情報処理学会論文誌 Vol.57 No.1 172–183 (Jan. 2016)

プライバシ保護と犯罪防止を両立させる監視カメラシステム

小林 健人[1,a)] 稲村 勝樹[2] 金田 北洋[3] 岩村 惠市[1]

受付日 2015年4月10日, 採録日 2015年10月2日

概要：近年，個人情報やプライバシについて取り上げられる場面が増加している．特に，監視カメラ映像に関するプライバシの問題が取り上げられることが多く，映像を取り扱うガイドラインも存在している．しかし，近年のプライバシ保護の概念である自身の情報のコントロールという観点から考えると，被撮影者自身によって匿名で顔情報が制御できることが望ましい．しかし，既存のシステムではそれを実現する技術的な仕組みを持たない．一方で，監視カメラは犯罪防止に利用されているため，被撮影者が犯罪者となる可能性を考慮すると，被撮影者によってのみ制御されることは好ましくない．そこで，我々は被撮影者がグループ署名と可逆モザイク技術を組み合わせ，さらに秘匿した顔を復元するために必要なモザイク鍵を犯罪捜査時のみ生成できる鍵管理法によって，プライバシ保護と犯罪時での監視カメラの有効利用を同時に実現するシステムを提案する．これによって，被撮影者は自身の顔情報を匿名で制御することができ，かつ，犯罪捜査時には，制御された顔情報を警察などに提供可能で，さらに顔が秘匿されていた被撮影者の特定が容易となる．

キーワード：監視カメラ，プライバシ保護，匿名署名，モザイク

A New Surveillance Camera System to Achieve Both Crime Prevention and Privacy Protection

Kento Kobayashi[1,a)] Katsuki Inamura[2] Kitahiro Kaneda[3] Keiichi Iwamura[1]

Received: April 10, 2015, Accepted: October 2, 2015

Abstract: Recently, personal information and privacy have been focused on. Especially, problems of surveillance camera image are taken up in many cases. There are many guidelines for dealing with the image. However, from the view point of privacy protection in recent year, it is desirable for personal information such as face to be anonymously controllable by the photographed people. However, the existing systems do not have a technical mechanism. Meanwhile, since the surveillance camera has been used for crime prevention, in view of the possibility that the person to be photographed is a criminal, it is not preferable to be controlled only by the person to be photographed. Therefore we propose a new surveillance camera system balancing the privacy protection and the surveillance image use. Our system is consist of group signatures and reversible mosaic. Moreover the hidden face information can be opened in the crime investigation by the generating the mosaic key which is used for reconstruction of the original face. Thereby, the photographed people can control their face information anonymously, and, at the time of criminal investigation, the controlled face information can provide for the police and specification of the person who had the face controlled to be taken becomes easy.

Keywords: surveillance camera, privacy protection, group signature, mosaic

1. はじめに

近年，インターネットの普及によりSNSやネット上に画像や映像をアップロードする機会が増えている．それにともないプライバシや個人情報について取り上げられる場面

[1] 東京理科大学工学科
Department of Engineering, Tokyo University of Science, Katsushika, Tokyo 125–8585, Japan
[2] 東京電機大学理工学部
School of Science and Engineering, Tokyo Denki University, Hiki, Saitama 350–0394, Japan
[3] 大阪府立大学工学部
Department of Engineering, Osaka Prefecture University, Habikino, Osaka 583–0872, Japan

[a)] kobayashi_k@sec.ee.kagu.tus.ac.jp

が増えている．プライバシとは，「私事，私生活，個人の秘密」そのものや，「それらが干渉・侵害されない権利」を指している．しかし，近年では「自身の情報についてのコントロール権」という解釈を含むようになっている [1], [2]．一方で，個人情報とは，「個人を特定することができる情報」を指し，例として氏名，住所，生年月日，顔情報を含む生体情報などの多くの情報を含んでいる．

ここで，近年プライバシに関する問題が起きている監視カメラについて考える．問題の 1 つとして，監視カメラ映像の流出（またはその一部）というものがある．実際に，芸能人がプライベートで訪れたコンビニやレンタルビデオショップに設置された監視カメラ映像の一部がその映像を見ることのできる人物によって SNS 上にアップロードされてしまうという問題が起きている [4]．しかし，監視カメラの必要性に関しては理解されており，平成 23 年 11 月に公開された「東京都の世論調査」[5] では，防犯カメラの設置に 64%の人が支持を示している．また，平成 24 年 7 月に行われた「けいしちょう安全安心モニター制度　第一回アンケート調査結果」[6] では，94%の人が「事件が起きた際に犯人が捕まりやすくなる」，87.5%の人が「犯罪の発生を抑止する効果がある」という回答をしている．一方，監視カメラの問題点として映像の流出などの懸念から，75.5%の人が「データの管理をしっかりしてほしい」と答えている．したがって，必要性が認知されている監視カメラに対して，プライバシの保護と犯罪防止を両立させるシステムを実現することは非常に重要である．

しかし，プライバシ保護と犯罪防止のバランスをとることは難しい．たとえば，プライバシを重視してモニタに映る人物の顔などをつねにマスクする監視カメラシステムを考える．その場合，リアルタイムで監視していても，万引きなどがあったとき，だれが万引きをしたか特定できず，監視カメラの利便性が失われる．それに対して，犯罪防止を重視して監視カメラのモニタでは何も秘匿せず，保存時にのみ暗号化などによる保護を施すシステムを考える．この場合，自身の情報に関するコントロール権という近年のプライバシの考え方はまったく反映されない．また，監視カメラを見る立場にある人がスマホなどで監視カメラ映像を盗撮すれば，前述した芸能人のプライベート映像の流出などは防止できない．

したがって，プライバシ保護と犯罪防止を両立させる監視カメラシステムとして以下の要件が最低限必要と考える．

1. 被撮影者の意志によって，自身の顔情報の公開または非公開を決定できる．
2. 顔情報の非公開を望む被撮影者は不正が行われない限り身元を特定されない．
3. 犯罪捜査などに映像を利用する場合，秘匿されている顔情報をすべて明かすことができる．

1 によって個人による個人情報（顔情報）の制御という近年のプライバシに関する考え方を実現できる．すなわち，顔情報の公開を気にする人はリアルタイムにその人の顔がマスクされ，気にしない人の映像には何の処理もされない．これによって，万引きなどが起こったとき，犯人が後者であれば犯人をリアルタイムに特定できる．犯人が前者である場合は，2 によって犯人が特定される．すなわち，顔情報の非公開を望む被撮影者は何らの方法でその意思を示す必要があり，システムはそれと引き換えに不正が行われたとき，その被撮影者を特定する仕組みを持つ．最後に，3 によって，警察などは必要なすべての情報を入手でき，従来と同じ犯罪捜査も可能にする．

本稿では，上記を実現する監視カメラシステムを提案し，考えられるいくつかの攻撃に対して安全であることを示す．2 章で監視カメラの問題点，3 章で関連する研究，4 章で提案システム，5 章でその安全性などを考察する．

2. プライバシと監視カメラ

2.1 プライバシ

プライバシとは「私生活をみだりに公開されない，法的保障」という解釈が一般的である．しかし，近年のプライバシに関する概念では，「自己の情報のコントロール」という意味を含ませることが多い [1], [2]．

