

## PriSurv : 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

知野見 健太<sup>†1</sup> 李 光 鎮<sup>†1</sup> 中 嶋 大 介<sup>†1</sup>  
新 田 直 子<sup>†1</sup> 伊 藤 義 道<sup>†1</sup> 馬 場 口 登<sup>†1</sup>

安心・安全な社会を実現するための技術である監視カメラによる映像サーベイランスは、犯罪抑止や犯罪捜査の手がかりとして有用である一方、被写体のプライバシーを侵害する恐れがある。本論文では、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一助となるよう、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 を提案する。また、PriSurv の構成技術として、近傍画素を参照したガウス混合モデルによる前景抽出法、RFID タグと映像解析を用いた被写体同定法、XACML を用いたアクセス制御、視覚的抽象化について述べる。プロトタイプでは、被写体と観察者の関係に基づいた視覚的抽象化による、被写体の実時間プライバシー保護を可能とした。さらに、このプロトタイプのシステム評価を行い、提案手法の有効性を確認した。

### PriSurv: Privacy Protected Video Surveillance System

KENTA CHINOMI,<sup>†1</sup> GUANGZHEN LI,<sup>†1</sup>  
DAISUKE NAKASHIMA,<sup>†1</sup> NAOKO NITTA,<sup>†1</sup>  
YOSHIMICHI ITO<sup>†1</sup> and NOBORU BABAGUCHI<sup>†1</sup>

Recently, video surveillance has received a lot of attention as a technology to realize a secure and safe community. Video surveillance is useful for crime deterrence and investigations, but may cause the invasion of privacy. In this paper, we propose a video surveillance system named PriSurv, which is characterized by protecting the object's privacy. PriSurv includes four main functions: foreground extraction using Gaussian mixture models with referring to neighbor pixels, object identification with a combination of RFID-tags and video analysis, access control using XACML and visual abstraction. The prototype of PriSurv is able to protect the object's privacy through visual abstraction in real time based on the relation between the objects and the viewers. Experimental results have demonstrated the effectiveness of our approach.

### 1. はじめに

近年、安心・安全な社会を構築するための監視カメラによる映像サーベイランスが、犯罪抑止や犯人捜査の手がかりとして非常に注目されている。しかし、映像サーベイランスは監視カメラの設置数増大による監視コストの増加の問題や、被写体のプライバシー侵害の問題<sup>1),2)</sup> をかかえている。

上述の問題に対し、映像サーベイランスとプライバシーとの関係を議論した多くの研究がなされてきている。Newton ら<sup>3)</sup>, Cavallaro ら<sup>4)</sup>, Kitahara ら<sup>5)</sup> は、映像中の被写体に対して、モザイクなどの画像処理を施すことによりプライバシーを保護する手法を提案した。Wickramasuriya ら<sup>6)</sup>, Senior ら<sup>7)</sup> は、被写体や観察者の権限に応じて、サーベイランス映像にプライバシー保護を施す手法を提案した。Zhang ら<sup>8)</sup> は、電子透かしを用いたサーベイランス映像へのプライバシー情報の埋め込み手法を提案し、権限を持つユーザが埋め込まれたプライバシー情報を秘密鍵によって安全に取り出すことを可能としている。関口<sup>9)</sup> は、被写体・観察者から各々プライバシー保護要求と映像の閲覧要求を受信し、双方の要求を示す制御ルールに従って画像処理を実行するシステムを提案した。このシステムでは、被写体・観察者の要求が衝突した場合、観察者の要求を優先して実行する点が特徴である。

しかし、これらの先行研究における、被写体や観察者の権限のみを参照したプライバシー保護手法では、各被写体のプライバシー感覚の差異を考慮した柔軟なプライバシー保護を実現できない。そこで本論文では、各被写体が観察者との関係に基づき設定したプライバシーポリシーに応じて、被写体の表情、服装、髪型といった視覚情報の開示量を制御する映像サーベイランスシステム PriSurv (Privacy Protected Video Surveillance System) を提案する。PriSurv では、抽象化オペレータと呼ばれる画像処理機能<sup>2),10)</sup> を指定することにより視覚情報が段階的に制御される。ここでは、被写体の視覚情報を抽象化オペレータによって隠蔽することを視覚的抽象化 (visual abstraction) と呼ぶ。

### 2. PriSurv の概要

PriSurv は図 1 のように、サーベイランス映像に対して被写体と観察者の関係に基づいた

<sup>†1</sup> 大阪大学大学院工学研究科  
Graduate School of Engineering, Osaka University

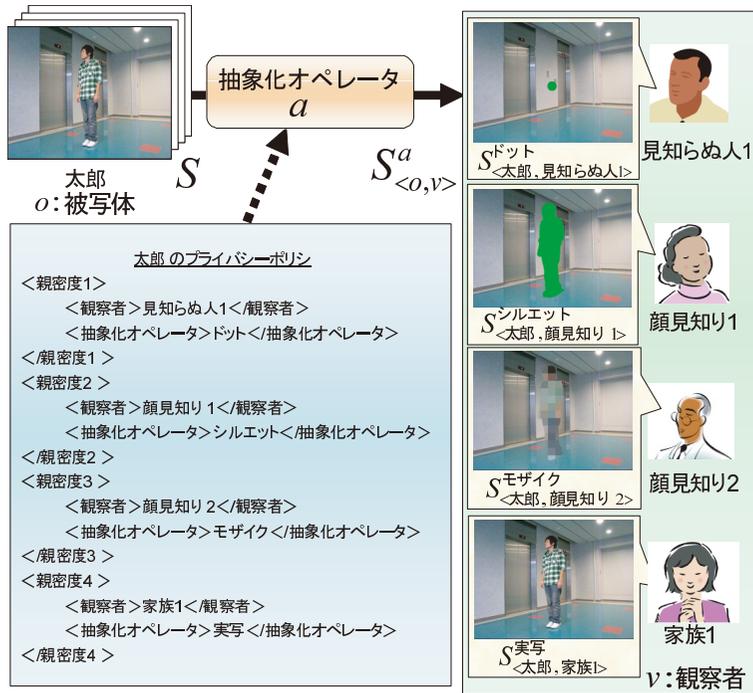


図 1 被写体と観察者の関係に基づいたプライバシー保護  
Fig. 1 Privacy protection based on relations between objects and viewers.

