A Secure Face Recognition Scheme Using Noisy Images Based on Kernel Sparse Representation

Masakazu FURUKAWA, Yuichi MURAKI, Masaaki FUJIYOSHI, and Hitoshi KIYA
Tokyo Metropolitan University, Hino, Tokyo 191–0065, Japan
E-mail: {furukawa-masakazu, muraki-yuichi}@sd.tmu.ac.jp, mfujiyoshi@ieee.org, kiya@sd.tmu.ac.jp

***Abstract*—This paper proposes a secure face recognition scheme based on kernel sparse representation where facial images are visually encrypted. In the proposed scheme, a noisy image is added to all facial images, including a query image, to protect facial images. Noise-added facial images are further clipped for preventing unauthorized noise removing. Thanks to these strategies, a leakage of facial images will not disclose users' privacy, even the noisy image is also leaked. That is, the proposed scheme protects users' privacy and does not need to manage the noisy image securely. The proposed scheme directly applies kernel sparse representation based face recognition to noisy facial images, viz., decryption-free. Experimental results demonstrate that the face recognition performance of kernel sparse representation is not degraded, even facial images are visually encrypted.**

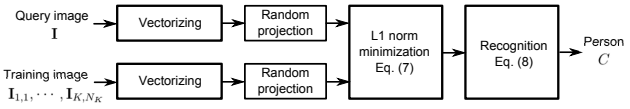


Fig. 1. Sparse representation based face recognition [6].

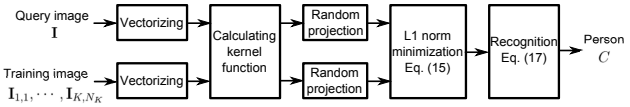


Fig. 2. Kernel sparse representation based face recognition [7].

I. Introduction

Face recognition is useful for various application such as personal authentication systems, video surveillance, and so on. Many researchers have studied various face recognition methods, for example, methods using eigenfaces [1], fisherfaces [2], graph matching [3], laplacianfaces [4], local binary patterns [5], and so on. Recently, a robust face recognition method based on sparse representation [6] has drawn a lot of attention. Furthermore, a kernel method has been introduced to this recognition method to improve the recognition performance [7]. These methods, however, have a problem; Facial images are not protected, i.e., users' privacy will be disclosed when facial images are leaked.

In order to protect original biometric images such as iris, fingerprint, and facial images, *cancelable biometric*s-based authentication systems have been proposed [8]–[10]. In these system, biometric signals are severely distorted by a series of intentional transformations to protect original biometric signals. Even so, signals can be compared in the distorted domain because all signals including a query signal are transformed in the same way. Transformations for cancelable biometrics are classified to invertible and non-invertible [10]. Parameters for the former have to be securely managed as a secret key so that it prevents impostors from reversing a distorted signal to the original signal. On contrast, the latter is good in terms of security, but it degrades the recognition performance [8].

The concept of cancelable biometrics has been introduced to sparse representation-based pattern recognition [6]. For iris recognition, a sparse representation-based secure method has been proposed [11] in which a dimension reduction technique called random projection [12] is used as a non-invertible transformation. Moreover, a cancelable biometrics-based privacy protection method has been proposed [13] for the sparse representation-based robust face recognition [6]; the non-invertible transformation in this method consists of adding a noisy image to all facial images and clipping the pixel values of noise-added image. A secure method is desired to be realized on kernel sparse representation-based face recognition because of the performance superiority of the face recognition method based on kernel sparse representation.

This paper proposes a new secure face recognition scheme; The proposed scheme introduces the essence of the cancelable biometrics-based privacy protection method [13] to the kernel sparse representation-based face recognition [7]. As described in Sect. III-B2, the recognition based on kernel sparse representation rather than the sparse representation-based recognition [6] is suitable for the privacy protection method from the viewpoint of cancelable biometrics. The recognition performance of the proposed secure scheme is almost the same as that of the original insecure kernel sparse representation-based face recognition method. The key, the noisy image, is not needed to be securely managed since the transformation for cancelable biometrics in the proposed scheme is non-invertible.

II. Preliminaries

This section introduces the sparse representation-based face recognition [6] and its improved version, i.e., the face recognition based on kernel sparse representation [7]. Figs. 1 and 2 show the block diagram of the these two conventional methods [6], [7], respectively.