たとえば，レガシー文献における「プライバシー：定義集」[16] によると，1960 年に，ウィリアム・プロッサーがプライバシ侵害を 4 つの型に分類しており，「私生活への侵入」「秘匿しておきたい私事の公表」「誤解を生じさせる私事の公表」「名前や写真の営利的使用」というものがある．1960 年代後半になると，アラン・ウェスティンによって，新しい定義が与えられ，プライバシ保護を「自己に関する情報をコントロールする権利」と定義づけた．また，1990 年にインターネットが普及し始め，1995 年には EU によって「個人データ保護指令」において個人データの定義を行っている．個人データには，氏名，写真，電子メール・アドレス，講座情報，医療情報などが含まれる．また，Microsoft Azure がプライバシコントロール国際基準 ISO/IEC27018 に準拠した初のクラウドコンピューティングプラットフォームとして確認されている [17]．このプライバシ国際基準 ISO/IEC27018 はクラウドサービスの運用にあたって 5 つの原則を設けており，同意，統制，透明性，情報伝達，独立性と年次監査というものがある．この中の統制では，「顧客は，自分が提供した情報の用途を明示的に統制できなければならない」とされている．これらのことより，プライバシにおいて自己の情報のコントロール権という概念が重要になってきていることが分かる．

またこれらのことをふまえると，プライバシの侵害とは個人についての情報が不当に公開され，または利用されるということであり，プライバシを保護するためには，個人の情報が各自によってコントロールされることが望まれる．

2.2 監視カメラにおける問題

近年，監視カメラ映像の一部がSNSなどに公開されてしまうという事案が起きている．2012年8月に，芸能人がプライベートでコンビニエンスストアに訪れている監視カメラ映像の一部が，そのコンビニエンスストアの店員によってtwitter上にアップロードされてしまっている．これは，被撮影者が自分に関する情報がコントロールできないという点で上記プライバシ保護の観点から好ましくない．

一方で，監視カメラ運用におけるガイドラインが存在していることも事実である．このガイドラインでは，監視カメラの設置場所や撮影範囲，管理責任者の指定，画像データの保存や取扱いについてなどが示されている．しかし，ガイドラインで画像の取扱いについての規定がされているにもかかわらず，監視カメラ映像の一部流出という事案が発生してしまっている．これは，そのガイドラインを実現する技術的な仕組みがないことを表している．また，監視カメラ運用のガイドラインでは，前記近年のプライバシの概念である監視カメラの被撮影者が監視カメラ映像に対して何らかのコントロール権を持つことについて考慮されていない．プライバシ保護の観点からすると，ガイドラインに示されていることが守られているとともに，被撮影者側が個人の情報（顔情報）についてのコントロール権が実現される必要がある．

しかしながら，監視カメラ映像は犯罪抑止や，犯罪捜査に利用される場合が多いことも事実である．監視カメラ映像を利用する際に，顔情報が被撮影者によって完全にコントロールされ，第三者（たとえば警察など）にまったく公開されない場合は監視カメラ映像を利用する価値が薄れてしまう．

したがって，監視カメラ映像が流出してしまった際でも，個人情報の保護を望む被撮影者が特定されず，かつ監視カメラの犯罪防止や犯罪捜査への有効性を維持できる新しい監視カメラシステムが必要であり，この新しい監視カメラシステムを実現するための研究は非常に重要である．

3. 関連研究

ここでは，3.1節で既存の監視カメラ映像に関する研究について関連技術を紹介する．

また，本稿で提案する監視カメラシステムで用いる技術として，3.2節では，Short Group Signatures [8]，3.3節では可逆透かしを用いたJPEG画像へのモザイク手法 [9] についての説明を行う．

3.1 既存の監視カメラ映像における研究の考察

2011年に福岡らによって観察者に応じたプライバシ保護映像を生成可能な映像配信手法 [11] が情報科学技術フォーラム講演論文集で公開されている．この手法では，観察者の権限に応じて，サーベイランスカメラの映像を制御するというものであり，映像の種類として，透明化された映像（被撮影者が映っていない），ボックス表示された映像，エッジ処理された映像，モザイク処理された映像，実写映像がある．

この手法において，プライバシ保護の一部は実現されているが，あくまで観察者による制御であり，被撮影者側による顔情報の制御については考慮されていない．また，権限を持つ観察者は特に指定されていないため，システム側で任意に設定できる．

このほかにも多数の関連研究がある．たとえば，被撮影者をauthorized personnelとunauthorized personnelに分け，前者はRFIDタグを持つことでシステム側に検知される [21]．また，観察者がlower level of security clearanceとhigher level of security clearanceとに分けられ，後者は秘密鍵を持っており，この秘密鍵を用いることで，顔が秘匿されていない状態の映像を見ることができる．一方前者は，秘密鍵を持たず，顔が秘匿された状態の映像のみ見ることができる．

この手法においても，文献 [11] と同様に，被撮影者のプライバシ保護の一部を実現し，RFIDタグを持つことで被撮影者の意思が確認できるが，匿名性を完全に実現していないため，プライバシが完全に保護されない可能性がある．たとえば，RFIDタグから出される信号が定型のものであれば偽造される可能性があり，通常の署名などであればその署名者が特定される．このほかにも，文献 [11] や [21] と同様に顔を隠すことによって，プライバシ保護の一部を実現し，かつ観察者の権限によって，見ることのできる映像が異なるという監視カメラシステムの研究は以下の4つがあげられる．Seniorらの研究 [22] では，被撮影物をシステム側で識別し，観察者に応じて識別した情報を提供することができる．Sohnらの研究 [23] では，被撮影者の顔部分にスクランブリングをかけることにより顔情報を秘匿し，スクランブリングを復号する鍵を持つ観察者のみが原動画を見ることができる．Carrilloらの研究 [24] は，監視カメラで撮影した人物の顔部分をエンコード前に暗号鍵で暗号化し，ディスプレイに表示する際には，デコード後に復号鍵を用いた場合のみ顔部分を正しく復号することができるというシステムである．Dufauxらの研究 [25] は監視カメラで撮影した映像にスクランブリングを施すことでプライバシを保護し，スクランブリングに用いた公開鍵に対応する秘密鍵を用いることで，元の映像を見ることができる．また，プライバシ保護の一部を実現するためにChenらの研究 [26] では，被撮影者に対してghost-imageを生成している．このghost-imageからは，被撮影者が着ている服なども含めたghost-imageを作成することで性別を判断することが困難となり，その人物をよく知る観察者に対しても有効な個人情報の秘匿になると考えられる．しかしながら，このghost-imageも被撮影者の意思によって生成されてい

るものではないので，自身の情報の制御の実現はされていない．

3.2 Short Group Signatures

Short Group Signatures [8] は次の 3 つの特徴を持っている．

1. グループに設定されたメンバのみが電子署名を生成することができる．
2. 署名検証者は署名の検証を行うことができるが，署名者を特定することができない．
3. 必要が生じた際，特別な権限を持つもののみが署名者を特定することができる．

