Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2009, Article ID 260148, 16 pages
doi:10.1155/2009/260148

Research Article

Sorted Index Numbers for Privacy Preserving Face Recognition

Yongjin Wang and Dimitrios Hatzinakos

The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, 10 King's College Road, Toronto, ON, Canada M5S 3G4

Correspondence should be addressed to Yongjin Wang, ywang@comm.utoronto.ca

Received 30 September 2008; Revised 3 April 2009; Accepted 18 August 2009

Recommended by Jonathon Phillips

This paper presents a novel approach for changeable and privacy preserving face recognition. We first introduce a new method of biometric matching using the sorted index numbers (SINs) of feature vectors. Since it is impossible to recover any of the exact values of the original features, the transformation from original features to the SIN vectors is noninvertible. To address the irrevocable nature of biometric signals whilst obtaining stronger privacy protection, a random projection-based method is employed in conjunction with the SIN approach to generate changeable and privacy preserving biometric templates. The effectiveness of the proposed method is demonstrated on a large generic data set, which contains images from several well-known face databases. Extensive experimentation shows that the proposed solution may improve the recognition accuracy.

1. Introduction

Biometric recognition has been an active research area in the past two decades. Biometrics-based recognition systems determine or confirm the identity of an individual based on the physiological and/or behavioral characteristics [1]. A wide variety of biometric modalities have been investigated in the past. Examples of these biometrics include physiological traits such as fingerprint, face, iris, and behavioral characteristics such as gait and keystroke. Each biometric has its strengths and weaknesses. The choice of a biometric is dependent on the properties of the biometric and the requirements of the specific application. Depending on different application context, a biometric system can operate in identification mode or verification mode [1]. Figure 1 depicts the general block diagram of biometric recognition systems.

During enrolment, a feature vector $\mathbf{g}_i$, $i = 1, 2, \ldots, N$, where N is the total number of users, is extracted from the biometric data of each user and stored in the system database as templates. Biometric identification is a one-to-many comparison to find an individual's identity. In identification mode, given an input feature vector $\mathbf{p}$, if the identity of $\mathbf{p}$, $\mathbf{I}_p$, is known to be in the system database, that is, $\mathbf{I}_p \in \{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_N\}$, then $\mathbf{I}_p$ can be determined by $\mathbf{I}_p = \mathbf{I}_k = \min_k\{S(\mathbf{p}, \mathbf{g}_k)\}$, $k = 1, 2, \ldots, N$, where S denotes the similarity measure. The performance of a biometric identification system is usually evaluated in terms of correct recognition rate (CRR).

A biometric verification system is a one-to-one match that determines whether the claim of an individual is true. At the verification stage, a feature vector $\mathbf{p}$ is extracted from the biometric signal of the authentication individual $\mathbf{I}_p$, and compared with the stored template $\mathbf{g}_k$ of the claimed identity $\mathbf{I}_k$ through a similarity function S. The evaluation of a verification system can be performed in terms of hypothesis testing [2], $\mathbf{H}_0$: $\mathbf{I}_p = \mathbf{I}_k$, the claimed identity is correct; $\mathbf{H}_1$: $\mathbf{I}_p \neq \mathbf{I}_k$, the claimed identity is not correct. The decision is made based on the system threshold τ, $\mathbf{H}_0$ is decided if $S(\mathbf{p}, \mathbf{g}_k) \leq \tau$, and $\mathbf{H}_1$ is decided if $S(\mathbf{p}, \mathbf{g}_k) > \tau$. A verification system makes two types of errors: false accept (deciding $\mathbf{H}_0$ when $\mathbf{H}_1$ is true), and false reject (deciding $\mathbf{H}_1$ when $\mathbf{H}_0$ is true). The performance of a biometric verification system is usually evaluated in terms of false accept rate (FAR, $P(\mathbf{H}_0 \mid \mathbf{H}_1)$), false reject rate (FRR, $P(\mathbf{H}_1 \mid \mathbf{H}_0)$), and equal error rate (EER, operating point where FAR and FRR are equal). The FAR and FRR are closely related functions of the system decision threshold τ.

While biometric technology provides various advantages, there exist some problems. In the first place, biometric data

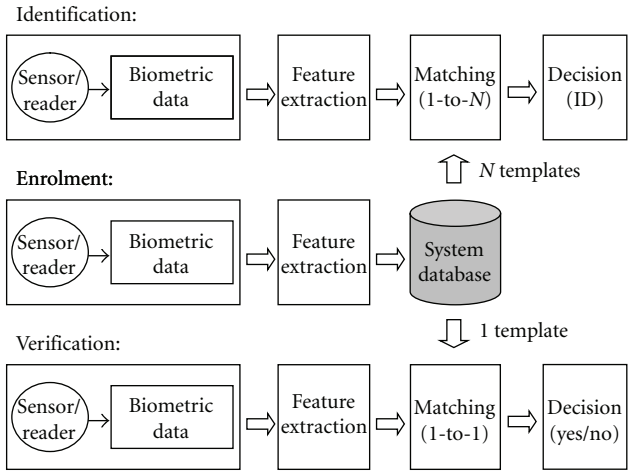

Figure 1: Block diagram of biometric recognition systems.

reflects the user's physiological/behavior characteristics. If the storage device of biometric templates is obtained by an adversary, the user's privacy may be compromised. The biometric templates should be stored in a format such that the user's privacy is preserved even when the storage device is attacked. Secondly, biometrics cannot be easily changed and reissued if compromised due to the limited number of biometric traits that a human has. This is of particular importance in biometric verification scenarios. Ideally, just like password, the biometrics should be changeable. The users may use different biometric representation for different applications. When the biometric template in one application is compromised, the biometric signal itself is not lost forever and a new biometric template can be issued.

A number of research works have been proposed in the recent years to address the changeability and privacy preserving problems of biometric systems. One approach is to combine the biometric technology with cryptographic systems [3]. In a biometric cryptosystem, a randomly generated cryptographic key is bound with the biometric features in a secure way such that both the key and the biometric features cannot be revealed if the stored template is compromised. The cryptographic key can be retrieved if sufficiently similar biometric features are presented. Error correction algorithms are usually employed to tolerate errors. Due to the binary nature of cryptographic keys, such systems usually require discrete representation of biometric data, such as minutia points for fingerprints and iris code. However, the feature vectors of many other biometrics, such as face, are usually represented in continuous domain. Therefore, to apply such a scheme, the continuous features need to be discretized first. It should be noted that such methods produce changeable cryptographic keys, while the biometric data is not changeable. Furthermore, the security level of such methods still needs to be further investigated [4, 5].

An alternative and effective solution is to apply repeatable and noninvertible transformations on the biometric features [2]. With this method, every enrollment (or application) can use a different transform. When a biometric template is compromised, a new one can be generated using a new transform. In mathematical language, the recognition problem can be formulated as follows. Given a biometric feature vector $\mathbf{u}$, the biometric template $\mathbf{g}$ is generated through a generation function $\mathbf{g} = \mathrm{Gen}(\mathbf{u}, \mathbf{k})$. Different templates can be generated by varying the control factor $\mathbf{k}$. During verification, the same transformation is applied to the authentication feature vector, $\mathbf{g}' = \mathrm{Gen}(\mathbf{u}', \mathbf{k})$, and the matching is based on similarity measure in the transformed domain, that is, $\mathrm{S}(\mathbf{g}, \mathbf{g}')$. The major challenge here lies in the difficulty of preserving the similarity measure in the transformed domain, that is, $\mathrm{S}(\mathbf{g}, \mathbf{g}') \approx \mathrm{S}(\mathbf{u}, \mathbf{u}')$. Further, to ensure the property of privacy protection, the generation function $\mathrm{Gen}(\mathbf{u}, \mathbf{k})$ should be nonfinvertible such that $\hat{\mathbf{u}} = \mathrm{Rec}(\mathbf{g}, \mathbf{k}) \neq \mathbf{u}$, where $\mathrm{Rec}(\mathbf{g}, \mathbf{k})$ is the reconstruction function when both the template $\mathbf{g}$ and control factor $\mathbf{k}$ are known.

Among various biometrics, face recognition has been one of the most passive, natural, and noninvasive types of biometrics. Such characteristics of face recognition make it a good choice for some surveillance and monitoring applications. It can also be used in supporting video search and indexing, video-conferencing, interactive games, physical access control, computer network login, and ATM. Many face recognition methods have been proposed in the literature, which can be roughly categorized into holistic template matching-based system, geometrical local feature-based system, and hybrid systems [6]. Promising results have also been reported under controlled condition [7]. In general, the selection of a face recognition scheme is dependent on the specific requirements of a given task [6]. Appearance-based approaches (such as principal component analysis (PCA) and linear discriminant analysis (LDA)) that treat the face image as a holistic pattern are among the most successful methods [6, 8]. In this paper, we first introduce a novel method for face recognition based on sorted index numbers (SINs) of appearance-based facial features. Unlike traditional face recognition methods which store either the original image or facial features as templates, the proposed method stores the SIN vectors only. A matching algorithm is introduced to measure the similarity between two SIN vectors. Because it is impossible to recover the exact values of the original features based on the index numbers, the SIN method is noninvertible. To further enhance the security and address the irrevocable problem, intentional random projection (RP) is applied prior to the sorting operation such that the generated biometrics template is both changeable and privacy preserving. Experimental results on a large data set demonstrate the effectiveness of the proposed solution.

The remainder of this paper is organized as follows. Section 2 provides a review of related works. Section 3 introduces the proposed method. Experimental results along with detailed discussion are presented in Section 4. Finally, conclusions are provided in Section 5.

2. Related Works

To address the privacy and irrevocability problem of biometric systems, many tentative solutions have been introduced

in the literature using various biometrics. Among the earliest efforts, Soutar et al. [9] presented a correlation-based method for fingerprint-based biometric verification, and Davida et al. [10] proposed to store a set of user specific error correction parameters as template for an iris-based system. However, both of these two works are lack of practical implementation and cannot provide rigorous security guarantees [3].

