Surveillance Camera System Balancing Privacy Protection and Effective Surveillance Image Use

Kent Kobayashi[1], Masaki Inamura[2], Kitahiro Kaneda[3], Keiichi Iwamura[1] and Isao Echizen[4]
[1]*Tokyo University of Science, Niijuku, Tokyo, Japan*
[2]*Tokyo Denki University, Ishizaka, Hiki-gun, Hatoyama-machi, Saitama, Japan*
[3]*Osaka Prefecture University, Sakai-shi, Osaka, Japan*
[4]*National Institute of Informatics, Chiyoda, Hitotsubashi, Tokyo, Japan*

Keywords: Privacy, Surveillance Camera, Reversible Mosaic.

Abstract: Privacy protection has been attracting considerable attention in recent years. Several instances of surveillance video recordings of famous people in public stores being uploaded to the Internet have been reported. Such instances of privacy infringement have become increasingly concerning. A simple solution to this problem is to obscure the facial features of individuals being recorded in surveillance camera systems. However, in some cases where surveillance camera recordings are required, such as criminal investigations, the solution fails. Therefore, we propose a new surveillance camera system that balances the requirements of privacy protection and those of cases in which unobscured images are required. Further, we present the protocol of the proposed system and evaluate the security of the system against attacks.

1 INTRODUCTION

In recent years, with the increasing popularity of social networking sites (SNSs), opportunities for sharing various types of media over the Internet, such as videos and images, have increased. However, this has led to a greater need for securing and protecting the privacy and personal information of individuals. Privacy refers to "private aaffairs, private life, and personal secrets" and "the right to not infringe them." In addition, privacy includes "the right to control one's information." Further, personal information refers to "personally identifiable information," such as name, address, date of birth, and bio-information.

Surveillance cameras have been increasingly installed in public spaces worldwide for various purposes, such as traffic monitoring, security, post-incident analysis, and so on. However, laws governing the collection and use of private information, such as facial images captured through surveillance camera systems, have not been established in many countries including Japan. Moreover, in most cases, people being monitored by surveillance camera systems have not been granted adequate rights over the use and distribution of their recorded facial images and information. For example, several incidents wherein surveillance camera recordings of a famous person visiting convenience stores or video rental shops being uploaded to SNSs by store employees have been reported.

From the perspective of privacy protection, the person being photographed or video recorded must be granted the right to control and manage the image or video. However, surveillance camera images are often used in criminal investigations. To this end, if individuals are granted the right to control their recorded information, criminal investigations might be obstructed.

Therefore, in this paper, we propose a surveillance camera system that balances the requirements of both privacy protection and criminal investigations. This feature is achieved by combining "a group signature technique" and "a reversible mosaic technique that employ reversible watermarks" in the proposed system. Moreover, we evaluate the security of our system against attacks.

The remainder of this paper is organized as follows. In Section 2, we explain privacy infringement issues associated with surveillance camera systems. In Section 3, we discuss related studies, namely, "Short Group Signatures" (Boneh, 2004), a group signature technique, and "Recoverable original video for mosaic system," (Kusama, 2015) a reversible mosaic technique using reversible watermarks. In Section 4, we explain our proposed

Kobayashi K., Inamura M., Kaneda K., Iwamura K. and Echizen I..
Surveillance Camera System Balancing Privacy Protection and Effective Surveillance Image Use.
DOI: 10.5220/0005511100410048
In *Proceedings of the 12th International Conference on e-Business* (ICE-B-2015), pages 41-48
ISBN: 978-989-758-113-7

system, and in Section 5, we discuss some attacks against the proposed system and security against those attacks. We conclude the paper in Section 6.

2 PRIVACY INFRINGEMENT ISSUES ASSOCIATED WITH SURVEILLANCE CAMERA

Privacy has been interpreted as the "right to not publish personal information without good reason." However, in general, privacy also includes "the right of a person to control his/her information" (Westin, 1967)

However, it is difficult to say that conventional surveillance camera systems provide privacy to individuals who are photographed by a system. In fact, there are cases in which a person is identified through the output of surveillance camera videos, and therefore, privacy is not ensured. Furthermore, such leaks can be prevented if individuals are granted the right to control their recorded videos and images. Writefix posted a privacy concern on a surveillance camera. The essay suggests the importance of balancing the need for respecting validity and personal privacy in surveillance camera security. Therefore, it is important to provide privacy on surveillance camera systems. To protect the right of privacy on a surveillance camera system, individuals need to have the right to control their personal information (face information).

