プライバシー保護と犯罪防止を両立する監視カメラにおける プロトコル及び安全性の設計

小林 健人† 岩村 惠市† 稲村 勝樹‡

†東京理科大学
125-8585 東京都葛飾区新宿 6-3-1
kobayashi_k@sec.ee.kagu.tus.ac.jp
iwamura@ee.kagu.tus.ac.jp

‡東京電機大学 理工学部 情報システムデザイン学系
350-0311 埼玉県比企郡鳩山町大字石坂 925-1
minamura@rd.dendai.ac.jp

あらまし 本稿では筆者らが2014年3月7日のEMM研究会にて発表した「プライバシー保護と犯罪防止を両立する監視カメラシステム」におけるプロトコル及び安全性についての具体的な設計を行った. 本プロトコルによって, 被撮影者の意志をその個人情報を特定することなく監視カメラシステム側にて検証することができる. また, 顔情報を秘匿するための可逆モザイクを生成するためのモザイク生成鍵の生成方法を本プロトコルにて示した. さらに, 本稿では本監視カメラにおける通信プロトコルを記述し, 想定される攻撃に対する安全性を示した.

Design the protocol and safety in the surveillance camera system that achieves both crime prevention and privacy protection

Kento Kobayashi† Keiichi Iwamura† Masaki Inamura‡

†Tokyo University of Science.
125-8585, 6-3-1 Niijuku, Katsushika-ku, Tokyo, Japan.
kobayashi_k@sec.ee.kagu.tus.ac.jp
iwamura@ee.kagu.tus.ac.jp
‡Division of Information System Design, College of Science and Engineering, Tokyo Denki University.
350-0311, 925-1 Oazaishizaka, Hatoyama-machi, Hiki-gun, Saitama, Japan
minamura@rd.dendai.ac.jp

Abstract In this paper, we design the protocol and safety in the surveillance camera system that achieves both crime prevention and privacy protection. With the protocol, the system can verify the will of the people who are photographed by the surveillance camera. In addition, we confirm the way of the mosaic key generation (the mosaic key is needed to hide the face.) in the protocol. Finally, we estimate attack and prove the safety in the communication protocol.

1. はじめに

近年，インターネットの普及が進み，プライバシーと個人情報について取り上げられる場面が増加している．プライバシーとは「私事，私生活，個人の秘密そのものを指し，また，それらが干渉または侵害されない権利」のことを言う．しかし，近年のプライバシーという考え方では「個人情報に関するコントロール権」というものを含むようになっている[1]．また，個人情報とは「個人を特定することのできる情報」のことを言い，例えば，氏名，生年月日，生体情報など多くの情報を含む．

ここで，近年関心が強まっている監視カメラについて考える．平成 23 年 11 月に公開されている「東京都の世論調査」[2]では，「効果が高いと思う行政の取り組みや地域活動」という項目において，「防犯カメラの設置」に対して 64%が支持している（標本数：2009 標本）．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 1 回アンケート調査結果」[3]では，防犯カメラに対するイメージのアンケート項目において，94%が「事件が起きた際に犯人がつかまりやすくなる」，また，87．5%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．

しかし，現在監視カメラにおけるプライバシーの問題が起きている．監視カメラ映像を見ることのできる人間による映像（またはその一部）の不正な流出が挙げられる．既存の監視カメラには個人情報の取り扱いが規定されていないことに起因すると考えられる．従って，監視カメラにおいて，プライバシーを考慮したシステムを実現することは非常に重要である．

筆者らは過去に，「プライバシー保護と犯罪防止を両立する監視カメラシステム」[4]を提案している．[4]では，以下の 3 つを実現するシステムを提案した．

1. 被撮影者の意志によって，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が特定されない．
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全て明かすことができる．

しかし，前述の論文はそのコンセプトを示しただけで，具体的な手順や通信プロトコルなどは示されていなかった．

本論文では，提案した監視カメラシステムにおける通信プロトコルを具体化し，さらにシステムに対する攻撃とそれに対する安全性を示した．

第 2 章にて，監視カメラにおける問題点について述べ，第 3 章にて，EMM において提案した，提案システムの概要やシステム構成，システムモデル，通信プロトコルを説明する．また，第 4 章にて想定される攻撃，第 5 章にてシステムの安全性について述べる．

