A Hybrid Approach for Generating Secure and Discriminating Face Template

Yi C. Feng, Pong C. Yuen, *Member, IEEE*, and Anil K. Jain, *Fellow, IEEE*

***Abstract*—Biometric template protection is one of the most important issues in deploying a practical biometric system. To tackle this problem, many algorithms, that do not store the template in its original form, have been reported in recent years. They can be categorized into two approaches, namely biometric cryptosystem and transform-based. However, most (if not all) algorithms in both approaches offer a trade-off between the template security and matching performance. Moreover, we believe that no single template protection method is capable of satisfying the security and performance simultaneously. In this paper, we propose a hybrid approach which takes advantage of both the biometric cryptosystem approach and the transform-based approach. A three-step hybrid algorithm is designed and developed based on random projection, discriminability-preserving (DP) transform, and fuzzy commitment scheme. The proposed algorithm not only provides good security, but also enhances the performance through the DP transform. Three publicly available face databases, namely FERET, CMU-PIE, and FRGC, are used for evaluation. The security strength of the binary templates generated from FERET, CMU-PIE, and FRGC databases are 206.3, 203.5, and 347.3 bits, respectively. Moreover, noninvertibility analysis and discussion on data leakage of the proposed hybrid algorithm are also reported. Experimental results show that, using Fisherface to construct the input facial feature vector (face template), the proposed hybrid method can improve the recognition accuracy by 4%, 11%, and 15% on the FERET, CMU-PIE, and FRGC databases, respectively. A comparison with the recently developed random multispace quantization biohashing algorithm is also reported.**

***Index Terms*—Biometric data security, face recognition, face template protection, Fisherface.**

I. Introduction

BIOMETRIC recognition is a reliable, robust, and convenient way for person authentication [2], [7], [9], [10]. With growing concerns about security and terrorism, several large-scale biometric systems such as US-VISIT program have been successfully deployed. Biometric systems are also being developed for many other applications [6] such as banking (for ATM machines), the credit card industry, and physical access control. With the growing use of biometrics, there is a rising concern about the security and privacy of the biometric data itself. Since each person is claimed to have a unique biometric (e.g., fingerprint, face, and iris), if this biometric data is compromised, it is impossible to have a replacement. Therefore, biometric data (template) security [7]–[9] is one of the most important issues in developing a practical biometric system (biometric template refers to the extracted biometric features stored in a central database or a smartcard). Recent studies [14], [15] have shown that the raw biometric data can be recovered from the biometric template stored in the database. As a result, protection of biometric template in biometric system applications is indispensable. To overcome this problem, a commonly proposed approach is not to store the original biometric template. Instead, a transformed version of the original template is stored. It has been suggested [51] that a biometric template protection algorithm should satisfy the following three requirements.

1) **Security:** It should be computationally hard to reconstruct the original biometric template from the transformed biometric template.
2) **Discriminability:** The discriminability of the original biometric template should not be degraded after the transformation.
3) **Cancelability (revocability + diversity):** If the transformed biometric template is stolen or lost, the algorithm should be able to generate another transformed template from the original template. Moreover, the algorithm should be able to generate different transformed templates of an individual for different applications.

The straightforward solution to template security is to apply a password-like encryption algorithm (hashing) on the biometric template and perform the matching process in the encrypted domain. However, due to the intraclass variations in biometric data, a small change in the raw biometric data input will result in a large change in the encrypted data, leading to degradation in system accuracy. Therefore, directly applying password-like encryption method is not feasible. On the other hand, if the encrypted secure template is decrypted for matching process, it is susceptible to interception by an impostor.

In order to solve the intraclass template variation problem while maintaining the template security, many algorithms have been proposed which can be categorized into two main approaches: 1) the biometric cryptosystem approach and 2) the transform-based approach. The basic idea of both approaches is

Manuscript received May 30, 2009; accepted November 17, 2009. First published December 31, 2009; current version published February 12, 2010. This project was supported by Hong Kong RGC General Research Fund 210908, by the Science Faculty Research Grant of the Hong Kong Baptist University, and by NSFC-GuangDong research grant U0835005. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Davide Maltoni.

Y. C. Feng and P. C. Yuen are with the Department of Computer Science, Hong Kong Baptist University, Hong Kong (e-mail: ycfeng@comp.hkbu.edu.hk; pcyuen@comp.hkbu.edu.hk).

A. K. Jain is with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824 USA, and also with the Department of Brain and Cognitive Engineering, Korea University, Anam-dong, Seoul 136-701, Korea (e-mail: jain@cse.msu.edu).

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/TIFS.2009.2038760

that instead of storing the original template, the transformed/encrypted template which is intended to be more secure, is stored. In case the transformed/encrypted template is stolen or lost, it is computationally hard to reconstruct the original template and to determine the original raw biometric data simply from the transformed/encrypted template.

In the biometric cryptosystem approach, the error-correcting coding techniques are employed to handle intraclass variations. Two popular techniques, namely fuzzy commitment scheme [20] and fuzzy vault scheme [21], have been proposed. The advantage of this approach is that, since the output is an encrypted template, its security level is high. However, the error-correcting ability of these schemes may not be strong enough to handle large intraclass variations such as face images captured under different illuminations and poses. Also, this approach is not designed to be revocable. Finally, the error-correcting coding techniques require input in certain format (e.g., binary strings [20] or integer vectors with limited range[21]), and it is hard to represent every biometric template in this desired format.

In the transform-based approach, a transformed template is generated using a "one-way" transform and the matching is performed in the transformed domain. The transform-based approach has a good cancelability (revocability) property, but the drawback of this approach is the trade-off between performance and security of the transformed template.

In view of the limitations of the existing approaches, we propose a hybrid approach for face template protection. The proposed approach retains the advantages of both the transform-based approach and biometric cryptosystem approach, and overcomes the limitations of individual approaches. The proposed hybrid algorithm consists of random projection, discriminability-preserving (DP) transform, and fuzzy commitment scheme. The DP transform compensates for the loss of template discriminability in a random projection process and converts the face template into a binary template so that the fuzzy commitment scheme can be applied. The rest of this paper is organized as follows. In Section II, a brief review of existing template security methods is presented. Section III introduces the proposed hybrid framework while Section IV reports the three-step hybrid algorithm. Experimental results and security analysis are presented in Sections V and VI, respectively. Finally, conclusions of this paper are given in Section VII.

II. Template Security Methods

This section reviews the existing schemes for biometric template protection. We categorize them into two approaches, namely the biometric cryptosystem approach and the transform-based approach.

A. Biometric Cryptosystems Approach

Here we follow the presentation in Jain *et al.* [51] and categorize the biometric cryptosystems approach into two subapproaches: key-binding biometric cryptosystem and key-generation biometric cryptosystem.

1) Key-Binding Biometric Cryptosystem: In a key-binding biometric cryptosystem, a secret key which is unrelated to the biometric data is linked to a reference template. Helper-data is generated from the secret key and the reference template. The helper data is used to compensate for the variations in query template without providing any significant information about the original reference template. If the query template is sufficiently similar to the reference template, after error-correcting decryption with helper-data, the correct secret key is released.

Davida *et al.* [19] first developed the off-line biometric identification scheme. In their scheme, an error-correcting code is employed to generate a check data K and the original template u_E is hashed to generate $\mathrm{Hash}(u_E)$. At authentication, an error-correcting decryption process using K is employed to correct the query biometric template from u_A to u'_A. The new template u'_A is then hashed and compared with $\mathrm{Hash}(u_E)$ and a decision is made. Since the error tolerance of this method is not very strong, multiple scans (images) were used in the training phase to learn the intraclass variations. While no security analysis of the template protection was provided, it provides a good foundation for protecting biometric template.

Juels and Watternberg [20] proposed a fuzzy commitment scheme which treats the biometric template itself as a corrupted codeword. The security of this method is linked to the number of codewords. The scheme encrypts the original template u_E to a pair $(\mathrm{Hash}(C), u_E - C)$, where C is a randomly generated codeword. At authentication, given a query template u_A, the method computes $u_A - (u_E - C)$ and corrects it to the closest codeword C'. If u_E is close to u_A, $u_A - (u_E - C) = C + (u_A - u_E)$ will be corrected to C, i.e., $C' = C$. Then $\mathrm{Hash}(C')$ and $\mathrm{Hash}(C)$ are compared to make the decision. This algorithm can tolerate a relatively large error rate with enhanced security level. However, the authors did not present any experimental results. Also, both the off-line scheme and the fuzzy commitment scheme require a binary input.

