An Analysis of Random Projection for Changeable and Privacy-Preserving Biometric Verification

Yongjin Wang, *Student Member, IEEE*, and Konstantinos N. Plataniotis, *Senior Member, IEEE*

***Abstract*—Changeability and privacy protection are important factors for widespread deployment of biometrics-based verification systems. This paper presents a systematic analysis of a random-projection (RP)-based method for addressing these problems. The employed method transforms biometric data using a random matrix with each entry an independent and identically distributed Gaussian random variable. The similarity- and privacy-preserving properties, as well as the changeability of the biometric information in the transformed domain, are analyzed in detail. Specifically, RP on both high-dimensional image vectors and dimensionality-reduced feature vectors is discussed and compared. A vector translation method is proposed to improve the changeability of the generated templates. The feasibility of the introduced solution is well supported by detailed theoretical analyses. Extensive experimentation on a face-based biometric verification problem shows the effectiveness of the proposed method.**

***Index Terms*—Biometrics, changeability, face recognition, privacy, random projection (RP).**

I. Introduction

TRADITIONAL methods of identity verification are based on knowledge (e.g., passwords and PIN) or possession factors (e.g., ID cards and token). Such methods afford low level of security since passwords and PIN can be forgotten and acquired by covert observation, while ID cards and token can be lost, stolen, and easily forged. Biometrics-based verification systems confirm an individual's identity based on the physiological and/or behavioral characteristics of the user. Biometrics-based methods provide direct link between the service and the actual user. With biometrics, there is nothing to lose or forget, and it is relatively difficult to circumvent [1].

A biometric verification system is a one-to-one match that determines whether the claim of an individual is true. Fig. 1 shows the general block diagram of a biometric verification system. During enrollment, a feature vector $\mathbf{x}$ is extracted from the biometric data of each user and stored in the system database as a template. At the verification stage, a feature vector $\mathbf{x}'$ is extracted from the biometric signal of the authentication individual $\mathcal{U}'$ and compared with the stored template $\mathbf{x}$ of the claimed identity $\mathcal{U}$ through a similarity function S. The evaluation of a verification system can be performed in terms of hypothesis testing [2]: $\mathbf{H}_0$: $\mathcal{U}' = \mathcal{U}$, the claimed identity is correct; $\mathbf{H}_1$: $\mathcal{U}' \neq \mathcal{U}$, the claimed identity is not correct. The decision is made based on the system threshold t: $\mathbf{H}_0$ is decided if $S(\mathbf{x}, \mathbf{x}') \leq t$, and $\mathbf{H}_1$ is decided if $S(\mathbf{x}, \mathbf{x}') > t$. 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); $P(\mathbf{H}_0|\mathbf{H}_1)$], false reject rate [(FRR); $P(\mathbf{H}_1|\mathbf{H}_0)$], 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 t.

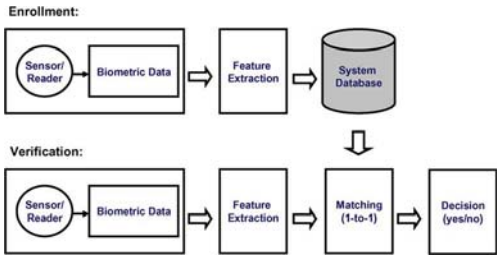


Fig. 1. General block diagram of a biometrics-based verification system.

While biometric technology provides various advantages, there exist some major problems [3].

1) *Changeability*: Biometrics cannot be easily changed or reissued if compromised due to the limited number of biometric traits that human has. Ideally, just like passwords, the users should be able to use different biometric representations 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 reissued [4].
2) *Privacy*: Biometric data reflect the user's physiological and/or behavior characteristics. If the storage device of the 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 the storage device is compromised.

One simple method to address the changeability and privacy problems is to use user-specific encryption keys to encrypt the biometric data during enrollment and decrypt at the time of authentication. However, this method provides limited privacy protection since the original biometric template will be exactly recovered if the key is stolen. To deal with this, a number of research works have been proposed in recent years. One approach is to combine biometric technology with cryptographic systems [4]. In a biometric cryptosystem, a randomly generated cryptographic key is bound with the biometric features in a

Manuscript received November 18, 2008; revised May 3, 2009 and September 17, 2009; accepted October 16, 2009. Date of publication January 15, 2010; date of current version September 15, 2010. The work of Y. Wang was supported by the Natural Sciences and Engineering Research Council of Canada. This paper was recommended by Associate Editor H. Qiao.

The authors are with The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: ywang@comm.utoronto.ca; kostas@comm.utoronto.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMCB.2009.2037131

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 the 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 the continuous domain. Although discrete features can be obtained by quantization, such methods usually suffer degradation of performance due to the quantization error. Furthermore, the security level of such methods still needs to be further investigated [5], [6].

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 verification problem can be formulated as follows: Given a biometric feature vector $\mathbf{y}$, the biometric template $\mathbf{x}$ is generated through a generation function $\mathbf{x} = Gen(\mathbf{y}, \mathbf{k})$. Different templates can be generated by varying the control factor $\mathbf{k}$. During verification, the same transformation is applied to the authentication feature vector $\mathbf{x}' = Gen(\mathbf{y}', \mathbf{k})$, and the matching is based on a similarity measure in the transformed domain, i.e., $S(\mathbf{x}, \mathbf{x}')$. The major challenge here lies in the difficulty of preserving the similarity measure in the transformed domain, i.e., $S(\mathbf{x}, \mathbf{x}') \approx S(\mathbf{y}, \mathbf{y}')$. Furthermore, to ensure the property of privacy protection, the generation function $Gen(\mathbf{y}, \mathbf{k})$ should be noninvertible such that $\widehat{\mathbf{y}} = Rec(\mathbf{x}, \mathbf{k}) \neq \mathbf{y}$, where $Rec(\mathbf{x}, \mathbf{k})$ denotes the reconstruction function when both the template $\mathbf{x}$ and the control factor $\mathbf{k}$ are known.

In this paper, we present a systematic analysis of random projection (RP) as an intentional, repeatable, and noninvertible transformation for a changeable and privacy-preserving biometric template generation. RP has been used as a dimensionality reduction or privacy-preserving tool for various applications in the literature. Recently, it has also been applied as a privacy-preserving tool in biometrics [7]. In this paper, we elaborate its application in biometric verification as both dimensionality reduction and privacy-preserving tools. This paper contributes comprehensive and detailed mathematical analysis on the similarity-preserving and privacy protection properties of RP. A vector-translation-based technique is introduced to enhance the changeability of the generated biometric template. The proposed method is capable of producing templates with zero FAR when the projection matrix is changed, which indicates strong changeability. This is well supported by both the probabilistic analysis and extensive experimentation.

In this paper, we demonstrate the feasibility of the proposed method in a face-verification scenario due to high user acceptability, easy to capture, and low-cost properties of face biometrics. The proposed framework can find wide applications in physical access control, ATM, and computer/network login. The remainder of this paper is organized as follows. In Section II, we review the related works. Section III introduces the proposed methods and provides detailed analysis. Experimental results, along with the detailed discussion, are presented in Section IV. Finally, conclusions are provided in Section V.

II. Related Works

The design of a privacy-preserving biometric system critically depends on the characteristics of the biometric data and features. Many tentative solutions have been proposed in the literature using various biometrics. Among the earliest efforts, Soutar *et al.* [8] presented a correlation-based method for fingerprint verification, and Davida *et al.* [9] proposed to store a set of user-specific error correction parameters as template for an iris-based system. However, both of the works lack practical implementation and cannot provide rigorous security guarantees [4].

In [10], Juels and Wattenberg introduced an error-correction-based method, a fuzzy commitment scheme, which generalized and improved Davida's methods. The fuzzy commitment scheme assumes binary representation of biometric features, and an XOR operation is used for binding of biometrics with randomly generated keys. Hao *et al.* [11] subsequently implemented a similar scheme on an iris-based problem using a two-level error correction mechanism. Later, a polynomial-reconstruction-based scheme, fuzzy vault, was proposed by Juels and Sudan [12]. The fuzzy vault scheme works with unordered set of features, such as the minutia points in fingerprints. Lee *et al.* [13] presented a fuzzy-vault-based private-key generation system using iris features. To produce an unordered set of features for vault encoding and decoding, multiple iris features were extracted from multiple local iris patches, and the exact values of the set were generated through the k-means clustering method. The security of the fuzzy vault method is based on the difficulty of polynomial reconstruction. Although it is shown that the fuzzy vault scheme is secure in an information-theoretic sense, it is generally computationally complex and also vulnerable to attacks via record multiplicity [6].

Dodis *et al.* [14] 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 the discrete domain. Different constructions for three metric spaces, namely, Hamming distance, set difference, and edit distance, are introduced. Sutcu *et al.* [15] 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 [16] showed that the fuzzy extractor may be not secure for multiple uses of the same biometric data.

Ratha *et al.* [17] introduced a framework of generating cancelable fingerprint templates. A few different methods, including Cartesian, polar, and surface folding transformations of the minutia positions, are discussed analytically and empirically. This paper demonstrates the revocability and noninvertibility of the proposed transformations and anticipates that the feature-level cancelable biometric construction can be applied in large biometric deployments. However, this paper focuses on fingerprints whose features are usually a set of unordered minutia positions, and the number of minutia points is variable. It is not clear how such methods can be applied to other biometrics such as face and iris, whose features are usually of fixed length and order.

Kevenaar *et al.* [18] proposed a helper data system for generation of renewable and privacy-preserving binary templates. A set of fiducial points is first identified from six key objects of

a 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 bits with a randomly generated key through an XOR operation, and a Bose–Chaudhuri–Hocquenghem (BCH) code is applied for error correction. The indexes of the selected reliable bits, 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 objects and fiducial points.

Savvides *et al.* [19] 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, a query face image is convolved with the same random kernel and then correlated 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 biometric data may be retrieved through deconvolution if the random kernel is known.

Boult [20] 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 algorithms, and the fractional part is remained for local approximation. A user-specific passcode is included to address the revocation problem. Their method demonstrates both improvements in accuracy and privacy. However, it is assumed that the private key cannot be obtained by an impostor. In the case of known private key and transform parameters, the biometric features can exactly be recovered.