視覚的抽象化を施す点に特徴がある。被写体と観察者を含むメンバの存在が PriSurv の前提条件となる。メンバが存在し、行動する領域を我々はコミュニティと呼び、それが PriSurv の観測環境となる。コミュニティの具体例には、マンション・オフィス・校区・町内・施設など種々のものが考えられるが、本論文では閉じた屋内領域を対象とする。図 1 では、被写体‘太郎’が‘見知らぬ人 1’、‘顔見知り 1’、‘顔見知り 2’、‘家族 1’ という 4 人の観察者により観察されており、‘太郎’の姿はそれぞれの観察者との関係に応じて、ドット、シルエット、モザイク、実写という異なる形で表示される。

PriSurv では、カメラから得られる画像サイズ  $M \times N$  の原画像  $S = \{s_{ij}\} (i = 1, 2, \dots, M; j = 1, 2, \dots, N)$  が、被写体 (object) の ID  $o$  と観察者 (viewer) の ID  $v$  に基づいて決定される抽象化オペレータ  $a$  によって処理され、プライバシー保護画像  $S^a_{<o,v>}$  が生成され

る。なお、 $s_{ij} = (s_{ij}^r, s_{ij}^g, s_{ij}^b)$  は RGB チャネルを持つ座標  $(i, j)$  における画素値ベクトルを表す。

原画像  $S$  中の背景領域を  $B$ 、前景領域を  $F$  とするとき、背景画像  $S_B$  と前景画像  $S_F$  を各々

$$S_B = \left\{ b_{ij} \mid \begin{array}{l} b_{ij} = \mathbf{0} \quad (i, j) \in \bar{B} \\ b_{ij} = s_{ij} \quad (i, j) \in B \end{array} \right\}$$

$$S_F = \left\{ f_{ij} \mid \begin{array}{l} f_{ij} = \mathbf{0} \quad (i, j) \in \bar{F} \\ f_{ij} = s_{ij} \quad (i, j) \in F \end{array} \right\}$$

とする。ただし、 $\bar{B}, \bar{F}$  は各々画像定義域より  $B, F$  の領域を除いた領域とする。被写体数が  $N_o$  である場合は、前景領域  $F$  を被写体 ID  $o_n (n = 1, 2, \dots, N_o)$  に対応する被写体領域  $F_n$  に分割し、被写体画像

$$S_{F_n} = \left\{ f_{ij}^n \mid \begin{array}{l} f_{ij}^n = \mathbf{0} \quad (i, j) \in \bar{F}_n \\ f_{ij}^n = s_{ij} \quad (i, j) \in F_n \end{array} \right\}$$

を生成する。 $s_{ij}$  と同様に、 $b_{ij}, f_{ij}, f_{ij}^n$  は各々  $S_B, S_F, S_{F_n}$  の座標  $(i, j)$  における画素値ベクトルを表す。原画像  $S$  は背景画像  $S_B$  と被写体画像  $S_{F_n}$  を用いて、以下のように表現される。

$$S = S_B + S_{F_1} + S_{F_2} + \dots + S_{F_{N_o}}$$

ここで演算+は、同じ座標における画素値の和をとることを表し、このように 1 枚の画像を層状に表現することを層状化と呼ぶ。

PriSurv の概要を図 2 に示す。PriSurv はオープンなネットワーク上に構築することを想定しており、システムの登録メンバである観察者はメインサーバにアクセスし、認証を受けることによりサーベイランス映像を閲覧する。

PriSurv の各モジュールの詳細な機能を以下に示す。

- Analyzer: カメラ映像から背景モデルを生成し、前景画像の抽出・層状化を行う。また、各被写体を持つ RFID (Radio Frequency Identification) タグと映像解析を用いて、被写体画像に対して被写体同定を行う<sup>12)</sup>。
- Access Controller: アクセス制御機能であり、被写体のプライバシーポリシーを参照し、観察者 ID と照合して適切な抽象化オペレータを決定する。この抽象化オペレータによ

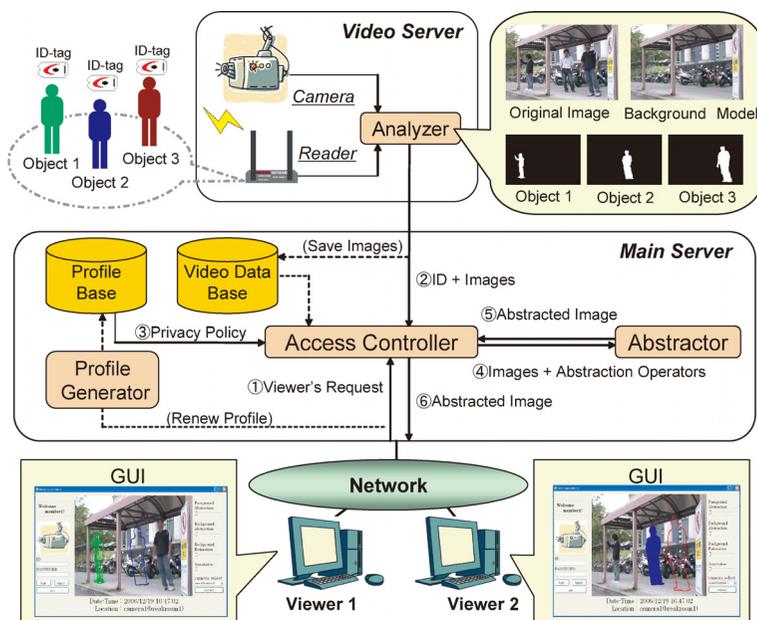


図2 PriSurv のシステム構成  
Fig. 2 System architecture of PriSurv.

る視覚的抽象化を Abstractor に対して指示する。

- Abstractor : 被写体画像に対して、Access Controller から指示された抽象化オペレータによる視覚的抽象化を実行する。
- Profile Base : プライバシーポリシーや被写体の属性情報が記述されたプロフィールを管理する。
- Profile Generator : 登録メンバがプロフィール設定を容易に行うための機能であり、メンバの設定項目をプロフィールに記述する。
- Video Data Base : 過去の映像データを蓄積する。

### 3. PriSurv の構成技術

#### 3.1 背景モデルの生成と前景の抽出・層状化

PriSurv では、ガウス混合モデル<sup>13)</sup>を用いた背景モデルの生成/前景抽出を行う<sup>11)</sup>。

この手法では、各画素において、過去の一定区間の画素値の変動を表したガウス混合モデルを参照し、背景モデルの推定と更新を行う。ここで、背景モデル画像  $\tilde{S}_B = \{\tilde{b}_{ij}\}$  ( $i = 1, 2, \dots, M; j = 1, 2, \dots, N$ ) は、被写体背後の不可視領域を含めて推定したモデル画像であり、原画像  $S$  における可視の背景領域  $B$  に対応する背景画像  $S_B$  とは異なる。なお、ガウス混合モデルを構成する各々のガウス分布を要素分布と呼ぶ。