Juels and Wattenberg [11] introduced a fuzzy commitment scheme, which generalized and improved Davida's methods. The fuzzy commitment scheme assumes binary representation of biometric features, and error correction algorithms are used to tolerate errors due to the noisy nature of biometric data. Hao et al. [12] presented a similar scheme on an iris-based problem using a two-level error correction mechanism. Later, a polynomial reconstruction-based scheme, fuzzy vault, is proposed by Juels and Sudan [13]. The fuzzy vault scheme assumes the biometric data being represented by discrete features (e.g., minutia points in fingerprints). In this scheme, error tolerance is achieved by using the property of secret sharing, while the security is obtained by hiding genuine points into randomly generated chaff points. A few implementation works of fuzzy vault have been reported in [14, 15] based on fingerprints. Although the paper proves that this scheme is secure in an information-theoretic sense, it is clear that it is vulnerable to attacks via record multiplicity [5]. Further drawbacks of the method include high computational complexity and high error rate [14, 15].

Dodis et al. [16] presented a theoretical work, fuzzy extractor, for generation of cryptographic keys from noisy biometric data using error correction code and hash functions. Their paper also assumes the biometric features in discrete domain. Different constructions for three metric spaces: Hamming distance, set difference, and edit distance are introduced. Yagiz et al. [17] introduced a quantization-based method for mapping of continuous face features to discrete form and utilized a known secure construction for secure key generation. However, Boyen [18] showed that the fuzzy extractor may be not secure for multiple use of the same biometrics data.

Kevenaar et al. [19] proposed a helper data system for generation of renewable and privacy preserving binary template. A set of fiducial points is first identified from six key objects of human face, and Gabor filters are applied to extract features from a small patch centered around every fiducial point. The extracted features are discretized by a thresholding method, and the reliability of each bit is measured based on statistical analysis. The binary template is generated by combining the extracted reliable bit with a randomly generated key through an XOR operation, and BCH code is applied for error correction. The indexes of the selected reliable bit, the mean vector for feature thresholding, the binary template, and the hash of the key are stored for verification. Their experiments demonstrate that the performance of the binary feature vectors is only degraded slightly comparing with the original features. However, the performance of their system depends on accurate localization of key object and fiducial points.

Savvides et al. [20, 21] proposed an approach for cancelable biometric authentication in the encrypted domain. The training face images are convolved with a random kernel first; the transformed images are then used to synthesize a single minimum average correlation energy filter. At the point of verification, query face image is convolved with the same random kernel and then correlates with the stored filer to examine the similarity. If the storage card is ever attacked, a new random kernel may be applied. They show that the performance is not affected by the random kernel. However, it is not clear how the system preserves privacy if the random kernel is known by an adversary. The original biometrics may be retrieved through deconvolution if the random kernel is known.

Boult [22] introduced a method for face-based revocable biometrics based on robust distance measures. In this scheme, the face features are first transformed through scaling and translation, and the resulting values are partitioned into two parts, the integer part and the fractional part. The integer part is encrypted using Public Key (PK) algorithms, and the fractional part is retained for local approximation. A user-specific passcode is included to address the revocation problem. In a subsequent paper [23], a similar scheme is applied on a fingerprint problem, and detailed security analysis is provided. Their methods demonstrate both improvement in accuracy and privacy. However, it is assumed that the private key cannot be obtained by an imposter. In the case of known private key and transform parameters, the biometrics features can be exactly recovered.

Teoh et al. [24] introduced a two-factor scheme, Bio-Hashing method, which produces changeable non-invertible biometric template, and also claimed good performance, near zero EER. In BioHashing, a feature vector $\mathbf{u} \in \mathbb{R}^n$ is first extracted from the user's biometric data. For each user, a user-specific transformation matrix $R \in \mathbb{R}^{n\times m}, m \leq n$, is generated randomly (associated with a key or token), and the Gram-Schmidt orthonormalization method is applied to R, such that all the columns of R are orthonormal. The extracted feature vector $\mathbf{u}$ is then transformed by $\mathbf{x} = R^T\mathbf{u}$, and the resulting vector $\mathbf{x}$ is quantized by $\mathbf{b}_i = 0$, if $\mathbf{x}_i < t$, and $\mathbf{b}_i = 1$, if $\mathbf{x}_i \geq t$, $i = 1, 2, \ldots, m$, where t is a predefined threshold value and usually set to 0. The binary vector $\mathbf{b}$ is stored as the template. The technique has been applied on various biometric traits [25, 26] and demonstrates zero or near zero equal error rate in ideal case; that is, both the biometric data and the key are legitimate. In the stolen key scenario, the BioHashing method usually degrades the verification accuracy. Lumini and Nanni [27] introduce some ideas to improve the performance of BioHashing in case of stolen key by utilizing different threshold values and fuse the scores. However, as shown in [28], as well as the experimental results in this paper, even in the both legitimate scenario, the performance of BioHashing technique is highly dependent on the characteristics and dimensionality of the extracted features.

In summary, existing works either can not provide robust privacy protection, or sacrifice recognition accuracy for privacy preservation. In this paper, we propose a new method for changeable and privacy preserving template generation

using random projection and sorted index numbers. As it will be shown, the proposed method is also capable of improving the recognition accuracy.

3. Methodology

This section presents the proposed method for privacy preserving face recognition. An overview of the sorted index numbers (SINs) method as well as the similarity measure algorithm is first introduced. Next, the analysis of the SIN algorithm is provided in detail. The random projection-based changeable biometrics scheme is then described. Finally, privacy analysis of the proposed method is presented.

3.1. Overview of SIN Method. The proposed method utilizes sorted index numbers instead of the original facial features as templates for recognition. The procedure of creating the proposed SIN feature vector is as follows.

(1) Extract feature vector $\mathbf{w} \in \mathbb{R}^n$ from the input face image $\mathbf{z}$.

(2) Compute $\mathbf{u} = \mathbf{w} - \overline{\mathbf{w}}$, where $\overline{\mathbf{w}}$ is the mean feature vector calculated from the training data.

(3) Sort the feature vector $\mathbf{u}$ in descending order, and store the corresponding index numbers in a new vector $\mathbf{g}$.

(4) The generated vector $\mathbf{g} \in \mathbb{Z}^n$ that contains the sorted index numbers is stored as template for recognition.

For example, given $\mathbf{u} = \{u_1, u_2, u_3, u_4, u_5, u_6\}$, the sorted vector in descending order is $\hat{\mathbf{g}} = \{u_4, u_6, u_2, u_1, u_3, u_5\}$, then the template is $\mathbf{g} = \{4, 6, 2, 1, 3, 5\}$.

The method for computing the similarity between two SIN vectors is as follows.

(1) Given two SIN feature vectors $\mathbf{g} \in \mathbb{Z}^n$ and $\mathbf{p} \in \mathbb{Z}^n$, where $\mathbf{g}$ denotes the template vector, and $\mathbf{p}$ denotes the probe vector. Start from the first element g_1 of $\mathbf{g}$.

(2) Search for the corresponding element in $\mathbf{p}$, that is, $p_j = g_1$. Record $d_1 = j - 1$, where j is the index number in $\mathbf{p}$.

(3) Eliminate the obtained p_j in the previous step from $\mathbf{p}$, and obtain $\mathbf{p}^1 = \{p_1, p_2, \ldots, p_{j-1}, p_{j+1}, \ldots, p_n\}$.

(4) Repeat steps 2 and 3 on the following elements of $\mathbf{g}$ until g_{n-1}. Record $d_2, d_3, \ldots, d_{n-1}$.

(5) The similarity measure of $\mathbf{g}$ and $\mathbf{p}$ is computed as $S(\mathbf{g}, \mathbf{p}) = \sum_{i=1}^{n-1} d_i$.

Illustration Example.

(1) For two SIN feature vectors $\mathbf{g} = \{4, 6, 2, 1, 3, 5\}$ and $\mathbf{p} = \{2, 5, 3, 6, 1, 4\}$, we first search the 1st element $g_1 = 4$, and find that $p_6 = 4$. Therefore $d_1 = 6 - 1 = 5$. Eliminate p_6 from $\mathbf{p}$ and we form a new vector of $\mathbf{p}^1 = \{2, 5, 3, 6, 1\}$.

(2) Search the 2nd element $g_2 = 6$, and find that $p_4^1 = 6$. Therefore $d_2 = 4 - 1 = 3$. Eliminate p_4^1 from $\mathbf{p}^1$ and form a new vector of $\mathbf{p}^2 = \{2, 5, 3, 1\}$.

(3) Search the 3rd element $g_3 = 2$, and find that $p_1^2 = 2$. Therefore $d_3 = 1 - 1 = 0$. Eliminate p_1^2 from $\mathbf{p}^2$ and form a new vector of $\mathbf{p}^3 = \{5, 3, 1\}$.

(4) Search the 4th element $g_4 = 1$, and find that $p_3^3 = 1$. Therefore $d_4 = 3 - 1 = 2$. Eliminate p_3^3 from $\mathbf{p}^3$ and form a new vector of $\mathbf{p}^4 = \{5, 3\}$.

(5) Search the 5th element $g_5 = 3$, and find that $p_2^4 = 1$. Therefore $d_5 = 2 - 1 = 1$.

(6) Compute $S(\mathbf{g}, \mathbf{p}) = \sum_{i=1}^{n-1} d_i = 5 + 3 + 0 + 2 + 1 = 11$.

3.2. Methodology Analysis. To understand the underlying rationale of the proposed algorithm, we first look into an alternative presentation of the method, named Pairwise Relational Discretization (PRD). The relative relation of different bins has been used to represent histogram shape in [29]. Here, the pairwise relative relation of features is used for Euclidean distance approximation. The procedure of producing the PRD feature vector is as follows.