Ngo *et al.* [21] introduced a BioHashing method, which produces changeable noninvertible biometric templates, and also claimed good performance. The BioHashing method is a two-factor authenticator based on user-specific RP of biometric features followed by a discretization procedure. In BioHashing, a feature vector $\mathbf{u} \in \Re^N$ is first extracted from the user's biometric data. For each user, a user-specific transformation matrix $R \in \Re^{N \times M}$, $M \leq N$, 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 $\mathbf{x} = R^{\mathrm{T}}\mathbf{u}$, and the resulting vector $\mathbf{x}$ is quantized by $\mathbf{b}_i = 0$, if $\mathbf{x}_i < \tau$, and $\mathbf{b}_i = 1$, if $\mathbf{x}_i \geq \tau$, $i = 1, 2, \ldots, M$, where τ is a predefined threshold value and usually set to zero. The binary vector $\mathbf{b}$ is stored as the template. It demonstrates zero or near-zero EER when both the biometric features and the random matrix generation key are legitimate. Theoretical analysis of the BioHashing technique is presented in [22] using the RP theory. However, the RP theory addresses the distance-preserving property in the domain of real numbers, and it is not clear how the distance is preserved in the quantized domain. The discretization procedure may also introduce degradation of verification accuracy. Moreover, it should be noted that, for a certain system threshold value, the FRR is not affected by the employment of a user-specific key. Therefore, the system threshold value that is selected for near-zero EER will produce a large FAR in the stolen-key scenario. Furthermore, for an M-bit BioHash code $\mathbf{b}$, assume that each bit in $\mathbf{b}$ is independent; let t be the threshold value in terms of the Hamming distance; then, when different keys are applied on the biometric features of the same user, the probability of false accept is $\sum_{i=0}^{t} \binom{M}{i} / 2^M$. This probability depends on two factors, the system threshold t and dimension M, which reflect the separability and characteristics of the data and feature extractors. Therefore, the changeability (as well as the performance in the user-specific key scenario) of BioHashing is highly dependent on the characteristics and the dimensionality of the extracted features [3].

Recently, Teoh and Yuang [7] have proposed a multispace RP (MRP) method, which applies user-specific RP on dimensionality-reduced feature vectors without the quantization procedure of BioHashing. The distance-preserving property of MRP is analyzed based on a normalized inner product, and a near-zero EER is achieved in the user-specific MRP scenario. However, their papers lack rigorous privacy and changeability analysis. As shown in this paper, the privacy protection of their method is subject to certain attacks. Similar to the BioHashing technique, the near-zero EER in the user-specific key scenario will produce a high FAR in the stolen-key scenario, and it does not provide strong changeability.

In this paper, we generalize the application of RP for changeable and privacy-preserving biometrics. Specifically, this paper discusses and compares the feasibility of two different approaches: 1) RP on high-dimensional biometric data vectors and 2) RP on low-dimensional biometric feature vectors (as that in [7]). This paper provides rigorous privacy analysis and demonstrates that RP on dimensionality-reduced feature vectors may provide limited privacy protection. This paper also presents a detailed analysis on the impact of utilizing different projection matrices. A vector translation method is introduced to produce biometric templates with strong changeability.

III. Methodology

This section presents the RP-based method for face-based biometric verification. We first introduce an overview of the method. The accuracy, changeability, and privacy analysis are then discussed in detail.

A. Overview of the Proposed Method

The proposed method is based on RP of face image vectors. An input image is first preprocessed by detecting the face region. The preprocessed face image $\mathbf{I}$ is converted into a vector of size $N \times 1$ by concatenating all rows of $\mathbf{I}$. The resulting vector $\mathbf{z}$ is regarded as the input vector for feature extraction. The procedure of producing the changeable and privacy-preserving biometric template is as follows.

1) Preprocess and obtain an image vector $\mathbf{z} \in \Re^N$ from the input face image.

2) Generate a new data vector $\mathbf{z}' = \mathbf{z} + \mathbf{d}$, $\mathbf{d} \in \Re^N$ and the elements $d_i \gg t$, where t is the system threshold.
3) Use a key $\mathbf{k}$ to generate an $N \times M$ $(M < N)$ random matrix R. Each entry of R is independent and identically distributed (i.i.d.) according to a Gaussian distribution of mean zero and variance $1/N$, $r_{ij} \sim \mathbf{N}(0, 1/N)$, $i = 1, \ldots, N$, $j = 1, \ldots, M$.
4) Compute $\mathbf{x} = \sqrt{N/M} R^{\mathrm{T}} \mathbf{z}'$, where the superscript T denotes transpose.

The extracted feature vector $\mathbf{x}$ is stored as the template for verification.

B. Accuracy Analysis

This section provides a detailed mathematical analysis of the similarity-preserving property of RP. RP is motivated by the Johnson–Lindenstrauss (J–L) lemma [23].

Lemma 3.1 (J–L Lemma): For any $0 < \epsilon < 1$ and an integer n, let M be a positive integer such that $M \geq M_0 = O(\epsilon^{-2} \log n)$. For any set B of n points in $\Re^N$, there exists a map f: $\Re^N \rightarrow \Re^M$ such that, for all $\mathbf{u}, \mathbf{v} \in B$

$$(1 - \epsilon)\|\mathbf{u} - \mathbf{v}\|^2 \leq \|f(\mathbf{u}) - f(\mathbf{v})\|^2 \leq (1 + \epsilon)\|\mathbf{u} - \mathbf{v}\|^2. \quad (1)$$

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-dimensional subspace. The original paper used heavy mathematical machinery to prove that such mapping can be achieved by using a random matrix with orthonormal columns. Simplified proofs of RP have been presented in [24]–[26]. In addition, Arriaga and Vempala [27], Achlioptas [28], and Li *et al.* [29] showed that it is possible to achieve such embedding through much simpler random matrices for fast operation. Vempala [30] also introduced an RP method for mapping high-dimensional binary vectors to low-dimensional ones with the Hamming distance between the binary vectors approximately preserved.

RP has been used as a dimensionality reduction or privacy-preserving tool in a wide variety of application context. Andoni and Indyk [31] introduced the locality-sensitive hashing (LSH) method to map high-dimensional vectors to low-dimensional binary code words. Every bit in the LSH code is computed by a RP followed by a random thresholding. In such, the Hamming distance between the code words approximates the Euclidean distance between the vectors. The LSH method has been applied for fast nearest neighbor search. Other applications of RP for dimensionality reduction include face recognition [32], image and text data processing [33] and clustering [34], and learning of mixture of Gaussian [35]. For privacy protection, in addition to the biometric applications in [7] and [21], RP has also been applied for data mining [36] and data clustering [37].

As illustrated in [26] and [28], the key issue in producing such distance-preserving mapping is to show that the squared length of a random vector is sharply concentrated around its mean when projected onto a random M-dimensional subspace. Then, the assertion of the J–L lemma can be proved by applying union bound on all $\binom{n}{2}$ pairs such that none of the pairwise distance can be distorted more than $(1 \pm \epsilon)$. Most of the existing works utilize inequality properties to provide a bound for the probability of distance preserving between two points and then extend to n points and compute the lower bound M_0. However, experimental results in [32] and [33] suggest that the lower bound M_0 is not tight, and it is possible to produce good results in a lower dimensionality. Therefore, we are interested in finding to what extent the distance between two vectors can approximately be preserved if they are projected to a lower dimensional subspace. This is particularly important for applications that have a high demand in storage or computational complexity. In [27] and [28], it is suggested that RP can be achieved by using a random matrix with i.i.d. Gaussian entries. Such methods do not need to conduct the computationally expensive Gram–Schmidt procedure for orthonormalization and therefore are more appropriate for practical applications. Following this line, this paper introduces a precise method for computing the probability of preserving the Euclidean distance between two vectors when projected onto an arbitrary M-dimensional subspace. The probability lower bound of preserving the pairwise distances for all n points with respect to arbitrary M is further analyzed. As will be demonstrated later, for the same probability of distance preserving for all n points, we can get a better lower bound M_0 than that shown in [28]. To begin with, we first look into the properties of a random matrix with i.i.d. Gaussian entries.

Lemma 3.2: Let R be an $N \times M$ $(M < N)$ matrix. Each entry of R is an i.i.d. Gaussian random variable with mean zero and variance $1/N$, $r_{ij} \sim \mathbf{N}(0, 1/N)$, $i = 1, \ldots, N$, $j = 1, \ldots, M$. Let $W = R^{\mathrm{T}} R$ and $W' = R R^{\mathrm{T}}$; then

$$\mathbf{E}[w_{i,j}] = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \qquad \mathbf{Var}[w_{i,j}] = \begin{cases} \frac{2}{N}, & i = j \\ \frac{1}{N}, & i \neq j \end{cases} \quad (2)$$

$$\mathbf{E}[w'_{i,j}] = \begin{cases} \frac{M}{N}, & i = j \\ 0, & i \neq j \end{cases} \qquad \mathbf{Var}[w'_{i,j}] = \begin{cases} \frac{2M}{N^2}, & i = j \\ \frac{M}{N^2}, & i \neq j \end{cases} \quad (3)$$

where $w_{i,j}$ and $w'_{i,j}$ are elements of W and W', respectively.

Proof: Please see Lemma 5.2 and Appendix I in [36] for the proof. ■

The results in Lemma 3.2 show that $\mathbf{E}[R^{\mathrm{T}} R] = I$, where I denotes an identity matrix. When N is large, the elements of $R^{\mathrm{T}} R$ are sharply concentrated around their mean with very small variance, i.e., $R^{\mathrm{T}} R \approx I$. This suggests that, in a high-dimensional space, when the entries of a random matrix R are i.i.d. Gaussian random variables, the vectors in R are almost orthogonal. The higher the dimensionality, the better the approximation of orthogonality. Intuitively, the results show that, in a high-dimensional space, vectors with random directions are very likely to be close to orthogonal [38]. In particular, it is straightforward to verify that, when $r_{ij} \sim \mathbf{N}(0, 1/N)$, $\mathbf{E}[\|\mathbf{r}_j\|^2] = \mathbf{E}[\sum_{i=1}^{N} r_{ij}^2] = 1$ and $\mathbf{Var}[\|\mathbf{r}_j\|^2] = \mathbf{Var}[\sum_{i=1}^{N} r_{ij}^2] = 2/N$, where $\mathbf{r}_j$ denotes each column of R. This demonstrates that the length of each column vector in R is strongly concentrated around one, and therefore, the vectors in R are close to orthonormal. These nice properties of the random matrix with i.i.d. Gaussian entries imply that it is possible to relax the enforced orthogonality and normality as in the original J–L lemma. Similarly, it can be shown that $\mathbf{E}[R R^{\mathrm{T}}] = (M/N) I$. When R is scaled by $\sqrt{N/M}$ and with large M, we have $\sqrt{N/M} R \sqrt{N/M} R^{\mathrm{T}} \approx I$.