Considering the threat to privacy from current surveillance systems, it is important to develop a surveillance system that ensures the privacy of individuals. To ensure privacy protection, individuals being recorded must have the right to control their recorded facial images. On the other hand, surveillance system recordings are important in criminal investigations. Therefore, it is not desirable for a perpetrator in a crime to have the right to control his or her recorded facial information.

Consequently, a surveillance system that achieves both "privacy protection" and "effective use of surveillance image" is required. Leaks of surveillance camera images bring to light the dire need for privacy protection in the current information society.

3 RELATED STUDIES

In this section, we introduce the key technologies used in the proposed system. In Section 3.1, we explain "Short Group Signatures" (Boneh, 2004), and in Section 3.2, "Recoverable original video for mosaic system" (Kusama, 2015) is explained.

3.1 Short Group Signatures

Short Group Signatures (Boneh, 2004), a group signature technique, has the following three features.

1. Only group members can produce signatures.
2. A verifier can verify a signature, but cannot identify the signer.
3. Only the Certification Authority can identify a signer.

Short Group Signatures is the technique used in the proposed system to confirm the identity of a recorded person.

3.1.1 Bilinear Group

A bilinear group has the following features.

1. G_1 and G_2 are two cyclic groups of prime order p.
2. g_1 and g_2 are generators of G_1 and G_2, respectively
3. ψ is a computable isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$.
4. e is a computable map, and $e : G_1 \times G_2 \rightarrow G_T$ with the following properties.
   - Bilinearity: for all $u \in G_1$, $v \in G_1$ and $(a, b) \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$
   - Nondegeneracy: $e(u^a, v^b) = e(u, v)^{ab}$

3.1.2 Algorithm

KeyGen(n).
The algorithm for Short Group Signatures takes a parameter n, the size of the group, as input and proceeds as follows. Select a generator g_2 in G_2 uniformly at random, and let $g_1 = \psi(g_2)$. Select $h \overset{R}{\leftarrow} G_1 \setminus \{1_{G_1}\}$ and $\xi_1, \xi_2 \overset{R}{\leftarrow} Z_p$, and let $u, v \in G_1$ such that $u^{\xi_1} = v^{\xi_2} = h$. Select $\gamma \overset{R}{\leftarrow} Z_p$, and let $w = g_2^{\gamma}$.

Using γ, generate for each user i, $1 \ll i \ll n$, a strong Diffie–Hellman (SDH) tuple (A_i, x_i): select $x_i \overset{R}{\leftarrow} Z_p$, and let $A_i^{\gamma + x_i} = g_1$.

The group public key is $gpk = (g_1, g_2, u, v, h, w)$. The private key of the group manager key is $gmk = (\xi_1, \xi_2)$, and a group member i's key is $gsk[i] = (A_i, x_i)$. No party is allowed to possess γ; it is known only to the private-key issuer.

Sign(gpk, gsk[i], M).
Given a group public key as $gpk = (g_1, g_2, u, v, h, w)$, a member's key as gsk[i] =

(A_i, x_i), and a message M, compute the signature as follows.

1. Compute the values $T_1, T_2, T_3, \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3, \mathrm{R}_4, \mathrm{R}_5$.

$$\delta_1 = x_i\alpha, \delta_2 = x_i\beta$$
$$T_1 = \mathrm{u}^{\alpha}, T_2 = \mathrm{u}^{\beta}, T_3 = A_i\mathrm{h}^{\alpha+\beta}$$
$$\mathrm{R}_1 = u^{\mathrm{r}_\alpha}, \mathrm{R}_2 = v^{\mathrm{r}_\beta}, \mathrm{R}_4 = {T_1}^{\mathrm{r}_{x_i}} u^{-\mathrm{r}_{\delta_1}},$$
$$\mathrm{R}_5 = {T_2}^{\mathrm{r}_{x_i}} v^{-\mathrm{r}_{\delta_2}}$$
$$\mathrm{R}_3 = e(T_3, g_2)^{r_{x_i}} \cdot e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-\mathrm{r}_{\delta_1} - \mathrm{r}_{\delta_2}}$$
$$\left(\alpha, \beta \overset{R}{\leftarrow} Z_p, \mathrm{r}_\alpha, \mathrm{r}_\beta, \mathrm{r}_{x_i}, \mathrm{r}_{\delta_1}, \mathrm{r}_{\delta_2} \in Z_p\right)$$