Juels and Sudan [21] proposed a fuzzy vault scheme. A secret is embedded in a fuzzy vault V_F with a data set S_A. In order to extract the secret, another set S_B needs to be presented to decrypt the vault V_F, which should be sufficient similar to the set S_A. The Reed–Solomon coding scheme [4] is employed. For this purpose, a secret is first embedded into a polynomial which is then used to transform the original set S_A into a new point set S_R. After that, chaff points are inserted into S_R to make it difficult to identify genuine points. At authentication, if S_B is close to S_A, genuine points can be detected from S_R to reconstruct the polynomial, and therefore the secret. This scheme has been further modified and applied to fingerprint biometric [22], [24], [30], face [48], and iris [26]. However, there are some limitations of this method. First, the point set S_R may leak some message because all the important information is stored without encryption. Second, insertion of chaff points will significantly increase the data size. Finally, the Reed–Solomon coding scheme assumes that the input data set S_A only contains integers in a limited range. Improved versions of the fuzzy vault scheme have been proposed such as the fingerprint security scheme by Uludag and Jain [23]. Helper data was employed for the alignment of the fingerprints to improve the authentication accuracy. Nagar *et al.* [25] proposed a fusion scheme combining fuzzy vault and fuzzy commitment. The fuzzy commitment scheme was used to encrypt the ordinate values in the fuzzy vault with

minutiae descriptor data. This way, even if the attacker can find the geniune points in the fuzzy vault, the secret key cannot be extracted.

A two-stage framework was proposed by Monrose *et al.* [37], [38], which described a cryptographic key generation scheme from biometrics. The error-correcting code is applied after a binary transformation of the feature vectors. In the first stage, the biometric data is transformed into a binary string "feature descriptor" via thresholding. In the second stage, a cryptographic key is generated from the feature descriptor with a cryptographic algorithm. This scheme provides an interesting approach to protect templates with large intraclass variations and transforms the original feature data into binary strings such that the error-correcting schemes can be applied. However, the security level is insufficient (at most 60 bits) and the false rejection rate is relatively high (almost 20%).

Another two-stage scheme with binarization was proposed by Goh and Ngo [40]. In this scheme, the original template is transformed using random projection and then thresholded to binary representation (string). An error-correcting encryption, namely cryptographic key interpolation, was employed to encrypt the binary string. This scheme has been further modified and reported in [41] and [43]. However, the discriminability of the binarized templates is not discussed.

Soutar *et al.* [18] transform the original template u_E to a new representation $f(u_E)$ with a filter function and embed a secret to $f(u_E)$ for protection. Tuyls *et al.* [34] proposed a δ-contracting function algorithm to deal with the intraclass variation with helper data. Kevenaar *et al.* [35] proposed a feature binarization scheme for face biometric, which selects the most important features for generating the binary template. However, these two algorithms used quantization to binarize the biometric data, which causes information loss. Draper *et al.* [36] suggested a metric for specifying the security level. Hao *et al.* [31] evaluated different types of errors which are introduced in iris recognition and then proposed a two-layer error correction coding method. They combined the Reed–Solomon code and the Hadamard code for handling burst errors and random errors, respectively. Draper *et al.* [32] applied the distributed source coding to protect fingerprint template and Sutcu *et al.* [33] analyzed and implemented the sketch, which is an error tolerant cryptographic technique, for face biometric.

2) Key-Generation Biometric Cryptosystem: In a key-generation scheme, the cryptographic key is directly generated from a biometric. The advantage of this approach is that, it does not need an extra cryptographic key and, therefore, one need not be concerned about the key security. The main issue in this approach is to generate a stable cryptographic key from a biometric template in the presence of intraclass variations.

The early key-generation schemes applied the quantization process to remove the intraclass variations during the key extraction process. Vielhauer *et al.* [41] proposed a signature biohash scheme which extracts 24-dimensional vector parameters from the original signature data. For each parameter, its upper bound and lower bound are used to determine a quantization value. After quantization, the parameters are expected to be the same within the same class. Dodis *et al.* [27] proposed two ideas for generating biometric key, namely secure sketch and fuzzy extractor. In secure sketch, helper data is used to model the intraclass variations such that the reference template (biometric key) can be exactly generated from a query template and the helper data. The rationale of fuzzy extractor is to transform biometric templates with intraclass variations into the same biometric key. While these two ideas sound good, practical implementation was not presented. Some researchers [28], [29] have followed this approach and proposed their own secure sketch and fuzzy extractor schemes.

B. Transform-Based Approach

The transform-based approach does not encrypt the biometric data but transforms the original templates into a new domain. A "one-way" function is applied such that the original feature template cannot be retrieved from the transformed one. Following Jain *et al.*'s [51] categorization, we further classify this approach into two subapproaches: noninvertible transform and salting.

1) Noninvertible Transform: Ratha *et al.* [7] first proposed the concept of cancelable biometrics or cancelable template. The original template is transformed to a new domain and, therefore, can be canceled and reissued by changing the transform parameters, if it is stolen or lost. Two distortion transforms in signal and feature domains were discussed to construct the cancelable template. The transform in the signal domain includes the grid morphing and block permutation. In the feature domain, high-order polynomials are used. With these transforms, the authors claimed that the original template cannot be reconstructed from the cancelable template. Ratha *et al.* [7] provided the basics of the cancelable biometrics but did not address the intraclass variation problem. Later on, Ratha *et al.* [46], [47] proposed a cancelable biometrics on fingerprint, based on three different transforms, namely Cartesian transformation, radial transformation, and functional transformation. While they achieved high template security, the experimental results show that the recognition performance using the cancelable template is degraded.

Tulyakov *et al.* [44] followed the cancelable template idea and proposed a symmetric hash function (polynomials) as a distortion transform for fingerprint. To handle the intraclass variation, sets of local features were extracted and a global matching of fingerprint was achieved by comparing with all the local feature sets. Ang *et al.* [45] proposed a key-dependent algorithm to transform the original fingerprint template into the new domain. They divided the original 2-D feature space into two halves based on the key. Because it is hard to know which minutiae are reflected, it is difficult to invert the transform. However, these two algorithms do not perform well in handling the intraclass variation problem, resulting in relatively large performance degeneration.

Sutcu *et al.* [43] proposed a functional distortion of the original template. With the extracted feature vector, they estimated the distribution of each element in the training data, and approximated it by the Gaussian functions. Fake Gaussian functions are combined together to confuse the attackers so as to increase the noninvertibility. However, a detailed performance analysis was not provided.

2) Salting: Salting means that a user-specific password or key is applied to increase the between-class variation and thus enhance the discriminability. A transform takes the original biometric template and the user-specific key as inputs. Different keys from different users will diverge the transformation results such that the discriminability of the transformed templates are enhanced. The transformed templates can be easily cancelled and reissued via changing the key.

The biohashing algorithm [40] can be classified in this approach. Teoh *et al.* proposed a two-factor authentication algorithm [39] for fingerprint and a random multispace quantization (RMQ) algorithm [42] for face biometric. In both methods, the original feature vectors are transformed into another domain using random projection. The transformed template is further converted into binary strings by a thresholding technique. In the RMQ algorithm, with the use of user supplied data, a user specific random projection matrix is adopted so as to reduce the false acceptance error. The authors claimed that a zero false acceptance rate can be achieved by the multisubspace projection based on user supplied data. The RMQ algorithm may have a security issue if the user data is stolen. However, without the user data, the performance of this scheme may be degraded.

III. Proposed Hybrid Approach

From the review in Section II, it can be seen that no one single template protection approach can simultaneously satisfy the cancelability, security, and accuracy requirements. In order to take the benefits of both approaches while avoiding their limitations, we propose to cascade the transform-based approach with the biometric cryptosystem approach to form a new hybrid approach for face biometric. Furthermore, we propose a discriminability enhancing binarization process to deal with the intraclass variations, thereby helping to satisfy both the discriminability and security requirements.

As illustrated in Fig. 1, the proposed hybrid framework consists of three major steps. The input is a face template extracted using a face representation algorithm such as the linear discriminant analysis (LDA). In the first step, a cancelable transform is designed to generate a cancelable template. Normally, this cancelable transform leads to a loss of discriminability. So in the second stage, a discriminability enhancement transform is applied to compensate for the discriminability lost in the first stage and convert the cancelable template into binary representation (binary template). These two steps can be viewed as a transform-based scheme. A biometric cryptosystem scheme is adopted to protect the binary template and generate a secure template. In this way, the hybrid framework makes an attempt to satisfy all the template protection requirements. This preliminary idea has been published in [52].

1) **Security:** First, since the main objective of the cancelable transform is to provide cancelable ability, a "near one-way" transform can be used. Second, the discriminability enhancement transform, which is normally a nonlinear transform that outputs a binary face template, provides additional protection. Finally, a biometric cryptosystem-based algorithm stores the template in hashed form, which is noninvertible. By using the three-stage protection, it will be computationally hard to reconstruct the original face template from the secure face template.
2) **Discriminability:** The first and second steps belong to the transform-based approach. However, existing transform-based schemes are not robust to intraclass variations. This problem is especially severe in the binarization step which will apparently cause information loss. Therefore, a good binarization method needs to be designed to transform the input cancelable template into a binary string and preserve its discriminability. This compensates the discriminability loss in the first step. In turn, the binary template will maintain the discriminability at least as good as the original template.
3) **Diversity and Revocability:** Different applications require different sets of parameters in the cancelable transform. The cancelable face templates and, therefore, the secure face templates of an individual in different applications will be different. In turn, the cross-matching across databases will not be feasible. Moreover, the secure face template can be canceled and reissued by changing the cancelable transform parameters.