これらの特徴を持つ Short Group Signatures [8] により提案システムでは，被撮影者の意志の確認を実現する．次に，Short Group Signatures [8] の説明を行う．

(1) Bilinear Groups

まず，BilinearGroups という設定を行い，以下の条件を満たす．

1. G_1 と G_2 は素数 p を法とした巡回群である．
2. g_1 は G_1 の元，g_2 は G_2 の元である．
3. ψ は計算可能な同型写像で，$\psi(g_2) = g_1$ を満たす．
4. e は $G_1 \times G_2 \to G_T$ とするペアリング関数であり，

・Bilinearity

すべての $u \in G_1$，$v \in G_1$，$(a, b) \in Z$ について，以下が成り立つ．

$$e(u^a, v^b) = e(u, v)^{ab}$$

・Non-degeneracy

$$e(g_1, g_2) \neq 1$$

を満たす．

(2) 署名アルゴリズム

次に署名アルゴリズムを示す．

・鍵生成

まず，認証局は，次の設定を行う．

$$g_2 \in G_2,\ \psi(g_2) = g_1,\ (h, \xi_1, \xi_2) \in G_1 \setminus \{1_{G_1}\}$$

また，$u^{\xi_1} = v^{\xi_2} = h$ を満たすような (u, v) を選ぶ．次に，γ を秘密のパラメータとして $w = {g_2}^{\gamma}$ を満たす w を設定する．

認証局は，検証鍵 gpk として

$$\mathrm{gpk} = (g_1, g_2, u, v, h, w)$$

を公開する．また，各グループメンバ i に署名鍵 gsk[i] を次のように生成し，配布する．

$$\mathrm{gsk[i]} = (A_i, x_i)$$

ここで，A_i および x_i は次の条件を満たす．

$$A_i \in G_1 \qquad {A_i}^{\gamma + x_i} = g_1$$

認証局は署名者を特定するための管理鍵 $\mathrm{gmk} = (\xi_1, \xi_2)$ を秘密鍵として管理する．

・署名生成

署名者であるグループメンバ i は署名を生成する際に，2 つの値を次のように設定する．

$$\alpha, \beta \xleftarrow{R} Z_p$$

そして，次の 5 つの値を計算する．

$$T_1 = u^{\alpha},\ T_2 = u^{\beta},\ T_3 = A_i h^{\alpha+\beta},\ \delta_1 = x_i\alpha,\ \delta_2 = x_i\beta$$

これらの値を計算した後，次の 5 つの値を選ぶ．

$$r_{\alpha},\ r_{\beta},\ r_{x_i},\ r_{\delta_1},\ r_{\delta_2} \in Z_p$$

これらの値を用いて次の値を計算する．

$$R_1 = u^{r_{\alpha}},\ R_2 = v^{r_{\beta}}$$
$$R_3 = e(T_3, g_2)^{r_{x_i}} \cdot e(h, w)^{-r_{\alpha}-r_{\beta}} \cdot e(h, g_2)^{-r_{\delta_1}-r_{\delta_2}}$$
$$R_4 = T_1^{r_{x_i}} u^{-r_{\delta_1}},\ R_5 = T_2^{r_{x_i}} v^{-r_{\delta_2}}$$
$$c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_p$$
$$s_{\alpha} = r_{\alpha} + c\alpha,\ s_{\beta} = r_{\beta} + c\beta,\ s_{x_i} = r_{x_i} + cx_i$$
$$s_{\delta_1} = r_{\delta_1} + c\delta_1,\ s_{\delta_2} = r_{\delta_2} + c\delta_2$$

そして，署名者メッセージ M に対する署名を以下のように公開する．

$$\sigma = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{\delta_1}, s_{\delta_2})$$

・署名検証

検証者は署名をもとに次の計算を行う．

$$\overline{R_1} = u^{s_{\alpha}} T_1^{-c},\ \overline{R_2} = u^{s_{\beta}} T_2^{-c}$$
$$\overline{R_3} = e(T_3, g_2)^{s_{x_i}} \cdot e(h, w)^{-s_{\alpha}-s_{\beta}} \cdot e(h, g_2)^{-s_{\delta_1}-s_{\delta_2}} \cdot \big(e(T_3, w)/e(g_1, g_2)\big)$$
$$\overline{R_4} = T_1^{s_{x_i}} u^{-s_{\delta_1}},\ \overline{R_5} = T_2^{s_{x_i}} v^{-s_{\delta_2}}$$

これらの計算をした後，次のように検証を行う．

$$c = H(M, T_1, T_2, T_3, \overline{R_1}, \overline{R_2}, \overline{R_3}, \overline{R_4}, \overline{R_5})$$

・署名者の特定

認証局は署名と自身の秘密鍵 $\mathrm{gmk} = (\xi_1, \xi_2)$ を用いて以下の計算を行うことで，署名者の署名鍵の一部を算出することができる．

$$\frac{T_3}{T_1^{\xi_1} \cdot T_2^{\xi_2}} = \frac{A_i h^{\alpha+\beta}}{u^{\alpha\xi_1} \cdot v^{\beta\xi_2}} = A_i$$

認証局はグループメンバの情報を管理しているため，署名鍵の一部を算出することにより，署名者を特定することができる．

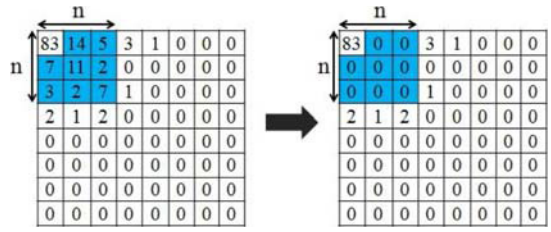

図 1 $n = 3$ のときのモザイク手法
Fig. 1 Mosaic method ($n = 3$).

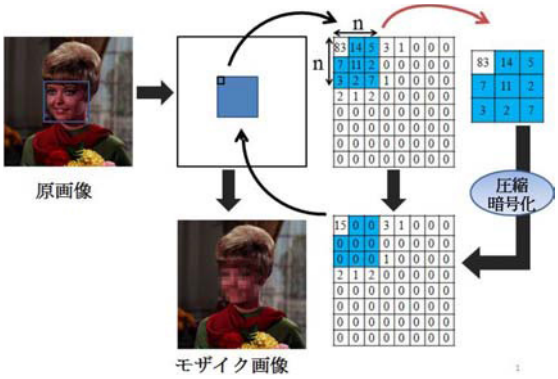

図 2 モザイク・埋め込みの全体の流れ
Fig. 2 Flow of mosaic processing.