2. Compute a challenge c using the hash function as

$$\mathrm{c} = \mathrm{H}(M, T_1, T_2, T_3, \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3, \mathrm{R}_4, \mathrm{R}_5) \in Z_p$$

3. Using c, construct the values:

$$s_\alpha = \mathrm{r}_\alpha + c\alpha, s_\beta = \mathrm{r}_\beta + c\beta$$
$$s_{x_i} = \mathrm{r}_{x_i} + cx_i$$
$$s_{\delta_1} = \mathrm{r}_{\delta_1} + c\delta_1, s_{\delta_2} = \mathrm{r}_{\delta_2} + c\delta_2$$
$$s_\alpha = \mathrm{r}_\alpha + c\alpha, s_\beta = \mathrm{r}_\beta + c\beta$$
$$s_{x_i} = \mathrm{r}_{x_i} + cx_i$$
$$s_{\delta_1} = \mathrm{r}_{\delta_1} + c\delta_1, s_{\delta_2} = \mathrm{r}_{\delta_2} + c\delta_2$$

4. Output the signature σ, computed as

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

Verify(gpk, M, σ).

Given a message M, a group signature σ, and group public key gpk = (g_1, g_2, u, v, h, w), , verify that σ is a valid signature as follows:

1. Re-drive $\mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3, \mathrm{R}_4$, and R_5 as follow:

2. $\overline{\mathrm{R}_1} = u^{s_\alpha} {T_1}^{-c}, \overline{\mathrm{R}_2} = u^{s_\beta} {T_2}^{-c}$
$$\overline{\mathrm{R}_3} = e(T_3, g_2)^{s_{x_i}} \cdot e(h, w)^{-s_\alpha - s_\beta} \cdot e(h, g_2)^{-\mathrm{s}_{\delta_1} - \mathrm{s}_{\delta_2}} \cdot \left(e(T_3, w) e(g_1, g_2)\right)$$
$$\overline{\mathrm{R}_4} = {T_1}^{s_{x_i}} u^{-\mathrm{s}_{\delta_1}}, \overline{\mathrm{R}_5} = {T_2}^{s_{x_i}} v^{-\mathrm{s}_{\delta_2}}$$

3. Check as follow:

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

Accept if this check succeeds, else reject.

Open(gpk, gmsk, M, σ).

This algorithm is used for tracing a signer. Group public key gpk = (g_1, g_2, u, v, h, w) and group manager's key gmk = (ξ_1, ξ_2) are used together with a message M and a signature $\sigma = \left(T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2}\right)$ to trace.

First, verify the signature. Second, recover the member's key A_i as $\frac{T_3}{{T_1}^{\xi_1} \cdot {T_2}^{\xi_2}} = \frac{A_i \mathrm{h}^{\alpha+\beta}}{u^{\alpha\xi_1} \cdot v^{\beta\xi_2}} = A_i$

The group manager can then identify the signer from a group member index.

3.2 Recoverable Original Video for Mosaic System

We employ "Recoverable original video for mosaic system" (Kusama, 2015) as the method for controlling an individual's facial information. This method provides the reversible mosaic on a video of MPEG2. In that paper, implementation evaluation is carried out on MPEG2 videos. We briefly explain the reversible mosaic generation method of "Recoverable original video for mosaic system" in this section.

3.2.1 Method for Generating the Mosaic

To obtain the JPEG image, the original image is divided into blocks that are converted into discrete cosine transformations after quantization. The n × n blocks around the DC component are set to zero (as shown in Figure 1), resulting in distortion, and the distortion acts as a mosaic. In addition, keep the value of the quantization output before the change, and remove the mosaic by replacing locations that are zero.

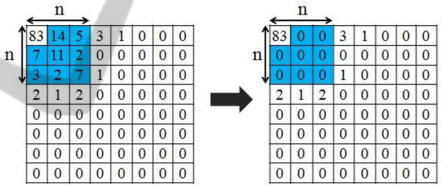

Figure 1: Mosaic method (n = 3).