A. Sparse Representation-Based Face Recognition

Training image $\mathbf{I} \in \mathbb{R}^{H \times W}$ is vectorized to feature vector $\mathbf{v} \in \mathbb{R}^M$, where M is often equal to HW. For the i-th person among K registered persons, set of training vectors

$$\mathbf{A}_i = [\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,N_i}]$$

are given ahead. In this method [6], it is assumed that $\mathbf{y} \in \mathbb{R}^M$, the feature vector of a query image which belongs to the i-th person, is linearly approximated by only the training vectors of the i-th person:

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

Therefore, with all training vectors of K registered persons, $\mathbf{y}$ can be written as

$$\begin{aligned}\mathbf{y} &= \mathbf{A}_1\mathbf{0} + \cdots + \mathbf{A}_{i-1}\mathbf{0} + \mathbf{A}_i\mathbf{x}_i + \mathbf{A}_{i+1}\mathbf{0} + \cdots + \mathbf{A}_K\mathbf{0} \\ &= \mathbf{A}\mathbf{x}_0,\end{aligned} \tag{2}$$

where

$$\begin{aligned}\mathbf{A} &= [\mathbf{A}_1 \ldots \mathbf{A}_K] \in \mathbb{R}^{M \times N}, \\ \mathbf{x}_0 &= [0, \ldots, 0, \mathbf{x}_i, 0, \ldots, 0]^T \in \mathbb{R}^N, \\ N &= \sum_{i=1}^{K} N_i.\end{aligned}$$

Here the coefficient vector, $\mathbf{x}_0$, is sparse because the coefficients unrelated to the i-th person are zero.

Solution $\mathbf{x}_0$ obtained by solving Eq. (2) is essential for recognizing faces. If Eq. (2) is overdetermined, i.e., $M > N$, the solution could be determined uniquely by using least squares. However, in the sparse representation-based face recognition [6], Eq. (2) is typically underdetermined, $M < N$. Therefore, the solution could not be determined uniquely. Even though, when optimal solution $\mathbf{x}_0$ is sparse, it is identical to solution $\hat{\mathbf{x}}$ determined by solving the ℓ^0-norm minimization problem:

$$\hat{\mathbf{x}}_0 = \min \|\mathbf{x}\|_0 \text{ subject to } \mathbf{y} = \mathbf{A}\mathbf{x}. \tag{3}$$

If optimal solution $\mathbf{x}_0$ is sufficiently sparse, $\hat{\mathbf{x}}$ is the same as the solution of the following ℓ^1-norm minimization problem:

$$\hat{\mathbf{x}}_1 = \min \|\mathbf{x}\|_1 \text{ subject to } \mathbf{y} = \mathbf{A}\mathbf{x}. \tag{4}$$

In this method [6], Eq. (4) is solved after the dimension of feature vectors are reduced. Though some techniques for dimension reduction are introduced in this method [6], this paper supposes random projection [12] as the dimension reduction technique. By random projection with random matrix $\mathbf{B} \in \mathbb{R}^{d \times M}$, feature vectors $\mathbf{v} \in \mathbb{R}^M$ are projected onto a d dimensional subspace where $d < M$. Therefore, a query vector, $\mathbf{y} \in \mathbb{R}^M$, and the set of training vectors, $\mathbf{A} \in \mathbb{R}^{M \times N}$, are projected as $\mathbf{y}' \in \mathbb{R}^d$ and $\mathbf{A}' \in \mathbb{R}^{d \times N}$ respectively:

$$\mathbf{y}' = \mathbf{B}\mathbf{y}, \tag{5}$$

$$\mathbf{A}' = \mathbf{B}\mathbf{A}. \tag{6}$$

Using Eqs. (5) and (6), Eq. (4) can be written as

$$\hat{\mathbf{x}}_1 = \min \|\mathbf{x}\|_1 \text{ subject to } \mathbf{y}' = \mathbf{A}'\mathbf{x}. \tag{7}$$

It is noted that Eqs. (4) and (7) can be solved in polynomial time. Furthermore, fast algorithms for solving these problem has been studied [14].