Lemma 3.3: Let $\mathbf{u}$ be an arbitrary vector in the N-dimensional Euclidean space, $\mathbf{u} \in \Re^N$. Let R be an $N \times M$ $(M < N)$ matrix. Each entry of R is an i.i.d. Gaussian random

variable with mean zero and variance $1/N$, $r_{ij} \sim \mathbf{N}(0, 1/N)$, $i = 1, \ldots, N$, $j = 1, \ldots, M$. Let $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{u}$; then

$$\mathbf{E}\left[\|\mathbf{x}\|^2\right] = \|\mathbf{u}\|^2 \quad \mathbf{Var}\left[\|\mathbf{x}\|^2\right] = \frac{2}{M}\|\mathbf{u}\|^4. \tag{4}$$

Proof: Please see the Appendix for the proof. ■

Lemma 3.3 shows that, up to a scaling factor $\sqrt{N/M}$, the squared length of an arbitrary vector is concentrated about its original one when the vector is projected onto a random M-dimensional subspace. This explains the key issue in producing distance-preserving mapping, as illustrated in [26] and [28]. The variation of the squared length is inversely proportional to the dimensionality of the projected subspace. As the dimensionality M increases, the degree of concentration becomes sharper. Lemma 3.3 can easily be extended to the following lemma.

Lemma 3.4: Let $\mathbf{u}$ and $\mathbf{v}$ be two arbitrary vectors in the N-dimensional Euclidean space, $\mathbf{u} \in \Re^N$ and $\mathbf{v} \in \Re^N$. Let R be an $N \times M$ $(M < N)$ matrix. Each entry of R is an i.i.d. Gaussian random variable with mean zero and variance $1/N$, $r_{ij} \sim \mathbf{N}(0, 1/N)$, $i = 1, \ldots, N$, $j = 1, \ldots, M$. Let $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{u}$ and $\mathbf{y} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{v}$; then

$$\mathbf{E}\left[\|\mathbf{x} - \mathbf{y}\|^2\right] = \|\mathbf{u} - \mathbf{v}\|^2 \quad \mathbf{Var}\left[\|\mathbf{x} - \mathbf{y}\|^2\right] = \frac{2}{M}\|\mathbf{u} - \mathbf{v}\|^4. \tag{5}$$

Proof: Replace $\mathbf{x}$ by $\mathbf{x} - \mathbf{y}$ and $\mathbf{u}$ by $\mathbf{u} - \mathbf{v}$ in Lemma 3.3. ■

Lemma 3.4 shows that the expectation of the squared Euclidean distance between two randomly projected vectors is the squared Euclidean distance between the two original vectors, and the variance is inversely proportional to the projected dimensionality. The higher the projected dimensionality, the smaller the variance, and hence, the better the squared Euclidean distance between two vectors in the transformed domain being preserved. Similar results of Lemma 3.4 can be found in [36]. It should be noted that, since the entries of the projection matrix R are i.i.d. Gaussian random variables, for a fixed vector $\mathbf{u}$, all elements in the projected vector $\mathbf{x} = R^{\mathrm{T}}\mathbf{u}$ are also independent Gaussian random variables. This is due to the two-stability of the Gaussian distribution [28]: For any real numbers $\mu_1, \mu_2, \ldots, \mu_d$, if $\{q_i\}_{i=1}^d$ is a family of independent Gaussian random variables with zero mean and unit variance, let $\mathbf{X} = \sum_{i=1}^d \mu_i q_i$; then, $\mathbf{X} \sim c\mathbf{N}(0, 1)$, where $c = (\mu_1^2 + \cdots + \mu_d^2)^{1/2}$. Similarly, for a vector $\mathbf{u} - \mathbf{v}$, the elements of $R^{\mathrm{T}}\mathbf{u} - R^{\mathrm{T}}\mathbf{v} = R^{\mathrm{T}}(\mathbf{u} - \mathbf{v})$ are independent Gaussian random variables.

Lemma 3.5: For any $\epsilon > 0$ and an integer M, let $\mathbf{u}$ and $\mathbf{v}$ be two arbitrary vectors in the N-dimensional Euclidean space, $\mathbf{u} \in \Re^N$ and $\mathbf{v} \in \Re^N$. Let R be an $N \times M$ $(M < N)$ matrix. Each entry of R is an i.i.d. Gaussian random variable with mean zero and variance $1/N$, $r_{ij} \sim \mathbf{N}(0, 1/N)$, $i = 1, \ldots, N$, $j = 1, \ldots, M$. Let $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{u}$ and $\mathbf{y} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{v}$; then

$$\begin{aligned} &P\left((1-\epsilon)\|\mathbf{u} - \mathbf{v}\|^2 \le \|\mathbf{x} - \mathbf{y}\|^2 \le (1+\epsilon)\|\mathbf{u} - \mathbf{v}\|^2\right) \\ &\quad = G\left(\frac{M}{2}, \frac{(1+\epsilon)M}{2}\right) - G\left(\frac{M}{2}, \frac{(1-\epsilon)M}{2}\right) \end{aligned} \tag{6}$$

where $G(a, x)$ is the regularized gamma function, $G(a, x) = (1/\Gamma(a))\int_0^x e^{-t}t^{a-1}dt$, and Γ denotes the gamma function [39].

Proof: Let x_j and u_i denote the elements of vectors $\mathbf{x}$ and $\mathbf{u}$, respectively; we have

$$\begin{aligned} \mathbf{E}[x_j] &= \mathbf{E}\left[\sum_{i=1}^N \sqrt{\frac{N}{M}} r_{ij}u_i\right] = \sqrt{\frac{N}{M}}\sum_{i=1}^N \mathbf{E}[r_{ij}]u_i = 0 \\ \mathbf{Var}[x_j] &= \mathbf{Var}\left[\sum_{i=1}^N \sqrt{\frac{N}{M}} r_{ij}u_i\right] = \frac{N}{M}\sum_{i=1}^N \mathbf{Var}[r_{ij}u_i] \\ &= \frac{N}{M}\sum_{i=1}^N \left(\mathbf{E}\left[r_{ij^2}u_i^2\right] - \mathbf{E}[r_{ij}u_i]^2\right) \\ &= \frac{N}{M}\sum_{i=1}^N \mathbf{E}\left[r_{ij^2}u_i^2\right] = \frac{N}{M}\sum_{i=1}^N \frac{1}{N}u_i^2 = \frac{1}{M}\|u\|^2. \end{aligned}$$

Therefore, $\sqrt{M/\|u\|^2}x_j \sim \mathbf{N}(0, 1)$. Since the elements of $\mathbf{x}$ are independent, let $\mathbf{Z} = (M\|\mathbf{x}\|^2)/\|\mathbf{u}\|^2$; then, the random variable $\mathbf{Z}$ is distributed according to a chi-square distribution. Replace $\mathbf{x}$ and $\mathbf{u}$ by $\mathbf{x} - \mathbf{y}$ and $\mathbf{u} - \mathbf{v}$, respectively; then, $\mathbf{Z} = (M\|\mathbf{x} - \mathbf{y}\|^2)/\|\mathbf{u} - \mathbf{v}\|^2$ also follows a chi-square distribution with degree of freedom M. We have

$$\begin{aligned} &P\left(\|\mathbf{x} - \mathbf{y}\|^2 \le (1+\epsilon)\|\mathbf{u} - \mathbf{v}\|^2\right) \\ &\quad = P\left(\mathbf{X} \le (1+\epsilon)M\right) = G\left(\frac{M}{2}, \frac{(1+\epsilon)M}{2}\right) \\ &P\left(\|\mathbf{x} - \mathbf{y}\|^2 \le (1-\epsilon)\|\mathbf{u} - \mathbf{v}\|^2\right) \\ &\quad = P(\mathbf{X} \le (1-\epsilon)M) = G\left(\frac{M}{2}, \frac{(1-\epsilon)M}{2}\right). \end{aligned}$$

Hence

$$\begin{aligned} &P\left((1-\epsilon)\|\mathbf{u} - \mathbf{v}\|^2 \le \|\mathbf{x} - \mathbf{y}\|^2 \le (1+\epsilon)\|\mathbf{u} - \mathbf{v}\|^2\right) \\ &\qquad = G\left(\frac{M}{2}, \frac{(1+\epsilon)M}{2}\right) - G\left(\frac{M}{2}, \frac{(1-\epsilon)M}{2}\right). \end{aligned}$$

Equation (6) provides a precise method for computing the probability of preserving the squared Euclidean distance between two vectors in the projected subspace. Fig. 2(a) shows the probability as a function of dimensionality M and error ϵ. It can be observed that, for any fixed error ϵ, the probability of preserving the distance between two vectors increases as the projected dimensionality increases. On the other hand, for any fixed projected dimensionality, the larger the error factor, the higher the probability of distance preserving. For example, even when projected to a low dimensionality of $M = 200$, with probability of 99.68%, the Euclidean distance between two vectors can be preserved up to an error factor of $\epsilon = 0.3$. ■

Having obtained the probability of preserving the distance between two fixed points, now, we can apply the union bound to analyze the probability of preserving the pairwise distance for all n points. Let α denote the probability in (6); then, for each of the $\binom{n}{2}$ pairs, the probability of distortion that is larger than $(1 \pm \epsilon)$ is $1 - \alpha$. For all the $\binom{n}{2}$ pairs, the chance of some pairs that do not preserve the distance is at most $\binom{n}{2} \times (1 - \alpha)$. Hence, the probability of preserving the pairwise distance for all the pairs simultaneously is $1 - \binom{n}{2} \times (1 - \alpha)$. This proves the following lemma.

Lemma 3.6: For any $\epsilon > 0$ and an integer M, let any set B of n points in $\Re^N$ be represented as a matrix D of size $N \times n$. Let R be an $N \times M$ $(M < N)$ matrix. Each entry of R is an i.i.d. Gaussian random variable with mean zero and variance

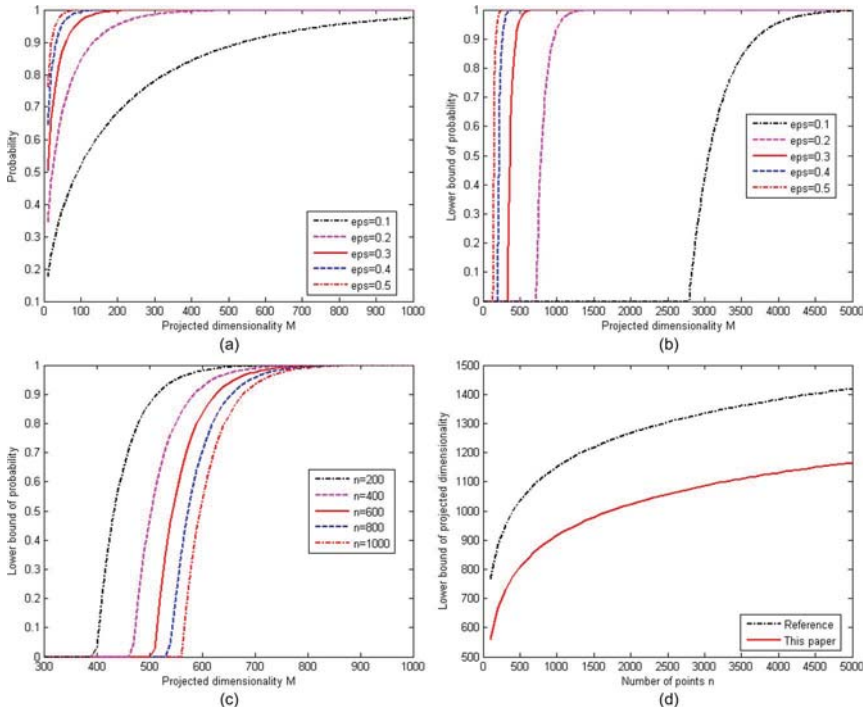


Fig. 2. (a) Probability of pairwise distance preserving as a function of M and ϵ. (b) Probability of distance preserving for all n points as a function of M and ϵ. (c) Probability of distance preserving for all n points as a function of M and n. (d) Comparison of the lower bound of M with that in [37].