3.3 原動画が復元可能なモザイクシステム

提案システムの要件を満たす顔情報の制御手法として，「原動画が復元可能なモザイクシステム」[9] についての説明を行う．

(1) 原理

JPEG 圧縮において，原画像をブロックに分割して離散コサイン変換を行い，量子化を行った後符号化することで JPEG 圧縮した画像を得られるが，量子化した後に，**図 1** のように DC 成分以外の周辺の $n \times n$ の周波数成分の値を 0 にすることにより，ブロック歪みが発生し，モザイクをかけたような状態になるためそれを利用する．また，変更前の量子化出力の値を保存しておき，0 にした箇所に置き換えることでモザイクの除去を行う．

(2) モザイク化・埋込み手順

モザイク化・埋め込み手順の流れを**図 2** に示す．原画像をブロック分割し，離散コサイン変換，量子化を行う．モザイクをかける顔情報の範囲に対して，得られた量子化出力の DC 成分以外の $n \times n$ の値を保存する．また，保存した箇所の量子化出力すべてに対して 0 を代入する．さらに，文献 [10] の手法により DCT 領域内に可逆電子透かしで埋め込む．最後に，エントロピー符号化を行うことで JPEG 圧縮された透かし情報を埋め込んだモザイク画像を得る．本稿ではこの画像を透かしモザイク画像と呼ぶ．

(3) 抽出・モザイク除去手順

全体の流れを**図 3** に示す．JPEG 圧縮された透かし情報を埋め込んだモザイク画像に対して，エントロピー復号を行う．それにより，透かし情報が埋め込まれた量子化出力

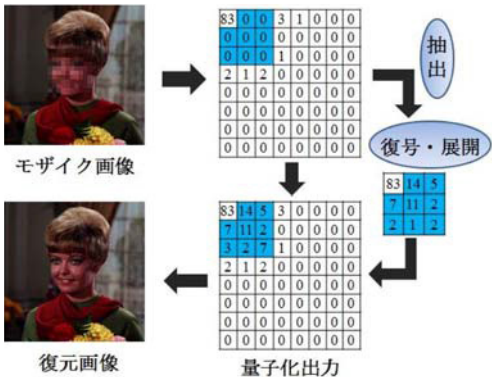

図 3 抽出・モザイク除去の流れ
Fig. 3 Flow of mosaic restoration.

の値を得る．ここから，文献 [10] の手法で透かし情報を抽出し元の情報を得る．得られた値を，DC 成分以外の $n \times n$ の範囲に再び代入し，最後にエントロピー符号化を行うことで，モザイクが除去された JPEG 圧縮の画像を得る．

4. 提案システム

4.1 提案システム概要

提案システムでは，2 章に示した監視カメラシステムに関する問題点を解決するために，以下のようなシステムを考える．

まず，近年のプライバシに関する概念である自分に関する情報のコントロールを実現するために，被撮影者は監視カメラシステムに対して，自分の意思（個人情報である顔情報を秘匿したいという意思）を示すことができ，システムはその意思に基づいて被撮影者の顔情報の秘匿を行う．

次に，被撮影者が顔情報の秘匿を望んでも，被撮影者が顔を隠して不正を行うことを前提に利用することは望ましくない．よって，システムは顔情報の秘匿を望む被撮影者を特定する仕組みを持つ．ただし，システムによって被撮影者が特定されるのは，その被撮影者が不正を行った場合のみとする．

さらに，犯罪が起こったときには，顔情報の秘匿を望んだ被撮影者も，警察などによる正式な捜査においてはその秘匿が解かれ，監視カメラを利用した従来の捜査を可能とする．

よって，提案システムは以下の 3 つの要件を実現する．

1. 監視カメラに映る被撮影者のうち，自身の顔情報を秘匿したい人物の顔情報を秘匿できる．
2. 顔情報の非公開を望む被撮影者は不正を行われない限り身元が特定されない．
3. 事件などが起きた場合に，必要が生じた際には，警察などが監視カメラ映像中の被撮影者の顔情報をすべて確認することができる．

上記 3 つの要件を実現する提案監視カメラシステムの概要を**図 4** に示す．

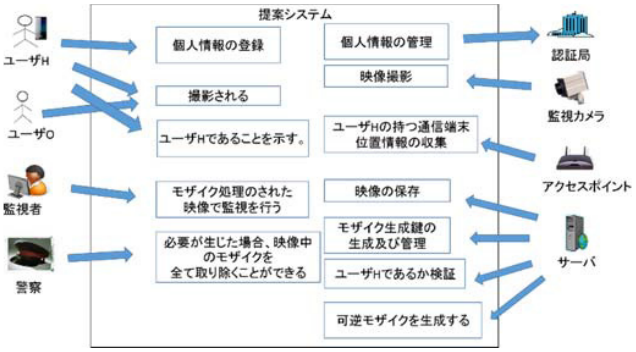

図 4 提案システムの概要
Fig. 4 Overview of proposed system.

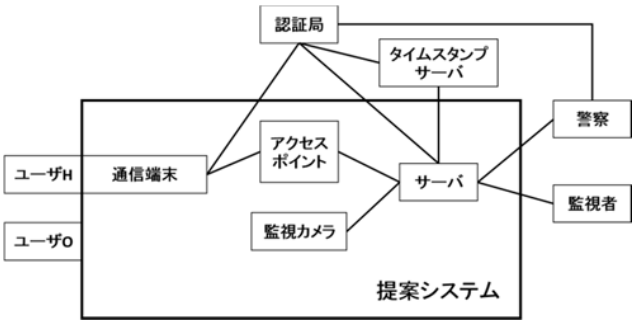

図 5 提案システムモデル
Fig. 5 Model of proposed system.

図 4 において，ユーザ H はプライバシに関心を持ち，監視者に対して，顔情報を秘匿したいと望む人である．それを示すための通信端末を持つ．また，ユーザ O はプライバシへの関心が低く，顔情報が監視者に対して公開されることに抵抗のない人である．監視者はサーバより送られてくる映像をリアルタイムに監視を行う人である．また，警察は犯罪捜査に監視カメラ映像を使用し，必要が生じた際には隠された顔情報をすべて確認することができる．認証局はユーザ H になることを望む人物の個人情報を登録し安全に管理を行う．さらに，ユーザ H の匿名性を実現する鍵情報を作成する．監視カメラは撮影した映像をサーバへと送信する．また，アクセスポイントはユーザ H の持つ通信端末より送られてくる情報をサーバへと送信し，同時にその通信端末の位置情報を収集しサーバへ送信する．サーバはアクセスポイントより送られてくる情報を基に，ユーザ H が正当なユーザ H であるかどうかを検証し，ユーザ H の顔部分に取り外し可能なモザイク（可逆モザイク）を生成する．また，可逆モザイク生成時に使用した情報を管理する．さらに，モザイク処理を施された映像を監視者へと送信し，サーバ内にその映像を保存する．

4.2 提案システム構成

図 5 に提案システムのシステム構成を示す．

(1) システム利用者

・被撮影者

被撮影者をユーザ H，ユーザ O に分類した．また，各ユーザは以下の要件を満たす．

・ユーザ H

1. 自分の顔情報の秘匿を希望する．
2. 自身の情報については認証局に登録しており，認証局からユーザ H であることを証明するための鍵を得ている．
3. 通信端末を持ち，アクセスポイントと通信を行い，認証局から得た鍵を用いてユーザ H であることを示す．

・ユーザ O

1. 自分の顔情報の秘匿に関して関心が低い．
2. 通信端末によるアクセスポイントとの通信を行わない．

・監視者

提案システムにおいて，監視者は以下の要件を満たす．ただし，監視画像を自身のスマホなどを用いて撮影し，不正に流出させる可能性がある．

1. サーバより送られてくる映像を用いて監視を行う．
2. サーバでの監視に必要な機能のみ操作でき，サーバの設定などは改変できない（サーバはパスワードなどの認証情報を知らない人に対しては設定を変更させない）．