3.2.2 Method for Generating Reversible Mosaic

As shown in Figure 2, the face section of the data to be hidden is extracted first. The extracted face data are divided into 8 × 8 pixel blocks. Discrete cosine transformations and quantization are performed on the blocks, as in the case of JPEG. In the blocks, all the values of low-frequency n × n pixels, except for

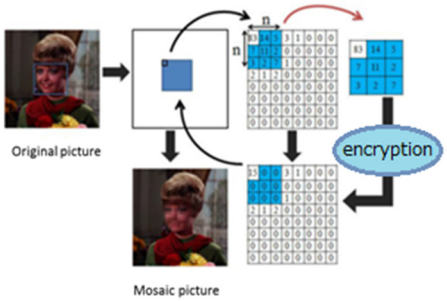

Figure 2: Generating a reversible mosaic.

the DC element of the quantization output, are replaced with zeroes after the original values are stored. Further, the encrypted original values are encrypted in the DCT domain of the mosaic image using the reversible watermark (Xuan, 2007). Finally, a compressed JPEG stream can be obtained after encoding is performed.

3.2.3 Method for Removing a Reversible Mosaic

Figure 3 shows decoding process. Through this process, we obtain the value of the quantization output, which includes the watermarked information. The watermarked information is extracted by decoding the reversible watermark; then, we decrypt the face data of each block. Finally, we obtain the original image after reversing the data of the low-frequency n × n matrix expect for the DC element.

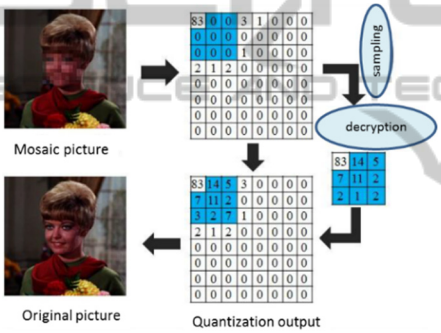

Figure 3: Removing the reversible mosaic.

4 PROPOSED SYSTEM

4.1 Outline of the Proposed System

The objectives of the proposed system for balancing the requirements of both privacy protection and crime investigation are as follows.

1. A person who wants to conceal his or her recorded face information can do so.
2. The identity of a person who wants to conceal his or her own face information mustn't be divulged, unless that person performs a criminal act.
3. In a crime investigation, the police department must be given access to unobscured face information, if required

Objective 1 considers the people's right to control their own recorded face information. People who care about their privacy can conceal their face information, whereas the face information of those who are not concerned about privacy is not concealed. A surveillant can identify a shoplifting culprit in real time, if the culprit is in the latter category. However, if the culprit is in the former, we can identify him or her through Objective 2, i.e., the system must have a mechanism to identify a person whose information is concealed, if the need arises, such as in the case of a criminal act. Further, the police department must receive unobscured face information related to a criminal investigation, so that the investigation can be conducted in a conventional manner; this is considered in Objective 3. Each element of the proposed system is shown in Figure 4.

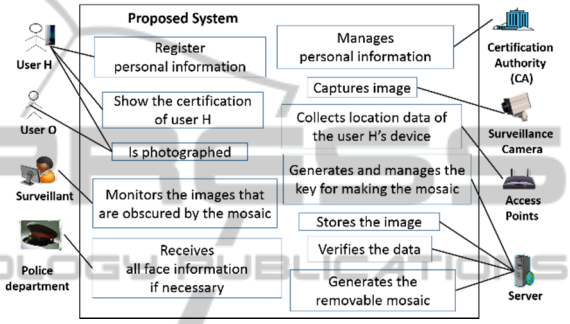

Figure 4: Elements of the proposed system.

In the following, we explain each element in Figure 4. User H is a person who has an interest in securing privacy and wants to conceal his/her face information. In contrast, user O is a person who is not concerned about privacy. The surveillant is a person who monitors the recordings of the surveillance cameras on the monitors in real time. The police department is the element that requires unobscured images for crime investigations. The Certification Authority (CA) manages the personal information of user H securely and generates secret keys for each user H. These secret keys preserve the anonymity of user H using Short Group Signatures. The surveillance camera sends the image to the server. The access points transfer data between user H and the server. The signature of user H is generated in the device such as smart phone owned by user H. Moreover, the access points collect the location data of the device and send them to the server. The server verifies the signature from the access points to confirm that the person is a legitimate user H. Furthermore, the server generates a removable mosaic on the face of user H, to obscure that person's identity. The server manages the data used for generating the mosaic. Finally, the server sends a modified image (one with the mosaic) to the surveillant.