$1/N$, $r_{ij} \sim \mathbf{N}(0, 1/N)$, $i = 1, \ldots, N$, $j = 1, \ldots, M$. Let $A = \sqrt{N/M}R^{\mathrm{T}}D$, and f denotes the map $\Re^N \rightarrow \Re^M$ from the ith column of D to the ith column of A. Then, with probability of at least $1 - \binom{n}{2} \times (1 - \alpha)$, for all $\mathbf{u}, \mathbf{v} \in B$

$$(1-\epsilon)\|\mathbf{u}-\mathbf{v}\|^2 \leq \|f(\mathbf{u}) - f(\mathbf{v})\|^2 \leq (1+\epsilon)\|\mathbf{u}-\mathbf{v}\|^2$$

where $\alpha = G(M/2, ((1+\epsilon)M)/2) - G(M/2, ((1-\epsilon)M)/2)$.

Lemma 3.6 offers a probability lower bound of distance preserving for all n points when projected onto an arbitrary M-dimensional subspace. It can be seen that the similarity-preserving property is determined by three factors, namely, the cardinality n, the error factor ϵ, and the projected dimensionality M. In a pattern recognition problem, the error factor ϵ depends on a discriminant power of data vectors, and the cardinality n depends on the number of classes. Fig. 2(b) shows the probability lower bound as a function of M and ϵ with fixed n. It can be observed that, for an n-class problem, if the original data vectors are well separated, i.e., it can tolerate large error, even with a lower dimensionality, the pairwise distances of all the points can be well preserved. Fig. 2(c) shows the relation of M and n with fixed ϵ. It can be observed that, when n is getting larger, the requirement of increasing the corresponding M becomes less stringent since, still with high probability, the distances can be well preserved. Therefore, with properly selected M, the projection does not need to be altered when n increases insignificantly. This is important for applications such as biometrics since we may not want to change the projection whenever a new user is added to the system.

Different from existing work [28], which uses inequality properties to analyze the distance-preserving probability between two points, this paper offers a method to compute the exact probability of pairwise distance preserving. A direct gain of this is the possibility of lowering the lower bound of the required projection dimensionality M_0. To verify this, Fig. 2(d) shows the lowest required projection dimensionality M according to Lemma 3.6, with the lower bound M_0 provided in [28], which, to our knowledge, is the best-known bound. In [28], it was shown that, with probability of at least $1 - n^{-\beta}$, where β controls the probability of success, the pairwise distance between all n points can be preserved when projected onto a lower bound of $M_0 = \lceil (4+2\beta)(\epsilon^2/2 - \epsilon^3/3)^{-1} \log n \rceil$. In the plot, the probability lower bound is set to $1 - (1/n)$ (corresponds to $\beta = 1$ in [28]). It can be seen that our analysis gets better dimensionality lower bound M_0 than illustrated in [28].

C. Changeability Analysis

In the proposed method, the biometric templates can be changed by simply varying the RP matrix. To ensure strong changeability, the biometric templates that are generated from the same user, using different RP matrices, should not be able to authenticate each other. Let us consider a scenario where an impostor compromises the template of a user. The user canceled the old template and generated a new one by using a different RP matrix. The impostor then tries to authenticate as the true user using the old template. Throughout this paper, we use the subscripts P and G to represent the probing template and the newly generated template of the claimed identity, respectively. Since different projection matrices are used, therefore, $R_P \neq R_G$. To quantify the probability of error and illustrate the importance of translating the biometric data, we first consider a case where RP is applied on the biometric data directly, i.e., $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{z}$.

Assume that $\sqrt{N/M}R_P = UQ_P$ and $\sqrt{N/M}R_G = UQ_G$, where U is an $N \times M$ matrix, with each entry an i.i.d. Gaussian random variable with mean zero and variance $1/N$, and Q_P and Q_G are two matrices of size $M \times M$. From Lemma 3.2,

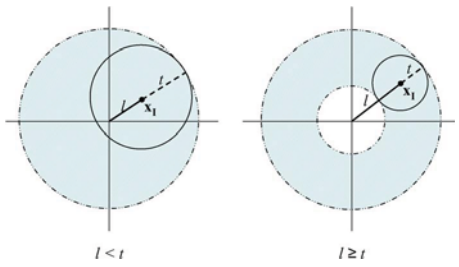


Fig. 3. Demonstration of computing the probability of error in a 2-D space.

$U^{\mathrm{T}}U \approx I$; we have $Q_P = \sqrt{N/M}U^{\mathrm{T}}R_P$ and $Q_G = \sqrt{N/M}U^{\mathrm{T}}R_G$. Due to the two-stability of the Gaussian distribution, the elements of Q_P and Q_G are also Gaussian random variables with zero mean and variance $1/M$, and the columns are almost orthonormal. Therefore, the problem can be formulated as $\mathbf{x}_P = \sqrt{N/M}R_P^{\mathrm{T}}\mathbf{z}_P = (UQ_P)^{\mathrm{T}}\mathbf{z}_P = Q_P^{\mathrm{T}}(U^{\mathrm{T}}\mathbf{z}_P)$ and $\mathbf{x}_G = \sqrt{N/M}R_G^{\mathrm{T}}\mathbf{z}_G = (UQ_G)^{\mathrm{T}}\mathbf{z}_G = Q_G^{\mathrm{T}}(U^{\mathrm{T}}\mathbf{z}_G)$. It is equivalent to first project the biometric data using the same projection matrix U and then transform the projected feature vector using different orthonormal matrices Q_P and Q_G. When the same projection matrix is applied on the biometric data, the Euclidean distance between $\mathbf{z}_P$ and $\mathbf{z}_G$ is preserved, as shown in the previous section.

For changeable biometrics, we are concerned with the probability of false accept when different transformations are applied on the biometric data of the same user, which is denoted as P_f in this paper. Accordingly, the changeability, which is the probability of a template being changeable, can be defined as $P_c = 1 - P_f$. The higher the P_c, the better the changeability. Since the transformation is random and almost orthogonal, it corresponds to the rotation of a point in the hypersphere whose radius is specified by the length (norm) of the point, i.e., the Euclidean distance between the point and the origin. We have

$$P_f = P\left(l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t, S(\mathbf{x}_G, \mathbf{x}_P) \le t\right) \tag{7}$$

where l denotes the length of the corresponding vector in the subscript, t is the system threshold, and S represents the similarity function, i.e., the Euclidean distance in this paper. As shown in Fig. 3, the computation of (7) needs to be split into two cases: $l_{\mathbf{x}_G} \le t$ and $l_{\mathbf{x}_G} > t$. In a 2-D space, $P(S(\mathbf{x}_P, \mathbf{x}_G) \le t | l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t) = \pi t^2/\pi(l_{\mathbf{x}_G} + t)^2$ when $l_{\mathbf{x}_G} \le t$, and $P(S(\mathbf{x}_P, \mathbf{x}_G) \le t | l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t) = \pi t^2/(\pi(l_{\mathbf{x}_G} + t)^2 - \pi(l_{\mathbf{x}_G} - t)^2)$ when $l_{\mathbf{x}_G} > t$. This can easily be extended to an M-dimensional space, where the volume of an M-dimensional hypersphere with radius r is defined as follows [40]: $V_M = S_M r^M/M$, where S_M is the hypersurface area of an M sphere of unit radius. In an M-dimensional space, we have

$$\begin{aligned} P_1 &= P\left(S(\mathbf{x}_P, \mathbf{x}_G) \le t | l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t, l_{\mathbf{x}_G} \le t\right) \\ &= \frac{\frac{S_M t^M}{M}}{\frac{S_M (l_{\mathbf{x}_G} + t)^M}{M}} = \frac{t^M}{(l_{\mathbf{x}_G} + t)^M} \end{aligned} \tag{8}$$

$$\begin{aligned} P_2 &= P\left(S(\mathbf{x}_P, \mathbf{x}_G) \le t | l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t, l_{\mathbf{x}_G} > t\right) \\ &= \frac{\frac{S_M t^M}{M}}{\frac{S_M (l_{\mathbf{x}_G} + t)^M}{M} - \frac{S_M (l_{\mathbf{x}_G} - t)^M}{M}} = \frac{t^M}{(l_{\mathbf{x}_G} + t)^M - (l_{\mathbf{x}_G} - t)^M} \end{aligned} \tag{9}$$

$$\begin{aligned} P_f = {} & P(l_{\mathbf{x}_G} \le t) P(l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t | l_{\mathbf{x}_G} \le t) P_1 + P(l_{\mathbf{x}_G} > t) \\ & \times P(l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t | l_{\mathbf{x}_G} > t) P_2. \end{aligned} \tag{10}$$

From (10), it is clear that the probability of error depends on the characteristics of the features, and the dimensionality M. In general, zero P_f cannot be achieved by applying RP on the biometric data directly. However, since $P(l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t | l_{\mathbf{x}_G} \le t) P_1 \le 1$ and $P(l_{\mathbf{x}_G} > t) P(l_{\mathbf{x}_G} - t \le l_{\mathbf{x}_P} \le l_{\mathbf{x}_G} + t | l_{\mathbf{x}_G} > t) \le 1$, (10) can be simplified as

$$P_f \le P(l_{\mathbf{x}_G} \le t) + \frac{t^M}{(l_{\mathbf{x}_G} + t)^M - (l_{\mathbf{x}_G} - t)^M}. \tag{11}$$

This probability can be minimized by adding an extra vector $\mathbf{d} \in \Re^N$, $d_i \gg t$, to the biometric data, $\mathbf{z}' = \mathbf{z} + \mathbf{d}$, such that, after RP, $P(l_{\mathbf{x}_G} < t) = 0$. We have

$$P_f \le \frac{t^M}{(l_{\mathbf{x}_G} + t)^M - (l_{\mathbf{x}_G} - t)^M} \tag{12}$$

$$\lim_{\frac{t}{l_{\mathbf{x}_G}} \to 0 \, \forall M} P_c = \lim_{\frac{t}{l_{\mathbf{x}_G}} \to 0 \, \forall M} (1 - P_f) = 1. \tag{13}$$

It should be noted that the addition of vector $\mathbf{d}$ does not change the similarity between two vectors since $\|R^{\mathrm{T}}(\mathbf{u}+\mathbf{d}) - R^{\mathrm{T}}(\mathbf{v}+\mathbf{d})\|^2 = \|R^{\mathrm{T}}\mathbf{u} - R^{\mathrm{T}}\mathbf{v}\|^2$. The preceding analysis shows that, with appropriate vector translation, the proposed method can produce biometric templates with changeability 1, by applying different RPs on the biometric data of the same user. The system threshold t determines the choice of vector $\mathbf{d}$. The vector $\mathbf{d}$ should be selected such that $l_{\mathbf{x}_G} \gg t$ and $P_c = 1$. This indicates the strong changeability of the proposed method.