・システム管理者

提案システムにおいて，システム管理者は以下の要件を満たす．

1. 監視カメラ，アクセスポイント，サーバが正常に動作するように管理をする．
2. システムに関して責任を持ち，不正は行わない．

・警察

警察は犯罪捜査時に捜査令状などの正式な手続きを踏み，監視カメラ映像を利用することができる．そのとき，提供される監視カメラ映像中のモザイクを除去する要請を行うことで，モザイク除去を行うための情報や，不正者がユーザ H であったときに，ユーザ H を特定できる登録情報を認証局より得ることができる．また，得た情報を不正に利用することなく，安全に管理する．

(2) システム構成要素

・監視カメラ

監視カメラには，近年普及しつつあるネットワークカメラの使用を想定している．ネットワークカメラには，映像を暗号化して出力する機能を持つものがある．提案システムにおける監視カメラは以下の要件を満たす．

1. 撮影した映像をシステム内に設置されているサーバに対して送信する．
2. 映像を送信する際，映像を暗号化する．
3. 耐タンパ性を持つ．

・アクセスポイント

提案システムにおいて，アクセスポイントは以下の要件を満たす．

1. 監視カメラの設置される設備内に複数設置される．
2. ユーザ H の持つ通信端末とシステム内に設置されるサーバと通信を行う．
3. ユーザ H の持つ通信端末の位置を特定するために必要な情報を収集しサーバへ送信する．
4. 耐タンパ性を持つ．

・サーバ

提案システムにおいてサーバは以下の要件を満たす．

1. アクセスポイントを介して，ユーザ H の持つ通信端末と通信を行う．
2. 被撮影者個人を特定することすることなく，被撮影者がユーザ H であることを検証することができる．
3. 可逆モザイクを施すことができる．
4. TDOA 方式により，ユーザ H の持つ通信端末位置情報を得ることができる．
5. 映像内の人物位置を推定することができる．
6. サーバは信頼できるシステム管理者によって管理されている．
7. 耐タンパ性を持つ．

要件 2 は「Short Group Signatures」[8] を用いることで実現する．

要件 3 にある可逆モザイクとは，取り外し可能なモザイクのことを指し，その一手法として「可逆透かしを用いた JPEG 画像へのモザイク手法」[9] を用いる．

要件 4 にある TDOA 方式とは，端末が送信した信号を複数の基地局で受信し，それぞれの基地局間での信号の受信時刻の差を用いることで端末位置を算出する方式である．また，TDOA 方式を用いた端末位置推定技術として「UWB-IR 無線方式による屋内位置検知」[14] などがある．

また，本稿で想定しているサーバのセキュリティレベルは，システム管理者のみがサーバの設定を実行できるようにパスワードなどによるアクセス制限をかけることが可能であり，内部に保存されている監視カメラ映像を含む情報にはシステム管理者による正規なアクセス以外ではアクセスできないようになっている．

・通信端末

提案システムにおいて，通信端末は以下の要件を満たす．

1. ユーザ H により安全に管理されている．
2. サーバに対し認証局から得た鍵を用いて Short Group Signatures を生成し，アクセスポイントを介してサーバへと送信する．

・タイムスタンプサーバ

タイムスタンプサーバはタイムスタンプ情報を監視カメラシステム内のサーバおよび認証局へ送信する．

・認証局

提案システムにおける認証局は以下の要件を満たす．

1. ユーザ H の個人情報を管理する．
2. ユーザ H に Short Group Signatures の署名鍵を生成する．
3. Short Group Signatures の検証鍵を生成し，公開する．
4. 犯罪捜査時に，警察からの要請があった場合，ユーザ H を特定し，その個人情報を警察へ提供する．

4.3 信頼を置いた役割の検討

本稿では，警察，認証局，タイムスタンプサーバ，サーバに対して，信頼する仮定を設けている．従来のガイドラインには，これらの信頼性に関して特に言及はされていない．ガイドラインには，監視カメラの設置場所の規定や設置の際に設置していることを示すこと，そして映像を記録する媒体（DVD やビデオテープ）を外部に漏らさないよう管理することが示されている．そこで，従来のガイドラインをふまえ我々が設けた仮定について検討する．

警察ついては，手に入れた情報を外部に流出する可能性を完全に否定することは困難であるが，それは捜査上得た情報や証拠を警察の担当者が漏洩することと同じで，どのような犯罪捜査においても起きうることである．しかし，それを根拠に警察を信頼できないとするのは一般的ではないため，信頼できる組織とするのは妥当であると考える．警察内の内部犯罪に関しては，社会的な別の方法で対応していく必要がある．また，認証局およびスタンプサーバについては，SSL などを含む今までの実績を考慮すれば，Short Group Signatures においても同様の安全性を仮定することは妥当だと考えられる．サーバについては，従来のガイドラインにも特に言及されているものではないが，記録媒体を外部に漏らさないよう管理することが示されている．提案システムではサーバの管理をサーバの管理について責任を持ち，サーバの機能を自分だけが設定できるシステム管理者と，そのサーバを用いて実際の監視業務を行う監視者の 2 つに大きく分けており，システム管理者は実際の監視業務は行わず，監視者はサーバに関してパスワードなどを知らないため不正な設定は行えない．また，システムに関する不備・不正はすべてシステム管理者の責任となることから，システム管理者は不正をするメリットがない．よって，サーバは信頼できる（監視者は不正をする可能性がある）という仮定を設けることは妥当であると考えられる．

4.4 通信プロトコル

本節で，提案システムにおける通信プロトコルを示す．ただし，アクセスポイント，監視カメラ，サーバ間，および認証局，サーバ，警察，タイムスタンプサーバ間で生じる通信については暗号化などにより安全に行われるとする．

(1) 事前設定

ここでは，被撮影者のうちユーザ H となることを望む人が行う設定について説明する．なお，この設定は監視カメラの撮影範囲内に入る前に行う．

・ステップ 1

ユーザ H となることを希望する人物は認証局に自身の個人情報を登録する．

・ステップ 2

認証局は，個人情報登録時にその情報を確認し，各ユーザ H に対し，署名鍵 gsk，ID を与える．また，検証鍵 gpk を公開し，認証局の秘密鍵 gmk を管理する．

・ステップ 3

サーバは，自身の秘密鍵 s（サーバ秘密鍵）を設定し，管理する．

(2) モザイク生成

ここでは，実際にユーザ H となった被撮影者が監視カメラの撮影範囲内に入った際に行う通信プロトコルを示す．

・ステップ 1

サーバは複数設置されているアクセスポイントを介し，自身の ID 情報（IDserver）をユーザ H に対して送信する．

・ステップ 2

ユーザ H は IDserver を受け取ると，乱数 r を生成する．

・ステップ 3

ユーザ H は受け取った IDserver，乱数 r，自身の ID を用いて，以下のように値 k を生成する．

$$k = H(ID \,\|\, IDserver \,\|\, r)$$

・ステップ 4

k に対して 3.2 節に従い署名 σ を署名鍵 gsk を用いて生成し，アクセスポイントを介して，σ，k を送信する．

$$\sigma = \left(T_1, T_2, T_3, k, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2}\right)$$