(1) Extract feature vector $\mathbf{w} \in \mathbb{R}^n$ from the input face image $\mathbf{z}$.

(2) Compute $\mathbf{u} = \mathbf{w} - \overline{\mathbf{w}}$, where $\overline{\mathbf{w}}$ is the mean feature vector calculated from the training data.

(3) Compute binary representation of $\mathbf{u}$ by comparing the pairwise relation of all the elements in $\mathbf{u}$ according to

$$b_{ij} = \begin{cases} 1, & u_i \geq u_j, \\ 0, & u_i < u_j. \end{cases} \tag{1}$$

(4) Concatenate all the generated binary bits into one vector $\mathbf{b} = \{b_{12}, \ldots, b_{1n}, b_{23}, \ldots, b_{2n}, b_{34}, \ldots, b_{n-1,n}\}$. Store the binary vector $\mathbf{b}$ as template for recognition.

The similarity measure of the PRD method is based on Hamming distance. Unlike traditional discretization method, which quantizes individual elements based on some predefined quantization levels, the proposed method takes the global characteristics of the feature vectors into consideration. This is interpreted by comparing the pairwise relation of all groups of two elements in the vector. The intuition behind the idea is to consider an n-dimensional space as combinations of 2-dimensional planes. In n-dimensional subspace, when the similarity of two vectors is evaluated by Euclidean distance, each element of the vectors is treated as coordinates in the corresponding basis $\{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n\}$, and the similarity is based on the spatial closeness. The elements are essentially the projection coefficients of the vector onto each basis (i.e., lines). Here, instead of projecting onto lines, we explore the projection onto 2D planes. Figure 2 offers a diagrammatic illustration of the PRD method. For two points in n-dimensional subspace, if they are spatially close to each other, then in large number of 2D planes, their projection location should be close to each other, that is, small Hamming distance, and vise versa. Therefore, the Euclidean distance between two vectors can

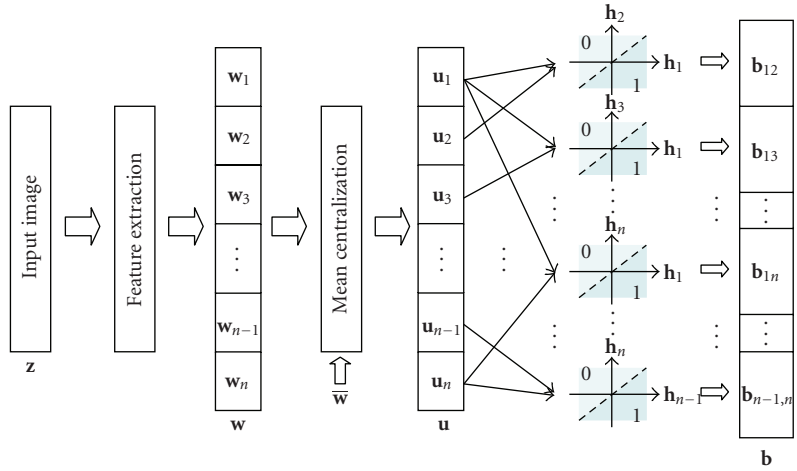

Figure 2: Diagram of Pairwise Relational Discretization (PRD) method.

be approximated by the Hamming distance between the corresponding PRD vectors. The mean centralization step is to leverage the significance of each element such that no single dimension will overwhelm others. The discretization step partitions a plane into two regions by comparing the pairwise relation. It reduces the sensitivity of the variation of individual elements and therefore possibly provides better error tolerance. Figure 3 shows the intra-class and inter-class distribution of 100 PCA coefficients based on 1000 randomly selected images from the experimental data set. The PCA vectors are normalized to unit length, and Euclidean distance and SIN distance are used as dissimilarity measure. Note that the size of the overlapping area of the intra-class and inter-class distributions indicates the recognition error. It can be observed that the SIN method produces smaller error than the original features, therefore will possibly provide better recognition performance.

A major drawback of the PRD method is the high dimensionality of the generated binary PRD vector. For an n-dimensional vector, the generated binary vector $\mathbf{b}$ will have a size of $n(n-1)/2$. For example, for a feature vector with $n = 100$, the PRD vector will have a size of 4950. This problem introduces high storage and computational requirements. This is particularly important for applications with high processing speed demand. To improve this, we note that the PRD method is based on pairwise relation of all the vector elements, and the same information can be exactly preserved from the sorted index numbers of the vector; that is, any single bit in $\mathbf{b}$ can be derived from the SIN vector.

Let $\mathbf{g}$ and $\mathbf{p}$ denote the SIN vector of template and probe images, respectively, $\mathbf{b}_g$ and $\mathbf{b}_p$ represent the corresponding PRD vectors, then we have

$$H\left(\mathbf{b}_g, \mathbf{b}_p\right) = S(\mathbf{g}, \mathbf{p}) = \sum_{i=1}^{n-1} d_i, \tag{2}$$

where $H(\mathbf{b}_g, \mathbf{b}_p)$ and $S(\mathbf{g}, \mathbf{p})$ denote the Hamming distance and SIN distance, respectively, and $d_i, i = 1, \ldots, n$, represents the Hamming distance associated with every single element in $\mathbf{g}$.

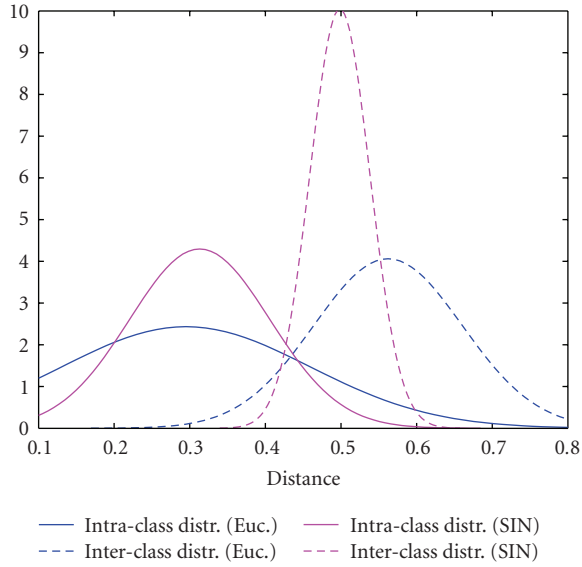

Figure 3: Comparison of intraclass and interclass distribution using Euclidean and SIN distances.

Proof of (2). Since $\mathbf{g}$ and $\mathbf{b}_g$ are derived from the same feature vector, in $\mathbf{b}_g$, there are $n-1$ bits that are associated with the first element of $\mathbf{g}$, g_1. If $p_j = g_1$, where j is the index number of the corresponding element in $\mathbf{p}$, then all the index numbers to the left of p_j will have different bit values in $\mathbf{b}_p$, that is, $d_1 = j - 1$. It should be noted that since the Hamming distance for all the bits associated with $p_j = g_1$ has been computed, the p_j element should be removed for the calculation of next iteration. After the Hamming distances for all the elements in $\mathbf{g}$ and $\mathbf{p}$ are computed, the sum of them will correspond to the Hamming distance of $\mathbf{b}_g$ and $\mathbf{b}_p$, that is, $H(\mathbf{b}_g, \mathbf{b}_p) = S(\mathbf{g}, \mathbf{p}) = \sum_{i=1}^{n-1} d_i$.

Equation (2) shows that the proposed SIN and PRD methods produce exactly the same results. To test the effectiveness of SIN over PRD in computational complexity, we performed experiments on a computer with Intel *Core*2

CPU 2.66 GHz. With an original feature vector of dimensionality 100, the average time for PRD feature extraction and matching is 26.2 milliseconds, while the SIN method only consumes less than 0.9 milliseconds. □

3.3. Changeable Biometrics. To address the changeability problem in biometric verification systems, one solution is to scramble the order of the features before the sorting operation. However, the security of such method is the same as the encryption/decryption key method, where the original SIN vectors will be obtained if the scrambling rule is compromised. In this paper, for the purpose of comparative study, we adopt the random projection-(RP-) based scheme as in [24].

Depending on the requirements of the application, the changeable biometric system can be implemented in two scenarios: user-independent projection and user-dependent projection. In the user-independent scenario, all the users use the same matrix for projection. This matrix can be controlled by the application provider, and therefore the users do not need to carry the matrix (or equivalently a key for matrix generation) for verification. The user-dependent scenario is a two-factor authentication scheme, and requires the presentation of both the biometrics data and projection matrix at the time and point of verification. In both scenarios, the biometric template can be regenerated by changing the projection matrix.

The theory of random projection is first introduced by the Johnson-Lindenstrauss lemma [30].