4.2 Proposed System Configuration

In Figure 5, we present the system model of the proposed system and explain each element in the model.

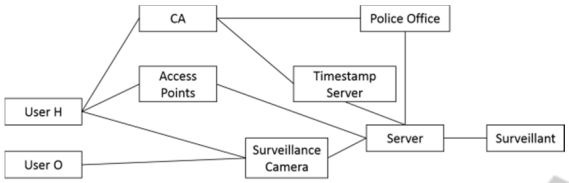

Figure 5: System model.

4.2.1 Photographed People

We classify the photographed people into two types (user H and user O). Each user has the following features.

– User H

1. Wants to hide face information.
2. Has a mobile device to establish legitimacy and communicate with access points.
3. Has registered personal information with the CA and has obtained a key for producing short group signatures.

– User O

1. Low interest in concealing face information.
2. Does not have a key for producing short group signatures.

4.2.2 Surveillant

The surveillant has the following features.

1. Monitors the images sent from the surveillance camera via the server.
2. Can operate only on the monitoring server and cannot modify the functions of the server.

4.2.3 Surveillance Camera

Here, we assume network cameras to be the surveillance cameras, as some network cameras can output encrypted images. A surveillance camera has the following features.

1. Encrypts and sends images to the server.
2. Is tamper-resistant against function changes.

4.2.4 Access Points

Two or more access points are installed and have the following features.

1. They are located at the site where the surveillance cameras are installed.
2. They communicate with user H's mobile device and the server.
3. They collect information for specifying user H's device position and send it to the server.
4. They are tamper-resistant against function changes.

4.2.5 Server

The server has the following features.

1. It is managed by a trusted administrator.
2. It communicates with user H's device via access points.
3. It verifies whether the person is user H without identifying the person.
4. It obtains the information for specifying user H's device position using the TDOA (Time Difference of Arrival) method.
5. It estimates the location of user H's face in the image.
6. It generates a reversible mosaic for the user's face.

Feature 3 listed above is achieved through short group signatures.

Reversible mosaic refers to the concept introduced in "Recoverable original video for mosaic system".

The TDOA method in feature 4 estimates the position of the mobile devices (Cong, 2004).

Face estimation is achieved through facial recognition technology for the person with the devices.

4.2.6 Certification Authority (CA)

The CA has the following features.

The CA has the following features.

1. It manages the personal information of user H securely.
2. It generates the sign key (for generating short group signatures) and provides the key to each user H.
3. It generates the verify key (for verifying the short group signatures), and publicizes it.
4. It provides the information of user H and removing mosaic to the police department that has a warrant

from the court with regard to a criminal investigation.

4.2.7 Timestamp Server

We use the inbuilt timestamp server. The timestamp server sends timestamp data to the server and the CA.

4.2.8 Police Department

The Police department demands the recording of a surveillance camera by producing a warrant with regard to a criminal investigation; the police department receives the mosaicked surveillance camera recording and information for removing the mosaic from the CA.

4.3 Communication Protocol

In this section, we present the protocol of the proposed system

4.3.1 Preconfigured

We present the protocol for short group signatures between the people who wish to be user H and the CA. This protocol is executed before entering the visibility range of the surveillance cameras.

Step 1: The people who want to be user H register their personal information with the CA.
Step 2: The CA confirms the personal information and provides sign key (gsk) and ID to user H.
Step 3: The CA publishes the verify key (gpk) and manages the secret key (gmk) for short group signatures.

4.3.2 Reversible Mosaic Generation

The reversible mosaic image generation protocol is executed when user H enters the visibility range of the surveillance camera. This system does not conduct mosaic generation for User O.

Step 1: The server sends the server ID (IDserver) periodically via the access points.
Step 2: User H Receives IDserver on his mobile device, and generates random number β.
Step 3: User H's mobile device calculates the following value k with IDserver, β, and user H's ID (ID).

$$\mathrm{k} = \mathrm{H}(ID \parallel IDserver \parallel \beta)$$

Step 4: User H's mobile device produces a short group signature (σ) for the value k by gsk and sends σ, k, and β to the server via the access points. The short group signature is calculated as follows.