・ステップ 5

サーバはユーザ H から各情報を受け取ると，検証鍵を用いて署名の検証を行う．ただし，同じ署名については 1 度しか行わない．

・ステップ 6

サーバは，検証した署名が正当なものであった場合，その署名を送信してきた通信端末を所有しているユーザ H の顔を特定し可逆モザイクを生成する．可逆モザイクを生成する際に使用する鍵 mk はタイムスタンプサーバより送られてくる情報 Ts，ユーザ H の署名 σ を用いてハッシュ値を生成し，その値をサーバ秘密鍵 s で暗号化し生成する．

$$mk = \mathrm{Enc}_s H(Ts \,\|\, \sigma)$$

・ステップ 7

サーバは，モザイク処理の施された映像を監視者へ出力する．また，モザイク処理を施した後，mk を削除し，サーバ内にそのモザイク映像と σ を保存する．

(3) モザイク除去

ここでは，警察が犯罪捜査時に監視カメラ映像を用いる際にモザイクを除去するためのプロトコルを示す．

・ステップ 1

警察は，捜査令状などの正規手続きを行い，その旨を認証局へ伝える．

・ステップ 2

認証局は警察の正規手続きを確認すると，サーバに対し，捜査対象のモザイク映像の撮影時刻，σ を認証局へ送信するよう要求する．

・ステップ 3

認証局は，サーバからの情報を用いて，撮影時刻に対応したタイムスタンプ情報 Ts をサーバと警察へ送信するようタイムスタンプサーバへ要求する．

・ステップ 4

サーバは，タイムスタンプ情報 Ts を受け取ると，モザイク鍵 mk を復元し，モザイク映像とともに警察へ送信する．

・ステップ 5

警察は，モザイク鍵 mk を用いてモザイクを除去し，顔情報の秘匿されている人物の中で個人を特定する必要が生じた際に，認証局へ登録された個人情報提供の申請を行う．

・ステップ 6

認証局は，警察から個人特定の申請を受けると，署名 σ，認証局の秘密鍵 gmk よりそのユーザ H を特定し，対応する個人情報を警察へ提供する．

5. 考察

5.1 要件の実現

提案システムで必要とした下記要件について考察を行う．

1. 監視カメラに映る被撮影者のうち，自身の顔情報を秘匿したい人物の顔情報を秘匿できる．
2. 顔情報の非公開を望む被撮影者は不正を行われない限り身元が特定されない．
3. 事件などが起きた場合に，必要が生じた際には，警察などが監視カメラ映像中の被撮影者の顔情報をすべて確認することができる．

・要件 1 について

自身の顔情報を秘匿したいと考える人物は個人情報を認証局へ登録し，ユーザ H となることで，監視カメラの撮影範囲内に入るとモザイク生成時のステップ 1〜3 にあるように，アクセスポイントを介してサーバと通信することで，可逆モザイク処理に必要な情報を送信し，モザイク生成時のステップ 6 により，顔部分に可逆モザイクを施され，監視者に対して顔情報を秘匿することができる．したがって，要件 1 を実現することができる．

・要件 2 について

ユーザ H が監視カメラシステム側に送信する情報はモ

ザイク生成時のステップ4における署名σ，値kのみであり，サーバはこの情報のみではユーザH個人を特定することができない．また，不正が発生したときに，認証局が認証局の秘密鍵gmkを使いユーザHの生成した署名より署名者を特定しない限り，ユーザHを特定することができないため，要件2を実現することができる．

・要件3について

事件が起きた場合には，モザイク除去のステップ1〜4を実行することで，警察などの組織は秘匿された顔情報を復元した映像を得ることができるため，被撮影者の顔情報を確認することができるようになり，要件3は実現することができる．

5.2 提案システムと他システムとの比較

3.1節で概要を説明したように，監視カメラにおいて顔を秘匿する技術は多く提案されている．それらの技術を使って想定されるシステムと提案システムとの比較検討を行う．

まず，多くの既存研究にある顔の秘匿は被撮影者の意思に関わりなくシステム側で行い，顔の復元は観察者の権限によって行うシステムを考える．この場合，近年のプライバシの概念である「自身の情報についてのコントロール権」は被撮影者の意思を尊重していないことから実現できない．また，管理者の権限については，犯罪捜査時に警察からの正式な要求がある場合などの限定がなく，鍵の管理に関しても十分な検討が行われていない場合，システム側の都合によって顔が復元される可能性があり，プライバシが十分保護されているとは言い難い．それに対して，提案システムでは，復元は犯罪捜査時の警察からの正式な要求がある場合に限定され，かつ認証局の協力がなければモザイク鍵が得られないことから，犯罪が起こらない限り被撮影者のプライバシは十分に保護されているといえる．

次に，提案されている顔秘匿技術のみを用いて，復元は犯罪捜査時に警察が行い，鍵の管理も安全に行われるが，被撮影者の意思に関わりなくすべての被撮影者の顔を秘匿するシステムを考える．この場合も，「自身の情報についてのコントロール権」は実現できない．特に，被撮影者がそこにいた証拠として監視カメラ映像に映ることを希望するなどの場合，被撮影者の意思に関わりなく被撮影者の顔を秘匿することは被撮影者の意思に反する．それに対して，提案システムではユーザHでも監視カメラに顔を映したい場合などは通信端末をオフにすればよく，まさに被撮影者の意思による顔情報の制御を実現する．

また，被撮影者の意思に関わりなく被撮影者の顔を秘匿する場合，監視者などによるリアルタイムの監視はほとんど意味がなくなる．すなわち，すべての被撮影者の顔が識別できないため，万引きなどの不正が行われた場合，顔の秘匿を復元した後でなければ不正者を特定できず，かつその不正者がだれか特定できないため，リアルタイムの検挙などができなくなる．それに対して提案システムでは，顔情報の秘匿を望む被撮影者は自分を認証局に登録する必要があり，自身が不正を働いたときその登録情報から自身が特定される．よって，一般に不正を働こうと思う被撮影者は認証局に登録しない，もしくは顔情報秘匿の意思を伝える通信端末をオフにすることが考えられる．その場合，顔は秘匿されないため監視カメラ映像をリアルタイムで監視する監視者によって不正者が特定され検挙などの即時の対応が可能となる．

次に，監視者によるリアルタイム監視を有効にするために，顔の秘匿は映像の保存時に行い，監視者による監視時には映像をまったく秘匿しないシステムの場合，監視者のスマホなどによる監視画面の盗撮によって監視カメラ映像が流出する可能性がある．それに対して提案システムでは，顔秘匿を希望するユーザHは監視画面上でも顔が秘匿されるので，ユーザHのプライバシは保護される（ユーザOは自身のプライバシ保護に関心が低いため問題としない）．

