Irreversible Privacy-Preserving Images Holding Spatial Information for HOG Feature Extraction

1st Masaki Kitayama
Tokyo Metropolitan University
Tokyo, Japan
kitayama-masaki@ed.tmu.ac.jp

2nd Hitoshi Kiya
Tokyo Metropolitan University
Tokyo, Japan
kiya@tmu.ac.jp

***Abstract*—In this paper, we propose a generation method of visually protected images and its application to privacy-preserving machine learning. Images generated by the proposed method hold the gradient direction information of the original images, but have no the information. Histogram-of-Oriented-Gradients (HOG) features are extracted from the protected images, and the features are applied to machine learning algorithms. In addition, the proposed generation method is an irreversible one, so there is no need to manage secret keys, unlike encryption methods. In an experiment, a face classification task is carried out under the use of a support vector machine algorithm with the HOG features to demonstrate the effectiveness of the proposed method.**

I. Introduction

In recent years, cloud computing has been rapidly spreading in many fields. However, cloud environments are generally semi-trusted, so there are some security concerns such as unauthorized use of data and privacy compromise. To solve the security concerns, machine learning with encrypted data has been researched [1]–[3].

In this paper, we propose a generation method of visually protected images (referred to as "protected images") which hold the spatial information of images. Moreover, we propose an extraction method of Histogram-of-Oriented-Gradients (HOG) [4] features from the protected images for machine learning. The generation of protected images is performed by generating random pixels under certain restrictions, and is irreversible. Therefore, the proposed method has no need to manage secret keys. Furthermore, since the protected images retains the spatial information of the original image, it can be applied to not only simple image recognition but also object detection. In an experiment, image recognition with a support vector machine algorithm is carried out to confirm the effectiveness of the proposed method.

II. Proposed Method

A. Overview of Proposed Method

Figure 1 shows a privacy-preserving image recognition system considered in this paper. In both training and testing phases, each user generates protected images in the user's local before sending the images to a cloud server. Then the cloud server carries out an image recognition algorithm with HOG features extracted from the protected images.

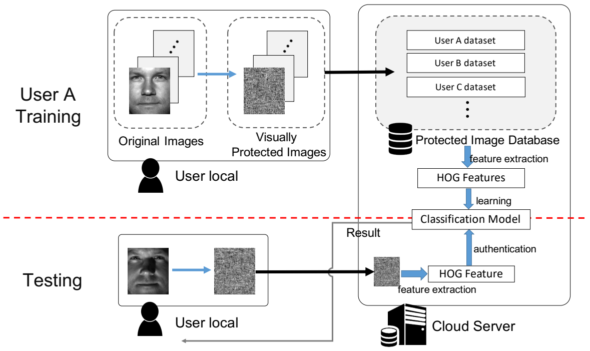


Fig. 1. Privacy-preserving image recognition system.

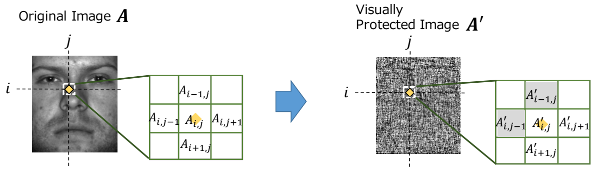


Fig. 2. Relation between $\boldsymbol{A}$ and $\boldsymbol{A}'_{j_s}$. Two pixels $A'_{i-1,j}$ and $A'_{i,j-1}$ were calculated prior to $A'_{i,j+1}$ and $A'_{i+1,j}$.

B. Generation of Protected Image

1) Restriction of The Protected Image: Now, let $\boldsymbol{A} \in \mathbb{R}^{I\times J}$ and $\boldsymbol{A}'_{j_s} \in \mathbb{R}^{I\times J}$ be an original image and the protected image, and let $A_{i,j}$ and $A'_{i,j}$ be pixel values at a position (i,j) of $\boldsymbol{A}$ and $\boldsymbol{A}'_{j_s}$, $i,j \in \mathbb{Z}$ respectively.

In Fig.2, we focus on a position (i,j) to explain the restriction between two images, $\boldsymbol{A}$ and $\boldsymbol{A}'_{j_s}$. At the position (i,j), the gradient direction $\theta_{i,j}$ is defined for $\boldsymbol{A}$ as

$$\theta_{i,j} = \tan^{-1}(y_{i,j}/x_{i,j}) \quad , \tag{1}$$

where $x_{i,j} = A_{i,j+1} - A_{i,j-1}$ and $y_{i,j} = A_{i+1,j} - A_{i-1,j}$.

Similarly as $\theta_{i,j}$, the gradient direction $\theta'_{i,j}$ is defined for image $\boldsymbol{A}'_{j_s}$ as

$$\theta'_{i,j} = \tan^{-1}(y'_{i,j}/x'_{i,j}) \quad , \tag{2}$$

where $x'_{i,j} = A'_{i,j+1} - A'_{i,j-1}$ and $y'_{i,j} = A'_{i+1,j} - A'_{i-1,j}$. If the relation

$$\theta'_{i,j} = \theta_{i,j} \quad , \tag{3}$$

is satisfied, $\boldsymbol{A}'_{j_s}$ has the same gradient direction as $\boldsymbol{A}$ at the position (i,j). In this paper, $\boldsymbol{A}'_{j_s}$ is designed under

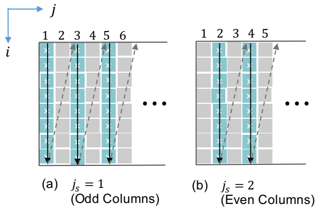


Fig. 3. Attention order of a position (i, j) in $\boldsymbol{A}'_{j_s}$

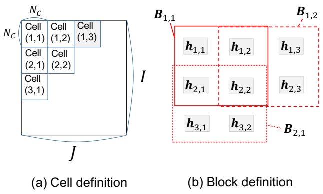


Fig. 4. Cell and block definition

Eq.(3).