2. 監視カメラの問題点

近年人々の関心が強くなっている監視カメラについて考える．監視カメラ映像において，個人情報（顔情報）の取り扱い方についての規定は具体的には設けられていない．また，監視カメラ映像の流出という問題も起きている[5]．特に，芸能人のプライベート時に撮影された映像やその一部がインターネット上に公開されてしまうということが実際に起きており，監視カメラの被撮影者のプライバシーを守ることが重要であると考えられる．近年のプライバシー権の考え方からすると，非撮影者によって個人の顔情報が制御されることが望ましい．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 1 回アンケート調査結果」[2]では，防犯カメラに対するイメージのアンケート項目において，設置についての意見では，75．5%が「データの管理をしっかりしてほしい」，39．2%が「プライバシーに配慮したルールを整備してほしい」という意見を述べている．

しかし，現在監視カメラは犯罪防止のために用いられることが多く，被撮影者によって制御されることが好ましくない場合が存在する．よって，監視カメラ映像に対し，プライバシー保護を実現し，かつ，その有効利用を両立させる研究は非常に重要である．

3. 提案システム

3.1　提案システム概要

提案システムでは，以下の要件を次の技術を用いて実現する．

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. ⇒顔のモザイク化により実現.
2. 被撮影者が特定されない. ⇒ Short Group Signatures[6]により実現.
3. 事件などが起きた場合に, 警察等が監視カメラにより全被撮影者の顔情報を確認できる. ⇒1 のモザイクは具体的には, 隠した顔情報を暗号化して埋め込む可逆透かしと, 必要な特に元に戻せる可逆モザイクにより実現.

3.2 提案システム構成

提案システムでは, 被撮影者を「顔情報を監視者に対して秘匿したい人」と「顔情報を監視者に対して公開しても構わない人」の 2 種類に分類した. 今後, 前者を User_H, 後者を User_O とする. 図 3.1 にシステムモデルを示し, 各要素について説明する. また, 提案システムでは屋内の監視を想定している.

また, 提案システムでは, Short Group Singatures[6], 可逆透かしを用いた JPEG 画像へのモザイク手法[7]を用いる. 3.3 節で Short Group Signtatures[6], 3.4 節で可逆透かしを用いた JPEG 画像へのモザイク手法[7]の説明を行う.

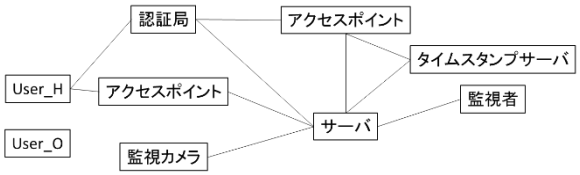

図 3.1 システムモデル

3.2.1 被撮影者

被撮影者を User_H 及び User_O に区分し, また, それぞれの User は以下の要件を満たす.
User_H
1. 自分の顔情報の保護(秘匿)を希望する.
2. 通信端末を持ち, 監視カメラシステムと通信を行い, 自分の意思を示す.
3. 自身の持つ情報については安全に管理する.

User_O
1. 自分の顔情報の保護(秘匿)に関して関心がない.
2. 通信端末などを持たず, 監視カメラとも通信を行わない.

3.2.2 監視カメラ

監視カメラには, 近年普及されることが多くなったネットワークカメラを想定している. 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. また, 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. 映像を送信する際には, その映像を暗号化し, サーバのみ復号できる形式にする.

3.2.3 アクセスポイント

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. User_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.

3.2.4 サーバ

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, User_H の持つ通信端末と通信を行う.
2. 被撮影者の身元を特定せず, 被撮影者が User_H であることを確認できる.
3. 可逆モザイクを施すことができる.
4. TODA 方式により, User_H の持つ端末位置情報を得ることができる.
5. 映像内の人物の位置を推定することができる.

要件 2 は Short Group Signatures [6]を用いて実現する.

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」[7]を用いる. 本提案では AES 暗号を用いて顔情報を秘匿し, その暗号・復号鍵としてモザイク鍵を用いる. モザイク鍵は, User_H, 時間ごとに異なる様設定する必要がある. 時間情報を用いるのは, 一度モザイクを除去した後にその User_H が映る他の映像のモザイクが除去できてしまうことを防ぐためである.

3.2.5 タイムスタンプサーバ

このタイムスタンプサーバは，既存に存在するものを想定しており，タイムスタンプ情報をサーバ及び認証局へ送信する.

3.2.6 認証局

1. User_H の個人情報を管理する.
2. User_H に Short Group Singatures 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. 犯罪捜査時には，署名者を特定し，警察へその署名者の個人情報を明かす.