Lemma 1 (J-L lemma). *For any* $0 < \epsilon < 1$*, and an integer s, let m be a positive integer such that* $m \geq m_0 = O(\epsilon^{-2}\log s)$*. For any set B of s points in* $\Re^n$*, there exists a map f:*$\Re^n \to \Re^m$ *such that for all* $\mathbf{u}, \mathbf{v} \in B$*,*

$$(1-\epsilon)\|\mathbf{u}-\mathbf{v}\|^2 \leq \left\|f(\mathbf{u})-f(\mathbf{v})\right\|^2 \leq (1-\epsilon)\|\mathbf{u}-\mathbf{v}\|^2. \tag{3}$$

This lemma states that the pairwise distance between any two vectors in the Euclidean space can be preserved up to a factor of ϵ, when projected onto a random m-dimension subspace. Random projection has been used as a dimension reduction tool in face recognition [31], image processing [32], and a privacy preserving tool in data mining [33] and biometrics [24]. The implementation of random projection can be carried out by generating a matrix of size $n \times m$, $m \leq n$, with each entry an independent and identically distributed (i.i.d.) random variable, and applying the Gram-Schmidt method for orthonormalization. Note that when $m = n$, it becomes the random orthonormal transformation (ROT). In user-independent scenario, for two facial feature vectors $\mathbf{u} \in \mathbb{R}^n$ and $\mathbf{v} \in \mathbb{R}^n$, since the same ROT matrix $R \in \mathbb{R}^{n \times n}$ is applied, we have the well-known property of ROT:

$$\begin{aligned}\left\|R^T\mathbf{u}-R^T\mathbf{v}\right\|^2 &= \left\|R^T\mathbf{u}\right\|^2 + \left\|R^T\mathbf{v}\right\|^2 - 2\mathbf{u}^T RR^T\mathbf{v} \\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\mathbf{u}^T\mathbf{v} \\ &= \|\mathbf{u}-\mathbf{v}\|^2.\end{aligned} \tag{4}$$

It can be seen that the ROT transform exactly preserves the Euclidean distance of original features. When the projected dimensionality is $m < n$, although exact preservation can not be obtained, the pairwise distance can be approximately preserved. The larger the m, the better the preservation. Since the SIN method also approximates the Euclidean distance, the SIN vectors obtained after RP can also approximately preserve the similarity between two original vectors.

In the user-dependent scenario, different users are associated with distinct projection matrices. The FAR corresponds to the probability of deciding $\mathbf{H}_0$ when $\mathbf{H}_1$ is true, $P(\mathbf{H}_0 \mid \mathbf{H}_1)$, and the FRR corresponds to $P(\mathbf{H}_1 \mid \mathbf{H}_0)$. Note that for the FRR, even in case of a user-dependent scenario, the same orthogonal matrix R is used for the same user, and hence the situation is the same as the user-independent scenario. Therefore we only need to analyze the influence of different projection matrix over the FAR.

Let R_u and R_v represent the RP matrices for feature vectors $\mathbf{u}$ and $\mathbf{v}$, respectively. Let $\mathbf{x} = R_u^T\mathbf{u}$ and $\mathbf{y} = R_v^T\mathbf{v}$, and $\mathbf{g}$ and $\mathbf{p}$ denote the SIN vectors for $\mathbf{x}$ and $\mathbf{y}$, respectively. Due to the randomness of RP, the total number of possible outputs for $\mathbf{g}$ and $\mathbf{p}$ is equal to the number of permutations $m!$. Let γ denote the number of index permutations that have a distance of less than τ to the vector $\mathbf{g}$, then the probability of $\mathbf{p}$ being falsely identified by $\mathbf{g}$ is $P(\mathbf{H}_0 \mid \mathbf{H}_1) = \gamma/m!$. It can be seen that the probability of false accept depends on the characteristics and dimensionality of the features. If the features are well separated, that is, smaller γ value, with relatively higher dimensionality, the false accept rate will be small. The above analysis in user-dependent scenario also applies if the biometrics data is stolen by an adversary, since the $\mathbf{v}$ vector can be exactly the same as $\mathbf{u}$. This also explains the changeability of the method.

Figure 4 shows the distribution of the distance between two feature vectors using user-independent and user-dependent random projections. We randomly selected two PCA features vectors ($n = 100$) of the same subject from the employed data set, performed the same key and different key scenario 2000 times, and plotted the distribution of the Euclidean distance and SIN distance, respectively, at different projection dimensions. The PCA feature vectors are normalized to unit length, and the distances are normalized by dividing the largest value, respectively, 2 for Euclidean distance and $m(m-1)/2$ for SIN. It can be observed that by applying the same key, the mean of the Euclidean distance in the projected domain is centered around the original Euclidean distance, and the variance of the distances decreases as the projected dimensionality increases. This demonstrates better distance preservation at higher projection dimension. When different keys are applied, the mean of the distance distribution shifts to the right, that is larger distance. The clear separation of the distribution indicates the changeability of the proposed method.

3.4. Privacy Analysis. Since the SIN method only stores the index numbers of the sorted feature vector $\mathbf{u}$, the transformation from $\mathbf{u}$ to the corresponding SIN vector $\mathbf{g}$ is non-invertible. There is no effective reconstruction being possible to recover the exact values of $\mathbf{u}$ from $\mathbf{g}$. The most an adversary can do is to estimate the values of $\mathbf{u}$ based on some statistics or his/her own features. By using such method, an

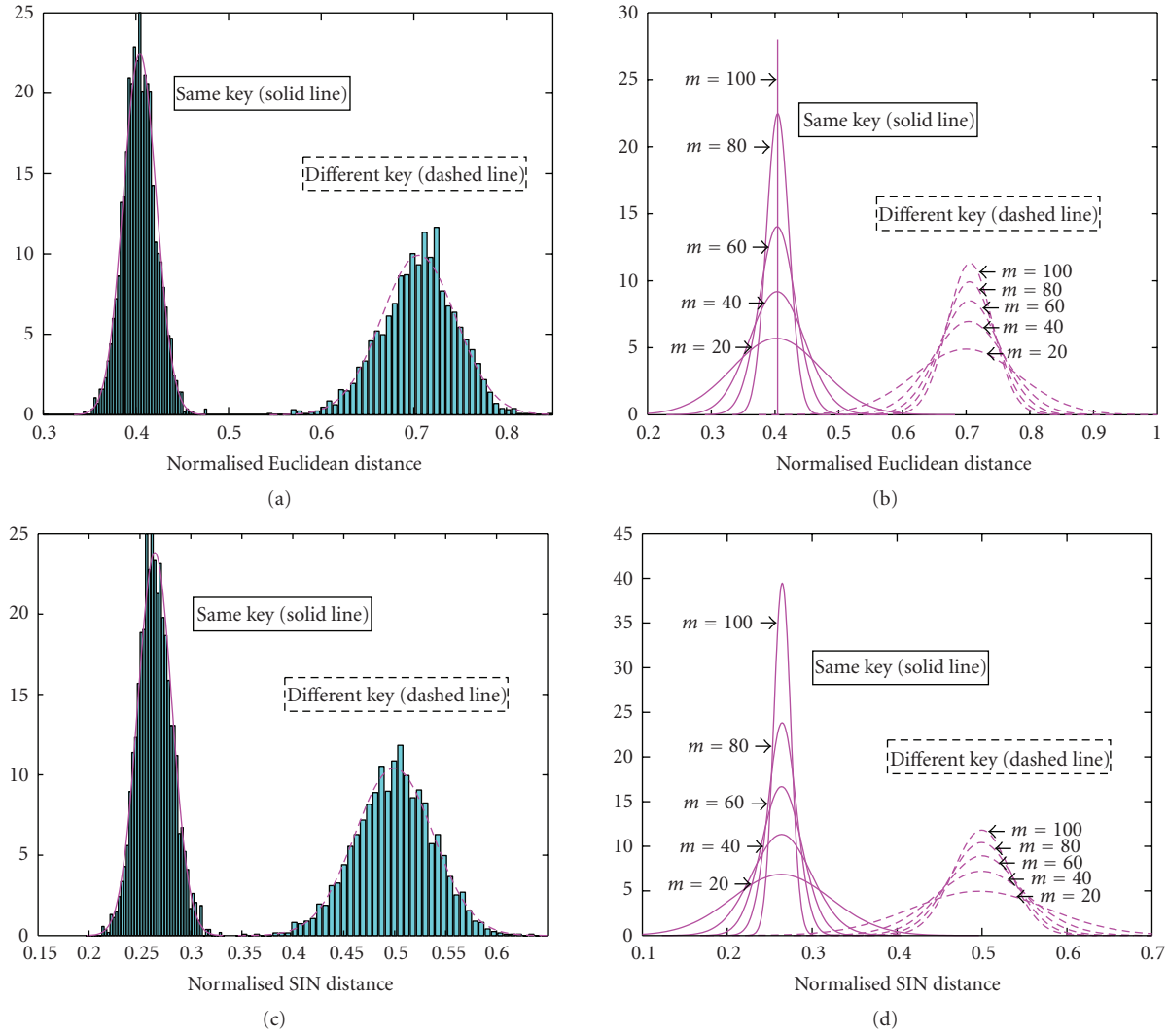

Figure 4: Gaussian approximation of the distribution of (a) normalized Euclidean distance (NED), (c) normalized SIN distance (NSD), with $n = 100$, $m = 80$. Distribution of (b) NED, and (d) NSD, at different projection dimensionality in same key and different key scenarios.

adversary can only produce an approximation of the original features. For RP, when the projected dimensionality m is smaller than the dimensionality n of the original features, even the worst case that the projection matrix is known by an adversary, an estimation will produce an approximation of the original features with variance inverse proportional to m, that is, the smaller the m, the larger the estimation variance [33]. Since both the RP and SIN methods are non-invertible transformations, the combination of these two is expected to produce stronger privacy protection.

To analyze the privacy preserving properties of the proposed method, we introduce the following privacy measures:

Definition 1. A feature vector $\mathbf{u} \in \Re^n$ is called privacy protected at element-wise level α, where α is computed as

$$\alpha = \frac{1}{n}\sum_{i=1}^{n} 1 - [1 - x_i]h(1 - x_i), \quad x_i = \frac{\mathbf{Var}(u_i - \hat{u}_i)}{\mathbf{Var}(u_i)}, \tag{5}$$

where $\mathbf{var}(\cdot)$ denotes variance, $\hat{u}_i$ is the estimated value of element u_i, and $h(x)$ is unit step function, that is, $h(x) = 1$ if $x \geq 0$ and $h(x) = 0$ otherwise. The function $h(x)$ is utilized to regulate the significance of all the elements, such that the variance ratio of any element is maximum 1.

