, 背景モデル \hat{B} を設定して, 環境の微細な変動にも耐える背景モデル同時学習型の背景差分法 [12] を導入する。得られる前景は, 人物等のオブジェクトが複数存在するが, PriSurv では, 立位の人物像をテンプレートにして, 個人ごとの人物像を得, 画像を層 (stratum) に分割する。

いま, サーベイランス画像 I は,

$$I = B \cup F_1 \cup F_2 \cup \dots \cup F_n$$

$$F_j \cap F_k = \phi \quad j, k \in \{1, 2, \dots, n\}$$

と表現され, B, F_i が各々背景画像, 第 i 前景画像 (第

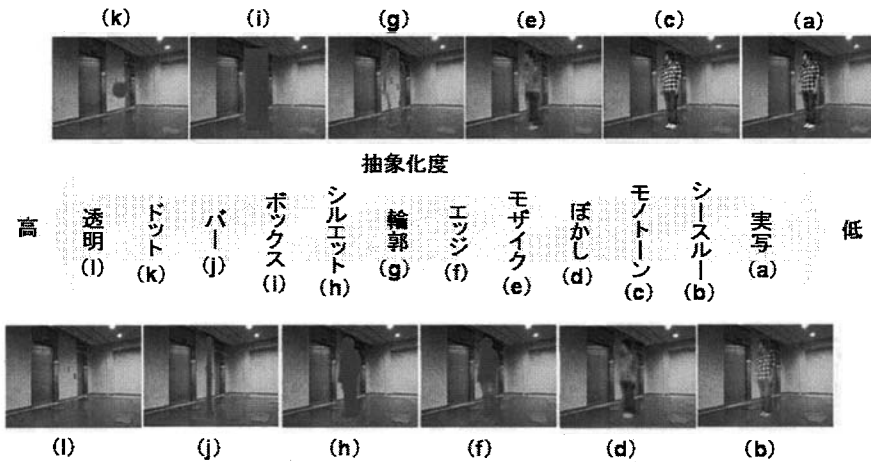


図 4: 抽象化オペレータの順序関係

i オブジェクト) であり, n はオブジェクト数である.

次に ID 獲得では, サーベイランス映像中の人物(被写体)が, PriSurv の登録メンバーか否かを分類し, さらに, 登録メンバーには ID 獲得を試みる. 現段階での PriSurv は, 屋内環境を対象とし, 登録メンバーには RF-ID タグを装着させることを前提とする. 2 個以上の ID タグリーダーを環境に設置し, ID タグの電波到来方向を推定して, 実環境での位置を定める. さらに, 環境固定カメラを前提としているため, 画像中のオブジェクトの位置を 2 次元平面に投影して, ID タグから推定された位置とマッチングを取ることによって, 第 i オブジェクトの ID を獲得する. なお, 現在は ID タグを利用することによって, 個人識別を行っているが, この処理は顔認識や歩容認識を援用することも可能である.

以上の処理により, 以下のような前景層 SF_i と背景層 SB からなる層状表現を得る.

$SF_i = \langle$ 被写体人物像 F_i , 被写体関連情報 \rangle
被写体関連情報: ID, 属性 (性別, 年齢など)

$SB = \langle$ 背景 B , 背景関連情報 \rangle
背景関連情報: 場所, 建物, 時間など

この被写体関連情報と背景関連情報はメタデータと見なしうるもので, 登録メンバーに対する被写体関連情報は ID タグから得るが, それ以外のデータは映像解析によって得ることになる.

この層状表現を基に視覚的抽象化を行う. 視覚的抽象化は, 観察者に対し, 主に被写体の ID や属性の同定に必要な視覚情報を隠蔽するために, 画像の表

現粒度を変えることである. PriSurv で実装されている抽象化オペレータは以下の通りである. この抽象化オペレータは, 実写と透明を各々抽象度最低, 最高とし, 半順序関係をなす. ここで, 抽象度の低い順から, どのような処理かを簡単に示す:

- (a) 実写: センサーから得られる映像情報そのもの
- (b) シースルー: 前景を通して背景が見えるもの
- (c) モノトーン: 前景のカラー情報を削除したもの
- (d) ぼかし: 前景をぼかしたもの
- (e) モザイク: 前景にモザイクをかけたもの
- (f) エッジ: 前景にエッジ抽出を施したもの
- (g) 輪郭: 前景を輪郭で表し背景が見えるもの
- (h) シルエット: 前景の領域を塗りつぶしたもの
- (i) ボックス: 前景を囲む領域を塗りつぶしたもの
- (j) バー: 前景を囲む領域の縦幅を表したもの
- (k) ドット: 前景の領域を点で表したもの
- (l) 透明: 前景を消去したもの

図 4 に上記の視覚的抽象化オペレータ間の順序関係と各オペレータの作用例を示す. さらに表 1 に視覚的抽象化オペレータにより開示, 隠蔽される視覚情報の一覧をまとめるが, 情報は段階的に増減し, オペレータが半順序をなすことが分かる. 各オペレータの具体的な処理内容を表 2 に示す.