Finally, for the i-th person, the dimension-reduced query vector, $\mathbf{y}'$, is reconstructed with Eq. (1) and $\hat{\mathbf{x}}_1$. Person C who minimizes the residual between $\mathbf{y}'$ and the reconstructed query vector for the i-th person is regarded as the recognition result:

$$C = \arg\min_i \left\|\mathbf{y}' - \mathbf{A}'\delta_i(\hat{\mathbf{x}})\right\|_2, \tag{8}$$

where $\delta_i(\hat{\mathbf{x}})$ is the function which replaces the coefficients for training vectors unrelated to the i-th person by zeros, i.e.,

$$\delta_i\left([\hat{x}_{1,1}, \ldots, \hat{x}_{K,N_K}]^T\right) = [0, \ldots, 0, \hat{x}_{i,1}, \ldots, \hat{x}_{i,N_i}, 0, \ldots, 0]^T.$$

B. Kernel Sparse Representation-Based Face Recognition

In this method [7], feature vectors are observed in a higher (possibly infinite) dimensional space to make training samples well separable by using mapping function $\mathbf{\Phi}$:

$$\Phi(\mathbf{v}) = [\phi_1(\mathbf{v}), \ldots, \phi_D(\mathbf{v})]^T \in \mathbb{R}^D, \tag{9}$$

where $M \ll D$. The inner product of two vectors on the high dimensional space can be calculated with the vectors on input space through a kernel function, $k(\cdot,\cdot)$, as

$$\Phi(\mathbf{v}_i)^T\Phi(\mathbf{v}_j) = k(\mathbf{v}_i, \mathbf{v}_j). \tag{10}$$

Sparse representation-based face recognition is performed to feature vectors in the high dimensional space. Eq. (2) is, then, described as

$$\Phi(\mathbf{y}) = \mathbf{\Phi}(\mathbf{A})\boldsymbol{\alpha}_0, \tag{11}$$

where

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

Eq. (11) can be transformed by $\mathbf{\Phi}^T$ as follows:

$$\begin{aligned}\mathbf{\Phi}(\mathbf{A})^T\Phi(\mathbf{y}) &= \mathbf{\Phi}(\mathbf{A})^T\mathbf{\Phi}(\mathbf{A})\boldsymbol{\alpha}_0, \\ \mathbf{k}(\cdot,\mathbf{y}) &= \mathbf{K}\boldsymbol{\alpha}_0,\end{aligned} \tag{12}$$

where

$$\begin{aligned}\mathbf{k}(\cdot,\mathbf{y}) &= [k(\mathbf{v}_{1,1},\mathbf{y}), \ldots, k(\mathbf{v}_{K,N_K},\mathbf{y})]^T \in \mathbb{R}^N \\ \mathbf{K} &= [\mathbf{k}(\cdot,\mathbf{v}_{1,1}), \ldots, \mathbf{k}(\cdot,\mathbf{v}_{K,N_K})] \in \mathbb{R}^{N \times N}.\end{aligned} \tag{13}$$

The solution is determined as well as Eq. (4):

$$\hat{\boldsymbol{\alpha}}_1 = \min \|\boldsymbol{\alpha}\|_1 \text{ subject to } \mathbf{k}(\cdot,\mathbf{y}) = \mathbf{K}\boldsymbol{\alpha}. \tag{14}$$

Similar to Eq. (7), applying random projection with random matrix $\mathbf{B} \in \mathbb{R}^{d \times N}$ makes Eq. (12) being

$$\hat{\boldsymbol{\alpha}}_1 = \min \|\boldsymbol{\alpha}\|_1 \text{ subject to } \mathbf{k}'(\cdot,\mathbf{y}) = \mathbf{K}'\boldsymbol{\alpha}, \tag{15}$$

where

$$\begin{aligned}\mathbf{k}'(\cdot,\mathbf{y}) &= \mathbf{B}\mathbf{k}(\cdot,\mathbf{y}) \in \mathbb{R}^d, \\ \mathbf{K}' &= \mathbf{B}\mathbf{K} \in \mathbb{R}^{d \times N}.\end{aligned} \tag{16}$$

As well as Eq. (8), person C is identified by

$$C = \arg\min_i \left\|\mathbf{k}'(\cdot,\mathbf{y}) - \mathbf{K}'\delta_i(\hat{\boldsymbol{\alpha}})\right\|_2. \tag{17}$$

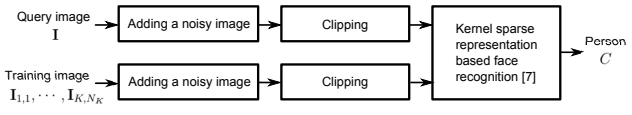


Fig. 3. The proposed scheme.