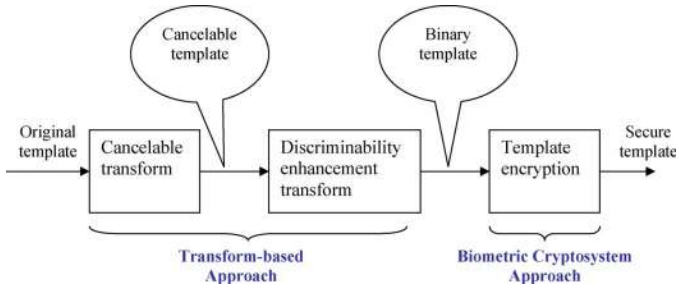


Fig. 1. Proposed hybrid framework for protecting face biometric template.

IV. Three-Step Hybrid Algorithm

Based on the proposed hybrid framework in Section III, a three-step hybrid algorithm is developed for protecting face biometric template and its block diagram is shown in Fig. 2. The algorithm consists of two phases, namely enrollment and query phases. In the enrollment phase, the user's face image is captured and the (original) face template is extracted through a feature extractor. In the first step, random projection is employed as a cancelable transform to project the original template into a subspace and generate a cancelable template. If it is compromised, the projection matrix can be changed in order to issue a new template. In the second step, we develop a DP transform to enhance the discriminability of the cancelable template and convert the real valued cancelable template into a binary template (the preliminary version has been reported in [49] and [50]). Finally, the fuzzy commitment scheme [20] is employed to protect the binary face template. Details of each step are discussed in the following sections.

A. Random Projection

Random projection is a popular dimensionality reduction technique and has been successfully applied in many computer vision and pattern recognition applications. Recently, it has

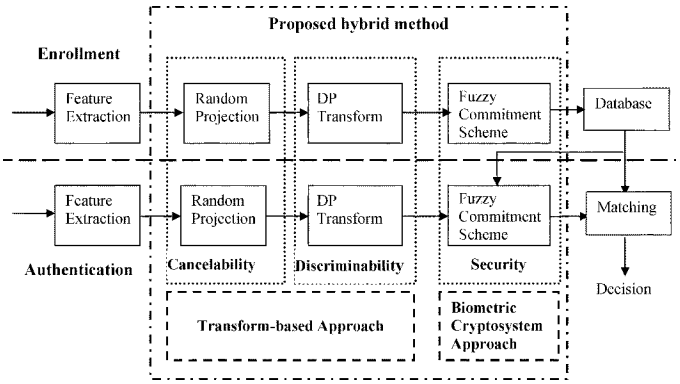


Fig. 2. Block diagram of the proposed three-step hybrid algorithm.

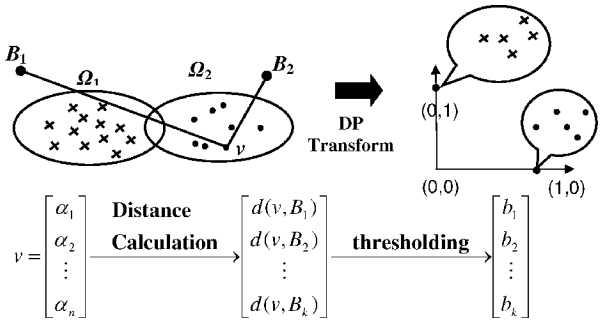


Fig. 3. Illustration of the DP transform.

also been employed as a cancelable transform [42] for face biometric. The main purpose of the original random projection is to project a set of vectors into a lower dimensional subspace while preserving the Euclidean distances between vectors before and after the transformation, with a certain probability. The idea was first developed by Johnson and Lindenstrauss [1] who proved the following Lemma:

Lemma 4.1 (Johnson-Lindenstrauss): Given $\epsilon > 0$ and an integer n, let k be a positive integer such that $k > k_0 = O(\epsilon^{-2}\log n)$. For every set Ω of n points in $\mathbb{R}^d$, there exists a transformation $f : \mathbb{R}^d \to \mathbb{R}^k$ such that for all $U, V \in \Omega$

$$(1-\epsilon)||U-V||^2 \le ||f(U)-f(V)||^2 \le (1+\epsilon)||U-V||^2.$$

In the hybrid algorithm, we adopt random projection in the first step to provide cancelability. A cancelable template $v = Ru$ is constructed from the original template u with a projection matrix R. If the cancelable template is compromised, a new cancelable template $v' = R'u$ can be reissued using another projection matrix R' to replace the old template v. Lemma 4.1 indicates that this step has certain capability of preserving the discriminability of the original feature vectors. However, this dissimilarity depends on the transformed vector length. If the transformed vector length is small, there will be a large discriminability loss. Also this step is not a "strong" one-way function. Although attackers cannot retrieve the original feature templates from the lower dimensional cancelable template, they can find an approximation $u^+ = R^+v$ with the pseudoinverse R^+ of the projection matrix R. Thus, the output of this step needs further protection.

B. Discriminability Preserving Transform

The DP transform is the key in the hybrid framework. It is developed for discriminability enhancement and conversion of a real valued template into binary template. This binarization step is specifically designed such that it has the capability of enhancing the discriminability of the original feature templates. In designing the transform, the following two criteria are considered.

- Criterion 1: If a cancelable template v belongs to a class Ω_i, then after DP transform, v should also belong to the same class.
- Criterion 2: If a cancelable template v does not belong to a class Ω_i, then after DP transform, v should also not belong to class Ω_i.

The above two criteria imply that the discriminability of the cancelable templates should be preserved after DP transform.

The rationale of our proposed DP transform is illustrated in Fig. 3. Consider a two-class problem with class Ω_1 (data points represented by cross) and Ω_2 (data points represented by circle). Given k distinguishing points, say B_1 and B_2, and $k = 2$ in this example, any real-valued feature vector (cancelable template) v in n-dimensional space can be transformed into a k-dimensional binary string $[b_1, b_2, \ldots, b_k]$, where

$$b_i = \begin{cases} 0 & : d(B_i, v) \le t_i \\ 1 & : d(B_i, v) > t_i \end{cases}$$

where d denotes the distance function and t_i is the distance threshold. The proposed DP transform assumes that the distribution of the original feature templates is spherical. This assumption is reasonable since the original feature templates are assumed to have good discrimination ability and, therefore, their distribution should be compact.

The original templates from the same class should be similar to each other, thus they will have about similar distances to the distinguishing points. With a given threshold, they will be transformed to have the same bit-value. The positions of the distinguishing points are determined such that templates from different classes will have significantly different distances to the distinguishing points, resulting in different transformed bits. Therefore, unlike a random thresholding process, we first determine the distinguishing points and thresholds based on the training data so as to maximize the discriminability of the transformed binary templates. Details are given below.

1) The DP Transform for Authentication System: Assume there are c classes $\{\Omega_1, \Omega_2, \ldots, \Omega_c\}$ in the training set C_T with cluster centers $\{M_1, M_2, \ldots, M_c\}$, respectively. For each class Ω_s $(s = 1, 2, \ldots, c)$, let r_s be the largest distance between a data point in Ω_s to the cluster center M_s. A biometric authentication system is considered as a two-class problem (genuine and imposter), and therefore, in determining the distinguishing point set for class Ω_s, we only need to consider the class Ω_s, and $C_T - \Omega_s = \{x \in C_T | x \notin \Omega_s\}$. Let D_1 and D_2 denote distance functions in input and transformed spaces, respectively, and h_s be the threshold in the transformed domain. Given a data point (cancelable template) v, we would like to find a transformation $f()$ which has the following two DP properties:

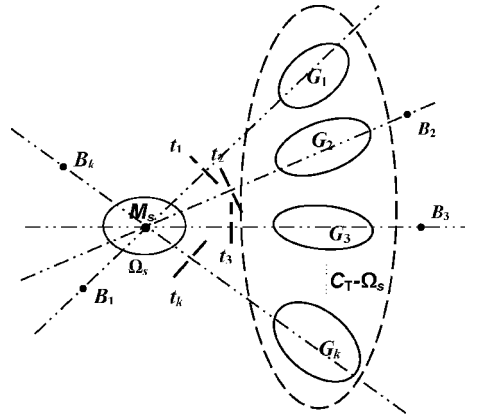


Fig. 4. Clustering in the DP-transform.

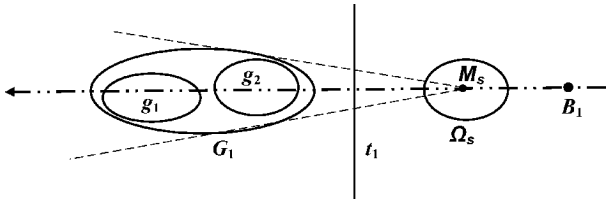


Fig. 5. Using direction as distance for clustering.

- *Property One*
  If $D_1(v, M_s) \leq r_s$, then $D_2(f(v), f(M_s)) \leq h_s$.
  This property ensures that if v belongs to class Ω_s, after transformation, v also belongs to the same class (Criterion 1).
- *Property Two*
  If $D_1(v, M_s) > r_s$, then $D_2(f(v), f(M_s)) > h_s$.
  This property ensures that if $f(v)$ does not belong to class Ω_s, after transformation, $f(v)$ will also not belong to class Ω_s (Criterion 2).