The proposed method for changeable and privacy-preserving biometric verification can also be applied in a two-factor scheme, in which different users apply user-specific RPs. Note that, in this case, for a fixed system threshold, the FRR is the same as that in user-independent projection (same projection for all the users), since the same random matrix is still applied for the biometric data from the same user. However, with proper vector translation, the proposed method is capable of producing zero FAR in the user-specific scenario since the $\mathbf{x}_P$ in (7) can also be generated from other user's biometric data. This also explains that zero FAR can be obtained if only the biometric data are stolen (correct biometric data, wrong projection matrix). If the projection matrix is stolen, then both the FAR and FRR will be the same as the user-independent projection scenario.

D. Privacy Analysis

To preserve the privacy of the users, it is expected that no information should be disclosed if the stored biometric template is compromised. The proposed method utilizes RP for biometric template generation. Due to the randomness of a projection matrix, the user's privacy information cannot be compromised if only the template is obtained by an adversary. However, it is possible that an attacker can obtain more knowledge and estimate the original signal. In this paper, we consider three different attack scenarios.

1) Correlation attack: An attacker obtains several projections of multiple users.
2) Known projection matrix: An attacker knows the projection matrix of the user.
3) Cross matching: An attacker obtains multiple projections of the same user.

1) Correlation Attack: In this attack scenario, assume that an attacker does not know the projection matrix R. However, the attacker obtains multiple projections of multiple users and utilizes the known information to estimate R. Considering the projection model, $X = R^{\mathrm{T}}Z,\ R \in \Re^{N\times M},\ Z \in \Re^{N\times P},\ X \in \Re^{M\times P}$, where P is the number of projections that are obtained by the attacker. Each column of Z is a biometric sample (or features), and each column of X is the projected features, i.e., $X_i = R^{\mathrm{T}}Z_i,\ i = 1, \ldots, P$. Note that, without knowing the set of original vectors Z, it is impossible for an attacker to estimate the projection matrix R. If both X and Z are obtained, an attacker may estimate the projection matrix R. Assuming that the columns of Z are linearly independent, then the projection matrix can exactly be recovered $R = (XZ^{-1})^{\mathrm{T}}$ if $P = N$. When $P < N$, the projection R matrix cannot exactly be recovered, and the error of reconstruction increases as P decreases, and vice versa [41]. Therefore, given a number of original and projected features known, it is possible for an attacker to estimate the projection matrix, and the accuracy of the estimation is inversely proportional to the number of known original and projected feature pairs. However, as shown in the next section, even if the projection matrix R is exactly recovered, the privacy of the users may still be protected.

2) Known Projection Matrix: Assuming the worst case that both the template and the projection matrix are compromised, then an adversary can estimate the original biometric data. For a robust privacy-preserving mechanism, the estimated individual elements in the data vector should not be exactly the same as the original ones. Furthermore, the global characteristics of the estimated data vector should be far apart from the genuine data vector up to some similarity functions.

Considering a projection function, $\mathbf{x} = R^{\mathrm{T}}\mathbf{z},\ R \in \Re^{N\times M}$, and the entries of R are i.i.d. Gaussian random variables. An adversary tries to estimate the values of $\mathbf{z}$. Since $M < N$, this is an underdetermined system, where there are more unknowns than linear equations. There are infinitely many solutions that satisfy $\mathbf{x} = R^{\mathrm{T}}\widehat{\mathbf{z}}$. To solve this problem, one classical approach is to find the minimum norm solutions, using $\widehat{\mathbf{z}} = R(R^{\mathrm{T}}R)^{-1}\mathbf{x}$, where $R(R^{\mathrm{T}}R)^{-1}$ is essentially the pseudoinverse of R. Since $R^{\mathrm{T}}R \approx I$, the aforementioned estimation function can be simplified as $\widehat{\mathbf{z}} = R\mathbf{x}$.

However, although the estimation involves an underdetermined system, and hence, there are infinitely many solutions, it is possible that an adversary can estimate the partial of the real values and therefore reveal the partial of the user's information. If as many linearly independent equations as the unknown elements can be found, then some elements may be completely identified. To solve this problem, Du *et al.* [42] introduced the concept of *k-secure*. For a matrix R, if the remaining submatrix after removing k columns of R is still of full row rank, the matrix R is called *k-secure*, which guarantees that it is impossible to generate an equation (except the trivial zero combination) that contains less than $k + 1$ variables [42]. It is further shown in [36] and [42] that, for a matrix Υ of size $(k + 1) \times N$, where each row of Υ is a nonzero linear combination of row vectors in R, if R is *k-secure*, the linear system of equations $\mathbf{y} = \Upsilon\mathbf{x}$ involves at least $2k + 1$ unknown variables. This property illustrates that, if R is *k-secure*, any linear combinations of the equations contain at least $k + 1$ variables. Therefore, to solve the problem of identifying partial of the elements, the projected dimensionality should satisfy $M \leq (N/2)$, such that each unknown variable is disguised by at least M other variables [41]. Since it is impossible to find M linearly independent equations that involve these M variables, the solutions to each of the unknown variable are infinite, and therefore, it is impossible to find the exact value of any element in the original data vector.

Recall that the projection model in this paper is $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{z}$; we can estimate $\widehat{\mathbf{z}}$ using $\widehat{\mathbf{z}} = \sqrt{N/M}R\mathbf{x}$ [36]. Since $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{z}$, we have $\widehat{\mathbf{z}} = \sqrt{N/M}R \times \sqrt{N/M}R^{\mathrm{T}}\mathbf{z} = (N/M)RR^{\mathrm{T}}\mathbf{z}$. To analyze the statistical properties of the estimated individual element, let $\widehat{z}_i$ be the ith element of the estimated data vector; using the results in Lemma 3.2, it is straightforward to derive that

$$\mathbf{E}[\widehat{z}_i] = \mathbf{E}\left[\sum_{j=1}^{N}\frac{N}{M}w'_{i,j}z_j\right] = z_i \tag{14}$$

$$\begin{aligned}
\mathbf{Var}[\widehat{z}_i] &= \mathbf{Var}\left[\sum_{j=1}^{N}\frac{N}{M}w'_{i,j}z_j\right] \\
&= \mathbf{E}\left[\left(\sum_{j=1}^{N}\frac{N}{M}w'_{i,j}z_j\right)^2\right] - \mathbf{E}\left[\sum_{j=1}^{N}\frac{N}{M}w'_{i,j}z_j\right]^2 \\
&= \frac{N^2}{M^2}\mathbf{E}\left[\sum_{j=1}^{N}\left(w'_{i,j}\right)^2 z_j^2 + 2\sum_{j\neq k}w'_{i,j}z_jw'_{i,k}z_k\right] - z_i^2 \\
&= \frac{N^2}{M^2}\mathbf{E}\left[\sum_{j=1}^{N}(w'_{i,j})^2 z_j^2\right] - z_i^2 \\
&= \left(\frac{2}{M}+1\right)z_i^2 + \frac{1}{M}\sum_{i\neq j}z_j^2 - z_i^2 \\
&= \frac{1}{M}\sum_{i\neq j}z_j^2 + \frac{2}{M}z_i^2 = \frac{1}{M}\left(\|\mathbf{z}\|^2 + z_i^2\right).
\end{aligned} \tag{15}$$

It can be seen that the expected value of each estimated element is equal to the true value. Since no single element can exactly be recovered when $M \leq (N/2)$, the variance of $\widehat{z}_i$ can be considered as a measure of privacy.

Although the individual element in the original data vector cannot be correctly estimated, it is possible that the characteristics of the whole estimated data vector still close to the original data vector up to some similarity function. In this case, the privacy of the user still cannot be protected. To solve this problem, we should make sure that the estimated data vector has a large distance to the original one, i.e., $\|\widehat{\mathbf{z}} - \mathbf{z}\|^2 > \tau$, where τ is a privacy threshold. For a biometric verification problem, the privacy threshold value τ represents the natural variance of face images and should be set as a value that is larger than the largest possible distance between data vectors of the same human subject.

To quantify the probability of preserving privacy, we first note that the estimation error of individual elements $z_i - \widehat{z}_i$ approximates a Gaussian distribution with zero mean and variance $(\|z\|^2 + z_i^2)/M$. This is due to the fact that the elements of $W' = RR^{\mathrm{T}}$ are almost Gaussian. To validate this, we generate a random vector of size $10\,000 \times 1$ and normalize it to a unity length. This vector is considered as the data vector. A $10\,000 \times 500$ matrix is then generated randomly with each

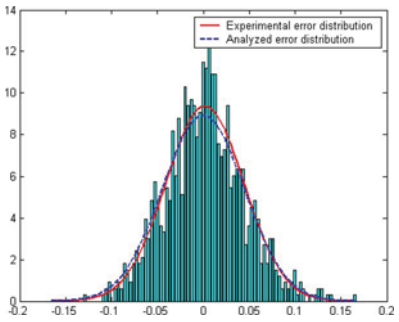


Fig. 4. Gaussian approximation of the estimation error.

entry an i.i.d. Gaussian random variable. The data vector is then projected onto the low-dimensional space using the generated random matrix, followed by a reconstruction procedure as described earlier. We repeat this process 1000 times on the same data vector using different random matrices. Fig. 4 shows the estimation error of the first element of the data vector. It can be seen that the experimental error distribution fits well with the statistics shown in (14) and (15).