The next section proposes a secure face recognition scheme based on this kernel sparse representation-based face recognition method [7].

III. Proposed scheme

In this section, a secure face recognition scheme based on the kernel sparse representation [7] using the cancelable biometrics-based privacy protection method [13] is proposed. Fig. 3 shows the block diagram of the proposed scheme.

A. Algorithms

The proposed scheme consists of three steps:

1) Add a noisy image to all facial images.
2) Clip the images generated in step 1 to the dynamic range of original images.
3) Perform kernel sparse representation-based face recognition [7].

Steps are described in the subsequent sections.

1) Adding a Noisy Image: For visual encryption of facial images, noisy image $\mathbf{R} \in \mathbb{R}^{H\times W}$ is added to facial image $\mathbf{I}$:

$$\tilde{\mathbf{I}} = \mathbf{I} + \mathbf{R}, \tag{18}$$

where $\tilde{\mathbf{I}}$ is the visually encrypted facial image. $\mathbf{R}$ is generated as a uniformly distributed random integer matrix in $[-s,s]$.

2) Clipping: Above mentioned noisy image addition does not make the proposed scheme well secure. If an adversary gets $\tilde{\mathbf{I}}$ and $\mathbf{R}$, he/she can easily reconstruct the original image $\mathbf{I}$ by subtracting $\mathbf{R}$ from $\tilde{\mathbf{I}}$. To prevent such unauthorized reconstruction, $\tilde{\mathbf{I}}$ is clipped to the dynamic range of the original images:

$$\check{\mathbf{I}} = \mathrm{clip}(\tilde{\mathbf{I}}), \tag{19}$$

where $\check{\mathbf{I}} \in [I_{\min}, I_{\max}]$ is the clipped image.

3) Recognition: Query vector $\check{\mathbf{y}}$ and set of training vectors $\check{\mathbf{A}} = [\check{\mathbf{v}}_{1,1},\ldots,\check{\mathbf{v}}_{K,N_K}]$ are generated from noise added-and-clipped facial images or cancelable biometrics transformed images. Then, kernel sparse representation-based face recognition [7] is performed on derived vectors. In the proposed scheme, Eq. (14) is expressed as below:

$$\check{\boldsymbol{\alpha}}_1 = \min \|\boldsymbol{\alpha}\|_1 \text{ subject to } \check{\mathbf{k}}'(\cdot,\check{\mathbf{y}}) = \check{\mathbf{K}}'\boldsymbol{\alpha}, \tag{20}$$

where

$$\check{\mathbf{k}}(\cdot,\check{\mathbf{y}}) = \mathbf{B}[k(\check{\mathbf{v}}_{1,1},\check{\mathbf{y}}),\ldots,k(\check{\mathbf{v}}_{N,N_K},\check{\mathbf{y}})]^T,$$
$$\check{\mathbf{K}} = \mathbf{B}[\check{\mathbf{k}}(\cdot,\check{\mathbf{v}}_{1,1})\ldots\check{\mathbf{k}}(\cdot,\check{\mathbf{v}}_{N,N_K})].$$

Then, as well as Eq. (17), person C is identified by

$$C = \arg\min_i \left\| \check{\mathbf{k}}'(\cdot,\check{\mathbf{y}}) - \check{\mathbf{K}}'\delta_i(\hat{\boldsymbol{\alpha}}) \right\|_2. \tag{21}$$

B. Features

This section summarizes the features of the proposed scheme.

1) Key Protection Free: By clipping in step 2, subtracting noisy image $\mathbf{R}$ from clipped image $\check{\mathbf{I}}$ cannot reconstruct original image $\mathbf{I}$, i.e., non-invertible. In addition, obtaining $\mathbf{R}$ does not help an adversary to reconstruct $\mathbf{I}$, i.e., $\mathbf{R}$, which is the key for privacy protection, can be disclosed to the public.