また、木の揺れなどによる細かな変動に対応するため、各画素において近傍画素を参照する手法<sup>14)</sup>を導入する。ガウス混合モデルにより、原画像  $S$  において  $(i, j) \in F$  と判定された場合、 $(i, j)$  を中心とした  $N_{BL} = n_{BL} \times n_{BL}$  のブロック中の各画素モデルの  $K$  個の要素分布を参照し、最大類似度を持つ要素分布を次式で求める。

$$(P, Q) = \arg \max_{p, q} \frac{\omega_{p, q}}{(s_{ij} - \mu_{p, q})^T \Sigma_{p, q} (s_{ij} - \mu_{p, q})}$$

$\mu_{p, q} = (\mu_{p, q}^r, \mu_{p, q}^g, \mu_{p, q}^b)$ ,  $\Sigma_{p, q}$ ,  $\omega_{p, q}$  は各々、 $(i, j)$  の  $p$  ( $1 \leq p \leq N_{BL}$ ) 番目の近傍画素におけるガウス混合モデルの  $q$  ( $1 \leq q \leq K$ ) 番目の要素分布の平均値ベクトル、共分散行列、重みである。ここで、重みが大きく偏差が小さい要素分布を背景を表す分布と見なし、この要素分布の平均値ベクトルを背景モデル画像  $\tilde{S}_B$  の画素値ベクトル  $\tilde{b}_{ij}$  に設定し、 $s_{ij}$  がこの要素分布に属する場合、 $(i, j)$  における画素を背景とする。ただし、 $\sigma_{P, Q}^{ch}$  を  $(i, j)$  の  $P$  番目の近傍画素における  $Q$  番目の要素分布の標準偏差ベクトル  $\sigma_{P, Q}$  の  $ch = (r, g, b)$  成分とすると、 $|s_{ij}^{ch} - \mu_{P, Q}^{ch}| \leq 2.5 \times \sigma_{P, Q}^{ch}$  をすべての  $ch$  に対して満たすとき、 $s_{ij}$  はこの要素分布に属するものとする。また、雑音などによる前景の誤検出領域を除くため、一定領域より小さい前景領域を除去する。

次に、このようにして抽出された前景画像  $S_F$  を層状化する。まず、前景画像  $S_F$  に対する閾値処理により 2 値画像を生成する。この 2 値画像において、0 でない値を持つ画素の領域を前景領域  $F$  と見なし、鉛直方向への投影プロフィールを生成し、連続した領域ごとに前景領域を分割する。図 3 では、前景領域  $F$  が被写体領域  $F_1, F_2, F_3$  へと分割されている様子が分かる。この領域をもとに、被写体画像  $S_{F_1}, S_{F_2}, S_{F_3}$  が生成される。

ただし、この層状化手法では、被写体領域が画像の大きさに対して比較的大きく、鉛直方向の領域内に被写体が 1 人であるという前提が必要となるため、今後、カメラ視野に応じた層状化手法を考察する必要がある。

#### 3.2 RFID タグと映像解析による被写体同定

被写体同定とは、被写体画像  $S_{F_n}$  の被写体 ID  $o_n$  を決定する処理である。PriSurv では、RFID タグと映像解析を用いて被写体同定を行う。この手法では、測定環境をいくつかのエ

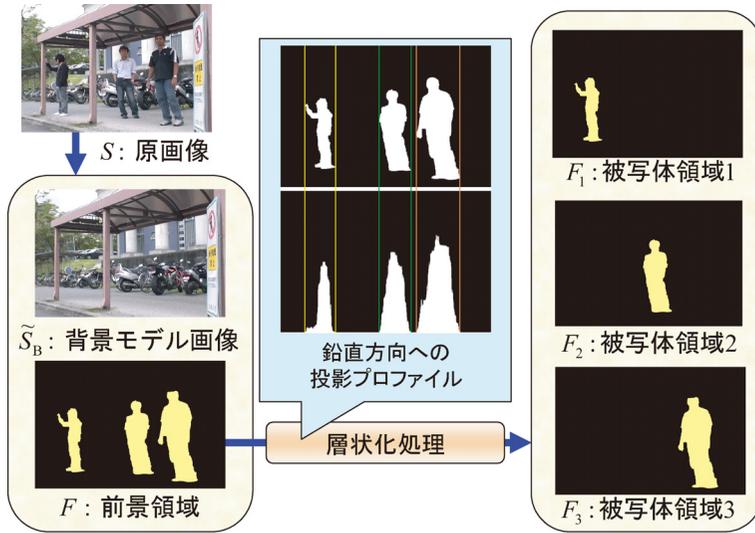


図 3 被写体画像生成のための層状化処理

Fig. 3 Stratification process for generating object images.

リアに分け、被写体の持つ RFID タグおよびカメラ映像から、それぞれ被写体が存在するエリアを推定する。これらの推定エリアの情報を統合し、RFID タグの ID と映像中の被写体を対応付けることにより被写体同定を行う。その概要を図 4 に示す。

RFID タグによるエリア推定法では、各エリアにおいて学習データとして取得しておいた受信電界強度に基づいて<sup>15)</sup>、RFID タグ  $t_m$  ( $m = 1, 2, \dots, N_o$ ) とエリアを対応付ける。RFID リーダは 2 本のアンテナを持ち、各々が RFID タグからの電波 (周波数 303.825 MHz) を感知し、電界強度の逆デシベル値 (SSI 値) を取得することができる。RFID リーダが  $d$  個設置されているとすると、タグ 1 つにつき  $2d$  個の SSI 値が得られ、これを  $2d$  次元のベクトル  $e = \{e_1, \dots, e_{2d}\}$  で表す。A 個の各エリアに対して、学習データとして取得した  $N_e$  個の SSI 値ベクトルを  $e_{k,l} = \{e_{k,l,1}, \dots, e_{k,l,2d}\}$  ( $k = 1, 2, \dots, A; l = 1, 2, \dots, N_e$ )、RFID タグ (ID)  $t_m$  から得られる SSI 値ベクトルを  $e_m = \{e_{m,1}, \dots, e_{m,2d}\}$  とし、 $e_{k,l}$  と  $e_m$  のユークリッド距離  $\|e_{k,l} - e_m\|_2$  のうち、値が小さいものから  $(k, l)$  の組を  $K_e$  個抽出し、エリア  $k$  の出現頻度を確率分布として求める。

カメラ映像の解析によるエリア推定では、各エリアごとに学習データとして取得しておいた、身長が異なる複数の被写体の 2 値画像に基づいて、被写体画像  $S_{F_n}$  ( $n = 1, 2, \dots, N_o$ )