視覚的抽象化は原則的に, 層状表現の層ごとに作用させる. 前景の場合は, オペレータの作用領域を制御することにより, 人物像の全体領域のみならず部分領域に作用させることも可能である. PriSurv で

表 2: 抽象化オペレータの処理内容

実写	抽象化処理なし
シースルー	前景 f と背景 b との画素ブレンド ($f \times \alpha + b \times (1 - \alpha)$) 透明度 α が大きいほど不透明 (ここでは $\alpha = 0.5$)
モノトーン	RGB 値から濃淡輝度値への置換 ($0.299 \times R + 0.587 \times G + 0.144 \times B$)
ぼかし	9×9 のブロック領域でメディアンフィルタによる平滑化
モザイク	15×15 のブロック領域内のすべての画素値をその領域の平均画素値で置換
エッジ	RGB の各成分ごと (モノクロ画像) に 8 方向のラプラシアンフィルタを用いてエッジ検出 \rightarrow 各成分の合成 (RGB 画像) \rightarrow エッジ部の塗りつぶし
輪郭	前景の輪郭検出 \rightarrow 輪郭線の塗りつぶし
シルエット	前景の塗りつぶし
ボックス	前景を囲む最小矩形 MBB (Minimum Bounding Box) 領域の抽出 \rightarrow MBB 領域の塗りつぶし
バー	前景の MBB 領域の抽出 \rightarrow MBB 領域の縦方向中心線領域の決定 \rightarrow 中心線領域の塗りつぶし
ドット	前景の MBB 領域の抽出 \rightarrow MBB 領域の円形中心領域の決定 \rightarrow 円形領域の塗りつぶし
透明	前景の画素値をゼロにする

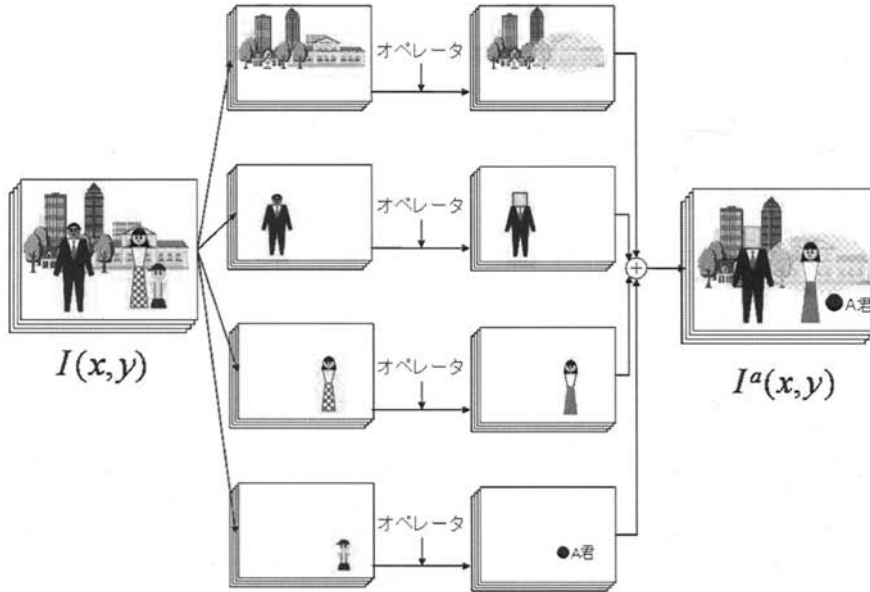


図 5: プライバシー保護画像の生成

は、部分領域として顔、胴体、衣服などを想定している。すなわち、顔のみモザイクをかけるということも可能である。一方、背景に対しては、透明（削除）、モザイク、ぼかしを想定するが、背景の一部に対する作用は、背景の詳細な解析が必要となる。

加えて、被写体関連情報をアノテーション（テキスト情報）として映像に重畳表示する機能も備えている。映像情報にテキスト情報を付加することによって被写体の存在・位置・属性の情報を観察者に伝えることができる。

最終的に観察者に表示する映像 I^a は、前景の各層ごとに抽象化された画像を時変型の背景モデル \hat{B} の前面に足しあわすことにより得られる。これを

$$I^a = \hat{B}^a \oplus F_1^a \oplus F_2^a \oplus \dots \oplus F_n^a$$

と表す。但し、 F^a は画像 F に抽象化オペレータを作用させることを表し、 $F \oplus G$ は画像 F の前面に画像 G を足しあわすことを表す。図 5 にプライバシー保護画像の生成の様子を示すが、同図のようにして、前景の人物ごとに異なる処理も可能となる。また、図 6 は生成の具体例である。PriSurv は以上の処理を実時間で実行可能である。