2) Immune to Adding a Noisy Image: Adding noisy image $\mathbf{R}$ does not degrade the recognition rate of the kernel sparse representation-based face recognition [7]. Let consider the inner product for two training vectors:

$$\tilde{\mathbf{v}}_{1,1} = \mathbf{v}_{1,1} + \mathbf{n}, \tag{22}$$
$$\tilde{\mathbf{v}}_{2,1} = \mathbf{v}_{2,1} + \mathbf{n}, \tag{23}$$

where $\mathbf{n}$ is the feature vector of noisy image $\mathbf{R}$. Here, kernel function is assumed to radial basis function (RBF) kernel:

$$k(\mathbf{a},\mathbf{b}) = \exp\left(-\gamma\|\mathbf{a}-\mathbf{b}\|_2^2\right), \tag{24}$$

where γ is a positive parameter. Then,

$$\begin{aligned} k(\tilde{\mathbf{v}}_{1,1},\tilde{\mathbf{v}}_{2,1}) &= \exp\left(-\gamma||\tilde{\mathbf{v}}_{1,1}-\tilde{\mathbf{v}}_{2,1}||_2^2\right) \\ &= \exp\left(-\gamma||\mathbf{v}_{1,1}+\mathbf{n}-\mathbf{v}_{2,1}-\mathbf{n}||_2^2\right) \\ &= \exp\left(-\gamma||\mathbf{v}_{1,1}-\mathbf{v}_{2,1}||_2^2\right) \\ &= k(\mathbf{v}_{1,1},\mathbf{v}_{2,1}). \end{aligned} \tag{25}$$

This relation holds for any possible pairs of training vectors. Therefore, in performing kernel sparse representation-based face recognition [7], adding a noisy image is a transformation of cancelable biometrics.

IV. Experimental results

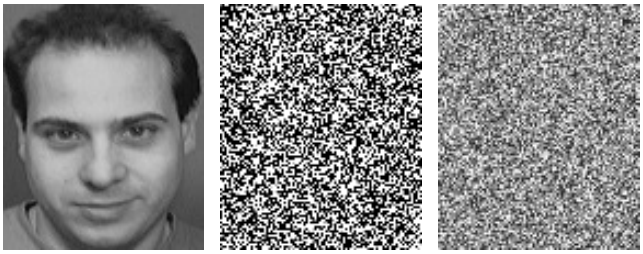
This section demonstrates that the proposed scheme keeps the recognition performance of kernel sparse representation-based face recognition [7], even facial images are visually encrypted.

The conventional methods [6], [7], [13] and the proposed scheme were performed for ORL face database [15] which consists of 400 frontal facial images of 40 individuals. Here, this database were randomly divided into 200 training images and 200 query images, and the recognition was performed for every query images. This trial was repeated ten times and the recognition rates was averaged over 2000 (200 images $\times$ 10 times) query images. Kernel function used in kernel sparse representation-based face recognition [7] and the proposed scheme was radial basis function kernel in Eq. (24), where parameter γ was calculated by

$$\gamma = \mathrm{median}\left(\frac{1}{\|\mathbf{v}_k - \bar{\mathbf{v}}\|_2^2}\right), \tag{26}$$

$$\bar{\mathbf{v}} = \frac{1}{N}\sum_{k=1}^{N}\mathbf{v}_k. \tag{27}$$

Noisy image $\mathbf{R}$ was generated as uniformly distributed random integer matrix in $[-s,s]$.



(a) Original $\mathbf{I}$. (b) Encrypted $\check{\mathbf{I}}$. (c) Attacked $\check{\mathbf{I}} - \mathbf{R}$.

Fig. 4. An example of visually encrypted image $\check{\mathbf{I}}$ and the image obtained by subtracting $\mathbf{R}$ from $\check{\mathbf{I}}$ in the proposed scheme.

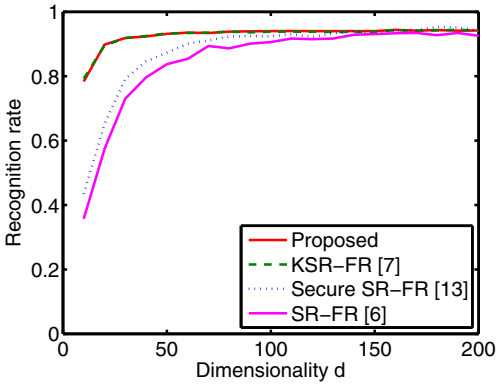


Fig. 5. Recognition rates of each method.