3.3 Short Group Singatures

Short Group Signatures[6]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署名を生成することができる.
2. 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. 必要が生じた際には，署名者を特定することができる.

次に Short Group Signatures[6]の説明を行う.

3.3.1 Bilinear Groups

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 $u\in G_1$，$v\in G_2$，$a,b\in Z$ について

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

・Non-degeneracy：

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

を満たす．ただし，G_T は p を法とした巡回群とする.

3.3.2 署名アルゴリズム

鍵生成

認証局は，次の設定を行う.

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

また，$u^{\xi_1}=v^{\xi_2}=h$ を満たすよう u,v を選ぶ.

次に，γ を秘密のパラメータとし，$w=g_2{}^{\gamma}$ を満たす w を設定する．認証局は検証鍵として，

$$gpk=(g_1,u,v,h,g_2,w)$$

を公開する.

また，認証局は各グループメンバ i に，署名鍵 gsk を次のように生成し，配布する.

$$gsk(i)=(A_i,x_i)$$

ここで，A_i，$A_i{}^{\gamma+x_i}$ は，次の条件を満たす.

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

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

署名生成

署名者は署名を生成する際に，2 つの値を次のように選択する.

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

そして，次の 5 つの値を計算する.

$$T_1=u^{\alpha}\quad T_2=v^{\beta}\quad T_3=Ah^{\alpha+\beta}$$

$$\delta_1=x\alpha\quad \delta_2=x\beta$$

これらの値を計算した後，次の 5 つの値を選ぶ.

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

これらの値を用いて次の値を計算する.

$$R_1=u^{r_{\alpha}} \qquad R_2=v^{r_{\beta}}$$

$$R_3=e(T_3,g_2)^{r_x}*e(h,w)^{-r_{\alpha}-r_{\beta}}*e(h,g_2)^{-r_{\delta_1}-r_{\delta_2}}$$

$$R_4=T_1^{r_x}u^{-r_{\delta_1}} \qquad R_5=T_2^{r_x}v^{-r_{\delta_2}}$$

$$s_{\alpha}=r_{\alpha}+c\alpha \qquad s_{\beta}=r_{\beta}+c\beta \qquad s_x=r_x+cx$$

$$s_{\delta_1}=r_{\delta_1}+c\delta_1 \qquad s_{\delta_2}=r_{\delta_2}+c\delta_2$$

そして，署名者はメッセージ M に対する署名を以下のように公開する.

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

ただし，c の値は以下のように計算する.

$$c=H(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)\in Z_p$$

検証

検証者は署名をもとに次の値を計算する.

$$\overline{R}_1=u^{s_{\alpha}}T_1^{-c} \qquad \overline{R}_2=v^{s_{\beta}}T_2^{-c}$$

$$\overline{R}_4=T_1^{s_x}u^{-s_{\delta_1}} \qquad \overline{R}_5=T_2^{s_x}v^{-s_{\delta_2}}$$

$$\overline{R}_3=e(T_3,g_2)^{s_x}*e(h,w)^{-s_{\alpha}-s_{\beta}}*e(h,g_2)^{-s_{\delta_1}-s_{\delta_2}}*(e(T_3,w)/e(g_1,g_2))^{c}$$

これらの値を計算した後，次のように検証を行

う.

$$\overset{?}{c} = H\left(M, T_1, T_2, T_3, \overline{R}_1, \overline{R}_2, \overline{R}_3, \overline{R}_4, \overline{R}_5\right)$$

署名者の特定

認証局は署名と自身の秘密鍵 gmk を用いて以下の計算を行うことで，署名者の署名鍵 gsk の一部を算出することができる.

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

認証鍵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って署名者を特定することができる.

3.4 可逆透かしを用いた JPEG 画像へのモザイク手法

可逆透かしを用いた JPEG 画像へのモザイク手法[7]についての説明をする.

3.4.1 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 3.2 の様に DC 成分以外の周辺の n×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，モザイクを掛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.

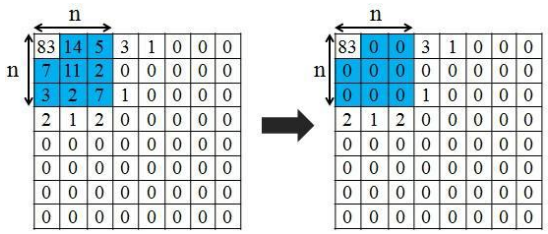

図 3.2 n=3 の時のモザイク手法

3.4.2 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 3.3 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. モザイクを掛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×n の値を保存する. また，保存した箇所の量子化出力全てに対して 0 を代入する. さらに，[8]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事で 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.