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

Step 5: After receiving each datum, the server verifies the signature σ. If the signature is the same as the previous signature, the server does not verify the signature.
Step 6: If the signature is valid, the server generates a reversible mosaic on the face of user H with a mosaic key (mk) using the technique shown in 3.2. The mosaic key consists of timestamp Ts and σ and encrypted by the server secret key sk as follows.

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

Step 7: The server sends the mosaicked image to the surveillant. The server stores σ, k, and the mosaicked image, and deletes mk after generating the reversible mosaic.

4.3.3 Removing Mosaic Generation

This protocol stated below is used for removing a reversible mosaic in the case of a crime investigation.

Step 1: The police department obtains a search warrant from a court to view surveillance camera recordings. The search warrant is presented to the CA.
Step 2: The CA requests the server to send the mosaic image of the investigation subject, σ and k.
Step 3: The CA sends the timestamp Ts to the server. (Timestamp Ts corresponds to the recording time.)
Step 4: The server restores the mosaic key mk from the Ts and sends mk and the mosaicked image to the police department.
Step 5: The police department requests the CA to provide identification information regarding user H, if necessary.
Step 6: Using the secret key gmk, the CA identifies the user H from σ and sends the personal information of the identified user H to the police department if requested.

5 CONSIDERATION

5.1 Achieving the Objective

The following are the objectives of the proposed system.

1. A person who wants to conceal his or her recorded face information can do so.
2. The identity of a person who wants to conceal the person's own face information mustn't be divulged, unless that person performs a criminal act.
3. In a crime investigation, the police department must be given access to unobscured face information, if required.

– Objective 1: A person who wants to conceal his or her recorded face information registers his/her personal information with the CA. The person can become user H after registering. The face information of user H is concealed by the reversible mosaic according to the "reversible mosaic generation protocol." User H communicates with the server via the access points and sends the information for reversible mosaic generation in Steps 1-3 of the reversible mosaic generation protocol. The face information of the user H is concealed with Step 6 of the protocol. Accordingly, we achieve Objective 1.

– Objective 2: The data that user H sends are only signature σ, calculated value k, and random number β. The server cannot identify the user H from these data. Objective 2 is achieved, because it is not possible to identify user H unless the CA uses the gmk and identifies the user H from that user's signature σ.

– Objective 3: With Steps 1-4 of "remove the reversible mosaic protocol," the police department can restore the face information from the mosaicked surveillance camera image. Objective 3 is achieved with the "remove the reversible mosaic protocol."

5.2 Attacks against Proposed System

We consider some attacks against the proposed system in this section. We assume that the attacker has the following agenda.

1. Impersonate user H.
2. Disrupt communication between the surveillance camera, the access point, and the server.
3. Tamper with or intercept the image stored on the server.

– Concrete attacks based on Purpose 1

Attack 1: The attacker intercepts the data that are sent by user H and resends them to the server.

Attack 2: The attacker uses the device of user H illegally.

– Concrete attacks based on Purpose 2

Attack 3: The attacker blocks the communication between the surveillance camera, the access points, and the server.

Attack 4: The attacker falsifies the data that are sent by user H, the access point, and the surveillance camera.

– Concrete attack based on Purpose 3

Attack 5: The attacker tampers with or intercepts the images stored on the server.

We consider the security for the aforementioned five attacks in Section 5.3.

5.3 Security for Proposed System

Attack 1: This attack can be prevented by step 5 of the "generation reversible mosaic" protocol (i.e., the server verifies the same signature only once). The signature for verifying user H consists of a calculated number. This number consists of a random number and two IDs (the server and user H). The attacker can create a valid signature on another random number, if he or she knows the sign key. It is possible to prevent this attack by securely managing the sign key of user H.

Attack 2: There are several ways to bypass security on a user's device. These are not considered. The argument that the attacker cannot use the device unless it is unlocked does not have enough strength. Please consider elaborating the suggestion. The CA can identify the signer through step 6 of the "remove the reverible mosaic" protocol in a crime investigation. The user has registered personal information including face information with the CA. The police department can confirm the face in the recording for a crime investigation after removing the reversible mosaic. However, the user might be suspected, if identification is performed based on the signature; therefore, it is necessary to confirm via a facial inspection in a crime investigation.

