# A Secure Face Recognition Method Based on Kernel Sparse Representation

Masakazu FURUKAWA, Yuichi MURAKI, Masaaki FUJIYOSHI, and Hitoshi KIYA
*Dept. of Information and Communication Systems, Tokyo Metropolitan University*
*Hino-shi, Tokyo 191–0065, Japan*

## Abstract

*This paper proposes a secure method for face recognition (FR) based on kernel sparse representation (KSR) in which facial images are visually protected. The proposed method does add a noisy image to all facial images before FR so that a leakage of facial images will not disclose user's privacy. This method recognizes faces based on KSR, whereas the conventional method is based on sparse representation. Experimental results show that the FR performance of KSR is not degraded, even facial images are visually protected.*

## 1. Introduction

Face recognition (FR) is useful for various applications such as personal authentication systems and computer vision. Many researchers have studied various FR method, for example, methods using eigenfaces, graph matching, local binary patterns, and so on. Lately, a robust FR based on sparse representation (SR) [1] has attracted a lot of attention. Furthermore, a kernel method has been introduced to this recognition method to improve the recognition performance [2]. However, these methods have a problem that the facial images are not protected, i.e., privacy will be disclosed when facial images are leaked.

To overcome this problem, a secure scheme using noisy images has been proposed [3] for the SR-based FR (SR-FR) [1]. This scheme degrades the FR performance little in spite of noisy images are added to facial images. However, it has not been investigated whether the privacy protection scheme is applicable for the kernel SR (KSR)-based FR (KSR-FR) [2].

This paper shows that the privacy protection scheme [3] is applicable to the KSR-FR [2] with keeping the performance of FR.

## 2. Conventional methods

### 2.1. SR based face recognition [1]

Training image $\mathbf{I} \in \mathbb{R}^{H \times W}$ is vectorized to feature vector $\mathbf{v} \in \mathbb{R}^{M}$. For the $i$-th person among $K$ registerd persons, set of training samples $\mathbf{A}_i = [\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,N_i}] \in \mathbb{R}^{M \times N_i}$ exists. Feature vector of a query image, $\mathbf{y}$, which belongs to $i$-th person is assumed to be linearly approximated by only the training samples of the $i$-th person as

$$\mathbf{y} = \mathbf{v}_{i,1}x_{i,1} + \cdots + \mathbf{v}_{i,N_i}x_{i,N_i} = \mathbf{A}_i\mathbf{x}_i. \quad (1)$$

Thus, with $N = \sum_{i=1}^{K} N_i$ of training samples, $\mathbf{y}$ can be represented as

$$\mathbf{y} = \mathbf{A}\mathbf{x}_0, \quad (2)$$

where $\mathbf{A} = [\mathbf{A}_1 \ldots \mathbf{A}_K]$ and $\mathbf{x}_0 = [0, \ldots, 0, \mathbf{x}_i, 0, \ldots, 0]^T \in \mathbb{R}^N$. Here $\mathbf{x}_0$ is sparse because the coefficients for training not belonging to the person may be zero.

In Eq. (2), if the solution $\mathbf{x}_0$ is sufficiently sparse, the solution is determined by solving the $\ell_1$ norm minimization problem:

$$\hat{\mathbf{x}} = \min ||\mathbf{x}||_1 \text{ subject to } \mathbf{y} = \mathbf{A}\mathbf{x}. \quad (3)$$

Finally, for the $i$-th person, the test sample is reconstructed by $\mathbf{y}_i = \mathbf{A}_i\hat{\mathbf{x}}_i$ like Eq. (1). Person $C$ who minimizes the residual between $\mathbf{y}$ and $\mathbf{y}_i$ is regarded as the result of the recognition:

$$C = \arg\min_i ||\mathbf{y} - \mathbf{y}_i||_2. \quad (4)$$

### 2.2. KSR based face recognition [2]

By using mapping function $\Phi$, feature vectors are observed in a possibly infinite dimensional space called kernel feature space to make training samples well separable. Eq. (2) is then

$$\Phi(\mathbf{y}) = \Phi(\mathbf{A})\boldsymbol{\alpha}, \quad (5)$$

where $\Phi(\mathbf{A}) = [\Phi(\mathbf{v}_{1,1}) \ldots \Phi(\mathbf{v}_{K,N_K})]$. Eq. (5) becomes

$$\Phi(\mathbf{A})^T\Phi(\mathbf{y}) = \Phi(\mathbf{A})^T\Phi(\mathbf{A})\boldsymbol{\alpha},$$
$$\mathbf{k}(\cdot, \mathbf{y}) = \mathbf{K}\boldsymbol{\alpha}, \quad (6)$$

where $\mathbf{k}(\cdot,\mathbf{y}) = [k(\mathbf{v}_{1,1},\mathbf{y}),\ldots,k(\mathbf{v}_{K,N_K},\mathbf{y})]^T \in \mathbb{R}^N$, $k(\cdot,\cdot)$ is a kernel function which outputs the inner product of input vectors, $\mathbf{K} = [K_{m,n}] \in \mathbb{R}^{N\times N}$, $K_{m,n} = k(\mathbf{v}_m,\mathbf{v}_n)$, $m = 1,\ldots,N$, and $n = 1,\ldots,N$. Solution $\boldsymbol{\alpha}_0$ is determined as $\hat{\boldsymbol{\alpha}}_1$ by

$$\hat{\boldsymbol{\alpha}}_1 = \min ||\boldsymbol{\alpha}||_1 \text{ subject to } \mathbf{k}(\cdot,\mathbf{y}) = \mathbf{K}\boldsymbol{\alpha}. \quad (7)$$

Person $C$ is identified by

$$C = \arg\min_i ||\mathbf{k}(\cdot,\mathbf{y}) - \mathbf{K}\boldsymbol{\alpha}_i||_2 \quad (8)$$

## 3. The proposed method

This section proposes a secure KSR-FR using the privacy protection scheme [3]. The proposed method applies the following two steps before KSR-FR.