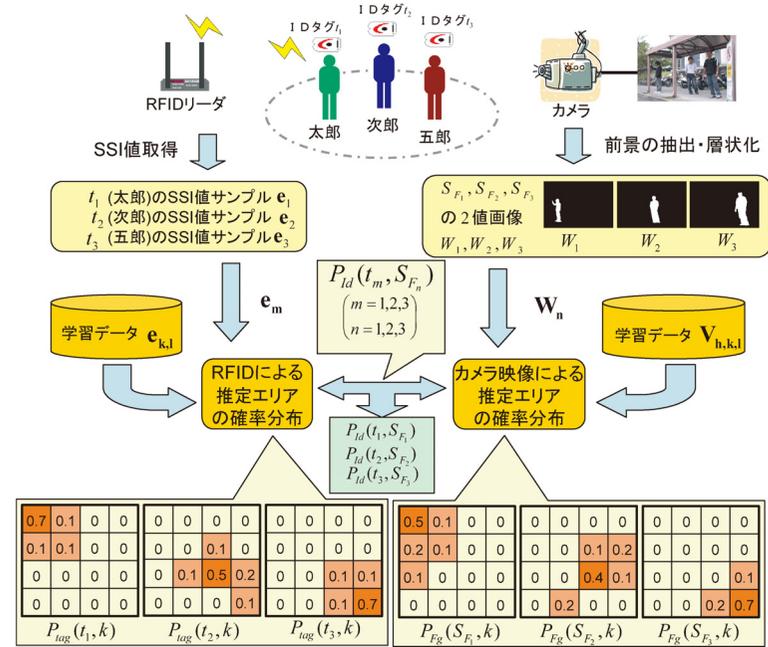


図 4 RFID タグと映像解析を用いた被写体同定

Fig. 4 Object identification by RFID tags and video analysis.

とエリアを対応付ける。A 個のエリアに対して H 人分の学習データを取得し、各被写体の 1 つのエリアあたりの学習データを  $N_V$  枚とする。ここで、学習データを  $V_{h,k,l} = \{v_{ij}^{h,k,l}\}$  ( $h = 1, 2, \dots, H; k = 1, \dots, A; l = 1, 2, \dots, N_V$ )、入力データを被写体画像  $S_{F_n}$  の 2 値画像  $W_n = \{w_{ij}^n\}$ 、また  $\|V_{h,k,l}\|$ 、 $\|W_n\|$  を各々  $V_{h,k,l}$ 、 $W_n$  の被写体領域の画素数とし、 $V_{h,k,l}$  と  $W_n$  の差異を各々  $\|V_{h,k,l}\|$ 、 $\|W_n\|$  で正規化したマンハッタン距離として

$$\sum_{i=1}^M \sum_{j=1}^N \left| \frac{v_{ij}^{h,k,l}}{\|V_{h,k,l}\|} - \frac{w_{ij}^n}{\|W_n\|} \right|$$

と定義する。この値の小さいものから  $(h, k, l)$  の組を  $K_F$  個抽出し、エリア  $k$  の出現頻度を確率分布として求める。

RFID タグとカメラ映像によって得られた確率分布では、被写体が実際に存在するエリア

の出現頻度がとも高くなると考えられるため、これらの確率分布を以下のように対応付けることにより被写体同定を行う。なお、映像中の  $N_o$  人の被写体は全員 RFID タグを所有しており、映像中に存在しない被写体の RFID タグは検知しないものとする。以下に手続きを示す。

- (1) RFID タグ  $t_m$  ( $m = 1, 2, \dots, N_o$ ) がエリア  $k$  ( $k = 1, 2, \dots, A$ ) に存在する確率を  $P_{Tag}(t_m, k)$ , 被写体画像  $S_{F_n}$  に対応する被写体がエリア  $k$  に存在する確率を  $P_{Fg}(S_{F_n}, k)$  とし, RFID タグ  $t_m$  と被写体画像  $S_{F_n}$  が対応する確率  $P_{Id}(t_m, S_{F_n})$  を

$$\max\{P_{Tag}(t_m, k) \times P_{Fg}(S_{F_n}, k)\}$$

として定める。この  $P_{Id}(t_m, S_{F_n})$  を、すべての  $m$  ( $m = 1, 2, \dots, N_o$ ) と  $n$  ( $n = 1, 2, \dots, N_o$ ) の組合せについて求める。

- (2) 以下の式により得られる, RFID タグ  $\hat{t}$  と被写体画像  $\hat{S}_F$  を対応付ける。

$$(\hat{t}, \hat{S}_F) = \arg \max_{t_m, S_{F_n}} P_{Id}(t_m, S_{F_n})$$

つまり,  $\hat{S}_F = S_{F_n}$  ( $n \in \{1, 2, \dots, N_o\}$ ) であるとき  $o_n = \hat{t}$  とする。

- (3)  $P_{Id}(t_m, S_{F_n})$  のうち,  $t_m = \hat{t}$  または  $S_{F_n} = \hat{S}_F$  となるものを除き, 再び (2) を行う。すべての RFID タグ  $t_m$  と被写体画像  $S_{F_n}$  が対応付けられた時点で, 被写体同定は完了する。

PriSurv では, 被写体同定により得られた ID から, 名前, 性別, 年齢といった被写体関連情報を Profile Base から参照し, 必要に応じてテキスト情報として画像に重畳することが可能である。これをアノテーション化と呼ぶ。

### 3.3 プライバシーポリシーに基づくアクセス制御

PriSurv では, 被写体ごとに柔軟にプライバシーポリシーを設定する枠組みとして, 拡張性のあるアクセス制御を実現するためのポリシー記述言語である XACML (eXtensible Access Control Markup Language) を用いる。

#### 3.3.1 XACML

XACML ではある情報資源に対して, 誰が (Subject), 何に (Resource), どのように (Action) アクセスできるのかをポリシーとして記述する。PriSurv においては, Subject, Resource, Action を各々, 観察者, 被写体, 閲覧として定める。また, 実際にアクセス制御を行う PEP (Policy Enforcement Point) とアクセス要求の認可/不認可を決定する PDP (Policy Decision Point) が重要なモジュールとなり, これらが PriSurv における

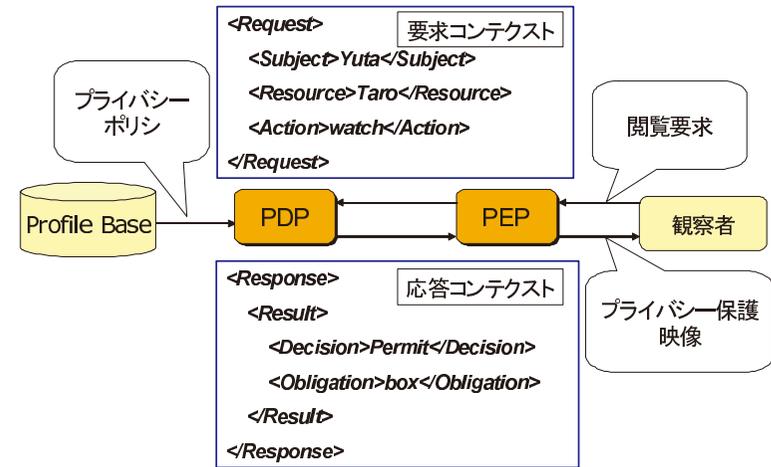


図 5 PEP・PDP によるアクセス制御  
Fig.5 Access control by PEP and PDP.