For real applications, such as face recognition, the dimensionality of a face image vector N is usually large, and $|z_i|^2 \ll \|\mathbf{z}\|^2$. The expected value and variance of $\widehat{z}_i - z_i$ are $\mathbf{E}[\widehat{z}_i - z_i] = 0$ and $\mathbf{Var}[\widehat{z}_i - z_i] \approx \|\mathbf{z}\|^2/M$. Due to $\widehat{z}_i - z_i \sim \mathbf{N}(0, \|\mathbf{z}\|^2/M)$, we have $(\sqrt{M/\|\mathbf{z}\|^2})(\widehat{z}_i - z_i) \sim \mathbf{N}(0,1)$, and therefore, $(M/\|\mathbf{z}\|^2)\|\widehat{\mathbf{z}} - \mathbf{z}\|^2 = (M/\|\mathbf{z}\|^2)\sum_{i=1}^{N}(\widehat{z}_i - z_i)^2$ follows a chi-square distribution with N degree of freedom. Then, the probability of $\|\widehat{\mathbf{z}} - \mathbf{z}\|^2 > \tau$ can be computed as

$$P\left(\|\widehat{\mathbf{z}} - \mathbf{z}\|^2 > \tau\right) = P\left(\frac{M}{\|\mathbf{z}\|^2}\|\widehat{\mathbf{z}} - \mathbf{z}\|^2 > \frac{M\tau}{\|\mathbf{z}\|^2}\right) = 1 - G\left(\frac{N}{2}, \frac{M\tau}{2\|\mathbf{z}\|^2}\right) \quad (16)$$

where G denotes the regularized gamma function.

It can be seen that the probability of privacy preserving with respect to τ is associated with the dimensionality N, the squared length of the data vector $\|\mathbf{z}\|^2$, and the projected dimensionality M. When N and $\|\mathbf{z}\|^2$ are fixed, the probability value monotonically increases as M decreases. However, as shown in the previous section, the M value is also associated with the similarity-preserving property. This demonstrates that the RP-based method has a tradeoff between the privacy level and the verification accuracy. The higher the projected dimensionality, the better the accuracy, but possibly, the lower the privacy level, and vice versa.

Recall that the variance of the estimated individual element [(15)] and the probability of privacy preserving [(16)] will both increase as the squared length of the data vector $\|\mathbf{z}\|^2$ increases. Therefore, the translation vector $\mathbf{d}$, which is used to enhance the changeability, can enlarge the vector length and can be used as a complementary approach to enhance the privacy. It should be noted that, when the vector $\mathbf{d}$ is also obtained by the adversary, the privacy level is not improved and remains the same as without translation. In real applications, the $\mathbf{d}$ vector is not associated with the user's key and can be kept secret by a central control.

3) Cross Matching: In this attack scenario, an attacker obtains multiple projections of the same user. Considering the projection model, $\mathbf{x} = R^{\mathrm{T}}\mathbf{z}$, $R \in \Re^{N\times M}$, if the projection matrix R is unknown; due to the randomness of the projection, the projected vectors $\mathbf{x}$ exhibit randomness when different projections are applied on the biometric data of the same user. Therefore, even if multiple projections of the same user are obtained, without knowing the projection matrices, no information will be disclosed for reconstruction of the original vector. However, if the projection matrices are also disclosed, an attacker may be able to reconstruct the vector. For an original vector of dimension N, the projected dimension is M; let P represent the number of projections that are compromised by the attacker; if $P \geq \lceil N/M \rceil$, where $\lceil N/M \rceil$ denotes the ceiling function, then the attacker can identify N linear equations with N unknowns, and the original vector can exactly be recovered. For $P < \lceil N/M \rceil$, it is equivalent to the known projection matrix scenario that is discussed in the previous section, with the projected dimension equal to $P \times M$. The larger the P, the smaller the probability of privacy preserving [(16)].

TABLE I
GENERIC DATA SET CONFIGURATION

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

IV. EXPERIMENTAL RESULTS AND DISCUSSION

To evaluate the performance of the introduced method, we conducted experiments on a generic database that consists of face images from several well-known databases [43]. In this section, we first give a description of the employed database, followed by the experimental results, along with a detailed discussion.

A. Generic Database

The generic database was initially organized for the purpose of demonstrating the effectiveness of the generic learning framework [43]. It originally contains 5676 images of 1020 subjects from five well-known databases, namely, FERET [44], [45], PIE [46], AR [47], Aging [48], and BioID [49]. The details of image selection can be found in [43]. Since the purpose of this work is for face verification, we exclude image samples with large pose variation ($> 15^\circ$) and select 4666 images from 1020 subjects for our experiments. All images are aligned and normalized based on the coordinate information of some facial feature points. The detailed configuration of the data set is illustrated in Table I.

The color images are first transformed into gray-scale images by taking the luminance component in the YC_bC_r color space. All images are preprocessed according to the recommendation of the FERET protocol, which includes the following: 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 nonface portions; and 3) the histogram equalized and the image normalized to have

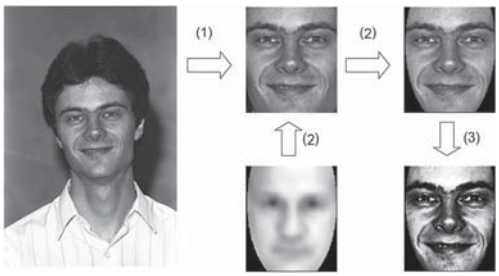


Fig. 5. Procedures for image preprocessing.

zero mean and unit standard deviation. The three steps for image preprocessing are shown in Fig. 5.

After preprocessing, the face images are converted into an image vector of dimension $N = 17\,154$. In our experiments, we randomly select samples from 520 subjects as the training set while samples of the rest 500 subjects as the testing set. The training set includes 2388 images, and the testing set contains 2278 images. There is no overlap between the training and the testing subjects. To simulate a real application, we perform evaluation on an exhaustive basis, where every single image is used as a template once and the rest of the images as the probe set. All the elements in the translation vector d_i, $i = 1, 2, \ldots, N$, are set to 100, and the same $\mathbf{d}$ is applied to all users. To minimize the effect of randomness, all the experiments were performed five times, and the average of the results is reported.

B. Experimental Results

1) RP Versus PCA: For the purpose of comparative study, we first compare the performance of RP with other dimensionality reduction tools. Principal component analysis (PCA) and linear discriminant analysis (LDA) are two of the most popular methods for dimensionality reduction and have been used extensively in the literature as powerful tools for face recognition applications. Although LDA-based algorithms are superior to PCA-based methods in some cases, it is shown in [50] that PCA outperforms LDA when the training sample size is small and the training images are less representative of the testing subjects. This is confirmed in [43] 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. Since the small-sample-size problem and unavailability of training images are common in real-life applications and PCA provides more reliable performance, we adopt the PCA algorithms for comparison in this paper.

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 [51], 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 $K = \sum_{i=1}^{C} C_i$ images, the PCA is applied to the training set $\mathcal{Z}$ to find the K eigenvectors of the covariance matrix

$$\mathbf{S}_{\text{cov}} = \frac{1}{K} \sum_{i=1}^{C} \sum_{j=1}^{C_i} (\mathbf{z}_{ij} - \bar{\mathbf{z}})(\mathbf{z}_{ij} - \bar{\mathbf{z}})^{\text{T}} \tag{17}$$

where $\bar{\mathbf{z}} = (1/K) \sum_{i=1}^{C} \sum_{j=1}^{C_i} \mathbf{z}_{ij}$ is the average of the ensemble. The eigenfaces are the first J $(\leq K)$ eigenvectors corresponding to the largest eigenvalues, denoted as Ψ. The original image is transformed into the J-dimensional face space by linear mapping: $\mathbf{y}_{ij} = \Psi^{\text{T}}(\mathbf{z}_{ij} - \bar{\mathbf{z}})$.

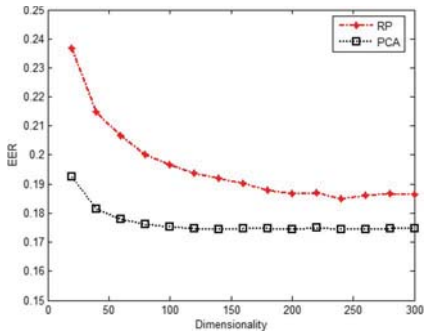


Fig. 6. EER obtained by using PCA and RP as feature extractors.

The PCA transformation matrix Ψ and the mean image $\bar{\mathbf{z}}$ are obtained based on the images in the training set, and the images in the testing set are used for evaluation. There is no overlap between the training and the testing human subjects. Since RP does not need a training process, to produce comparable results, we perform evaluation on the same set of testing images as PCA. In the report of the experimental results, RP denotes applying RP on the image vectors directly. Fig. 6 shows the EER as a function of dimensionality when RP and PCA are applied as feature extractors. It can be seen that PCA provides better EER at lower dimensions, and the verification accuracy of RP improves at higher dimensions. This is because PCA projects the image vectors to directions with the highest variance, while RP projects to random directions. As shown in Lemma 3.6, as the dimensionality M increases, with higher probability, the Euclidean distance can be preserved up to a smaller error factor, and hence, the performance improves.

Another observation is that the verification accuracy of both methods levels off after certain dimensions, 100 for PCA $(\text{EER} = 17.54\%)$ and 200 for RP $(\text{EER} = 18.68\%)$ in our experiments. For PCA, the projected features after a certain dimension will have very small variance, therefore contributing little to the classification. For RP, the verification accuracy is associated with both the dimensionality of the projected features and the discriminant power of the image vectors. When M exceeds a certain dimension, with probability one, the Euclidean distance can be preserved up to a very small error factor, and therefore, the verification accuracy depends on the separability of the original image vectors. To illustrate this, we performed experiments on the nonprojected original image vectors, where the Euclidean distance is used as a dissimilarity measure. This produces an EER of 18.19%. Fig. 7 shows the receiver operating characteristic (ROC) curves of RP $(M = 200)$ and the verification results of the original image vectors. The ROC curves are plotted by the genuine acceptance rate (complement of FRR) against FAR. It can be observed that the RP and original images have almost overlapping ROC curves. This demonstrates that the Euclidean distance of the original images can approximately be preserved. Generally, in a face recognition problem, PCA provides better discriminant representation than original noisy face images. This explains why PCA outperforms RP in our experimentation.

2) RP Versus PCARP: Although the PCA algorithm performs better than RP in general, it provides neither privacy

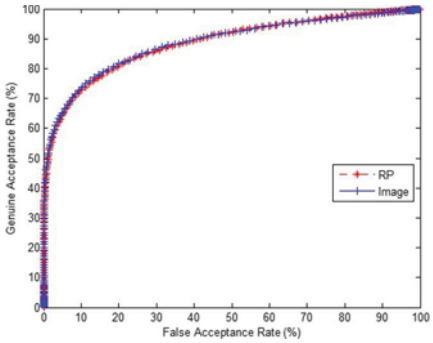


Fig. 7. ROC curve of RP and original image vectors.