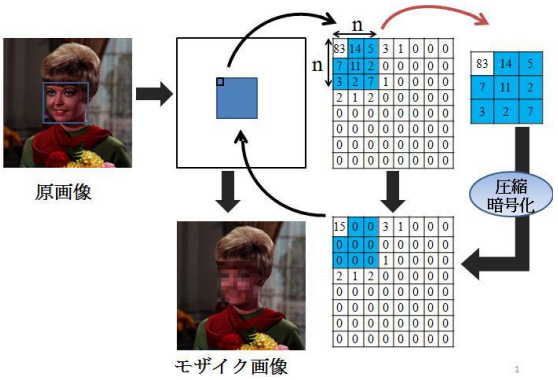

図 3.3 モザイク・埋め込みの全体の流れ

3.4.3 抽出・モザイク除去手順

全体の流れを図 3.4 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の値を得る. ここから，[8]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×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事で，モザイクが除去された JPEG 圧縮の画像を得る.

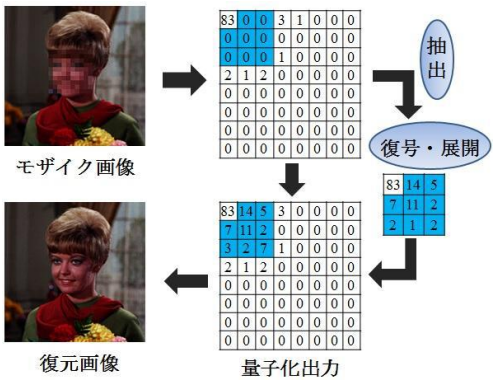

図 3.4 抽出・モザイク除去の流れ

3.5 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.

3.5.1 前提条件

本論文では，前提条件として以下の条件を設定した.

1. サーバは信頼できる管理者によって管理されている.
2. 監視カメラ，アクセスポイントは解析されない.
3. 監視カメラシステム内における通信は安全に行われる.
   ここで，監視カメラシステムとは，監視カメラ，アクセスポイント，サーバ，認証局，警察としている.
4. 各構成要素は正しく動作する.

3.5.2 事前設定

ここでは，被撮影者が監視カメラの撮影範囲内に入る前に行う設定について説明する.

ステップ 1.
User_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，User_H の個人情報を確認し，また，各 User_H に対して署名鍵 gsk と ID を生成し，配布する. 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.
認証局はサーバと値 s を共有する. この共有値はモザイク鍵生成時に用いる.

3.5.3 モザイク生成

ここでは，実際に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. ただしタイムスタンプサーバについては，設定された一定時間ごとにタイムスタンプ情報 Ts をサーバ及び認証局へ送信しているとする.

ステップ 1.
複数設置されているアクセスポイントは，自身の Ida1, Ida2, , 情報を User_H に対して送信する.

ステップ 2.
User_H は各 Ida を受け取ると，乱数 β を生成する. また，乱数 β に対し gsk を用いて署名 σ_β を生成する.

ステップ 3.
User_H は受け取った各 Ida に対し，ハッシュ関数 H を用いて，以下の様に k を計算する.

$$k = H(ID \| Ida \| \beta)$$

ステップ 4.
k に対する署名 σ を gsk を用いて生成し，アクセスポイントを介してサーバへ σ, k, β, σ_β を送信する.

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

$$\sigma_\beta = \left(T_{1\beta}, T_{2\beta}, T_{3\beta}, \beta, s_{\alpha\beta}, s_{\beta\beta}, s_{x\beta}, s_{\delta_1\beta}, s_{\delta_2\beta}\right)$$

ステップ 5.
サーバは User_H から各情報を受け取ると，各値についての署名を検証鍵 gpk を用いて検証する. ただし，同じ署名についての検証は 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端末を所有している User_H に対して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モザイク鍵 mk を以下のように生成する.

$$mk = Enc_{s_{Ts}}\left(H\left(T_s \| \sigma\right)\right)$$

$$s_{Ts} = H^{(Ts)}(s)$$

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と出力する. また，サーバは映像を保存する際には，User_O に s_{Ts} をモザイク鍵として用いて可逆モザイクを施す. その後, s_{Ts}, mk の情報を破棄し, σ と k をサーバ内に映像とともに保存する.

3.5.4 モザイク除去

ここでは，警察が犯罪捜査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.
警察からの正規手続きを受けると，サーバへ対し，以下の要求を行う.
1. 捜査対象のモザイク映像の撮影時刻，署名 σ, k を認証局に送信する.