Access Controller に相当する。以下にアクセス制御の流れを示す。

- (1) 観察者が PEP に対してサーベイランス映像の閲覧要求をする。
- (2) PEP は観察者が映像中の被写体の映像にアクセスするための要求コンテキストを生成して PDP に送る。
- (3) PDP は要求コンテキストを受け取ると, 観察者 ID と被写体のプライバシーポリシーを照合し, アクセスの認可・不認可を決定する。アクセスが認可された場合, PDP は PEP にアクセスを認可する条件として Obligation (責務) を課す。この責務として抽象化オペレータを指定し, 応答コンテキストを PEP へ送る。
- (4) PEP は責務として, 指定された抽象化オペレータによる視覚的抽象化の実行を図 2 の Abstractor へ指示する。

PEP と PDP で行われる要求・応答は図 5 のようになる。この例では, 観察者 'Yuta' がサーベイランス映像中の被写体 'Taro' を見るという要求コンテキストが PEP から PDP へ送られ, PDP はそのアクセスを許可し, 責務として被写体画像のボックスによる視覚的抽象化を指示している。以上の処理が毎フレーム, 映像中のすべての被写体に対して行われる。

$a_0$  を背景モデル画像  $\hat{S}_B$  に対する抽象化オペレータ,  $a_n$  を  $o_n$  の被写体 ID が与えられた被写体画像  $S_{F_n}$  に対する抽象化オペレータとし, これらを  $o = (o_1, o_2, \dots, o_{N_o})$ ,



図 6 XACML による '太郎' のプライバシーポリシー設定例  
Fig. 6 Example of privacy policy expressed in XACML.

$a = (a_0, a_1, a_2, \dots, a_{N_o})$  のようにリストで表現すると, このアクセス制御は, 閲覧要求から得られる観察者 ID  $v$  と, 被写体同定により決定された被写体 ID  $o$  を入力として, 抽象化オペレータ  $a$  を決定する処理であるといえる.

### 3.3.2 プライバシーポリシーの記述

登録メンバはプライバシーポリシーを設定する際, 被写体と観察者の間の親密度に基づいて視覚的抽象化方法を設定することが有効であることから<sup>16)</sup>, 観察者を数段階の親密度ごとにグループ分けを行い, 各々に抽象化オペレータを指定する. グループ分けされなかったメンバは非指定メンバとしてグループ化される. 図 6 に図 1 における被写体 '太郎' のプラ

イバシーポリシーを XACML を用いて設定した例を示す. 観察者は並列記述することにより, 複数設定することが可能である. なお, 図 6 のプライバシーポリシーは簡単のため一部を省略している.

また, プライバシーポリシーや被写体の属性情報が記述されたプロファイルは個人情報であるため, サーバで厳重に管理する必要がある. プロファイルは所有者のみが内容の更新を行うことができ, 他者が直接参照することはできない. ただし, 正規メンバの閲覧リクエストに応じて, システムがこのプロファイルの一部の情報を参照するため, 他者が間接的にプロファイルの内容を知りうるという問題がある.

### 3.4 視覚的抽象化

被写体のプライバシーの保護は, 存在・位置・表情・服装などの視覚情報を隠蔽することで実現される. PriSurv では, 安全性とプライバシー保護を同時に実現するため, 視覚情報を段階的に制御する複数の抽象化オペレータを実装する.

実装した各抽象化オペレータによる被写体の抽象化例を図 7 に示す. また, 各抽象化オペレータにより開示・隠蔽される視覚情報の例<sup>2)</sup>を表 1 に示す. ここで,  $\times$  は開示,  $\times$  は隠蔽を意味する. 隠蔽される視覚情報の量に基づき, 各抽象化オペレータは列挙した順に抽象化レベルが高くなると考えられる. さらに, ぼかし, シルエット, ボックスなどの抽象化オペレータを頭部領域, または胴体領域のみに適用することにより, 抽象化レベルをより詳細に設定することも可能である.

抽象化オペレータ  $a$  による視覚的抽象化を背景モデル画像  $S_{\tilde{B}}$  や被写体画像  $S_{F_n}$  に作用させることにより,

$$\tilde{S}_B^{a_0} = \left\{ \tilde{b}_{ij}^{a_0} \left| \begin{array}{ll} \tilde{b}_{ij}^{a_0} = \mathbf{0} & (i, j) \in \tilde{B}^{a_0} \\ \tilde{b}_{ij}^{a_0} = a_0(\tilde{b}_{ij}) & (i, j) \in \tilde{B}^{a_0} \end{array} \right. \right\}$$

$$S_{F_n}^{a_n} = \left\{ f_{n,ij}^{a_n} \left| \begin{array}{ll} f_{n,ij}^{a_n} = \mathbf{0} & (i, j) \in \tilde{F}_n^{a_n} \\ f_{n,ij}^{a_n} = a_n(s_{ij}) & (i, j) \in F_n^{a_n} \end{array} \right. \right\}$$

が得られる. 視覚的抽象化の具体的操作は文献 17) を参照されたい. なお  $\tilde{B}^{a_0}$  は, 視覚的抽象化にともない可視となる背景モデルの領域,  $F_n^{a_n}$  は被写体領域  $F_n$  に対して抽象化オペレータを作用させた領域を表す. これにより, ID  $v$  を持つ観察者へ送られるプライバシー保護画像  $S_{< o, v >}^{a_0}$  は, 以下のように表現される.

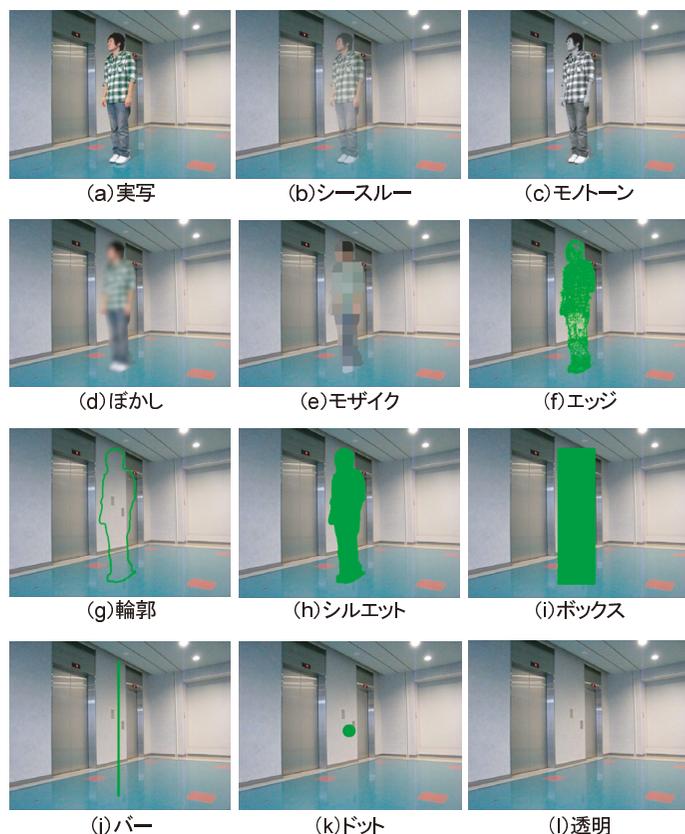


図7 各抽象化オペレータによる視覚的抽象化の例  
Fig. 7 Example of visual abstraction.