Using the variance of difference between the actual and perturbed values has been widely adopted as a privacy measure for individual attributes in data mining [34]. Similarly, here we take the variance of difference between the original and estimated values as a measure of the privacy protection of individual elements. When the variance ratio of any attribute is greater or equal to 1, that is, $\mathbf{Var}(u_i - \hat{u}_i) \geq \mathbf{Var}(u_i)$, then the estimation of that attribute essentially provides no useful information, and the attribute is strongly protected. The element-wise privacy level α measures the average privacy protection of individual elements. The greater the α value, the better the privacy protection.

Besides measuring the privacy protection of the individual elements, it is also important to measure the global characteristics of the feature vectors such that the estimated vector is not close to the original one up to certain similarity functions. In [35], it is shown that any arbitrary distance functions can be approximately mapped to Euclidean distance domain through certain algorithms. In this paper, we take the squared Euclidean distance between the estimated and original feature vectors as a measure of privacy.

Definition 2. A feature vector $\mathbf{u} \in \Re^n$ is called privacy protected at vector-wise level β, where β is computed as:

$$\beta = \frac{\mathbf{E}\left(\|\hat{\mathbf{u}} - \mathbf{u}\|^2\right)}{\mathbf{E}\left(\|\mathbf{r} - \mathbf{u}\|^2\right)}, \tag{6}$$

where $\mathbf{E}(\cdot)$ denotes expectation, $\|\cdot\|$ denotes the squared Euclidean distance, and $\mathbf{r}$ is any random vector in the estimation feature space. If the average distance between the estimated and original vector is approaching the average distance between any random vector and the original vector, then the estimated vector essentially exhibits randomness, and therefore does not disclose information about $\mathbf{u}$; that is, the larger the β, the better privacy. Without loss of generality, we assume that all the vectors have unit length. Since the vectors are centralized to zero mean, the average distance between any randomly selected vector $\mathbf{r}$ and the original vector $\mathbf{u}$ is

$$\begin{aligned}\mathbf{E}\left(\|\mathbf{r} - \mathbf{u}\|^2\right) &= \mathbf{E}\left(\|\mathbf{r}\|^2 + \|\mathbf{u}\|^2 - 2\mathbf{r}^T\mathbf{u}\right) \\ &= 2 - 2\mathbf{E}\left(\mathbf{r}^T\mathbf{u}\right) = 2,\end{aligned} \tag{7}$$

where we use the fact that $\mathbf{E}(\mathbf{r}^T\mathbf{u}) = \mathbf{E}(\sum_{i=1}^n r_i u_i) = \sum_{i=1}^n \mathbf{E}(r_i u_i) = \sum_{i=1}^n \mathbf{E}(r_i)\mathbf{E}(u_i) = 0$, since r_i is independent of u_i and has zero mean. Therefore, for unit length vectors, (6) can be written as

$$\beta = \frac{\mathbf{E}\left(\|\hat{\mathbf{u}} - \mathbf{u}\|^2\right)}{2}. \tag{8}$$

Figure 5 shows the privacy measures α and β as functions of projected dimension m, with the original dimensionality $n = 100$. Figure 5(a) plots the results generated from 1000 random unit vectors, and Figure 5(b) is obtained from 1000 randomly selected PCA feature vectors in the experimental data set. The random vectors are generated with each element an i.i.d. Gaussian random variable, followed by normalization to unit length. The PCA vectors are normalized to have the same variance and unit length. The estimation $\hat{\mathbf{u}}$ of an original vector $\mathbf{u}$ is performed as follows. For an original vector $\mathbf{u}$ with RP matrix $\mathbf{R}$, we obtain the SIN vector $\mathbf{g}$ by $\mathbf{g} = \text{sort}(\mathbf{R}^T\mathbf{u})$, where sort denotes the operation of getting the sorted index numbers. Given the worst case that an adversary obtains $\mathbf{g}$ and $\mathbf{R}$, he can estimate $\mathbf{u}$ by using a randomly generated unit vector $\mathbf{e}$ according to an i.i.d. Gaussian distribution, mapping to the estimated vector $\hat{\mathbf{e}}$ based on $\mathbf{g}$, then computing $\hat{\mathbf{u}} = \mathbf{R}\mathbf{R}^T\hat{\mathbf{e}}$, and normalizing to unit length. It can be observed from Figure 5 that both the element-wise and vector-wise privacy levels improve as the projected dimension decreases.

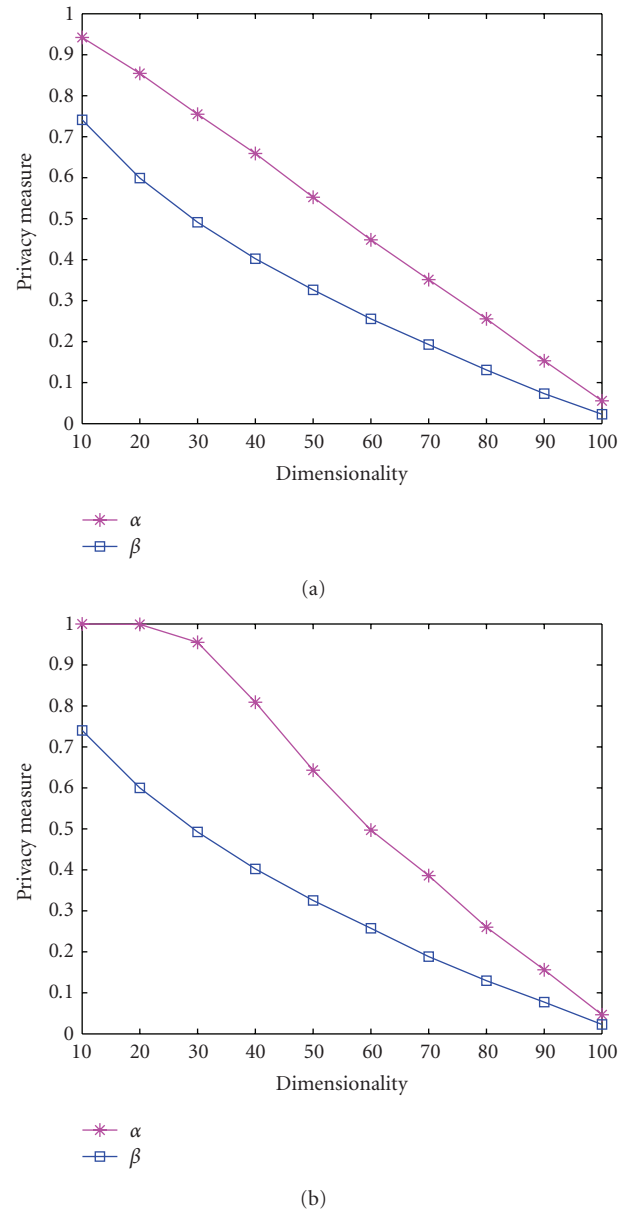

Figure 5: Privacy measure as a function of dimensionality. (a) random vectors, (b) PCA feature vectors.

To provide some insight into the privacy protection property of the proposed method, we compare the reconstructed image with the original image through different methods in Figure 6. The images are randomly selected from the FERET database [36, 37]. A PCA vector $\mathbf{u}$ is first extracted from image $\mathbf{z}$ (Figure 6(a)). A new vector is then generated by $\mathbf{x} = R_u^T\mathbf{u}$, where R_u is a random projection matrix, and the sorted index numbers of $\mathbf{x}$ are stored in a SIN vector $\mathbf{g}$. Here the dimensionality of PCA is selected as $n = 100$, and the projection dimension is $m = 50$. Assuming the worst case that $\mathbf{g}$ and R_u are all compromised, an adversary can only reconstruct the original image based on a vector $\mathbf{v}$,

which is either a PCA feature vector of some other subjects, or a randomly generated vector. The reconstruction can be performed by first sorting and mapping $\mathbf{v}$ to another vector $\tilde{\mathbf{v}}$ based on $\mathbf{g}$, and followed by $\hat{\mathbf{z}} = \Psi(R_u\tilde{\mathbf{v}} + \Psi^T\bar{\mathbf{z}})$. Figure 6(a) shows an original image $\mathbf{z}$ and Figure 6(b) is the reconstructed image from its first 100 PCA coefficients $\mathbf{u}$. The reconstruction is performed by $\hat{\mathbf{z}} = \Psi(\mathbf{u} + \Psi^T\bar{\mathbf{z}})$, where Ψ is the PCA projection matrix, and $\bar{\mathbf{z}}$ is the mean image obtained from the training set. It is obvious that the PCA approach cannot preserve privacy since the original visual information is very well approximated. Figures 6(d) and 6(f) are the reconstructed images from the features of images, Figures 6(c) and 6(d), respectively, while Figure 6(g) and Figure 6(h) are reconstructed from randomly generated vectors, all using the SIN vector $\mathbf{g}$ of image Figure 6(a). All the reconstructed images demonstrate large distortion from the original image. The results in Figure 6 are meant to provide some insight into the privacy preserving property of the proposed method. It can be seen that the original values of the feature vectors can not be recovered, and an estimation can only produce a distorted version of the original image, which has a significant visual difference from the original one. The above analysis, although not exact in the mathematical sense, illustrates that the privacy of the user can be protected by using the proposed method.

4. Experimental Results

To evaluate the performance of the proposed method, we conducted experiments on a generic data set that consists of face images from several well-known databases [38]. In this section, we first give a description of the employed data set. The adopted feature extraction methods are then briefly discussed. Finally, the experimental results along with detailed discussion are presented.

4.1. Generic Data Set. To approach more realistic face recognition applications, this paper tests the effectiveness of the proposed method using a generic data set, in which the intrinsic properties of the human subjects are trained from subjects other than those to be recognized. The generic database was initially organized for the purpose of demonstrating the effectiveness of the generic learning framework [38]. It originally contains 5676 images of 1020 subjects from 5 well-known databases, FERET [36, 37], PIE [39], AR [40], Aging [41], and BioID [42]. All images are aligned and normalized based on the coordinate information of some facial feature points. The details of image selection can be found in [38].