Attack 3: Falsification of the surveillance camera and the access points is prevented by the tamper-resistant feature. The falsification of the server can be prevented, if a legitimate administrator manages the server. However, if the attacker routes the communication link, this solution will still allow you to send and receive the "hello message. The surveillant can detect blocking of the

communication between the surveillance camera and the server, because the image would not appear on the monitor, if the communication were blocked. The administrator can deal with this attack by setting in place a mechanism for reporting unsuccessful communication.

Attack 4: Falsification of the data sent to the server by the surveillance camera can be prevented using the encryption function of the surveillance camera. To detect falsification of the data sent by the access points, the server produces a signature of the data of the server. Therefore, user H can detect the falsification easily. On the other hand, detection of falsified data sent by user H is easy. The server can verify it by verifying the data. The surveillant must deal with user H, if the server fails several times to verify the signature of the same device.

Attack 5: Detection of falsification of the image stored in the server can be achieved by producing a signature on the image data where the server stores the image. The key for this signature must be securely managed by the administrator. This signature must be decided at a predetermined time interval (for example, each day). An alternate method is that the administrator encrypts the image using his secret key. In this manner, falsification can be prevented.

6 CONCLUSIONS

In this paper, we proposed a new surveillance camera system that balances the requirements of both privacy protection and criminal investigations. Further, we presented the communication protocol of the proposed system. We also assumed possible attacks to the system and presented security measures these attacks.

REFERENCES

Warren, S., Brandeis, L., 1890. *The Righ to Privacy*. Harvard Law Review. Vol.4, pp.193.

Westin, A., 1967. *Privacy and Freedom.* Washington and Lee Law Review, vol.25, pp.197-170.

Murakami, Y., 2004. *Privacy Issues in the Ubiquitous Information Society and Law in Japan*. Systems, Man and Cybernetics, 2004 IEEE International Conference on, vol.6, pp.5645-5650.

Xiaoyi, Y., Chinomi, K., Koshimizu, T., Nitta, N., Ito, Y., Babaguchi, N., 2008. *Privacy protecting visual processing for secure video surveillance.* 15th IEEE International Conference on, pp.1672-1675.

Chaum, D., Heyast, E., 1991. *Group Signatures* Proceedings of Eurocrypt 1991, vol.547, pp.257-265.

Boneh, D, Boyen, X, Shacham, H., 2004. *Short Group Signatures*. Advances in Cryptology -CRYPTO 2004-, pp.41-55.

Kusama, Y., Kang, H., Iwamura, K., 2015. *Recoverable original video for mosaic system.(japanese).*

Xuan, G., Shi, G., Ni, Z., Chai, , Z., Cui, X., Tong, X., 2007. *Reversible Data Hiding for JPEG Images Based on Histogram Pairs.* Image Analysis and Recognition, pp.715-727.

Cong, L., Z., Zhuang, W., 2001. *Non-line-of-sight error mitigation in TDOA mobile location.* GLOBECOM'01. IEEE, vol.1, pp.680-684.

Gezici, Z., 2008. *A Survey on Wireless Position Estimation*. Wireless Personal Communications, vol.44, pp.263-282.

Comaniciu, D., Ramesh, V., 2000. *Real-time tracking of non-rigid objects using mean shift*. Computer Vision and Pattern Recognition, 2000. Proceedings. IEEE Conference on, vol.2, pp.142-149.

Ross, D., Lim, J., Lin, R., Yang, M., 2008. *Incremental Learning for Robust Visual Tracking.* International Journal of Computer Vision, vol.77, pp.125-141.

Viola, P., Jones, M., 2004. *Robust Real-Time Face Detection*. International Journal of Computer Vision, vol.57, pp137-154.

Wright, J., Yang, Y., Ganesh, A., Sastry, S., Yi M., 2008. *Robust Face Recognition via Sparse Representation*. Pattern Analysis and Machine Intelligence, IEEE Transaction on, vol.31, pp.210-227.

Andrew, S., 2009. *Privacy Protection in Video Surveillance System.* Protecting Privacy in Video Surveillance, pp.35-47.

Writefix. *Security Cameras and Privacy*. http://writefix.com/?page_id=1584.