表1 視覚情報の開示と隠蔽 ( : 開示, △ : 一部開示, × : 隠蔽)  
Table 1 Disclosed or hidden visual information  
( : disclosed, △ : partially-hidden, × : hidden).

	存在	位置	身長	横幅	シルエット	姿勢	顔の向き	髪型	服装	表情
実写										
シースルー										
モノトーン										
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	×	×	×	×	×	×	×	×	×	×

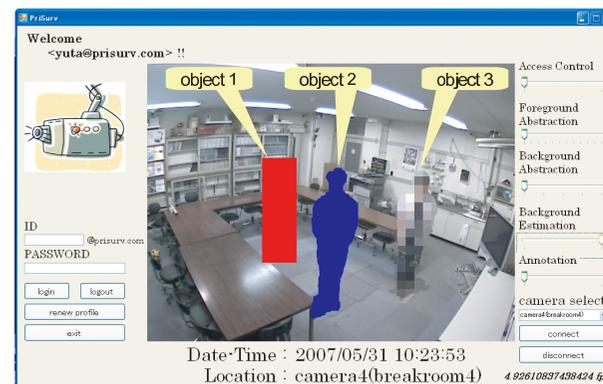


図8 PriSurv のユーザインタフェース  
Fig. 8 Graphical user interface of PriSurv.

$$S_{\langle o, v \rangle}^a = \tilde{S}_B^{a_0} + S_{F_1}^{a_1} + S_{F_2}^{a_2} + \dots + S_{F_{N_o}}^{a_{N_o}}$$

#### 4. プロトタイプの評価

図8はプロトタイプのユーザインタフェースである。観察者は被写体に対する抽象化オペレータとカメラの選択をすることができる。いま、'yuta'が映像左から'object1', 'object2',

'object3'の3人の被写体を観察しているとする。'yuta'に表示されるプライバシー保護画像  $S_{\langle o, v \rangle}^a$  において、 $v = yuta$ ,  $o = (object1, object2, object3)$ ,  $a = (\text{ボックス}, \text{シルエット}, \text{モザイク})$ となる。

以下では、各機能およびシステム全体の評価について述べる。

#### 4.1 前景抽出と層状化の精度

前景抽出と層状化の精度評価実験において用いた映像の画像サイズは  $480 \times 720$  であり、近傍画素の参照においては、近傍のブロックサイズを  $5 \times 5$  とした。実験の結果、近傍画素を参照することにより、前景と誤検出された背景領域の画素数は近傍画素を参照しなかった場合に比べ、各フレームにおいて最大 66%、最小 30.8%、平均で 50.4% 減少し、細かい背景変動を抑えることができた。前景の層状化においては、実験映像の 100 フレームに対して、層状化により得られた各被写体領域の外接矩形領域を求め、実際の被写体の外接矩形領域を 90% 以上、その他の領域を 10% 以下含む場合、被写体領域が正しい層として抽出されたものとし、

$$\text{再現率} = \frac{\text{正しく抽出された層の数}}{\text{実際の層の数}}$$

$$\text{適合率} = \frac{\text{正しく抽出された層の数}}{\text{提案手法により抽出された層の数}}$$

により評価した。その結果、再現率 79.3%、適合率 77.6% で被写体領域が正しく検出された。

#### 4.2 被写体同定の精度

被写体同定の精度評価は、屋内の一室を利用し、部屋に 2 人の RFID タグを持った被写体が存在する状況で行った。部屋の大きさは、 $4.75 \text{ m} \times 4.5 \text{ m}$  であり、これを等間隔に  $4 \times 4$ 、計 16 個のエリアに分割した。RFID リーダは部屋の天井の四隅に 1 個ずつ、計 4 個設置した。人体が電波へ及ぼす影響を考え、RFID タグはヘルメットに取り付けた。RFID タグとカメラ映像によるエリア推定の正解は、各々求めた推定エリアの確率分布において、値が最大となるエリアを推定結果としたときに、2 人とも正しいエリアが推定された場合とし、被写体同定の正解は、2 人とも正しく被写体が同定された場合とする。RFID タグ、およびカメラ映像によるエリア推定の正解率の平均は各々 14%、77%、被写体同定の正解率は 81% という結果が得られた。ただし、2 人の被写体が重なった場合は無視している。この結果は、RFID タグとカメラ映像に基づくエリア推定結果が一致しない場合でも、それぞれの確率分布を統合し、被写体の存在確率がともに高くなるエリアを求めることにより、比較的精度の良い被写体同定が可能であることを示している。

#### 4.3 視覚的抽象化の評価

##### 4.3.1 視覚的抽象化の処理速度

ここでは、視覚的抽象化の処理速度を評価するために、フレームレートの測定を行った。画像サイズは  $640 \times 480$  で、被写体は 1~2 人とした。被写体が全身像となるように撮影し、

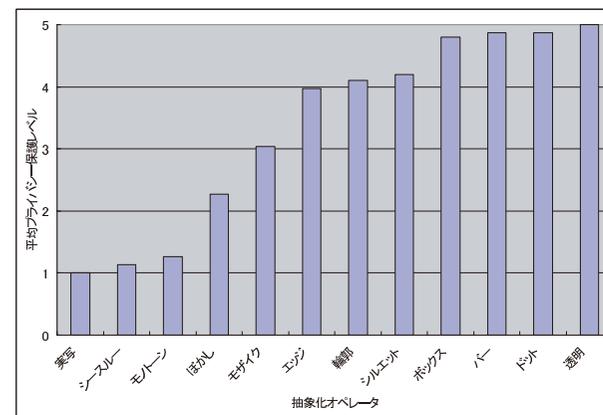


図 9 抽象化オペレータのプライバシー保護レベルに関する主観評価実験結果

Fig. 9 Result of subjective evaluation for privacy protection levels of abstraction operators.