Our proposed transform consists of two steps. First, we cluster point in $C_T - \Omega_s$. Next, for each cluster, a corresponding distinguishing point is determined to distinguish the cluster from Ω_s (illustrated in Fig. 4). So given the set of distinguishing points, the set $C_T - \Omega_s$ will be distinguished from Ω_s.

Clustering in $C_T - \Omega_s$: A spatial distance function such as Euclidean distance is typically used in clustering. However, in this paper, we propose to use directional measurement instead of spatial distance measurement. As illustrated in Fig. 5, g_1 and g_2 are two clusters obtained using spatial distance measurement, which have different locations but similar directions w.r.t. Ω_s. Since two clusters are found, two distinguishing points will be used. However, it can be easily seen that the two distinguishing points are redundant and, in fact, one distinguishing point (B_1) is sufficient to distinguish the two clusters g_1 and g_2 from the set Ω_s.

To facilitate the use of directional measurement, we use M_s as an origin such that each cancelable template P_j in $C_T - \Omega_s$ can be represented by a unit vector e_j using the following equation:

$$e_j = \frac{P_j - M_s}{||P_j - M_s||}, \qquad j = 1, 2 \ldots, p$$

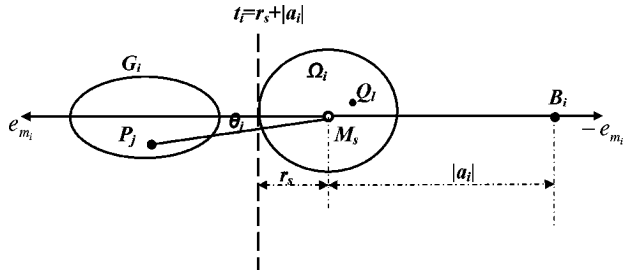


Fig. 6. Scenario one in proving the DP properties.

where p denotes the number of cancelable templates in $C_T - \Omega_s$. We determine k representative directions from these p unit vectors ($p \gg k$) with the largest angular separation. A k-means algorithm is applied to find the k directions. First we find the direction e_{m_1} which has the largest angle with the other unit vectors. Then find e_{m_2} which has the largest angle to e_{m_1}, find e_{m_3} which has the largest angles to e_{m_1} and e_{m_2}, and so on. Using each of the k vectors as a cluster center, each vector e_j in $C_T - \Omega_s$ will be classified into one of the k groups or clusters based on the nearest neighbors of $\{e_{m_i}\}, m_i \in \{1, 2, \ldots, p\}, i = 1, 2, \ldots, k$. This way, k groups $\{G_1, G_2, \ldots, G_k\}$ and the corresponding unit vectors (named group directions) $\{e_{m_1}, e_{m_2}, \ldots, e_{m_k}\}$ are obtained.

Although we assume that the class distribution is spherical, we do not have prior knowledge on the class distribution for $C_T - \Omega_s$. In order to ensure the two DP properties hold, two additional conditions are required on the template distribution in each group described as follows. For a template P_j in group G_i with group direction e_{m_i}, denote θ_j as the angle between $M_s P_j$ and the group direction e_{m_i} as shown in Fig. 6. For all P_j in G_i, the θ_j must satisfy the following two conditions (the two conditions can be merged into one, but for clear presentation and better understanding, we state here as two conditions):

$$\cos\theta_j > \frac{r_s}{|P_j M_s|} \tag{1}$$

and

$$\cos\theta_j > \frac{1}{4} + \frac{r_s}{|P_j M_s|} - \frac{1}{4}\left(\frac{r_s}{|P_j M_s|}\right)^2. \tag{2}$$

It is easy to show that the right-hand side of (1) and (2) are bounded. Since P_j does not belong to Ω_s, i.e., $|P_j M_s| > r_s$

$$0 < \frac{r_s}{|P_j M_s|} < 1. \tag{3}$$

Therefore,

$$0 < \frac{1}{4} + \frac{r_s}{|P_j M_s|} - \frac{1}{4}\left(\frac{r_s}{|P_j M_s|}\right)^2 < 1. \tag{4}$$

An analysis of the above conditions will be given in Section IV-B2. If the above conditions for G_i are not satisfied, the group G_i will be split into two groups until the conditions are satisfied.

Determining $\{B_i, T_i\}$ Pair for Each Cluster G_i: This step determines the positions of distinguishing points in each direction (unit vector) and the threshold value. The position of the ith

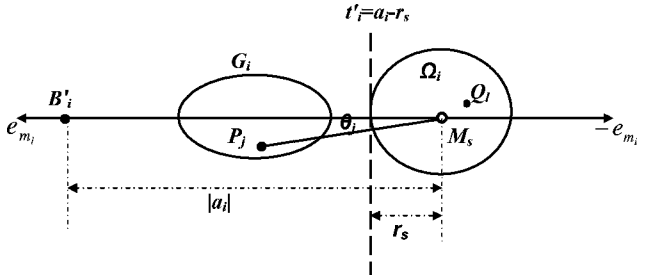


Fig. 7. Scenario two in proving the DP properties.

distinguishing point on the unit vector e_{m_i} can be written as

$$B_i = M_s + a_i e_{m_i} \tag{5}$$

where a_i is a real value (parameter) that controls the position of B_i along e_{m_i}.

The value of a_i can be positive or negative. $a_i < 0$ means that B_iM_i has the same direction as e_{m_i} and $t_i = |B_iM_s| + r_s$ as shown in Fig. 6. If $a_i > 0$, B_iM_s is in the opposite direction of e_{m_i} and $t_i = |B_iM_s| - r_s$ as shown in Fig. 7. Combining these two cases, the threshold t_i for the distinguishing point B_s is then determined as

$$t_i = |a_i - r_s|. \tag{6}$$

Therefore, what we need is a value a_i which is defined as follows:

$$a_i = \pm(2+\epsilon_i)\beta, \qquad i = 1, 2, \ldots, k. \tag{7}$$

where $\beta = \max|P_jM_s|(j = 1, 2, \ldots, p)$ and ϵ_i is a randomly generated value in interval $[0, 1]$. As a result, value of the parameters $\{a_i\}$ fall between 2β and 3β. With these carefully determined parameter values, the DP transform can satisfy the above DP properties.

2) Analysis of DP Properties: This section proves that the proposed method satisfies the above-mentioned DP properties. Let $P_j \in (C_T - \Omega_s)$ and $Q_l \in \Omega_s$ be the cancelable templates, where $l = 1, 2, \ldots, q$ and q denotes the number of cancelable templates in Ω_s. Assume that the (B_i, t_i) pair transforms P_j, Q_l and M_s (cluster center of class Ω_s) into bits b_P, b_Q, and b_M, respectively. We need to prove that $b_P \neq b_M$ and $b_Q = b_M$. Here we consider two scenarios in which a distinguishing point is located in the same and opposite directions of e_{m_i}, respectively with respect to M_s.

Scenario One: In scenario one, a distinguishing point B_i is located in the opposite direction of e_{m_i} (illustrated in Fig. 6 where $a_i \leq 0$). In this case, $t_i = |B_iM_s| + r_s$. For any cancelable template P_j in G_i and Q_l in Ω_s, let θ_j be the angle between B_iM_s and M_sP_j. The distance between the distinguishing point B_i and P_j can be written as

$$|B_iP_j| \geq |B_iM_s| + |P_jM_s|\cos\theta_j. \tag{8}$$

Substitute (1) into (8), we have

$$|B_iP_j| > |B_iM_s| + r_s = t_i.$$

Similarly, the distances between the distinguishing point B_i and Q_l, M_s can be written as

$$|B_iQ_l| \leq |B_iM_s| + |Q_lM_s| \leq |B_iM_s| + r_s = t_i$$

and

$$|B_iM_s| < |B_iM_s| + r_s = t_i.$$

That is, $|B_iP_j| > t_i$, $|B_iM_s| \leq t_i$ and $|B_iQ_l| \leq t_i$. Therefore, using B_i as a distinguishing point, P_j, M_s, and Q_l are transformed into bits $b_P = 1$, $b_M = 0$, and $b_Q = 0$, respectively. That means, cancelable templates in the class Ω_s will be transformed into the same bit value "0" while cancelable templates not belonging to the class Ω_s will be transformed into the opposite bit value "1".