映像表示のための視覚的インタフェースでは、観察者が ID、ユーザクラスを入力し、認証過程を経た後、被写体 ID あるいはエリアをクエリとして検索すると、プロフィールベースのプライバシーポリシーに合致した被写体の映像を表示する。また、層を区別して、抽象化の度合いを変化させるスライダーも装備しており、許容される範囲の抽象度で被写体を変化

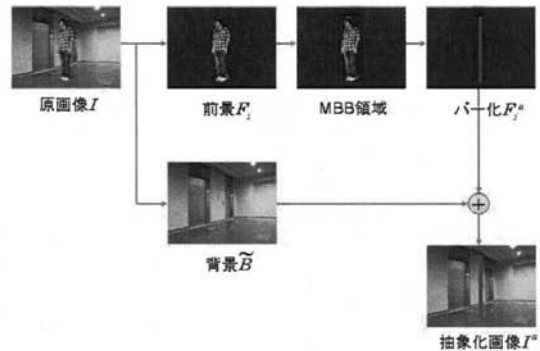


図 6: プライバシー保護画像の具体例

させて観察できる。図 7 に実験用に作成した PriSurv のインタフェースを示す。4 分割画面で構成され、左上、右上、左下、右下は各々背景モデル、前景、サーベイランス画像、抽象化画像である。

6 むすび

本稿では、映像サーベイランスを安心な社会システムとして定着させるため、プライバシー処理に関する課題を種々の観点から考察するとともに、筆者らが開発を進める PriSurv について述べた。今後、詳細



図 7: PriSurv のインタフェース

の具体化を図り、性能評価を重ねたいと考えている。

さて、本アプローチは、図 1 に示す映像サーベイランスの第 3 の軸に沿うものであるが、第 1、第 2 の軸に関しても未だ不十分という点にも注意する必要がある。監視カメラが事件解決に役立ったといっても、重大事件が起きて以後に監視カメラ映像の分析が役立ったわけで、即時的に、あるいは未然に事件・犯罪を防ぐレベルには至っていない。広域のサーベイランスをどうするのか、不審 X (X = 者, 物, 車両, 行動, 状況, ...) をどう検出するのか、時間空間的に離れたモニター画像群を的確に表現する視覚インタフェースはどんなものか、など課題も多い。映像サーベイランスを今後バランスの取れた形で進化させていくために一層の研究蓄積が期待される。

謝辞 日頃から御討論いただく ATR の萩田紀博博士、鳥山朋二博士、西尾修一氏、馬田一郎博士、阪大馬場口研究室の小清水隆氏、知野見健太氏を始めとする各位に感謝する。本研究の一部は、総務省・SCOPE、文部科学省・科研費による。

参考文献

- [1] 馬場口登: プライバシーを考慮した映像サーベイランス, 情報処理, vol.48, no.1 (2007)
- [2] 小清水隆, 鳥山朋二, 西尾修一, 馬場口登, 萩田紀博: 映像サーベイランスにおけるプライバシー保護のための視覚的抽象化の提案, 電子情報通信学会技術研究報告, PRMU2005-270, pp.75-80, (2006)
- [3] Koshimizu, T., Toriyama, T. and Babaguchi, N.: Factors on the Sense of Privacy in Video Surveillance, Proc. of Workshop on Capture, Archival and Retrieval of Personal Experiences (2006).
- [4] 小林正啓: ネットワークロボットの法的問題について, 平成 17 年度ネットワークロボットフォーラム技術部会報告 (2006)
- [5] 新保史生: ユビキタスメディアの利用とプライバシー保護の限界 - 個人情報保護の交錯点も踏まえて -, 電子情報通信学会技術研究報告, PRMU2005-148, pp.75-82 (2006).
- [6] Newton, E. M., Sweeney, L. and Malin, B.: Preserving Privacy by De-Identifying Face Images, IEEE Trans. KDE, vol.17, no.2, pp.232-243(2005).
- [7] Cavallaro, A., Steiger, O. and Ebrahimi, T.: Semantic Video Analysis for Adaptive Content Delivery and Automatic Description, IEEE Trans. CASVT, vol.15, no.10, pp.1200-1209(2005).
- [8] Kitahara, I., Kogure, K. and Hagita, N.: Stealth Vision for Protecting Privacy, Proc. 17th ICPR, Vol.4, pp.404-407 (2004).
- [9] Wickramasuriya, J. et al.: Privacy-protecting Video Surveillance, Proc. SPIE International Symposium on Electronic Imaging (2005).
- [10] Senior, A. et al.: Enabling Video Privacy through Computer Vision. IEEE Security & Privacy Magazine, pp. 50-57 (2005).
- [11] Zhang, W., Cheung, S. S. and Chen M.: Hiding Privacy Information in Video Surveillance System, Proc. IEEE International Conference on Image Processing (ICIP2005), pp.868-871 (2005).
- [12] Stauffer, C. and Grimson, W.E.L.: Adaptive Background Mixture Models for Real-Time Tracking, Proc. CVPR'99, vol.2, pp.246-252(1999).