また，RFIDタグなどを用いて被撮影者の意思に応じて顔情報の秘匿を行うがShort Group Signaturesを用いない監視カメラシステムの場合，顔情報の秘匿を望む被撮影者はシステムに自身のIDなどを登録して，RFIDタグでその意思を示すことになると考えられる．この場合，同じIDを持つ被撮影者が存在すれば，その人物は同一人物と特定されるため被撮影者のプライバシの一部が漏洩することになる．よって，ある被撮影者がある時間帯などにそこに現れることを知る人物は，同一のID情報からその被撮影者を特定できる可能性がある．それに対して，提案システムはShort Group Signaturesを用いるため，同じ被撮影者でもそれが同一人物であることが特定されず，プライバシが十分に保護されるといえる．

最後に，可逆モザイクとShort Group Signaturesを連動させず独立に用いるシステムを考える．この場合，ユーザHの意思を匿名でシステムに伝え，システムがユーザHの顔にモザイクをかけるため，そこまでは問題なく動作する．しかし，モザイク鍵の管理がまったく考慮されていない場合，だれでも容易に顔を復元できるシステムになる可能性がある．たとえば，モザイク鍵をそのままサーバに保存していれば，システム側の都合によってモザイクが復元できる最初のシステムと等価になる．それに対して提案システムは復元時のモザイク鍵生成は警察による要請と認証局の協力がなければできず，警察と認証局が信頼できる組織であるとするとシステム側の都合による復元は行われず，被撮影者のプライバシは保証される．

5.3 想定される外部からの攻撃

本節では攻撃者をシステム外の攻撃者とシステム内の攻撃者に大きく分類し，システム外の攻撃者は通信される情

報を盗聴することや改竄することができる程度の能力を持ち，システム内において攻撃者となりうる監視者は自身のスマホなどを用いてモニタに写る監視カメラ映像を，写真や動画として撮影することができるとする（システム管理者による不正はすべて自分の責任となることから，ここでは想定しない）．システム内の攻撃者は5.2節で説明したように対処できることから，ここでは外部からの攻撃に絞って説明する．

攻撃者の目的としてあげられるのは，次のようなものが考えられる．

1. ユーザHへの成りすまし．
2. 監視カメラ，アクセスポイント，サーバ間の通信を混乱させる．
3. サーバに保存されている映像の改ざんまたは盗聴．

1のユーザHへの成りすましを行うために想定される具体的攻撃は以下のようになる．

・攻撃1

ユーザHの送信する情報を盗聴し，監視カメラシステムに対して再送信を行う．

・攻撃2

ユーザHの持つ通信端末を不正に使用する．

2の監視カメラ，アクセスポイント，サーバ間の通信を傍受および混乱させる目的として想定される具体的攻撃は以下のようになる．

・攻撃3

監視カメラ，アクセスポイント，サーバ間の通信を遮断する．

・攻撃4

監視カメラ，アクセスポイント，サーバ間の通信を傍受する．

・攻撃5

監視カメラ，アクセスポイントの送信する情報を改ざんする．

また，目的3としてあげられる具体的攻撃は

・攻撃6

サーバに進入して保存されている映像を改ざんまたは盗聴

となる．

5.4 安全性

ここでは，5.2節であげられた提案システムに対する攻撃への安全性をについて考察する．

(1) 攻撃1について

攻撃者がユーザHの送る情報を盗聴し，再度監視カメラシステムへ送信した場合は，モザイク生成時のステップ5で「サーバは同じ署名についての検証は1度しか行わない.」としているため防ぐことができる．

ユーザHであることを示すための署名はユーザHが署名生成時に乱数を生成し，それの乱数も用いることで署名を生成することで，監視カメラシステムに送られる．攻撃者が異なる乱数を用いて有効な署名を作るためにはユーザHの署名鍵を知る必要があるが，ユーザHが署名鍵を安全に管理することにより，この攻撃を防ぐことができる．

(2) 攻撃2について

基本的には，ユーザHの用いる通信端末はユーザHにより安全に管理されているため，この攻撃を防ぐことができる．通信端末が安全に管理されているとは，端末へのログインがパスワードやバイオメトリクスなどによりアクセス制御されており，正当なユーザしか使えないことを指す．

たとえ，通信端末へのアクセス制御が何らかの方法で破られたとしても，犯罪捜査時に監視カメラ映像を利用する場合にモザイク除去時のステップ6で認証局は署名者を特定する．しかし，正規のユーザHは顔情報を含む個人情報を認証局へ登録しているので，モザイクを除去した後の犯人の顔と登録されたユーザHの顔から本人ではないことが確認される．よって，認証局による署名確認だけではユーザHが容疑者とされる可能性があるため，警察はユーザHの個人情報が提供されても，顔情報の確認など初動捜査などには注意が必要となる．

(3) 攻撃3について

監視カメラやアクセスポイント自体の改変は耐タンパ性により防ぐ．また，サーバの改変もシステム管理者が正当で，設定変更などがパスワードなどで保護されていれば防ぐことができる．また，アクセスポイントはサーバとハローメッセージを定期的に送受信し合うことで，アクセスポイント—サーバ間の通信が妨害された際には検知することができる．サーバへの通信妨害が検知されると，システム管理者へ監視カメラやアクセスポイントなどがサーバ間の通信が正常に行われていないことを報告する仕組みを入れることで，システム管理者が対処することができる．また，偽画像の差し替えなどは画像の差分をとり，大きな差分が生じた場合にシステム管理者に通報する仕組みを導入することにより対処できる．ただし，これらの対策は説明が煩雑になるため提案システムには明示していない．

(4) 攻撃4について

監視カメラ，アクセスポイント，サーバ間の通信を傍受された場合，について考える．監視カメラ，アクセスポイント，サーバ間の通信は暗号化などにより安全な通信ができるため，攻撃者によって元の情報を傍受されることを防ぐことができる．

(5) 攻撃 5 について

監視カメラ，アクセスポイントからの送信情報を辻褄が合うように改ざんするためには，まず暗号化を破る必要がある．しかし，前提として監視カメラ，アクセスポイント，サーバ間の通信は安全に行われるという前提があるため，AES のような安全性が認められている暗号を正しく使っていれば辻褄があうような改ざんは困難である．単に，攻撃者が送信データを改ざんすることを望む場合，辻褄の合わないデータ（画像であればノイズ画像）となるため検知可能である．ただし，そのような改ざんを自動的に検知したい場合には，各通信において電子署名または MAC を作成し送信することで，情報の改ざんを検知できる．提案システムでは，監視者の存在を仮定しているため，辻褄の合わない情報は検知可能として，電子署名または MAC による自動検知は含まない．

(6) 攻撃 6 について

サーバに進入し保存されている映像の改ざんまたは盗聴は，サーバは信頼できるシステム管理者によって管理され，サーバは耐タンパ性を持ち，パスワードなどを知らない攻撃者には設定などを変更できないため困難である．また，監視カメラ画像やパラメータの保存に際して，システム管理者がそのハッシュ値に対して電子署名を生成して一緒に保存してもよい．この場合，定期的に保存されている映像やパラメータと電子署名を検証する仕組みを導入すれば，よりいっそうの安全性が実現できる．