2) Generation of $\boldsymbol{A}'_{j_s}$: In Fig.3, a position (i, j) with $\theta'_{i,j}$ in $\boldsymbol{A}'_{j_s}$ is illustrated. There are attention positions every two columns, where the initial value of the attention positions is decided by the parameter $j_s \in \{1, 2\}$, and the attention position moves in the order of the arrow. At a position (i, j), four pixel values: $A'_{i-1,j}, A'_{i,j-1}, A'_{i,j+1}$, and $A'_{i+1,j}$ have to be decided under the condition of Eq.(3), where two pixels $A'_{i,j+1}$ and $A'_{i+1,j}$ are the pixels randomly generated under the condition of Eq.(3). The remaining two pixels $A'_{i-1,j}$ and $A'_{i,j-1}$ were generated in the previous processing.

C. HOG Feature Extraction

Next, we propose a method of extracting HOG features from a protected image $\boldsymbol{A}'_{j_s}$ as follows.

step-1 **gradient direction map** : The gradient direction map $\boldsymbol{\theta'} \in \mathbb{R}^{I \times J}$ is calculated in accordance with Eq.(2).

step-2 **histogram voting map** : The histogram voting map $\boldsymbol{M'} \in \mathbb{R}^{I \times J}$ is generated by using j_s as

$$M'_{i,j} = \begin{cases} 0 & (j \in \{js + 2m \mid m \in \mathbb{Z}\}) \\ 1 & (\text{the others}) \end{cases} , \tag{4}$$

where $M'_{i,j}$ is a pixel value of $\boldsymbol{M'}$ at a position (i, j).

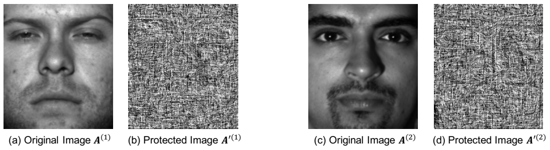
step-3 **histograms of gradient direction** : As shown in Fig.4 (a), maps $\boldsymbol{\theta'}$ and $\boldsymbol{M'}$ are commonly divided into small grids called "cells" with $N_C \times N_C$ pixels, and then, $\theta'_{i,j}$ is quantized and its histogram, $\boldsymbol{h}_{p,l}$ is made up per each cell, where (p, l) is a index of the histogram. The quantization level of $\theta'_{i,j}$ is b, and the votes are weighted by $M'_{i,j}$. In this paper, $N_C = 8$ and $b = 9$ are chosen as parameters.

step-4 **block normalization** : Let us define "blocks" as the concatenation of 2×2 cell histograms, allowing overlapping of the middle cells (see Fig.4 (b)). Each block is normalized by the L2 norm, and the HOG feature of $\boldsymbol{A}'_{j_s}$ is the vector produced by concatenating all blocks.

The difference between the proposed HOG feature extraction and the conventional one [4] is that the proposed one uses the histogram voting map $\boldsymbol{M'}$ instead of the gradient strength map $\boldsymbol{G}$ as the weight for voting $\boldsymbol{h}_{p,l}$ in *step-3*.

III. Experiment

A face recognition experiment was carried out using the Extended Yale Face Database B with a support vector machine (SVM) algorithm. This dataset contains 38 individuals and 64 frontal facial images with 168 × 192 pixels per each person. The images for each person were divided into 16 for training and 48 for testing. Fig.5 shows two samples from the dataset and the protected images.



(a) Original Image $\boldsymbol{A}^{(1)}$
(b) Protected Image $\boldsymbol{A}'^{(1)}$
(c) Original Image $\boldsymbol{A}^{(2)}$
(d) Protected Image $\boldsymbol{A}'^{(2)}$

Fig. 5. Original images and their protected images.

TABLE I
Face recognition performances with SVM

feature set	EER
Set-1: conventional with non-protected HOG	0.0033
Set-2: proposed with protected HOG	0.0049
Set-3: conventional with non-protected Eigen Face	0.0742

TABLE I shows the experimental result. To evaluate the effectiveness, equal error rate (EER), which is the point at which false reject rate (FRR) is equal to false accept rate (FAR), was used. EER is acquired by changing the threshold of classiication score. *Set-1* is a set of HOG features extracted with the conventional method [4], and *Set-2* is a set extracted with the proposed one. *Set-3* is "Eigen Face" [5] features (150 dimension) which is an representative one for face recognition.

TABLE I indicates that the proposed method (*Set-2*) has a good performance than *Set-3*. The difference of EER values between *Set-1* and *Set-2* is caused due to no information on gradient strength.

IV. Conclusion

We proposed a generation method of visually protected images, which allows us to extract HOG features from the protected ones without any keys, while maintaining a reasonable performance.

References

[1] Mauro Barni, Giulia Droandi, and Riccardo Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 66–76, 2015.

[2] Takahiro Maekawa, Ayana Kawamura, Takayuki Nakachi, and Hitoshi Kiya, "Privacy-preserving support vector machine computing using random unitary transformation," *arXiv preprint arXiv:1908.07915*, 2019.

[3] W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, and H. Kiya, "Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain," in *2019 IEEE International Conference on Image Processing (ICIP)*, Sep. 2019, pp. 674–678.

[4] Navneet Dalal and Bill Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE International conference on Computer Vision and Pattern Recognition*, 2005, pp. 886–893.

[5] Jun Zhang, Yong Yan, and Martin Lades, "Face recognition: eigenface, elastic matching, and neural nets," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1423–1435, 1997.