Fig. 4 shows images in the proposed scheme in which an adversary can not obtain original image $\mathbf{I}$ by subtracting $\mathbf{R}$ from $\check{\mathbf{I}}$, where $s = 1000$. Fig. 5 shows the recognition rates of the conventional [6], [7], [13] and proposed methods versus reduced dimension d, where $s = 1000$. It is found that the privacy protection method using a noisy image [13] is applicable for kernel sparse representation-based face recognition [7] with keeping the face recognition performance.

Fig. 6 shows the recognition rates versus the range of noisy image $\mathbf{R}$, s, of the conventional [13] and proposed methods, under the condition that dimension d's were 100 (underdetermined) and 200 (overdetermined). The more s increases, the more the number of clipped pixels in a facial image increases. Even so, the recognition rate of the proposed scheme degrades more gradually than that of the conventional method [13]. This result shows that the proposed scheme is more robust to clipping than the conventional method [13].

V. Conclusions

This paper has proposed a secure face recognition scheme for kernel sparse representation. The proposed scheme makes kernel sparse representation-based face recognition [7] secure based on the cancelable biometics-based privacy protection method [13]. The kernel sparse representation-based face recognition is suitable for the protection method [13], and the proposed scheme is superior in the recognition performance to the conventional sparse representation-based secure

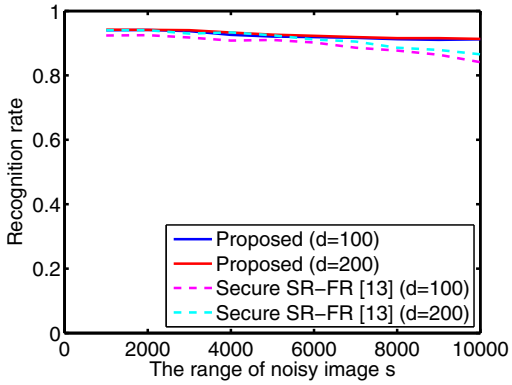


Fig. 6. Recognition rates for noise range, i.e., the value of s.

method [13].

Further works include the robustness evaluation of the privacy protection method [13] against noise reduction filters and analysis of the clipping effect to the recognition performance theoretically.

References

[1] M.A. Turk and A.P. Pentland, "Face recognition using eigenfaces," in *Proc. IEEE CVPR*, 1991.

[2] P.N. Belhumeur, J.P. Hespanha, and D.J. Kriengman, "Eigenfaces versus fisherfaces: Recognition using class specific linear projection," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.19, pp.711–720, Jul. 1997.

[3] L. Wiskott, J.-M. Fellous, N. Küiger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.19, pp.775–779, Jul. 1997.

[4] X. He, S. Yan, Y. Hu, P. Niyogi, and H.J. Zhang, "Face recognition using laplacianfaces," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.27, pp.328–340, Mar. 2005.

[5] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.28, pp.2037–2041, Dec. 2006.

[6] J. Wright, A.Y. Yang, A. Ganesh, S.S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.31, pp.210–227, Feb. 2009.

[7] 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. Signal Process.*, vol.60, pp.1684–1695, Apr. 2012.

[8] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol.40, no.3, pp.614–634, 2001.

[9] N.K. Ratha, S. Chikkerur, J.H. Connell, and R.M. Bolle, "Generating cancelable fingerprint templetes," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.29, pp.–, Apr. 2007.

[10] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. in Signal Process.*, no.113, Jan. 2008.

[11] J.K. Pillai, V.M. Patel, R. Chellappa, and N.K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.33, pp. 1877–1893, Sept. 2011.

[12] P. Indyk and R. Motowani, "Approximate nearest neighbors: Towards removing the curse of dimensionality," in *ACM STOC*, 1998, pp.604–613.

[13] Y. Muraki, M. Fujiyoshi, and H. Kiya, "A decryption-free secure face recognition system," in *Proc. IEICE//ITE/KSBE IWAIT*, p.780, 2013.

[14] A.Y. Yang, S.S. Sastry, A. Ganesh, and Y. Ma, "Fast l1-minimization algorithms and application in robust face recognition: A review," in *Proc. IEEE ICIP*, 2010.

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