6. まとめ

本稿における新規性・貢献は，以下のとおりである．

(1) 今後のプライバシに関する考え方の基本になる個人による個人情報の制御が可能な仕組みを実現するため匿名署名である「Short Group Signatures」[8] とか逆モザイク手法である「元画像が復元可能なモザイクシステム」[9] を組み合わせ，監視カメラシステムを例に示した．[8] によって，被撮影者は匿名のままでシステム側に顔情報を秘匿する意思あることを伝えることが可能となる．また，[9] により一度秘匿された顔情報も鍵（モザイク鍵）を用いることで復元可能となり，犯罪捜査の際も監視カメラ映像の活用が可能となる．

(2) (1) と監視カメラの重要な機能である犯罪防止の両立が技術的に可能であることを示し，具体的なプロトコルを提案した．

(3) その安全性を評価し，考えられる攻撃に対して安全なシステムを示した．

今後は，提案システムの実装などにより，その有効性や使い勝手を実際に検証していく必要がある．

謝辞 今回の研究のサポートをしていただいた岩村研究室メンバの皆様に感謝いたします．

参考文献

[1] 堀部政男：プライバシー保護制の歴史的経緯，14 巻，pp.18–21, 法律文化/東京リーガルマインド (2002).
[2] 開原成允：医療分野における自己情報コントロールの権の意味，16 巻，pp.20–23, 法律文化/東京リーガルマインド (2004).
[3] 独立行政法人情報処理推進機構：パーソナル情報保護と IT 技術に関する調査—調査報告書 (2012).
[4] BIGLOBE ニュース，2012 年 8 月 16 日，入手先 ⟨http://news.biglobe.ne.jp/entertainment/0816/jc_120⟩.
[5] 生活文化局：都民生活に関する世論調査（平成 23 年 11 月 24 日）.
[6] 平成 24 年度 けいしちょう安全安心モニター制度 第 1 回アンケート調査結果
[7] 京都府：防犯カメラの管理・運用に関するガイドライン（平成 18 年 12 月）.
[8] Boneh, D., Boyen, X. and Shacham, H.: Short Group Signatures.
[9] 草間雄一，姜 玄浩，岩村惠市：現動画が復元可能なモザイクシステム，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，EMM2014-85, pp.37–42 (2015).
[10] Xuan, G., Shi, Y.Q., Ni, Z., Chail, P., Cui, X. and Tong, X.: Reversible Data Hiding for JPEG Images Based on Histogram Pairs, *ICIAR 2007*, LNCS 4633, pp.715–727 (2007).
[11] 福岡直也，伊藤義道，馬場口登：観察者に応じたプライバシー保護映像を生成可能な映像配信手法，第 10 回情報科学技術フォーラム，RK-006, pp.97–100, 函館大学 (Sep. 2011).
[12] Boneh, D., Boyen, X. and Shacham, H.: Group Signatures, *EUROCRYPTO'91*, Lecture Notes in Computer Science, Vol.547, pp.257–265 (1991).
[13] 濱田直人，中山卓也，中西 透，船曳信生：所属無効化可能なグループ署名方式の素数情報を用いた高速化とその実装，電子情報通信学会技術研究報告．ISEC, 情報セキュリティ，Vol.106, No.411, pp.47–54 (2006).
[14] 水垣健一：UWB-IR 無線方式による屋内位置検知，電子情報通信学会誌，Vol.92, No.4, pp.256–261.
[15] 株式会社矢野経済研究所：世界のネットカメラ市場に関する調査結果 2013—アジア・中東圏で高成長，2015 年 575 万台のネットワークカメラ世界市場を予測，2013 年度版ネットワークカメラ/VCA 画像解析システム市場—ビジュアル・コミュニケーション調査シリーズ (May 2013).
[16] 名和小太郎：プライバシー：定義，情報管理，Vol.55, pp.521–523 (2012).
[17] Microsoft Azure Japan Team Blog: available from ⟨http://blogs.msdn.com/b/windowsazurej/archive/2015/02/17/microsoft-azure-the-first-cloud-computing-platform-to-conform-to-iso-iec-27018-the-only-international-set-of-privacy-controls-in-the-cloud.aspx⟩.
[18] 埼玉県防犯指針（平成 17 年 3 月）.
[19] 防犯カメラのガイドライン—神奈川県 第二章（平成 17 年）.
[20] 福岡県防犯カメラの設置及び運用に関するガイドライン（平成 19 年 8 月）.
[21] Zhang, W., Cheung, S.-C.S. and Chen, M.: Hiding privacy information in video surveillance system, *ICIP*, Vol.3, pp.868–871 (2005).
[22] Senior, A., Pankanti, S., Hampur, A., Brown, L., Tian, Y.-l. and Ekin, A.: Blinkering Surveillance: Enabling Video Privacy through Computer Vision, *IEEE Security & Privacy*, Vol.3, pp.50–57 (2005).
[23] Sohn, H., De Neve, W. and Ro, Y.M.: Privacy

Protection in Video Surveillance Systems: Analysis of Subband-Adaptive Scrambling in JPEG XR, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.21, pp.170–177 (2011).
[24] Carrillo, P., Kalva, H. and Magliveras, S.: Compression independent object encryption for ensuring privacy in video surveillance, *2008 IEEE International Conference on Multimedia and Expo*, pp.273–276 (2008).
[25] Dufaux, F. and Montreux, Ebrahimi, T.: Scrambling for Privacy Protection in Video Surveillance Systems, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.18, pp.1168–1174 (2008).
[26] Chen, D., Chang, Y., Yan, R. and Yang, J.: Tools for protecting the privacy of specific individuals in video, *EURASIP Journal on Applied Signal Processing*, Vol.2007 (2007).

小林 健人

平成 2 年生．平成 26 年東京理科大学工学部電気工学科卒業．平成 26 年東京理科大学工学研究科電気工学専攻入学．

稲村 勝樹

昭和 47 年生．平成 10 年東京工業大学工学部有機材料工学科卒業．平成 12 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年第二電電（株）（現 KDDI（株））入社，（株）京セラ DDI 未来通信研究所（現（株）KDDI 研究所）配属．平成 27 年東京理科大学博士（工学）．現在，東京電機大学理工学部情報システムデザイン学系助教．暗号・電子署名アルゴリズム，情報セキュリティの研究に従事．電子情報通信学会，映像情報メディア学会，INSTICC 各会員．

金田 北洋 （正会員）

昭和 59 年早稲田大学理工学部機械工学科卒業．昭和 61 年同大学院修士課程修了．同年キヤノン株式会社入社．平成 7 年米国デューク大学電気工学科修士課程修了．平成 22 年東京理科大学大学院理工学研究科博士課程修了，工学博士．現在，キヤノン株式会社アドバンスト IRT 開発センター，および大阪府立大学連携大学院客員教授，同文書解析・知識科学研究所客員研究員．主に文書画像解析/認識，言語処理，ビッグデータ解析の研究・製品開発に従事．画像電子学会会員．

岩村 恵市 （正会員）

昭和 55 年九州大学工学部情報工学科卒業．昭和 57 年同大学院修士課程修了．同年キヤノン株式会社入社．平成 6 年東京大学工学博士．現在，東京理科大学工学部電気工学科教授．主に符号理論，並列処理，情報セキュリティ，電子透かしの研究に従事．電子情報通信学会，情報処理学会，情報理論とその応用学会各会員，情報ハイディングおよびその評価基準研究会委員長，本会フェロー．