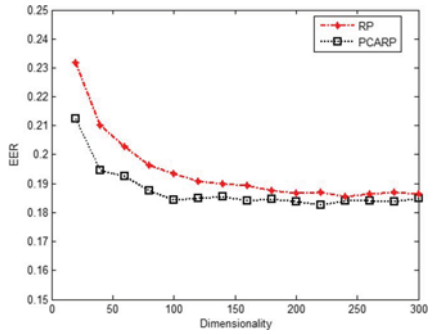


Fig. 8. EER obtained by using RP and PCARP.

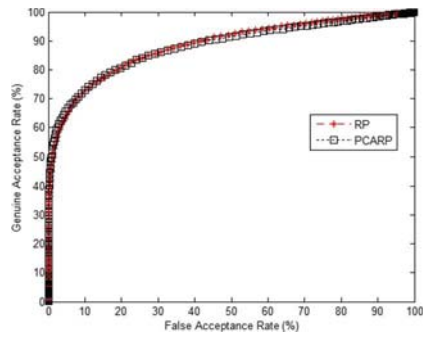


Fig. 9. ROC curves of RP and PCARP.

protection nor revocability. To solve these problems, a possible solution is to apply RP on dimensionality-reduced PCA feature vectors, as in [7]. In this paper, this method is denoted as PCARP. Due to that the original image can approximately be reconstructed from its PCA coefficients, the reveal of these PCA coefficients can be considered as a breach of privacy. To protect these PCA coefficients, the PCARP-projected features should satisfy $M \leq (J/2)$, where J is the dimensionality of the PCA feature vectors.

Fig. 8 shows the obtained EER of PCARP and RP at different M, with the dimensionality of the PCA vectors $J = 2 \times M$. Overall, RP and PCARP achieve similar performance. Due to the fact that PCA features provide better discriminant power than the original image vectors, the PCARP method requires lower dimensionality than the RP method to achieve the same accuracy. Fig. 9 shows the ROC curves of RP and PCARP at $M = 200$. It can be observed that RP and PCARP have almost overlapping ROC curves.

3) Changeability: To demonstrate the changeability of the proposed method, we performed experiments on the RP- and PCARP-projected features. The image samples from the same user are projected using different RP matrices and matched against each other. Each individual image is also matched against itself by using different projection matrices. The experiment consists of a total number of 13 922 verification attempts. The experimental results are shown in Fig. 10, where the changeability is plotted as a function of the system threshold. The system threshold is normalized such that zero represents the lowest value and one is the highest value. Since the Euclidean distance is applied as the dissimilarity measure, a smaller threshold value means lower FAR and higher FRR, and vice versa. It can be observed that, without vector translation, the changeability is dependent on the system threshold value and hence cannot produce strong changeability. On the other hand, with proper translation, it is capable of producing changeability with probability one for all selections of system threshold values, i.e., for any system. This demonstrates the strong changeability of the proposed method.

C. Discussion

The experimental results show that RP offers slight degradation in the verification accuracy comparing with the PCA-based method. However, the RP method preserves the user's privacy if the stored template is compromised. The RP-based privacy-preserving solution can be applied on either image vectors or dimensionality-reduced feature vectors. As shown in our experiments, the PCARP and RP methods produce similar performance. It is further shown that, through proper vector translation, both methods are capable of producing strong changeability, by which means that two biometric vectors that are generated from the same biometric data using different projection matrices cannot be used to authenticate each other successfully.

One advantage of the PCARP method is that it can produce similar performance at a lower dimensionality. However, the PCA-based method requires a training process, which usually involves a large number of training images, and hence, it has much higher computational requirements. Furthermore, the collection of a large number of training images poses a privacy problem. On the other hand, the RP method is data independent, does not require training, and is much easier to implement. More importantly, the PCARP method may be vulnerable to a cross-matching attack. For example, given a PCA vector of dimensionality $J = 200$, to produce a privacy-preserving template, and also highest possible accuracy, we can project the PCA features to a vector of size $M = 100$ using RP. However, if the templates of two applications that use the same PCA transformation matrix are revealed and the projection matrix for these two applications is different and also obtained, then an adversary can form a set of J linear equations with J unknowns, and the PCA feature vectors can exactly be reconstructed. By using RP directly on the image vectors, since the dimensionality of such vectors is usually very high (e.g., $N = 17\,154$ in the generic data set) and the projected dimensionality is low (e.g., $M = 200$), an adversary will need to compromise $\lceil N/M \rceil = 85$ templates from one user to recover the original image. Although it is possible to produce better verification accuracy using an advanced feature extraction method, the vulnerability to a cross-matching attack is essentially a weakness of applying RP to such

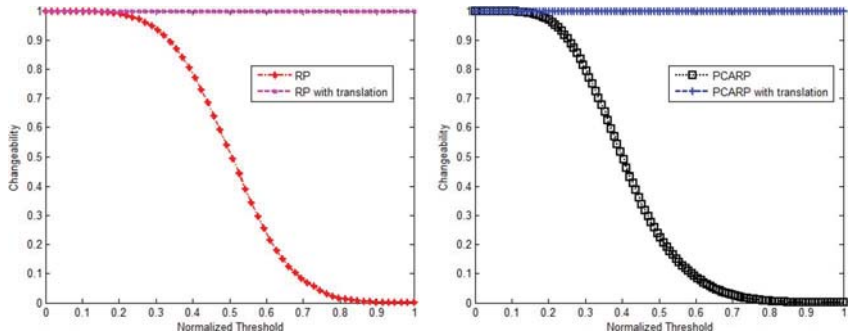


Fig. 10. Changeability as a function of the system threshold. (Left) RP and (right) PCARP.

low-dimensional feature vectors. Considering all these aspects, RP on image vectors is a more appropriate solution for privacy-preserving biometric verification.

V. Conclusion

This paper has presented a systematic analysis of the RP-based method for addressing the challenging problem of template changeability and privacy protection in biometrics-enabled verification systems. Detailed mathematical analysis shows that the similarity between two vectors can approximately be preserved when projected onto a random subspace with appropriate dimensionality. We have introduced a precise method for computing the probability of distance preserving between two points with respect to the error factor and the projected dimensionality and provided a probability lower bound of pairwise distance preserving for all the points. Our method achieves a better dimensionality lower bound than existing works. Furthermore, a geometric-based approach has been presented to analyze the impact of applying different projection matrices, and an effective method of vector translation has been introduced to improve the changeability of the generated templates.

The proposed method produces changeable biometric templates which can be achieved by simply varying the RP matrix. To explore the privacy-preserving characteristics of such a method, we have provided detailed analysis in three different attack scenarios, namely, correlation attack, known projection matrix, and cross matching. For the purpose of comparative study, we have performed computer simulations by using RP on both image vectors and PCA-reduced feature vectors. Experimental results show that these two methods have similar verification accuracy and are both capable of producing templates with strong changeability through appropriate vector translation. However, it is pointed out that better privacy protection can be obtained by applying RP on high-dimensional image vectors directly. Furthermore, such method is data independent, computationally economical, and easy to implement. In this paper, we focus on face-based biometric verification. However, the analysis is general, and it is expected that such methods can also be applied to other biometrics.

Appendix
Proof of Lemma 3.3

Let $\mathbf{x} = \sqrt{N/M}R^{\mathrm{T}}\mathbf{u}$, where $\mathbf{u} \in \Re^N$, $R \in \Re^{N\times M}$, and the entries of R are i.i.d. Gaussian random variables, $r_{ij} \sim \mathbf{N}(0, 1/N)$. Let u_i denote the elements of $\mathbf{u}$; we have

$$\begin{aligned}\mathbf{E}\left[\|\mathbf{x}\|^2\right] &= \mathbf{E}\left[\sum_{j=1}^{M}\left(\sum_{i=1}^{N}\sqrt{\frac{N}{M}}r_{ij}u_i\right)^2\right]\\ &= \frac{N}{M}\sum_{j=1}^{M}\mathbf{E}\left[\left(\sum_{i=1}^{N}r_{ij}u_i\right)^2\right]\\ &= \frac{N}{M}\sum_{j=1}^{M}\mathbf{E}\left[\sum_{i=1}^{N}r_{ij}^2u_i^2 + 2\sum_{l\neq k}r_{lj}u_lr_{kj}u_k\right]\\ &= \frac{N}{M}\sum_{j=1}^{M}\mathbf{E}\left[\sum_{i=1}^{N}r_{ij}^2u_i^2\right] = \frac{N}{M}\sum_{j=1}^{M}\frac{1}{N}\|\mathbf{u}\|^2 = \|\mathbf{u}\|^2.\end{aligned}$$

To compute $\mathbf{Var}[\|\mathbf{x}\|^2]$, we first define $\alpha_j = (\sum_{i=1}^{N} r_{ij}u_i)^2$; we have

$$\begin{aligned}\mathbf{E}[\alpha_j] &= \mathbf{E}\left[\left(\sum_{i=1}^{N}r_{ij}u_i\right)^2\right]\\ &= \mathbf{E}\left[\sum_{i=1}^{N}r_{ij}^2u_i^2 + 2\sum_{l\neq k}r_{lj}u_lr_{kj}u_k\right]\\ &= \mathbf{E}\left[\sum_{i=1}^{N}r_{ij}^2u_i^2\right] = \sum_{i=1}^{N}\frac{1}{N}u_i^2 = \frac{1}{N}\|\mathbf{u}\|^2.\end{aligned}$$

Since $r_{ij} \sim \mathbf{N}(0, 1/N)$, $\mathbf{E}[r_{ij}^4] = 3/N^2$; then

$$\begin{aligned}\mathbf{E}\left[\alpha_j^2\right] &= \mathbf{E}\left[\left(\sum_{i=1}^{N}r_{ij}u_i\right)^4\right]\\ &= \mathbf{E}\left[\sum_{i=1}^{N}r_{ij}^4u_i^4 + 6\sum_{l\neq k}r_{lj}^2u_l^2r_{kj}^2u_k^2\right]\\ &= \frac{3}{N^2}\sum_{i=1}^{N}u_i^4 + \frac{6}{N^2}\sum_{l\neq k}u_l^2u_k^2\\ &= \frac{3}{N^2}\left(\sum_{i=1}^{N}u_i^4 + 2\sum_{l\neq k}u_l^2u_k^2\right) = \frac{3}{N^2}\left(\sum_{i=1}^{N}u_i^2\right)^2 = \frac{3}{N^2}\|\mathbf{u}\|^4.\end{aligned}$$