First, for visually encrypting, random matrix $\mathbf{R} \in \mathbb{R}^{H\times W}$ is added to facial image $\mathbf{I} \in \mathbb{R}^{H\times W}$ whose dynamic range is $[I_{\min}, I_{\max}]$;

$$\tilde{\mathbf{I}} = \mathbf{I} + \mathbf{R}, \quad (9)$$

where $\tilde{\mathbf{I}}$ is the visually encrypted image. Second, for making an illegal decryption difficult, noisy image $\tilde{\mathbf{I}}$ is clipped to its original dynamic range $[I_{\min}, I_{\max}]$;

$$\check{\mathbf{I}} = \text{clip}(\tilde{\mathbf{I}}), \quad (10)$$

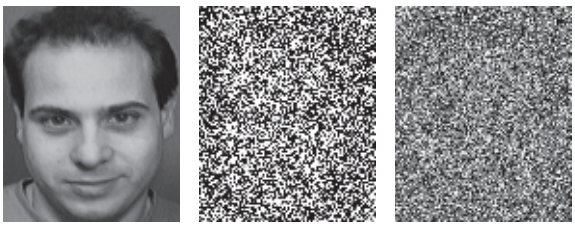
where $\check{\mathbf{I}} \in [I_{\min}, I_{\max}]$ is the clipped noisy image and $\text{clip}(\cdot)$ is the clipping function. Because of this step, even if an adversary gets $\mathbf{R}$ and $\check{\mathbf{I}}$, he/she can not get original image $\mathbf{I}$ by subtracting $\mathbf{R}$ from $\check{\mathbf{I}}$.

In the proposed method, after generating the noisy images of training and test images and vectorizing them, KSR-FR is performed.

## 4. Experimental results

The conventional methods [1]–[3] and the proposed method were performed for ORL face database [4] which consists of 400 frontal facial images of 40 individuals. Here, this database is divided fairly into 200 training images and 200 test images. Random matrix $\mathbf{R}$ for visual encryption is an integer matrix distributed uniformly from $-500$ to 500. The dimensionality of feature vectors are reduced by random projections [1]. Gaussian kernel function $k(\mathbf{a},\mathbf{b}) = \exp(\frac{1}{L}||\mathbf{a}-\mathbf{b}||_2)$ is used in the conventional [2] and proposed methods, where $L$ is the mean of residuals between all possible pairs of training samples.

Fig. 1 shows images in the proposed method in which an adversary cannot get original image $\mathbf{I}$ by subtracting $\mathbf{R}$ from $\check{\mathbf{I}}$. Fig. 2 shows that the recognitions rates for dimensionality which is $M$ in SR based methods [1], [3] and $N$ in KSR based conventional method [2] and the proposed method. This figure shows the privacy protection scheme using noisy images [3] for SR-FR [1] is applicable for KSR-FR [2] with keeping the performance of FR.



(a) Original. (b) Encrypted. (c) Attacked.

Figure 1. An example of visually encrypted image $\check{\mathbf{I}}$ and image attacked by subtracting $\mathbf{R}$ from $\check{\mathbf{I}}$.

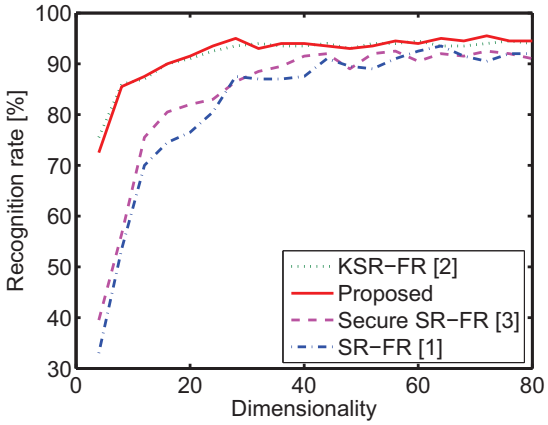



Figure 2. Recognition rate of each method.

## 5. Conclusions

This paper has proposed a secure method for KSR-FR. The proposed method confirms that the privacy protection scheme using noisy images [3] for SR-FR [1] is applicable to KSR-FR [2] with keeping the FR performance.

## References

[1] J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," *IEEE Trans. on Pattern Anal. Mach. Intell.*, vol. 31, no. 2, pp. 210–227, Feb. 2009.

[2] L. Zhang, W.-D. Zhou, P.-C. Chang, J. Liu, Z. Yan, T. Wang, and F. Z. Li, "Kernel sparse representation-based classifier," *IEEE Trans. on Sig. Proc.*, vol. 60, no. 4, pp. 1684–1695, Apr. 2012.

[3] Y. Muraki, M. Fujiyoshi, and H. Kiya, "A decryption-free secure face recognition system," *Proc. Intern. Workshop on Adv. Image Tech.*, p. 780, Jan. 2013.

[4] AT&T Laboratories Cambridge, "The database of faces," http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.