そのサイズは  $150 \times 420$  程度であった。この条件で、100 フレームを処理する間の平均フレームレートを測定した。その結果、被写体が 1 人である場合は、抽象化オペレータの透明化で最大の 12.2 fps、シースルー化で最小の 8.8 fps、すべての抽象化オペレータの平均は 10.8 fps であり、被写体が 2 人である場合は、平均で 7.8 fps であった。なお、被写体が存在しない場合のフレームレートは 15.0 fps であった。これにより、適用する抽象化オペレータによりフレームレートが大きく変化することが分かった。

##### 4.3.2 抽象化オペレータによるプライバシー保護に関する主観評価

図 7 の各抽象化オペレータによってどの程度プライバシーが保護されるかは、客観的には表 1 に示された隠蔽される視覚情報の量に基づいて判断される。しかし、表 1 は各抽象化オペレータの相違を示す例にすぎず、プライバシーの個人性を考慮すれば、プライバシー保護の程度は主観的に判断されるべきである。そこで、各抽象化オペレータによる視覚情報の開示・隠蔽により、主観的にどの程度プライバシーが保護されるかを調べるため、評価実験を行った。被験者は 14 歳から 39 歳までの男性 15 人、女性 15 人の計 30 人であり、各抽象化オペレータに対して、どの程度プライバシーが保護されていると感じるかを、プライバシー保護レベルとして 5 段階評価させた。

図 9 は各抽象化オペレータの平均プライバシー保護レベルを棒グラフ化したものである。ただし、実写と透明に関しては、質問において基準となるプライバシー保護レベルを、それ

ぞれ1, 5として与えてある。この結果より、隠蔽する視覚情報が多いほど主観的なプライバシー保護レベルが高くなるのが分かる。また、モノトーン・ぼかし間、ぼかし・モザイク・エッジ間、シルエット・ボックス間、においてその差が大きいことから、表1を参照すると、表情、服装・髪型、シルエットが分かるかどうか、被写体のプライバシー感覚に大きく影響を与えていると考えられる。さらに、この5段階評価の結果において、たとえば、ボックス、バー、ドット、透明の平均プライバシー保護レベルはおおよそ等しく、プライバシー保護の観点ではこの4つの抽象化オペレータを1つに集約することも考えられる。

#### 4.4 提案システムに対する主観評価実験

現在実装している構成技術により生成されるプライバシー保護映像が、被写体の立場から十分なプライバシー保護がなされているか、また観察者の立場からサーベイランス映像として有効であるかを評価するための主観評価実験を行った。被験者には、2章で述べたPriSurvの動作環境・前提条件を教示として与えた。実験プロセスは以下のとおりである。

- (1) 各被験者が1人で屋内の一室を歩き回る様子を、設置されたカメラを用いて30秒程度撮影する。
- (2) 各被験者は、親密度の異なる4人の観察者を想定し、自分が映っている映像を各観察者に提示する際に用いる抽象化オペレータを設定する。
- (3) 設定された抽象化オペレータを用いて、図10のような4種類のプライバシー保護映像を生成する。
- (4) 各被験者は、被写体、観察者の立場から生成された映像を評価する。

なお、本評価実験では以下のことを条件として課した。

- 被写体同定の精度を $\alpha\%$ とし、各フレームにおいて $(100 - \alpha)\%$ の確率で被写体は正しく同定されないとする。
- 被写体が正しく同定されない場合は、同じサーベイランス環境にいる他の被写体として誤同定されるとし、その被写体のプライバシーポリシーに従って決定された抽象化オペレータにより視覚的抽象化が行われるとする。ここで、4.3.2項における議論に基づき、抽象化オペレータを以下のような4つのグループに分類する。

グループ1: 実写, シースルー, モノトーン

グループ2: ぼかし, モザイク

グループ3: エッジ, 輪郭, シルエット

グループ4: ボックス, バー, ドット, 透明

上記の各グループにおいて最も抽象化レベルの低い、実写、ぼかし、エッジ、ボックス

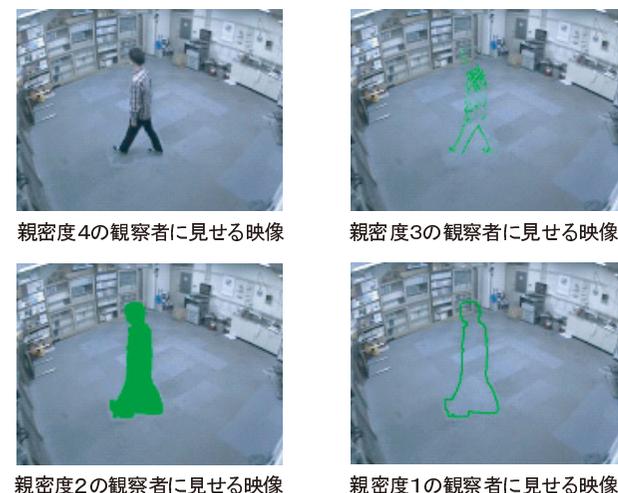


図10 4種類の実験映像の例

Fig. 10 Example of four experimental videos.

の4つのうち、ランダムに選択されたものを、他の被写体のプライバシーポリシーに従って決定された抽象化オペレータとする。

被験者に対する質問内容は、

- Q1: 被写体の立場から、生成された映像に十分プライバシー保護がなされていると感じるか、
- Q2: 観察者の立場から、生成された映像がサーベイランス映像として有効であると思うか、

の2点である。本実験では被験者を10人、 $\alpha = 80, 90, 95, 97, 99$ として映像を生成し、それぞれの映像に対して上記の質問を行った。

Q1, Q2の回答結果は、表2のとおりである。この結果より、提案システムによって生成されたプライバシー保護映像は、観察者の観点からサーベイランス映像としての有効性を保つことができるが、被写体が正しく同定されないことにより、プライバシーの侵害を招く恐れがあるといえる。 $\alpha = 80, 90$ の映像に対しては、半数以上の被験者がプライバシー保護が十分になされていないと答えたのに対して、 $\alpha = 95$ 以上の映像に対しては、半数以上の被験者がプライバシー保護が十分になされていると答えていることから、被写体同定の精

表 2 提案システムに対する主観評価実験の結果  
Table 2 Results of subjective evaluation for proposed system.

	Q1		Q2	
	はい	いいえ	はい	いいえ
$\alpha = 80$	1	9	9	1
$\alpha = 90$	3	7	9	1
$\alpha = 95$	5	5	9	1
$\alpha = 97$	8	2	9	1
$\alpha = 99$	9	1	9	1

度は現在の 81%では不十分であり, 95%以上を達成することが今後の大きな課題であるといえる.