Scenario Two: In this scenario, B'_i is located in the same direction as e_{m_i} (illustrated in Fig. 7 where $a_i > 0$). P_j is a cancelable template in G_i. In this case, $t'_i = |B'_iM_s| - r_s$. Let θ_j be the angle between B'_iM_s and M_sP_j. The distances between the distinguishing point B'_i and Q_l, M_s can be written as

$$|B'_iQ_l| \geq |B'_iM_s| - |Q_lM_s| \geq |B'_iM_s| - r_s = t'_i$$
$$|B'_iM_s| > |B'_iM_s| - r_i = t'_i.$$

Since both $|B'_iQ_l|$ and $|B'_iM_s|$ are greater than t'_i, $|B'_iP_j|$ should be smaller than t'_i. That is,

$$|B'_iP_j|^2 = |B'_iM_s|^2 + |P_jM_s|^2 - 2\cos\theta_j \cdot |B'_iM_s| \cdot |P_jM_s|$$
$$< t'^2_i = (|B'_iM_s| - r_s)^2 = |B'_iM_s|^2 - 2r_s|B'_iM_s| + r_s^2.$$

It is equivalent to

$$\cos\theta_j > \frac{|P_jM_s|}{2|B'_iM_s|} + \frac{r_s}{|P_jM_s|} - \frac{r_s^2}{2|B'_iM_s| \cdot |P_jM_s|}. \tag{9}$$

So, we need to prove (9). From (7), we have

$$|B'_iM_s| = |a_i| = (2+\epsilon_i)\beta \geq 2\beta \geq 2|P_jM_s|.$$

Substitute it into the right-hand side of (9), we have,

$$\frac{|P_jM_s|}{2|B'_iM_s|} + \frac{r_s}{|P_jM_s|} - \frac{r_s^2}{2|B'_iM_s| \cdot |P_jM_s|}$$
$$\leq \frac{1}{4} + \frac{r_s}{|P_jM_s|} - \frac{1}{4}\left(\frac{r_s}{|P_jM_s|}\right)^2$$
$$< \cos\theta_j \ \text{(from Equation 2)}.$$

So (9) is satisfied, thus $|B'_iP_j| < t'_i$. Then we have $|B'_iP_j| \leq t'_i$, $|B'_iM_s| > t'_i$, and $|B'_iQ_l| > t'_i$. So, using B'_i as a distinguishing point, P_j, M_s, and Q_l are transformed into bits $b_P = 0, b_M = 1$, and $b_Q = 1$, respectively, thereby satisfying the DP properties.

C. The Fuzzy Commitment Scheme

The fuzzy commitment scheme [20] is employed for the binary template protection. To encrypt w, the fuzzy commitment scheme randomly chooses a codeword C with the same length as w from an error-correcting code (e.g., BCH code). This is used to compute $w - C$ and $\mathrm{Hash}(C)$. These two data items are stored in database. $w - C$ is used as a helper data for error-correcting, while $\mathrm{Hash}(C)$ is used for matching process. Since

the proposed DP transform enhances the template discriminative power such that cancelable templates belonging to the same class will be transformed into the same binary template w, we do not employ the error-correcting ability of the fuzzy commitment scheme. So C here is just a randomly generated binary string with the same length as w.

D. Hybrid Scheme

This section summarizes the proposed method for face template protection.

Enrollment:

1) Input $c * q$ training face templates u_{gl} ($g = 1,2,\ldots,c$; $l = 1,2,\ldots,q$) from c classes, each class has q training samples.
2) Denote ko as the length of the training template. Randomly generate a series of $ko \times kr$ matrices R_s ($s = 1,2,\ldots,c$), and orthogonalize the columns of R_s with Gram–Schmidt algorithm, where kr is the length of the generated cancelable template.
3) For $s = 1,2,\ldots,c$,
   i) Transform each training template u_{gl} to cancelable template $v_{gl} = R_s^T u_{gl}$ ($g = 1,2,\ldots,c$; $l = 1,2,\ldots,q$).
   ii) Compute the cluster center M_s of the cancelable templates in cluster s.
   iii) For each cancelable template v_{gl} ($g \neq s$), compute the direction e_{gl} from M_s to v_{gl}.
   iv) Apply k-means algorithm to determine kc centroid $e_{m_1}, e_{m_2}, \ldots, e_{m_{kc}}$, where kc is the length of the binary template.
   v) Determine the kc distinguishing points $\{B_{si}\}$ and thresholds $\{t_{si}\}$ using (5) and (6) ($i = 1,2,\ldots,kc$).
   vi) Transform M_s to the reference binary template w_s with the distinguishing points and thersholds.
   vii) Randomly generate a binary string C_s with the same length as w_s. Each binary template w_s is encrypted to $(w_s - C_s, \mathrm{Hash}(C_s))$.
   viii)$(w_s - C_s, \mathrm{Hash}(C_s))$, $\{B_{si}\}$ and $\{t_{si}\}$ are stored in the database.
   ix) The projection matrix R_s is issued to the corresponding user.

Authentication:

1) A query template u' is presented with a projection matrix R' which is claimed to belong to class s.
2) Generate a cancelable template $v' = R'^T u'$.
3) Release distinguishing points $\{B_{si}\}$ and thresholds $\{t_{si}\}$ to the query ($i = 1,2,\ldots,kc$) and generate a binary template w'.
4) Release the stored data $(w_s - C_s, \mathrm{Hash}(C_s))$. Compute $w' - (w_s - C_s)$ and compare $\mathrm{Hash}(w' - (w_s - C_s))$ with $\mathrm{Hash}(C_s)$.

V. Experimental Results

The experimental results in this section are divided into three parts. Part I reports the template discriminability at each stage and illustrates the discriminability enhancement using the proposed DP transform. The accuracy of the proposed three-step hybrid algorithm is evaluated and reported in Part II. The cancelability of the hybrid algorithm is discussed in Part III.

Fig. 8. Sample images of three persons in the FERET database.

Fig. 9. Sample images of three persons in the CMU PIE database.

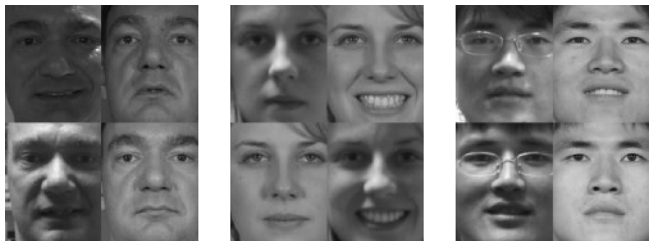


Fig. 10. Sample images of three persons in the FRGC database.

TABLE I
Experiment Settings

Database	c	m	q	variations
CMU PIE	68	105	10	illumination, pose
FERET	250	4	2	mild expression, illumination
FRGC	350	40	5	expression, illumination, mild pose

A. Face Databases

Three popular and public domain databases, namely FERET,[1] CMU PIE,[2] and FRGC,[3] are employed in our experiments. The face image variations include mild facial expression and illumination in the FERET database, illumination and pose in the CMU PIE database, and illumination, expression, and mild pose variation in the FRGC database. Sample images from these databases are shown in Figs. 8–10, respectively. The database parameters are shown in Table I, where c is the number of users in the database, m denotes the number of images per user, and q is the number of images per user used for training.

[1]Available: http://www.itl.nist.gov/iad/humanid/feret/

[2]Available: http://vasc.ri.cmu.edu/idb/html/face/index.html

[3]Available: http://www.frvt.org/FRGC/

TABLE II
EXPERIMENT SETTINGS OF PART I

Variations	c	m	q	kr	kc
Pose	68	4	2	40	56
Illumination	68	21	4	40	84
Pose & Illumination	68	105	10	40	210

In these databases, the face region is manually extracted and aligned. Fisherface [3] is used to extract the facial feature vector which is considered as the original face template.

B. Part I: Evaluation of the Template Discriminability

The hybrid framework (Fig. 2) generates three different face templates, namely cancelable template, binary template, and secure template. In this section, we evaluate the discriminability of each template in terms of the genuine and imposter histograms, as well as ROC curve. In particular, we illustrate that 1) the cancelable template discriminability is not as good as the original template, and 2) the discriminability of the binary cancelable template is enhanced, in comparison with the cancelable template, using the DP transform.

We also evaluate the template discriminabilities under pose and/or illumination variations. The CMU-PIE database is selected for the experiments. The detailed experimental parameter settings are shown in Table II, where kr and kc denote the length of the cancelable template and binary template, respectively. For pose variation (no illumination change), the results are illustrated in Fig. 11. Fig. 11(a) shows the imposter and genuine distributions using the original input face template. The percentage value in the figure shows the percentage of the overlapped area divided by total area. Therefore, the smaller the overlapped value, the better the discriminability. This value is 79.73% for the original template and 81.25% for the cancelable template [Fig. 11(b)] showing that the discriminability is decreased after random projection. This is expected as cancelable transform provides a trade-off between cancelability and discriminability. By applying the DP transform on the cancelable template, a binary template is obtained. The histogram for the binary cancelable face template is plotted in Fig. 11(c). The overlapped value drops to 58.32% which shows that the template discriminability is greatly enhanced after the DP transform. Fig. 11(d) plots the ROC curves of the original face template, cancelable face template, and the binary face template. It illustrates that the discriminability of the cancelable face template is not as good as the original face template while the discriminability of the binary cancelable face template is much improved. Similar experiments were performed on images with only the illumination changes in the CMU PIE database. The results in Fig. 12 show that same conclusion as that of pose variation can be drawn. Even with the presence of both pose and illumination variations, similar results are obtained (Fig. 13).