For preprocessing, the color images are first transformed to gray-scale images by taking the luminance component in YC_bC_r color space. All images are preprocessed according to the recommendation of the FERET protocol, which includes: (1) images are rotated and scaled so that the centers of the eyes are placed on specific pixels and the image size is 150×130; (2) a standard mask is applied to remove non-face portions; (3) histogram equalized and image normalized to have zero mean and unit standard deviation. After preprocessing, the face images are converted to an image vector of dimension $J = 17154$. Table 1 illustrates the configuration of the whole data set. Figure 7 shows some example images from the generic data set.

Table 1: Generic data set configuration.

Database	No. of subjects	No. of images per subject	No. of images
FERET	750	≥3	3881
AR	119	4	476
Aging	63	≥3	276
BioID	20	≥6	227
PIE	68	12	816
Total	1020	≥3	5676

4.2. Feature Extraction. To study the effects of different feature extractors on the performance of proposed methods, we compare Principal Component Analysis (PCA) and Kernel Direct Discriminant Analysis (KDDA). PCA is an unsupervised learning technique which provides an optimal, in the least mean square error sense, representation of the input in a lower-dimensional space. In the Eigenfaces method [43], given a training set $\mathcal{Z} = \{\mathcal{Z}_i\}_{i=1}^{C}$, containing C classes with each class $\mathcal{Z}_i = \{\mathbf{z}_{ij}\}_{j=1}^{C_i}$ consisting of a number of face images $\mathbf{z}_{ij}$, a total of $M = \sum_{i=1}^{C} C_i$ images, the PCA is applied to the training set $\mathcal{Z}$ to find the M eigenvectors of the covariance matrix

$$\mathbf{S}_{\text{cov}} = \frac{1}{M}\sum_{i=1}^{C}\sum_{j=1}^{C_i}\left(\mathbf{z}_{ij} - \bar{\mathbf{z}}\right)\left(\mathbf{z}_{ij} - \bar{\mathbf{z}}\right)^T, \tag{9}$$

where $\bar{\mathbf{z}} = (1/M)\sum_{i=1}^{C}\sum_{j=1}^{C_i}\mathbf{z}_{ij}$ is the average of the ensemble. The Eigenfaces are the first $N(\leq M)$ eigenvectors corresponding to the largest eigenvalues, denoted as Ψ. The original image is transformed to the N-dimension face space by a linear mapping

$$\mathbf{y}_{ij} = \Psi^T\left(\mathbf{z}_{ij} - \bar{\mathbf{z}}\right). \tag{10}$$

PCA produces the most expressive subspace for face representation but is not necessarily the most discriminating one. This is due to the fact that the underlying class structure of the data is not considered in the PCA technique. Linear Discriminant Analysis (LDA) is a supervised learning technique that provides a class specific solution. It produces the optimal feature subspace in such a way that the ratio of between-class scatter and within-class scatter is maximized. Although LDA-based algorithms are superior to PCA-based methods in some cases, it is shown in [44] that PCA outperforms LDA when the training sample size is small and the training images is less representative of the testing subjects. This is confirmed in [38] that PCA performs much better than LDA in a generic learning scenario, where the image samples of the human subjects are not available for training. It was also shown in [38] that KDDA outperforms other techniques in most of the cases. Therefore we also adopt KDDA in this paper.

Figure 6: Comparison of original image with reconstructed images.

Figure 7: Example images for identification (top row) and verification (bottom row).

KDDA was proposed by Lu et al. [45] to address the nonlinearities in complex face patterns. Kernel-based solution find a nonlinear transform from the original image space $\mathcal{R}^J$ to a high-dimensional feature space $\mathcal{F}$ using a nonlinear function $\phi(\cdot)$. In the transformed high-dimensional feature space $\mathcal{F}$, the convexity of the distribution is expected to be retained so that traditional linear methodologies such as PCA and LDA can be applied. The optimal nonlinear discriminant feature representation of $\mathbf{z}$ can be obtained by

$$\mathbf{y} = \Theta \cdot \nu(\phi(\mathbf{z})), \tag{11}$$

where Θ is a matrix representing the found kernel discriminant subspace, and $\nu(\phi(\mathbf{z}))$ is the kernel vector of the input $\mathbf{z}$. The detailed implementation algorithm of KDDA can be found in [45].

4.3. Experimental Results on Face Identification. For face identification, we use all the 5676 images in the data set for experiments. A set of 2836 images from 520 human subjects was randomly selected for training, and the rest of 2840 images from 500 subjects for testing. There is no overlap between the training and testing subjects and images. The test is performed on an exhaustive basis, such that each time, one image is taken from the test set as probe image, while the rest of the images in the test set as gallery images. This is repeated until all the images in the test set were used as the probe once. The classification is based on nearest neighbor.

Table 2 compares the correct recognition rate (CRR) of SIN method with Euclidean and Cosine distance measures at different dimensions. It can be observed that at higher dimensionality, the SIN method may boost the recognition accuracy of PCA significantly, while maintain the good performance of the stronger feature extractor KDDA. The PCA method projects images to directions with highest variance, but not the discriminant ones. This will become more severe in large image variations due to illumination, expression, pose, and aging. When computing the similarity between two PCA vectors, the distance measure is sensitive to the variation of individual element, particularly those directions corresponding to noise. The SIN method, on the other hand, reduces this sensitivity by simply comparing the relative

Table 2: Face identification results (in %).

	PCA			KDDA		
Dim.	Euc.	Cos.	SIN	Euc.	Cos.	SIN
20	56.30	56.31	52.32	40.04	41.09	34.86
40	60.09	61.09	61.94	61.44	65.28	61.94
60	63.52	62.96	66.06	71.73	74.86	74.68
80	64.37	64.44	68.84	81.76	83.27	81.76
100	65.14	65.18	71.27	79.05	80.42	80.07

Table 3: Verification data set configuration.

Database	No. of subjects	No. of images per subject	No. of images
FERET	750	≥2	3029
AR	119	4	476
Aging	63	≥3	276
BioID	20	≥6	227
PIE	68	≥8	658
Total	1020	≥2	4666

Table 4: Obtained EER (in %) for face verification.

	PCA			KDDA		
Dim.	Euc.	Cos.	SIN	Euc.	Cos.	SIN
20	20.05	19.23	13.78	25.22	20.42	20.97
40	19.09	17.81	11.46	21.49	16.22	14.54
60	18.52	17.42	10.28	18.80	13.41	10.97
80	18.50	17.15	9.72	10.96	9.90	7.19
100	18.20	16.94	9.46	10.41	8.84	6.52

relation of the projections, and therefore possibly provides better error tolerance. In the case of strong extractors such as KDDA, the SIN method will approximate the distance between two vectors and hence preserves the recognition accuracy.

4.4. Experimental Results on Face Verification. For face verification, we exclude image samples with large pose variation (>15°) and select 4666 images from 1020 subjects for our experiments. Table 3 illustrates the detailed configuration of the verification data set. In our experiments, we randomly select 2388 images from 520 subjects as the training set, and 2278 images of the rest 500 subjects as the testing set. There is no overlap between the training and the testing subjects and images. The evaluation was also performed on an exhaustive basis, where every single image is used as a template once, and the rest of the images in the test set as the probe images.

Table 4 compares the obtained equal error rate (EER) of SIN with Euclidean and Cosine distance at different dimensions when PCA and KDDA are used as feature extractors. In general, the Cosine metric outperforms the Euclidean distance measure, and the proposed SIN method improves both the verification accuracy of PCA and KDDA at almost all dimensions. This further demonstrates that the sorted index numbers indeed offer better error tolerance and provide more discriminant representation.

4.5. Changeable Face Verification. To enhance the privacy protection level as well as addressing the irrevocable problem of biometric verification systems, this paper adopts the random projection method. For the purpose of comparative study, we compared the performance of the proposed method with that of the BioHashing (BH) technique in this paper. For the BH method, as illustrated in [24], each of the generated BH code should have a probability of 50% to be 1 or 0. To achieve this, we centralize all the feature vectors by subtracting the mean, and then compare with the threshold value $t = 0$.

In the experiments, the same data set as the one for face verification is employed. The images for training and testing are also exactly the same as those for face verification. To minimize the effect of randomness, all the experiments were performed 5 times, and the average of the results is reported. Table 5 gives the obtained EER of BH and SIN methods in both user-independent and user-dependent scenarios at different projected dimension m, with the dimensionality of the original features set to $n = 100$.

In the user-independent scenario, all the users apply the same RP matrix. In the user-dependent scenario, different users have distinct RP matrices. The user-dependent scenario is essentially a two-factor scheme, and it requires correct presentation of both the RP matrix (or a generation key) and biometrics data. The proposed user-dependent scheme assumes that the RP matrix and the biometrics data can not be stolen at the same time. If the RP matrix is stolen, the evaluation can be performed by considering the worst case that the key of all the users is stolen by others. This is equivalent to use the same random projection matrix for all the users. Therefore, the performance of stolen key case will be the same as the user-independent scenario. If only the biometric data is stolen, then the performance will be the same as the both-legitimate case due to the randomness of the transformation, as discussed in Section 3.3.