## 5. む す び

本論文では, 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 を提案した. PriSurv では, 被写体と観察者の親密度に応じて, 観察者に表示される被写体の視覚情報を段階的に制御することにより, 個人性のあるプライバシーを柔軟に保護することが可能である. プロトタイプでは, 近傍画素を参照したガウス混合モデルによる前景抽出法や, RFID タグと映像解析を用いた被写体同定法を提案し, 実験結果からその有効性を確認した. また, 視覚情報を制御するための画像処理機能である 12 種類の抽象化オペレータを用い, 被写体の実時間プライバシー保護処理を実現した. さらに, XACML を用いて被写体と観察者の親密度に基づいたアクセス制御を実現することにより, 柔軟なプライバシー保護の基本的な枠組みが整ったといえる.

しかし, PriSurv には以下のような技術的課題, 1) 抽象化オペレータの集約・追加, あるいは作用対象の詳細化, 2) 各モジュール, 特に被写体同定の高精度化・高速化, 3) より複雑な監視環境への適用, が残されている. また, プロファイルにおける個人情報の利用と保護を両立させる詳細な仕組みが必要となる<sup>18)</sup>. さらに, PriSurv を安心・安全な社会システムとして定着させるにあたっては, 社会的コンセンサスが得られるのか, 法的整備は十分であるのか, といった問題があり, プライバシーの個人性に関するさらなる心理学的評価・調査や, 個人情報保護法などとの整合性が課題となる. なお, 本研究の一部は, 総務省・SCOPE による.

## 参 考 文 献

- 1) 新保生: 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).
- 2) 馬場口登: プライバシーを考慮した映像サーベイランスシステム, 情報処理, Vol.48, No.1, pp.30-36 (2007).
- 3) Newton, E.M., Sweeny, L. and Malin, B.: Preserving Privacy by De-Identifying Face Images, *IEEE Trans. Knowledge and Data Engineering*, Vol.17, No.2, pp.232-243 (2005).
- 4) Cavallaro, A., Steiger, O. and Ebrahimi, T.: Semantic Video Analysis for Adaptive Content Delivery and Automatic Description, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.15, No.10, pp.1200-1209 (2005).
- 5) Kitahara, I., Kogure, K. and Hagita, N.: Stealth Vision for Protecting Privacy, *Proc. International Conference on Pattern Recognition*, Vol.4, pp.404-407 (2004).
- 6) Wickramasuriya, J., Alhazzazi, M., Datt, M., Mehrotra, S. and Venkatasubramanian, N.: Privacy-Protecting Video Surveillance, *Proc. SPIE International Symposium on Electronic Imaging*, Vol.5671, pp.64-75 (2005).
- 7) Senior, A., Pankati, S., Hampapur, A., Brown, L., Tian, Y.-L., Ekin, A., Connell, J., Shu, C.-F. and Lu, M.: Enabling Video Privacy Through Computer Vision, *IEEE Security and Privacy Magazine*, Vol.3, Issue.3, pp.50-57 (2005).
- 8) Zhang, W., Cheung, S.S. and Chen, M.: Hiding Privacy Information in Video Surveillance System, *Proc. IEEE International Conference on Image Processing*, pp.868-871 (2005).
- 9) 関口隆昭, 加藤博光: カメラ映像における閲覧者と被写体の関係に基づくプライバシー保護システムの提案と評価, 情報処理学会論文誌, Vol.47, No.8, pp.2660-2668 (2006).
- 10) 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).
- 11) 李 光鎮, 新田直子, 伊藤義道, 馬場口登: 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 における前景抽出, 電子情報通信学会総合大会, D-12-101 (2007).
- 12) 中嶋大介, 伊藤義道, 新田直子, 馬場口登: 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 における人物同定, 電子情報通信学会総合大会, D-12-102 (2007).
- 13) Stauffer, C. and Grimson, W.E.L.: Learning Patterns of Activity Using Real-Time Tracking, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.22, pp.747-757 (2000).
- 14) Elgammal, A., Harwood, D. and Davis, L.S.: Non-Parametric Model for Back-

ground Subtraction, *Proc. European Conference on Computer Vision*, pp.751-767 (2000).

- 15) Ogawa, T., Yoshino, S. and Shimizu, M.: Location Determination Method for Wireless Systems Based on Learning Vector Quantization, *NTT Technical Review*, Vol.1, No.9, pp.27-36 (2003).
- 16) Koshimizu, T., Toriyama, T. and Babaguchi, N.: Factors on the Sense of Privacy in Video Surveillance, *Proc. Workshop on Capture, Archival and Retrieval of Personal Experiences*, pp.35-43 (2006).
- 17) 知野見健太, 李 光鎮, 中嶋大介, 新田直子, 伊藤義道, 馬場口登: 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, 画像の認識・理解シンポジウム (MIRU2007), pp.73-80 (2007).
- 18) 沼尾雅之: プライバシーと AI, *人工知能学会誌*, Vol.21, No.5, pp.593-601 (2006).

(平成 19 年 9 月 22 日受付)

(平成 20 年 3 月 10 日採録)

(担当編集委員 奥富 正敏)



知野見健太

2007 年大阪大学工学部電子情報エネルギー工学科卒業。現在、同大学大学院工学研究科電気電子情報工学専攻修士課程在学中。映像サーベイランスに関する研究に従事。



李 光鎮

2007 年大阪大学工学部電子情報エネルギー工学科卒業。現在、同大学大学院工学研究科電気電子情報工学専攻修士課程在学中。情報ハイディングに関する研究に従事。



中嶋 大介

2007 年大阪大学工学部電子情報エネルギー工学科卒業。現在、同大学大学院工学研究科電気電子情報工学専攻修士課程在学中。2008 年電子情報通信学会総合大会優秀ポスター賞受賞。映像サーベイランスに関する研究に従事。



新田 直子

1998 年大阪大学基礎工学部情報工学科卒業。2003 年同大学大学院博士課程修了。2002~2004 年日本学術振興会特別研究員。2003~2004 年コンビア大学客員研究員。現在、大阪大学大学院工学研究科助教。博士(工学)。メディア理解に関する研究に従事。



伊藤 義道

1990 年京都大学工学部電気工学第二学科卒業。1992 年同大学大学院前期課程修了。1994~1998 年大阪大学工学部助手。現在、大阪大学大学院工学研究科助教。システム制御理論、マルチメディア信号処理、ネットワークセキュリティの研究に従事。



馬場口 登 (正会員)

1979 年大阪大学工学部通信工学科卒業。1981 年同大学大学院前期課程修了。愛媛大学工学部、大阪大学産業科学研究所を経て現在、大阪大学大学院工学研究科教授。1996~1997 年 UCSD・文部省在外研究員。マルチメディア処理、知的コミュニケーションの研究に従事。工学博士。IEEE, ACM, 電子情報通信学会, 映像情報メディア学会, 人工知能学会各会員。