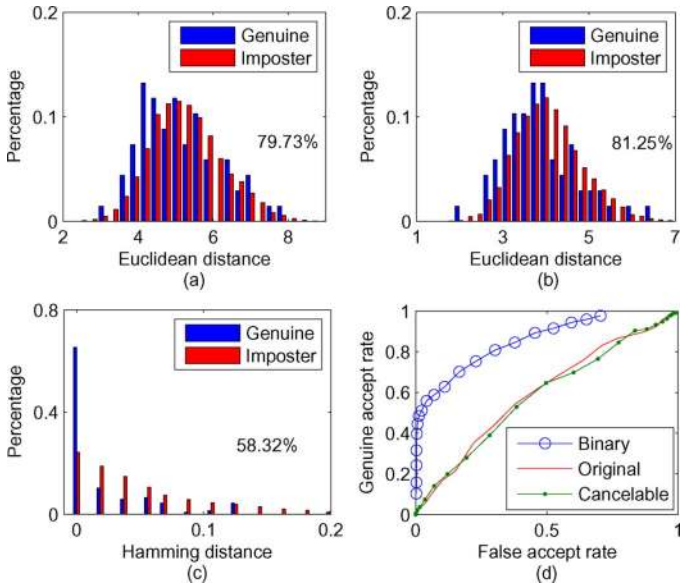


Fig. 11. Histogram and ROC curves for the CMU PIE database with pose variations: (a) histogram of original template; (b) histogram of cancelable template; (c) histogram of binary template; and (d) ROC curves of original template, cancelable template, and binary template.

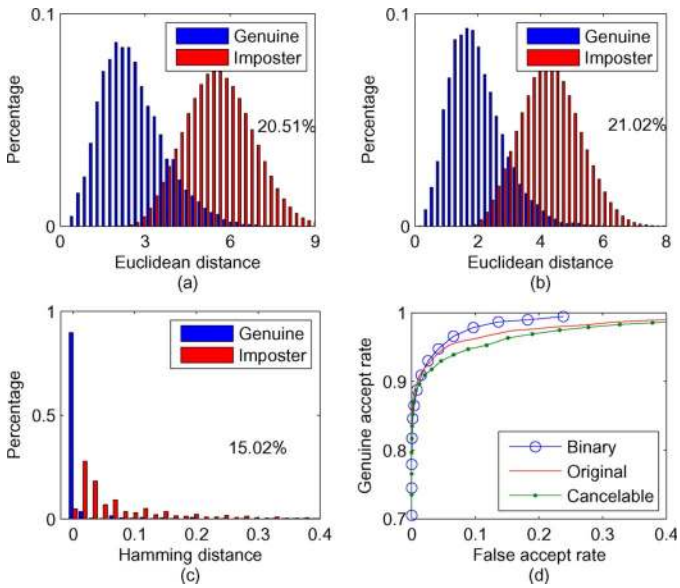


Fig. 12. Histogram and ROC curves on the CMU PIE database with illumination variation: (a) histogram of original template; (b) histogram of cancelable template; (c) histogram of binary template; and (d) ROC curves of original template, cancelable template, and binary template.

C. Part II: Accuracy Evaluation of the Hybrid Algorithm

This section evaluates and compares the accuracy of the hybrid algorithm with the recently developed RMQ algorithm [42]. The parameters in the proposed three-step hybrid algorithm are selected as follows. The dimensions after random projection (kr) in the first step are selected as 40, 150, and 250 for the CMU PIE database, FERET database, and FRGC database, respectively. Four different numbers (kc) of distinguishing points in the DP transform, namely 120, 150, 180, 210, are used in both the CMU PIE and FERET databases. In the FRGC database, 150, 200, 250, 350 are chosen as the number of distinguishing points.

Experiments are performed in two scenarios. In scenario one, the original feature template is projected into the same subspace (use the same projection matrix for all the users). In scenario two, original feature templates of different individuals are projected into different subspaces.

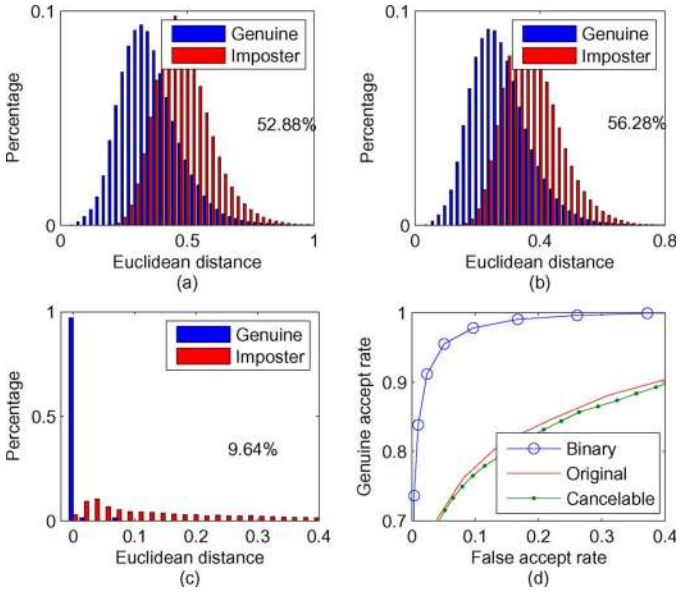


Fig. 13. Histogram and ROC curve on the CMU PIE database with illumination and pose variations: (a) histogram of original template; (b) histogram of cancelable template; (c) histogram of binary template; and (d) ROC curves of original template, cancelable template, and binary template.

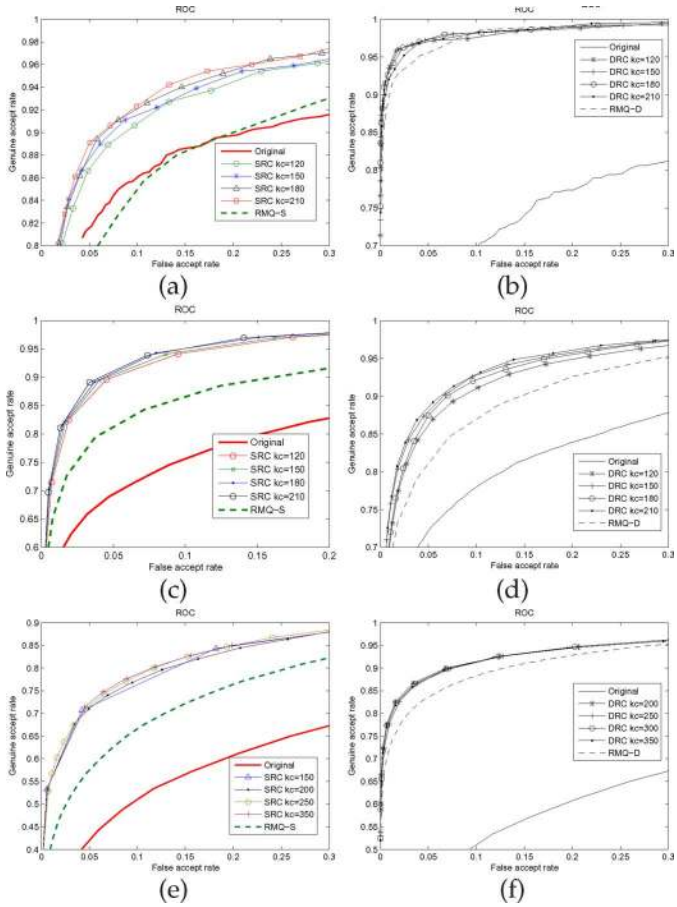


Fig. 14. Experimental results. (a) and (b) are on FERET database with $kr = 150$; (c) and (d) are on CMU PIE database with $kr = 40$; (e) and (f) are on FRGC database with $kr = 250$. (a), (c), and (e) are in scenario one while (b), (d), and (f) are in scenario two.

1) Scenario One: Authentication With the Same Subspace: Fig. 14(a), (c), and (e) show the experimental results with projection in the same subspace on the three databases, respectively. That means, query and reference templates share the same distinguishing points, thresholds, and projection matrix. In these figures, the labels "SRC," "original," and "RMQ-S" refer to the proposed hybrid algorithm, the original template (i.e., Fisherface), and the RMQ algorithm, respectively. The original template is used as a benchmark. These figures illustrate that, for all the selected parameter values, the proposed hybrid algorithm outperforms the RMQ algorithm as well as the Fisherrface. The equal error rate (EER) of these methods are also recorded and tabulated in Table III. With the use of the hybrid algorithm on the original template, the EER can be reduced from 12.58% to 8.55% for the FERET database, from 18.18% to 6.81% for the CMU PIE database, and from 31.75% to 16.68% for the FRGC database, respectively. This shows that the DP transform can enhance the template discriminability. Moreover, the proposed algorithm outperforms the RMQ algorithm.

2) Scenario Two: Authentication With Different Subspaces: Figs. 14(b), (d), and (f) show the experimental results with projections in different subspaces for the three databases, respectively. In these figures, the labels "DRC" and "RMQ-D" refer to the proposed hybrid algorithm and the RMQ algorithm, respectively. It can be seen from the figures that, for all selected parameters, our proposed hybrid algorithm outperforms the RMQ algorithm. The EER of these methods are recorded and tabulated in Table IV.

All the experiments were performed on a typical personal computer with a Pentium IV processor and the hybrid algorithm was implemented using MATLAB. Table V shows the computation time for training one class in the training process (t_{training}) and the time for testing one input query template (t_{testing}). These times include random projection, DP transform, and fuzzy commitment scheme.