We have

$$\begin{aligned}\mathbf{E}\left[\|\mathbf{x}\|^4\right] &= \mathbf{E}\left[\left(\sum_{j=1}^{M}\left(\sum_{i=1}^{N}\sqrt{\frac{N}{M}}r_{ij}u_i\right)^2\right)^2\right] \\ &= \frac{N^2}{M^2}\mathbf{E}\left[\left(\sum_{j=1}^{M}\alpha_j\right)^2\right] \\ &= \frac{N^2}{M^2}\mathbf{E}\left[\sum_{j=1}^{M}\alpha_j^2 + 2\sum_{l\neq k}\alpha_l\alpha_k\right] \\ &= \frac{N^2}{M^2}\left(\sum_{j=1}^{M}\mathbf{E}\left[\alpha_j^2\right] + 2\sum_{l\neq k}\mathbf{E}[\alpha_l]\mathbf{E}[\alpha_k]\right) \\ &= \frac{N^2}{M^2}\left(\frac{3M}{N^2}\|\mathbf{u}\|^4 + 2\frac{M(M-1)}{2}\frac{\|\mathbf{u}\|^2}{N}\frac{\|\mathbf{u}\|^2}{N}\right) \\ &= \left(1+\frac{2}{M}\right)\|\mathbf{u}\|^4\end{aligned}$$

and the variance of $\|\mathbf{x}\|^2$ can be computed as

$$\mathbf{Var}\left[\|\mathbf{x}\|^2\right] = \mathbf{E}\left[\|\mathbf{x}\|^4\right] - \mathbf{E}\left[\|\mathbf{x}\|^2\right]^2 = \frac{2}{M}\|\mathbf{u}\|^4.$$

■

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

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

[3] Y. Wang and K. Plataniotis, "Face based biometric authentication with changeable and privacy preserving templates," in *Proc. BSYM*, Baltimore, MD, Sep. 2007.

[4] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[5] A. Adler, "Vulnerabilities in biometric encryption systems," in *Proc. Audio Video Based Biometric Person Authentication*, Tarrytown, NY, Jul. 2005, pp. 1100–1109.

[6] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proc. BSYM*, Baltimore, MD, Sep. 2007.

[7] A. B. J. Teoh and C. T. Yuang, "Cancellable biometrics realization with multispace random projections," *IEEE Trans. Syst., Man, Cybern. B, Cybern.—Special Issue on Recent Advances in Biometrics Systems*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.

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

[9] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security Privacy*, 1998, pp. 148–157.

[10] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Security*, 1999, pp. 28–36.

[11] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometric effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[12] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, 2002, p. 408.

[13] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, and J. Kim, "A new method for generating an invariant iris private key based on the fuzzy vault system," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 38, no. 5, pp. 1302–1313, Oct. 2008.

[14] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Eurocrypt*, 2004, pp. 523–540.

[15] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[16] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. CCS*, 2004, pp. 82–91.

[17] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[18] 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 *Proc. 4th IEEE Workshop Autom. Identification Adv. Technol.*, Oct. 17–18, 2005, pp. 21–26.

[19] M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proc. 17th Int. Conf. Pattern Recog.*, 2004, pp. 922–925.

[20] T. E. Boult, "Robust distance measures for face-recognition supporting revocable biometric tokens," in *Proc. IEEE Conf. Face Gesture*, Apr. 2006, pp. 560–566.

[21] D. C. L. Ngo, A. B. J. Teoh, and A. Goh, "Biometric hash: high-confidence face recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 6, pp. 771–775, Jun. 2006.

[22] A. B. J. Teoh, T. Connie, D. Ngo, and C. Ling, "Remarks on BioHash and its mathematical foundation," *Inf. Process. Lett.*, vol. 100, no. 4, pp. 145–150, Nov. 2006.

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

[24] P. Frankl and H. Maehara, "The Johnson–Lindenstrauss lemma and the sphericity of some graphs," *J. Combin. Theory, Ser. A*, vol. 44, no. 3, pp. 355–362, Jun. 1987.

[25] P. Indyk and R. Motwani, "Approximate nearest neighbors: Towards removing the curse of dimensionality," in *Proc. 30th Annu. ACM Symp. Theory Comput.*, Dallas, TX, 1998, pp. 604–613.

[26] S. Dasgupta and A. Gupta, "An elementary proof of the Johnson–Lindenstrauss lemma," UC Berkeley, Berkeley, CA, Tech. Rep. 99-006, Mar. 1999.

[27] R. I. Arriaga and S. Vempala, "An algorithmic theory of learning: Robust concepts and random projection," in *Proc. 40th Annu. Symp. Foundations Comput. Sci.*, Oct. 17–18, 1999, pp. 616–623.

[28] D. Achlioptas, "Database-friendly random projections," in *Proc. 20th Annu. Symp. Principles Database Syst.*, Santa Barbara, CA, 2001, pp. 274–281.

[29] P. Li, T. J. Hastie, and K. W. Church, "Very sparse random projections," in *Proc. 12th ACM Int. Conf. Knowl. Discovery Data Mining SIGKDD*, Philadelphia, PA, 2006, pp. 287–296.

[30] S. Vempala, *The Random Projection Method*, vol. 65. Providence, RI: AMS, 2004, ser. DIMACS Series in Discrete Mathematics and Theoretical Computer Science.

[31] A. Andoni and P. Indyk, "Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions," in *Proc. 47th Annu. IEEE Symp. FOCS*, 2006, pp. 459–468.

[32] N. Goel and G. Bebis, "Face recognition experiments with random projection," in *Proc. SPIE Defense Security Symp.*, Orlando, FL, Mar. 2005, p. 426.

[33] E. Brigham and H. Maninila, "Random projection in dimensionality reduction: Applications to image and text data," in *Proc. Int. Conf. Knowl. Discovery Data Mining*, 2001, pp. 245–250.

[34] S. Kaski, "Dimensionality reduction by random mapping: Fast similarity computation for clustering," in *Proc. Int. Joint Conf. Neural Netw.*, Piscataway, NJ, 1998, vol. 1, pp. 413–418.

[35] S. Dasgupta, "Experiments with random projection," in *Proc. 16th Conf. Uncertainty Artif. Intell.*, 2000, pp. 143–151.

[36] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 1, pp. 92–106, Jan. 2006.

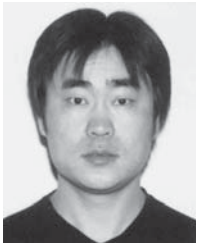
[37] S. T. M. Oliveira and O.R. Zaiane, "Privacy-preserving clustering by object similarity-based representation and dimensionality reduction transformation," in *Proc. Workshop PSADM, 4th IEEE ICDM*, 2004, pp. 21–30.

[38] R. Hecht-Nielsen, *Context Vectors: General Purpose Approximate Meaning Representations Self-Organized From Raw Data, Computational Intelligence: Imitating Life*. Piscataway, NJ: IEEE Press, 1994, pp. 43–56.

[39] E. W. Weisstein, *Regularized Gamma Function*, From MathWorld—A Wolfram Web Resource. [Online]. Available: http://mathworld.wolfram.com/RegularizedGammaFunction.html

[40] E. W. Weisstein, *Hypersphere*, From MathWorld—A Wolfram Web Resource. [Online]. Available: http://mathworld.wolfram.com/Hypersphere.html

[41] K. Liu, "Multiplicative data perturbation for privacy preserving data mining," Ph.D. dissertation, Univ. Maryland, Baltimore, MD, Jan., 2007.
[42] W. Du, Y. S. Han, and S. Chen, "Privacy-preserving multivariate statistical analysis: Linear regression and classification," in *Proc. SIAM Int. Conf. Data Mining SDM*, Apr. 2004, pp. 222–233.
[43] J. Wang, K. N. Plataniotis, J. Lu, and A. N. Venetsanopoulos, "On solving the face recognition problem with one training sample per subject," *Pattern Recognit.*, vol. 39, no. 9, pp. 1746–1762, Sep. 2006.
[44] P. J. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image Vis. Comput.*, vol. 16, no. 5, pp. 295–306, Apr. 1998.
[45] P. J. Phillips, H. Moon, P. J. Rauss, and S. Rizvi, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 10, pp. 1090–1104, Oct. 2000.
[46] T. Sim, S. Baker, and M. Bsat, "The CMU Pose, Illumination, and Expression database," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 12, pp. 1615–1618, Dec. 2003.
[47] A. M. Martinez and R. Benavente, "The AR face database," CVC Tech. Rep. 24, Purdue Univ., Jun. 1998.
[48] *Aging Database*. [Online]. Available: http://www.fgnet.rsunit.com/
[49] *BioID Database*. [Online]. Available: http://www.humanscan.de/support/downloads/facedb.php
[50] A. M. Martinez and A. C. Kak, "PCA versus LDA," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 2, pp. 228–233, Feb. 2001.
[51] M. Turk and A. Pentland, "Eigenfaces for recognition," *J. Cogn. Neurosci.*, vol. 13, no. 1, pp. 71–86, 1991.



Yongjin Wang (S'04) received the M.A.Sc. degree in electrical and computer engineering from Ryerson University, Toronto, ON, Canada, in 2005. He is currently working toward the Ph.D. degree in The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto.

In 2005, he was a Research Assistant with the Ryerson University Multimedia Research Laboratory. His research interests include biometrics, speech and image processing, computer vision, and pattern recognition.

Mr. Wang is a recipient of the Natural Sciences and Engineering Research Council Canadian Graduate Scholarship Doctoral Award from 2007 to 2009.

Konstantinos N. Plataniotis (S'90–M'92–SM'03) received the B.Eng. degree in computer engineering from the University of Patras, Patras, Greece, in 1988 and the M.S. and Ph.D. degrees in electrical engineering from Florida Institute of Technology, Melbourne, in 1992 and 1994, respectively.

He is currently a Professor with The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada, where he is also a member of the Knowledge Media Design Institute and the Director of Research with the Identity, Privacy and Security Institute. He is also an Adjunct Professor with the Department of Computer Science, Ryerson University, Toronto. His research interests include biometrics, communication systems, multimedia systems, and signal and image processing.

Dr. Plataniotis is the Editor in Chief (2009–2011) for the IEEE SIGNAL PROCESSING LETTERS, a Registered Professional Engineer in the province of Ontario, and a member of the Technical Chamber of Greece. He was the 2005 recipient of IEEE Canada's Outstanding Engineering Educator Award "for contributions to engineering education and inspirational guidance of graduate students" and the corecipient of the 2006 IEEE TRANSACTIONS ON NEURAL NETWORKS Outstanding Paper Award for the paper entitled "Face Recognition Using Kernel Direct Discriminant Analysis Algorithms" published in 2003.