ステップ 3.
認証局はサーバから情報を受け取ると，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.
また，k に対する署名 σ を検証し，その署名 σ の正当性が検証された場合に，署名生成者である User_H を特定する.

ステップ 4.
サーバは，認証局からタイムスタンプ情報 Ts を受け取ると，s_{Ts} を復元し，モザイク映像とともに署名 σ, s_{Ts} , Ts を警察へ送信する.
また，認証局は警察へ特定した User_H の個人情報を提供する.

ステップ 5.
警察は，サーバより送られてくる情報をもとにモザイク鍵を復元し，可逆モザイクを除去するとともに，認証局により提供される User_H の個人情報を犯罪捜査に利用する.

4. 想定される攻撃

本論文で，想定した提案システムに対する攻撃について述べる.
攻撃者の目的として挙げられるのは User_H への成りすましである. 成りすましを実現させるために想定される攻撃は,

攻撃 1.
User_H の送信する情報を盗聴し，監視カメラシステムに対し再度送信する.

攻撃 2.
User_H の持つ通信端末を不正に使用する.
また，通信を混乱または遮断させる攻撃については想定していない.
5 章にて，これらの攻撃に対する安全性を示す.

5. 安全性

ここでは，4 章で挙げられた提案システムに対する攻撃への安全性を示す.

5.1 攻撃 1. について

User_H に成りすますため，攻撃者は User_H がアクセスポイントへ送信する情報を盗聴し，再度アクセスポイントを介してサーバへ送信することが考えられる.
3.5.3 節モザイク生成のステップ 2. では User_H は通信ごとに乱数 β を生成し，乱数 β に対して署名 $σ_β$ を生成する. この乱数は一定時間内では同じものは用いられないため，同じ乱数を用いた署名が送られた場合，サーバは 2 回目の情報は不正情報として用いない. 攻撃者が異なる乱数に対して署名を作るためには User_H が持つ署名鍵を知る必要があるが，User_H は自身の情報を安全に管理しているため，この攻撃を防ぐことができる.

5.2 攻撃 2. について

基本的には User_H が用いるモバイル端末の使用についてパスワードやバイオメトリクスなどによるアクセス制御を行うことで防御する. これにより，他人が User_H に成りすますことを防止するが，万が一 User_H の端末が不正に利用されたとしても，犯罪捜査時に監視カメラ映像を利用する際には 3.5.4 節モザイク除去のステップ 3. で認証局は署名者を特定する. 正規の User_H は顔情報を含む個人情報を認証局へ登録しているため，モザイク除去をしたのちに顔情報と照らし合わせることで User_H 本人ではないことが確認することができる. ただし，最初は認証局による署名確認から User_H が容疑者とされるため初動捜査などにおいて注意が必要である.

6. まとめ

本論文で，我々は過去に提案した，プライバシー保護と犯罪防止を両立する監視カメラシステムにおけるシステムプロトコルを提案した. また，提案したプロトコルに対する攻撃を想定し，その攻撃に対する安全性を示した. 今後の課題は，提案システムの実装評価などが挙げられる.

参考文献

[1] プライバシー保護制の歴史的経緯
堀部政男 LEC 東京リーガルマインド
2002 November 法律文化

[2] 都民生活に関する世論調査
生活文化局 平成 23 年 11 月 24 日

[3] 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

[4] プライバシー保護と犯罪防止を両立する監視カメラシステム
小林健人, 岩村恵市, 越前功
信学技報, vol. 113, no. 480,
EMM2013-103, pp. 21-26, 2014 年 3 月

[5] BIGLOBE ニュース 2012 年 8 月 16 日
http://news.biglobe.ne.jp/entertainment/0816/jc_120

[6] Short Group Signatures
Dan Boneh, Xavier Boyen, Hovav Shacham
CRYPTO2004, volume 3152 of Lecture Notes in Computer Science, pp.41–55

[7] 可逆透かしを用いた JPEG 画像へのモザイク手法
山崎淳也, 柿崎淑郎, 岩村恵市, 越前功
信学技報, vol. 112, no. 293, EMM2012-81, pp. 105-110, November 2012

[8] Reversible Data Hiding for JPEG Images Based on Histogram Pairs
Guorong Xuan, Yun Q. Shi, Zhicheng Ni, Peiqi Chai1, Xia Cui, and Xuefeng Tong
ICIAR 2007, LNCS 4633, pp. 715–727, 2007