D. Part III: Cancelability Analysis of the Hybrid Algorithm

As mentioned earlier, a new cancelable template can be generated by changing the random projection mapping. In this section, we would like to see whether an attacker could successfully access the system using a compromised cancelable template as well as all the user-specific information. In this case, we assume that the attacker has accessed to the original template, distinguishing points, thresholds, and the compromised random projection matrix.

To evaluate the cancelability of the proposed algorithm, three random projection matrices R_1, R_2, R_3 are randomly generated for testing. Six sets of experiments with $R_1 - R_1, R_2 - R_2, R_3 - R_3, R_1 - R_2, R_2 - R_3, R_3 - R_1$ are conducted, where $R_i - R_j$ means that matrix R_i is used for the enrollment while matrix R_j is used as query. The attacker has compromised a secure template and has all the user-specific information including the DP transform parameters (distinguishing points and thresholds), the original biometric data of the genuine user, and the compromised projection matrix R_j. A new secure template is generated and issued using the "new" projection matrix R_i by the system to replace the compromised one. The attacker attempts

TABLE III
EER (IN %) FOR THE HYBRID ALGORITHM, RMQ ALGORITHM AND THE ORIGINAL TEMPLATE (FISHERFACE) IN SCENARIO ONE

EER(%)	Original	SRC-kc_1	SRC-kc_2	SRC-kc_3	SRC-kc_4	RMQ-S
FERET	12.58	9.52	8.86	8.61	8.55	12.83
CMU	18.18	7.61	7.30	6.95	6.81	11.93
FRGC	31.75	17.93	17.40	16.70	16.68	21.87

TABLE IV
EER (IN %) FOR THE HYBRID ALGORITHM, RMQ ALGORITHM AND THE ORIGINAL TEMPLATE (FISHERFACE) IN SCENARIO TWO

EER(%)	Original	DRC-kc_1	DRC-kc_2	DRC-kc_3	DRC-kc_4	RMQ-D
FERET	21.66	3.38	3.36	3.34	3.62	4.49
CMU	18.18	9.41	8.41	8.70	8.26	11.68
FRGC	31.75	9.03	9.18	9.08	9.13	11.03

TABLE V
COMPUTATION TIME (IN SECONDS) OF THE HYBRID ALGORITHM

Time (sec)	$t_{training}$	$t_{testing}$
FERET	1.57	1.67×10^{-4}
CMU	2.00	1.41×10^{-4}
FRGC	24.75	3.01×10^{-4}

to match the reissued secure binary template via presenting the compromised R_j with the original biometric data of the genuine user. If the probability of successful matching is low, then the system has a high cancelability. We test the cancelability using the FERET, CMU PIE, and FRGC databases, with parameters $kr = 150$ and $kc = 210$, $kr = 40$ and $kc = 210$, and $kr = 250$ and $kc = 250$, respectively.

The results in Figs. 15(a)–(c) show that using templates generated by the matrix R_i to access a system in which the enrollment templates are generated using matrix $R_j, j \neq i$, is not feasible. The genuine accept rate (GAR) is as low as the false accept rate (FAR), implying that the query applying different projection matrix to the reference will mostly be rejected. This shows that the hybrid algorithm has good diversity. At the same time, the accuracy of matching between templates generated by the same matrix is high. The three ROC curves for three different matrices in each figure are very close, which implies that the replacement of projection matrix will not significantly affect the system accuracy. This shows that the proposed algorithm has a good revocability. Based on this, we conclude that the proposed algorithm has good cancelability.

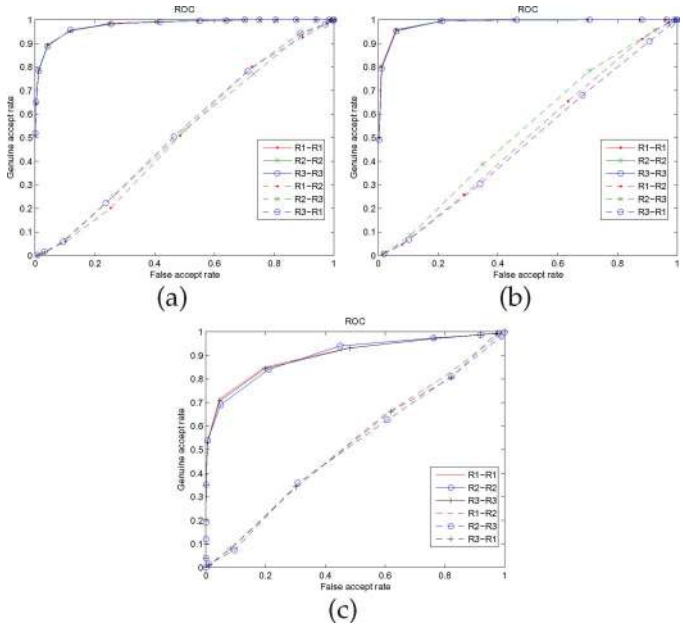


Fig. 15. Cancelability test. (a) On the FERET database with $kr = 150, kc = 210$, (b) on the CMU PIE database with $kr = 40$, $kc = 210$, and (c) on the FRGC database with $kr = 250, kc = 250$.

VI. SECURITY ANALYSIS

This section analyzes the security strength of the proposed algorithm as well as each step in the proposed algorithm. Two types of potential attacks, namely brute-force and "smart" attacks, are considered. The brute-force attack tries to guess the biometric data without any information while "smart" attacks make use of available information, such as matching score, to attack the system. Three smart attacks, namely masquerade [12] attack, hill-climbing attack [9], [13]–[16], and affine transformation attack [17], are considered in this paper. The summary is given in Table VI. It can be seen that the security strength of the random projection and DP transform are low and medium, respectively, in smart attacks, but the full hybrid algorithm is very secure. This justifies that a hybrid algorithm is required. Before reporting the analysis, we first discuss the data leakage of our scheme.

A. Data Leakage

Some information/data used in the algorithm are stored without protection. In a smart attack, an attacker may make use of this information. In order to consider the worst-case scenario, we assume that all the following unprotected data will be leaked to the attacker as follows:

1) the projection matrix in random projection;
2) the distinguishing points and thresholds in DP transform;
3) the unencrypted part $w_s - C_s$ in fuzzy commitment scheme.

B. Random Projection

The random projection step is secure against the brute-force attack because the original templates are real-valued and high-dimension. However, since the projection matrix is not protected, an attacker could make use of the projection matrix and

TABLE VI
SECURITY STRENGTH OF THE PROPOSED ALGORITHM AS WELL AS EACH STEP IN THE ALGORITHM

Attack	Random Projection	DP Transform	Fuzzy Commitment Scheme	Full Algorithm
Brute-force	High	High	High	High
Masquerade [12]	Low	Medium	High	High
Hill-climbing [9], [13]–[16]	Low	Medium	High	High
Affine transformation [17]	Low	High	High	High

construct its pseudoinverse matrix to recover the (approximated) original template from the projected templates. So this step is vulnerable to the masquerade attack. Also, since the matching scores between projected templates reflect the distance between original templates, the random projection is not secure against the hill-climbing attack and affine transformation attack.

In conclusion, the random projection is insecure.

C. DP Transform

In the second step, the DP transform converts the cancelable template into a binary cancelable template which is relatively secure. The distinguishing points and thresholds are exposed to attackers and may cause a smart brute-force attack because they contain the original template's information. However, to utilize them, the attackers need to know these distinguishing points are chosen under scenario one or scenario two (as discussed in Section IV-B2). As we have kc distinguishing points, there are totally 2^{kc} combinations. So it is hard to implement a smart brute-force attack with the known distinguishing points and thresholds. Therefore, DP transform has a high security against a brute-force attack.

Recovery of the cancelable template from the binary cancelable template might still be feasible because the transformed binary template contains discrimination information of the cancelable templates. Due to the information loss in the binarization, it would not be as easy as the first step. However, a masquerade attack may still be feasible. The attacker may not try to recover the original template, but constructs a fake original template directly. So, after random projection and DP transform, the input real-valued fake template will be converted to the same binary template. And therefore the attacker could access the system. While this attack is not straightforward, it is feasible. Therefore, the DP transform has a medium security against a masquerade attack.

Although the matching score from the DP transform is an integer value, an attacker may consider it a quantized matching score and adopt the hill climbing algorithm [14], [15]. In this way, the cancelable template could be approximately reconstructed. In turn, the DP transform has a medium security against the hill-climbing-based attack.

Finally, for the affine transformation attack, the real-valued cancelable template is very hard to be reconstructed from a binary template. Moreover, the quantized matching score, distinguishing points, and thresholds are not useful in affine transform attack. Therefore, the DP transform is very secure against an affine transform attack.

D. Fuzzy Commitment Scheme

In the fuzzy commitment scheme step, binary templates are encrypted and divided into two parts: $w_s - C_s$ and $\mathrm{Hash}(C_s)$.

For the masquerade attack, an attacker can get information from $w_s - C_s$. As long as the attacker does not know C_s, he cannot extract w_s from $w_s - C_s$. This is why a hash function is employed to protect C_s. Note that it is very hard to recover C_s from the hashed data $\mathrm{Hash}(C_s)$. For example, with the MD5 hashing algorithm [5], an attacker would require 2^{256-1} operations to recover the hashed data, on average, which is more expensive than the brute force attack. On the other hand, the attacker may try to guess C_s. In the proposed algorithm, C_s is a randomly generated kc bits binary template (kc is 210 or 350). Therefore, it will cost the attacker 2^{kc-1} operations to guess it. So the fuzzy commitment scheme step has high security strength against the masquerade attack.