The experimental results in Table 5 show that the proposed SIN method outperforms the BH method in both user-dependent and user-independent scenarios, at all dimensions, when PCA and KDDA are used as feature extractors. Although the previous works on BH demonstrate near zero EER in both-legitimate cases, the performance of it depends on the characteristics of the data and feature extractors. For an m bit BioHash code $\mathbf{b}$, assume that each bit in $\mathbf{b}$ is independent, let τ be the threshold value in terms of Hamming distance, then the probability of false accept $P(\mathbf{H}_0 \mid \mathbf{H}_1) = \sum_{i=0}^{\tau} \binom{m}{i} / 2^n$. This probability depends on two factors, the system threshold τ and dimension m, which reflect the separability and characteristics of the data and feature extractors. Figure 8 shows the intra-class and inter-class distribution of the generic data set. It can be observed that the SIN method provides better distribution separation than the BH method, in both user-independent and user-dependent scenarios, with both PCA and KDDA feature extractors. This demonstrates that the proposed SIN method

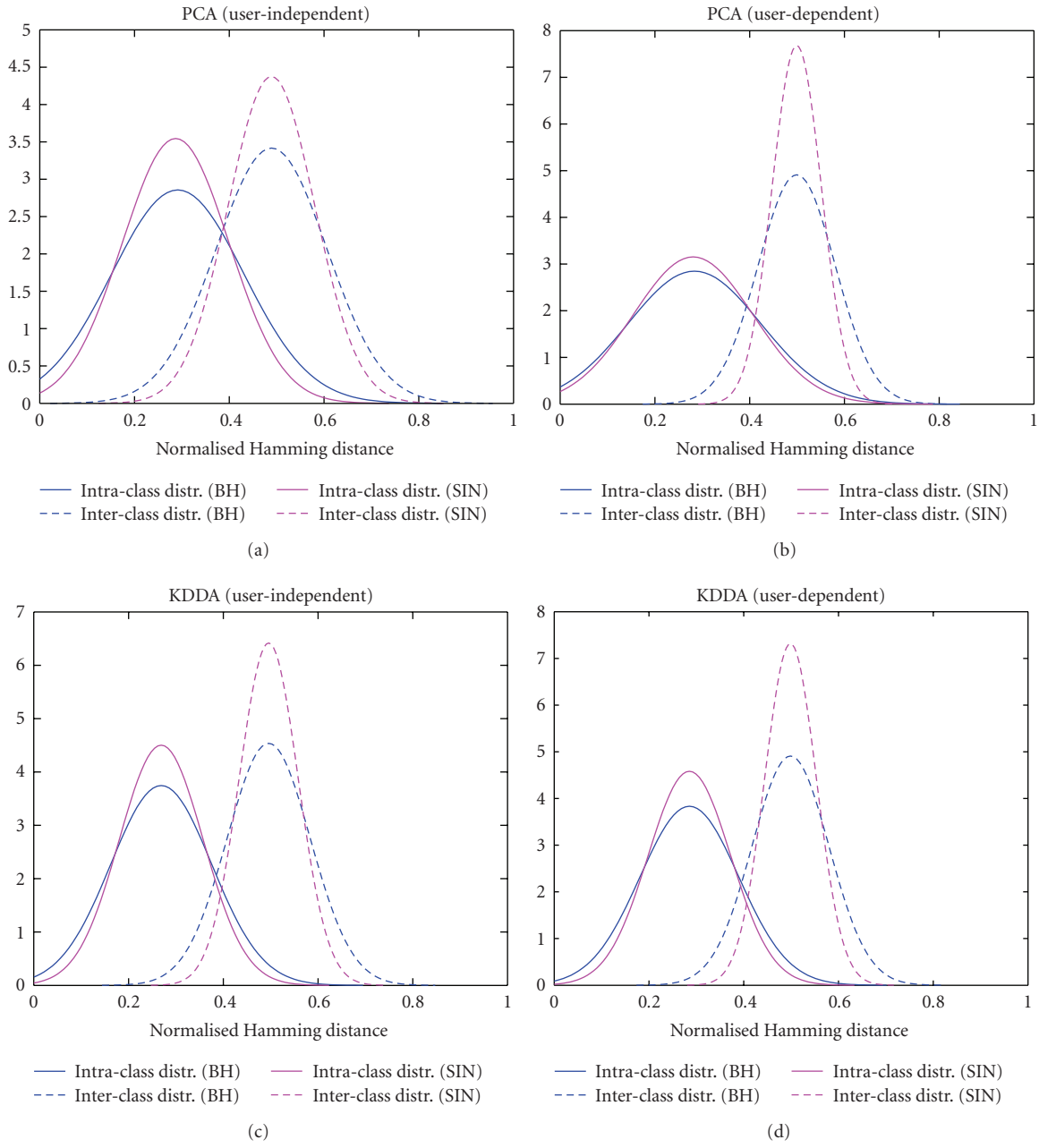

Figure 8: Intra-class and inter-class distributions of SIN and BH, using PCA and KDDA feature extractors, in both user-independent and user-dependent scenarios.

Table 5: Obtained EER (in %) for changeable face verification.

	PCA				KDDA			
	User-dependent		User-independent		User-dependent		User-independent	
Dim.	BH	SIN	BH	SIN	BH	SIN	BH	SIN
20	22.13	16.92	25.25	20.82	18.77	12.96	18.63	13.58
40	17.80	13.44	21.43	18.69	13.03	7.70	13.96	9.23
60	15.54	11.76	19.24	17.63	9.85	5.68	10.92	7.38
80	14.38	10.76	18.34	17.18	7.97	4.54	9.37	6.64
100	12.98	9.89	17.79	16.83	6.84	3.83	8.63	6.05

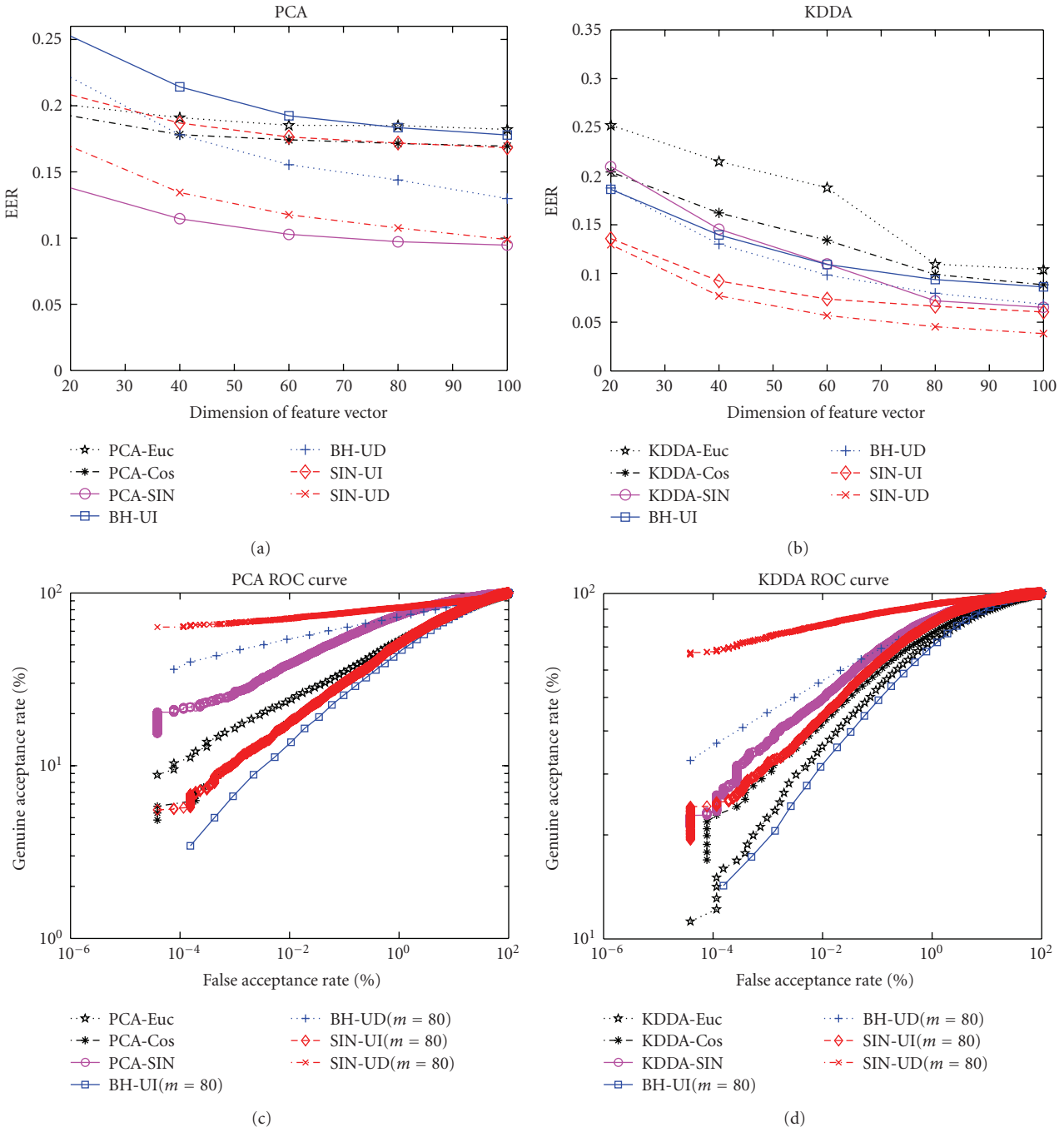

Figure 9: Obtained EER and ROC plots for PCA and KDDA (UI: user-independent, UD: user-dependent).

provides more discriminant representation than the simple thresholding method in BioHashing.

For a complete comparison, Figure 9 plots the EER of all verification scenarios as well as the Receiver Operating Curve (ROC) for both feature extractors at dimensionality of 100. The ROC curve is plotted by Genuine Acceptance Rate (GAR, complement of FRR) against FAR, and the axes are log scaled for better visualization. When the SIN method is applied on facial features directly, it improves the verification accuracy for both feature extractors. In the user-independent scenario of PCA, the verification accuracy is degraded compared to apply SIN directly on PCA features. This is possibly due to the randomness of RP changes the inherent pairwise relations of original PCA features, and therefore the SIN method can not produce more discriminant representation, but approximate the Euclidean distance only. In spite of this, it can be observed that by integrating the RP transform, the proposed SIN method introduces changeability, enhances privacy protection, and achieves better performance than original features, as well as existing work.

