A Decryption-Free Secure Face Recognition System

Yuichi MURAKI, Masaaki FUJIYOSHI, and Hitoshi KIYA
Department of Information and Communication Systems, Tokyo Metropolitan University, Hino, Tokyo 191–0065, Japan

***Index Terms*—ℓ_1 minimization, random matrix, clipping, compressed sensing, sparse representation**

I. Introduction

This paper proposes a secure and robust face recognition system which requires no decryption of facial images.

Face recognition systems are needed for safe living environments, and a robust system based on sparse representation have been proposed [1]. From the viewpoint of privacy protection, facial images stored in the systems should be protected, and a decryption of images is not desired because of computational cost and security. This paper proposes a secure face recognition system requiring no decryption of images based on the conventional robust system using sparse representation [1].

II. Robust System Using Sparse Representation

The method [1]classifies feature vector $\mathbf{y} \in \mathbb{R}^M$ of a new facial image to the κ-th person among K registered persons by

$$\kappa = \arg\min_k \|\hat{\mathbf{y}} - \mathbf{v}_{k,n_k}\|_2, \; k = 1,2,\dots,K, \; n_k = 1,2,\dots,N_k, \quad (1)$$

where

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

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_1 \text{ s.t. } \mathbf{y} = \mathbf{A}\mathbf{x}, \quad (3)$$

$$\mathbf{A} = [\mathbf{v}_{1,1}, \mathbf{v}_{1,2}, \dots, \mathbf{v}_{1,N_1}, \mathbf{v}_{2,1}, \dots, \mathbf{v}_{K,N_K}] \in \mathbb{R}^{M \times N}, \quad (4)$$

$\mathbf{v}_{k,n_k} \in \mathbb{R}^M$ is the feature vector of the n_k-th image for the k-th registered person, and $N = \sum_k N_k$. The method is based on the assumption that $\mathbf{y}$ can be linearly approximated with $\mathbf{v}_{k,n_k}$'s as $\mathbf{y} = \mathbf{A}\mathbf{x}_0$, where $\mathbf{x}_0 \in \mathbb{R}^N$'s entries are zero expect those associated with the k-th person.

Though this method robustly recognizes faces, facial images are not securely protected. We will propose a secure face recognition system based on this method in the next section.

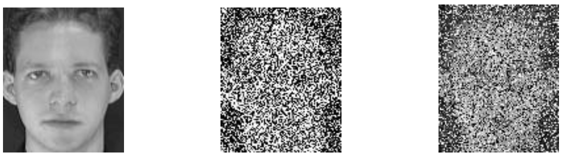
III. Proposed Method

The proposed method applies the following algorithm to each image regardless of registered and query images, before extracting a M-dimensional feature vector from the image.

1. Add random matrix $\mathbf{R} \in \mathbb{R}^{W \times H}$ to $W \times H$-sized image $\mathbf{I}$.
2. Clip image $(\mathbf{I} + \mathbf{R})$ to its original dynamic range.

The former makes image $\mathbf{I}$ visually protected, and the latter makes it difficult to recover $\mathbf{I}$ from the protected image even $\mathbf{R}$ is leaked.

From image $(\mathbf{I} + \mathbf{R} + \mathbf{c})$ where $\mathbf{c} \in \mathbb{R}^{W \times H}$ is the clipping noise matrix, a M-dimensional feature vector is generated. Face recognition is achieved based on the conventional method [1] with extracted feature vectors, so no decryption of images is required in the proposed system.



(a) Original $\mathbf{I}$. (b) Image $(\mathbf{I}+\mathbf{R}+\mathbf{c})$. (c) Image $(\mathbf{I}+\mathbf{c})$.

Fig. 1. Image examples in the proposed system.

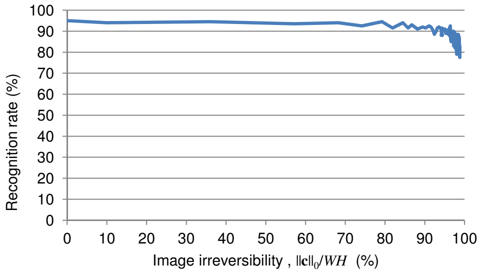


Fig. 2. The recognition rate versus the irreversibility of I.

It is noted that larger $\|\mathbf{c}\|_0$ makes protected images more irreversibly but it may degrade recognition performance.

IV. Experimental Results

400 frontal-face images of 40 individuals [2] is split to two sets which each set consists of 200 images of 40 individuals; one is for $\mathbf{v}_{k,n_k}$ and the other is for $\mathbf{y}$. Random matrix $\mathbf{R}$ has a uniform distribution.

It is confirmed from Fig. 1 that clipping at Step 2 protects images even random matrix $\mathbf{R}$ is subtracted. Figure 2 shows the recognition rate versus $\|\mathbf{c}\|_0$ in which $\mathbf{R}$ is not added to images at 0 % of the horizontal axis, i.e., it is the same as the conventional method [1]. Up to approximately 80 % in the irreversibility, the proposed system recognizes faces well.

V. Conclusions

This paper has proposed a decryption-free secure face recognition system with a random matrix and pixel clipping. The proposed method recognizes faces well even images are protected.

References

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

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