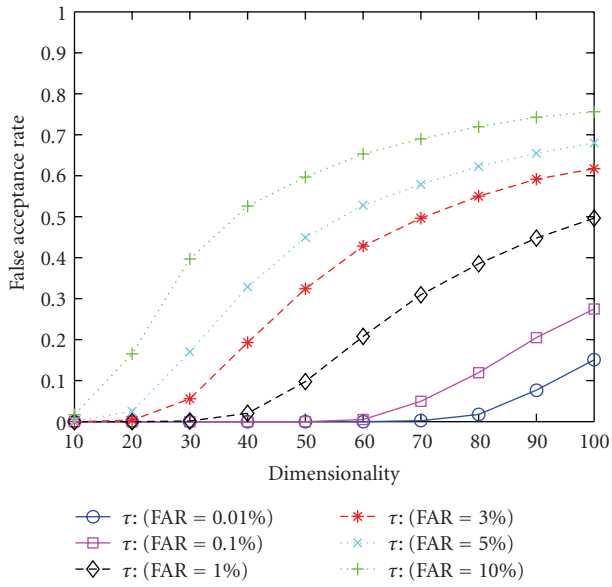

Figure 10: Experimental results based on reconstructed images.

4.6. Experimental Results on Reconstructed Images. To further study the privacy preserving property of the proposed method, we performed experiments on reconstructed images from the estimated PCA coefficients. The original n-dimensional PCA features are projected onto an m-dimensional vector, and the resulting SIN vector is stored as templates. Considering the worst case that the SIN vector, the random projection matrix, the PCA transformation matrix, and the mean image are all obtained, an adversary can reconstruct the original image using the method discussed in Section 3.4. The adversary may then try to compromise the user using the reconstructed image. Figure 10 reports the false acceptance rate obtained when the reconstructed images are utilized to compromise the original PCA-based system. The dimensionality of the PCA vectors is $n = 100$. All the PCA vectors are normalized to unit length, and Euclidean distance is adopted as dissimilarity measure. The system threshold values are selected based on the FAR of the original system. It can be observed that the false acceptance rate decreases as the projection dimension m decreases. This is consistent with our analysis in Section 3.4 that the privacy preserving level increases as m decreases. It can be also seen that the security level is also dependent on the system threshold of the original system, which is closely related to the requirement of the application. In general, applications that require a higher level of security will have a smaller threshold, that is, smaller FAR. In such, the proposed method can provide stronger privacy protection even at a relatively higher projected dimension. On the other hand, when the τ is large, it requires smaller projected dimension m to achieve higher level of security. However, as shown in Figure 9, since the recognition accuracy also degrades as the m getting smaller, the proposed method has a tradeoff between privacy and accuracy. The balancing point of these two is dependent on the requirement of the application.

5. Conclusion

This paper introduced a novel approach for addressing the challenging problem of changeable and privacy preserving face recognition. The proposed method is based on random projection (RP) in conjunction with a sorted index numbers (SINs) approach. A similarity measure is introduced for computing the distance between two SIN vectors. Two different scenarios, namely, user-independent and user-dependent transformation are discussed. In the user-independent scenario, all the users apply the same RP matrix for transformation. Due to the distance preserving property of RP, the similarity of features in the transformed domain can be approximately preserved. The user-dependent scenario is a two-factor authenticator that utilizes user-specific RP matrix for transformation. In both scenarios, the biometrics template can be changed by varying the RP matrix.

Experimental results on a large database demonstrate that the SIN method may improve the recognition accuracy of the original features in both identification and verification scenarios. The combination of RP and SIN method outperforms comparable existing works for all scenarios and feature extractors. In conclusion, the proposed method may improve recognition accuracy, preserve the user's privacy, and generate changeable biometric template. Although we focus on face recognition problem in this paper, the proposed method is general for continuous domain features, and it is expected that such method can also be applied to other biometrics.

Acknowledgment

Y.Wang would like to acknowledge the Natural Sciences and Engineering Research Council of Canada (NSERC) for financial support.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.

[3] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–959, 2004.

[4] A. Adler, "Vulnerabilities in biometric encryption systems," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '05)*, vol. 3546, pp. 1100–1109, Tarrytown, NY, USA, July 2005.

[5] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proceedings of the Biometrics Symposium (BSYM '07)*, Baltimore, Md, USA, September 2007.

[6] W. Zhao, R. Chellappa, A. Rosenfeld, and P. J. Phillips, "Face recognition: a literature survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, 2003.

[7] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, and W. Worek, "Preliminary face recognition grand challenge results," in *Proceedings of the 7th International Conference on Automatic Face and Gesture Recognition (FGR '06)*, pp. 15–24, Southampton, UK, April 2006.

[8] G. Shakhnarovich and B. Moghaddam, "Face recognition in subspaces," in *Handbook of Face Recognition*, S. Z. Li and A. K. Jain, Eds., Springer, New York, NY, USA, December 2004.

[9] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric encryption," in *ICSA Guide to Cryptography*, McGraw-Hill, New York, NY, USA , 1999.

[10] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 148–157, Oakland, Calif, USA, May 1998.

[11] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of 6th Conference on Computer and Communication Security (ACM '99)*, pp. 28–36, Singapore, November 1999.

[12] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[13] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, p. 408, Lausanne, Switzerland, June 2002.

[14] R. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smart card based fingerprint authentication," in *Proceedings of the ACM SIGMM Workshop on Biometrics Methods and Applications*, pp. 45–52, Berkley, Calif, USA, November 2003.

[15] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '05*, vol. 3546, pp. 310–319, Hilton Rye Town, NY, USA, July 2005.

[16] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '04)*, pp. 523–540, Interlaken, Switzerland, May 2004.

[17] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–511, 2007.

[18] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 82–91, Washington, DC, USA, October 2004.

[19] T. A. M. Kevenaar, G. G. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in *Proceedings of the 4th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID '05)*, pp. 21–26, Buffalo, NY, USA, October 2005.

[20] M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proceedings of the 17th International Conference on Pattern Recognition*, pp. 922–925, Cambridge, UK, August 2004.

[21] M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla, "Authentication-invariant cancellable biometric filters for illumination-tolerant face verification," in *Proceedings of the IEEE International Conference Cancellable Biometric Filters for Face Recognition*, vol. 5404 of *Proceedings of SPIE*, pp. 156–163, Los Alamitos, Calif, USA, 2004.

[22] T. E. Boult, "Robust distance measures for face recognition supporting revocable biometric tokens," in *Proceedings of the 7th IEEE Conference on Face and Gesture*, Southampton, UK, April 2006.

[23] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: accuracy and security analysis," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, New York, NY, USA, June 2007.

[24] A. B. J. Teoh, D. C. L Ngo, and A. Goh, "BioHashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, pp. 2245–2255, 2004.

[25] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for dual-factor authentication," *Pattern Analysis and Applications*, vol. 7, no. 3, pp. 255–268, 2004.

[26] D. C. L. Ngo, A. B. J. Teoh, and A. Goh, "Biometric hash: high-confidence face recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 6, pp. 771–775, 2006.

[27] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.

[28] Y. Wang and K. Plataniotis, "Face based biometric authentication with changeable and privacy preserving templates," in *Proceedings of the Biometrics Symposium (BSYM '07)*, Baltimore, Md, USA, September 2007.

[29] S. Xiang, H. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," in *Proceedings of the 9th Workshop on Multimedia and Security*, pp. 121–128, Dallas, Tex, USA, September 2007.

[30] W. B. Johnson and J. Lindenstrauss, "Extensions of Lipshitz mapping into Hilbert space," *Contemporary Mathematics*, vol. 26, pp. 189–206, 1984.

[31] N. Goel and G. Bebis, "Face recognition experiments with random projection," in *Proceedings of the Defense and Security Symposium (DSS '05)*, vol. 5779 of *Proceedings of SPIE*, pp. 426–437, Orlando, Fla, USA, March 2005.

[32] E. Brigham and H. Maninila, "Random projection in dimensionality reduction: applications to image and text data," in *Proceedings of the 7th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. C245–C250, San Francisco, Calif, USA, August 2001.

[33] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Transactions on Knowledge and Data Engineering*, vol. 18, no. 1, pp. 92–106, 2006.

[34] K. Muralidhar, R. Parsa, and R. Sarathy, "A general additive data perturbation method for database security," *Management Science*, vol. 45, no. 10, pp. 1399–1415, 1999.

[35] J. T. Wang, X. Wang, K. I. Lin, D. Shasha, B. A. Shapiro, and K. Zhang, "Evaluating a class of distancemapping algorithms for data mining and clustering," in *Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 307–311, San Diego, Calif, USA, August 1999.

[36] P. J. Phillips, H. Wechsler, J. Huang, and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image and Vision Computing Journal*, vol. 16, no. 5, pp. 295–306, 1998.

[37] P. J. Phillips, H. Moon, P. J. Rauss, and S. A. Rizvi, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090–1104, 2000.

[38] J. Wang, K. N. Plataniotis, J. Lu, and A. N. Venetsanopoulos, "On solving the face recognition problem with one training sample per subject," *Pattern Recognition*, vol. 39, pp. 1746–1762, 2006.

[39] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression database," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 12, pp. 1615–1618, 2003.

[40] A. M. Martinez and R. Benavente, "The AR face database," CVC Technical report 24, 1998.

[41] Aging Database,http://www.fgnet.rsunit.com/.

[42] BioID Database, http://www.humanscan.de/support/downloads/facedb.php.

[43] M. Turk and A. Pentland, "EigenFaces for recognition," *Journal of Cognitive Neuroscience*, vol. 13, no. 1, pp. 71–86, 1991.

[44] A. M. Martinez and A. C. Kak, "PCA versus LDA," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 2, pp. 228–233, 2001.

[45] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Face recognition using kernel direct discriminant analysis algorithms," *IEEE Transactions on Neural Networks*, vol. 14, no. 1, pp. 117–126, 2003.