The fuzzy commitment scheme performs matching between two hashed data $\mathrm{Hash}(w' - (w_s - C_s))$ and $\mathrm{Hash}(C_s)$. Because of the property of the hash function, the distance between $\mathrm{Hash}(w' - (w_s - C_s))$ and $\mathrm{Hash}(C_s)$ will not reveal distance information between $w' - (w_s - C_s)$ and C_s. Therefore, the matching score between two hashed data is useless for the hill-climbing attack and affine transformation attack. Therefore, the fuzzy commitment scheme is very secure against their attacks.

Since the binary template is hashed, it is extremely hard for attackers to directly extract the binary template from the stored data. However, a brute-force attack is still feasible. The probability of success of such an attack depends on the amount of information contained in the binary template. Here we measure the information content of the binary template.

In the ideal case, the entropy of the transformed binary template is the bit string length kc. So a brute force attack would require 2^{kc-1} operations, on average, to guess the binary template. In our experiments, kc is equal to 210 or 350 which is very secure with respect to the current industry standard. Unfortunately, in practice, due to the distribution of the original biometric data, the corresponding transformed binary template may not be uniformly distributed and may not have the maximum entropy kc. In this case, we need to calculate the true entropy of the binary templates. A direct calculation of the entropy of a bit string with large length kc is not feasible. Therefore, we choose two different ways to compute the entropy of the binary template: summation bit entropy and degrees of freedom.

In the first method, we calculate the entropy of the whole binary template via summing the entropies of each bit together. The entropy of each bit b_i ($i = 1, 2, \ldots, kc$) is computed by the binary entropy function

$$H(q_i) = -(q_i \log_2 q_i + (1 - q_i)\log_2(1 - q_i)) \tag{10}$$

where $q_i = \Pr(b_i = 1)$. The summation of these entropies for each bit is the total entropy of the binary template, which is shown in Table VII.

TABLE VII
INFORMATION CONTENT OF THE BINARY TEMPLATES

	FERET length = 210	CMU length = 210	FRGC length = 350
Summation Bit Entropy	208.5	207.8	349.3
Degrees of Freedom	206.3	203.5	347.3

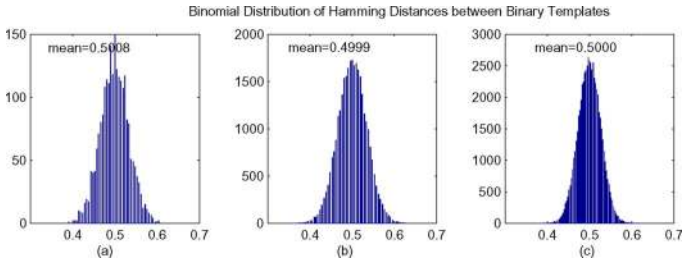


Fig. 16. Distributions of the Hamming distance between the reference binary template for the (a) CMU-PIE, (b) FERET, and (c) FRGC databases, respectively.

The equation assumes that bits in the binary template are uncorrelated to each other. However, in practice, the bits may not be totally independent, and thus the summation of the entropy of each bit is not equal to the entropy of the binary templates. To estimate the true entropy of the binary template, we adopt the degrees of freedom proposed by Daugman [11]. In Daugman's experiments, it was observed that the Hamming distances between different iriscodes (binary strings) follow a fractional binomial distribution, so the comparison between different iriscodes can be treated as a sequence of Bernoulli trials. Daugman calculated the degrees of freedom N as the discrimination entropy of the iriscodes. To estimate N, the variance σ^2 of the fractional binomial distribution is utilized, which has the following relationship with N:

$$N = \frac{p(1-p)}{\sigma^2} \tag{11}$$

where p is the average normalized Hamming distance and σ^2 is the variance of the normalized Hamming distances between binary templates from different individuals.

Note that (11) is applicable only in the situation that the Hamming distances between different binary strings closely follow a binomial distribution. In our case, the Hamming distances between different binary templates do fit the binomial distribution as shown in Fig. 16. So we use (11) to calculate the entropy of the binary templates.

We calculate the entropy of the reference binary templates of each face database, respectively, with the above two methods, and the results are shown in Table VII. It shows that the two measures are sufficiently close to each other as well as to binary template length kc. This implies that the bits in the reference binary template are almost uncorrelated and have a nearly equal chance to be either "0" or "1".

From the above analysis, it can be seen that the entropy of the binary template is very high, and therefore, the fuzzy commitment scheme is very secure against brute-force attack.

E. Full Algorithm

Since the three steps are integrated together in the proposed hybrid algorithm, the attacker cannot get the output from the first and/or second steps. Thus, the data leakage (projection matrix, distinguishing points and thresholds) of our algorithm will not reveal important information to attackers. Also, since the binary templates are encrypted, attackers would not be able to access the binary templates. Therefore, neither the masquerade attack nor the hill-climbing attack/affine transformation attack would effectively break the algorithm. In conclusion, the proposed hybrid algorithm has high security strength against both the brute-force attack and smart attacks.

VII. CONCLUSION

A hybrid framework for face template protection has been developed. The proposed hybrid approach takes advantage of both the transform-based approach and biometric cryptosystem approach. The proposed framework consists of three parts, namely cancelable transform, discriminability enhancement conversion, and template protection. Each part provides the template cancelable ability, discriminability, and security, respectively.

Based on the proposed framework, a hybrid algorithm composed of random projection, DP transform, and a fuzzy commitment scheme is also developed. The random projection is used to provide the cancelability. The DP transform is developed to convert real-valued cancelable templates to binary templates while the discriminability is preserved, so that it can be easily encrypted in the fuzzy commitment scheme. Since there may have a discriminability loss in the random projection step, DP transform could compensate the lost in the projection step. This algorithm overcomes the limitation of the random projection and the fuzzy commitment scheme. The fuzzy commitment scheme is finally employed to encrypt the binary cancelable face template. A comprehensive security analysis of the proposed algorithm is also reported. It is shown that the proposed algorithm is secure against both burst force and smart attacks. Three publicly available face databases, namely the FERET, CMU PIE, and FRGC databases, have been used to evaluate the proposed method. Experimental results show that the proposed method not only protects the template but is also able to increase the template discriminability.

ACKNOWLEDGMENT

The authors would like to thank CMU and NIST for the CMU-PIE, FERET, and FRGC databases used in this paper.

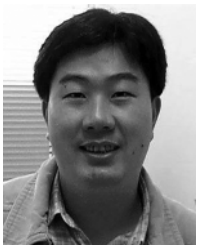
REFERENCES

[1] W. B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," in *Proc. Int. Conf. Modern Analysis and Probability*, 1984, pp. 189–206.
[2] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, pp. 2019–2040, 2003.
[3] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 711–720, Jul. 1997.
[4] J. I. Hall, "Generalized Reed–Solomon codes," *Notes on Coding Theory*, pp. 63–76, 2003.

[5] R. L. Rivest, The MD5 message-digest algorithm Network Working Group, MIT Laboratory for Computer Science and RSA Data Security, Inc., RFC1321, 1992.
[6] A. K. Jain and S. Pankanti, "A touch of money," *IEEE Spectrum*, vol. 43, no. 7, pp. 22–27, Jul. 2006.
[7] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometric-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.
[8] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag.*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[9] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, pp. 948–960, 2004.
[10] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.
[11] J. Daugman, "The importance of being random: Statistical principles of iris recognition," *Pattern Recogni.*, vol. 36, no. 2, pp. 279–291, 2003.
[12] C. Hill, "Risk of Masquerade Arising from the Storage of Biometrics," B.S. thesis, Australian National Univ., Canberra, Australia [Online]. Available: http://chris.fornax.net/biometrics.html
[13] A. Alder, "Sample images can be independently restored from face recognition templates," *Elect. Comput. Eng.*, vol. 2, pp. 1163–1166, 2003.
[14] A. Adler, "Images can be regenerated from quantized biometric match score data," in *Proc. Canadian Conf. Electrical and Computer Engineering*, 2004, pp. 469–472.
[15] A. Alder, "Vulnerabilities in biometric encryption systems," in *Proc. IEEE Int. Conf. Audio- and Video-Based Biometric Person Authentication*, 2005, vol. 3546, pp. 1100–1109.
[16] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," *Proc. SPIE*, vol. 5306, pp. 622–633, 2004.
[17] P. Mohanty, S. Sarkar, and R. Kasturi, "Privacy & security issues related to match scores," in *Proc. Conf. Computer Vision and Pattern Recognition Workshop*, 2006, pp. 162–165.
[18] C. Soutar, D. Roberge, A. Stoinav, G. Gilroy, and V. Kumar, "Biometric encryption using image processing," *Proc. SPIE*, vol. 3314, pp. 174–188, 1998.
[19] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *IEEE Symp. Privacy and Security*, 1998, pp. 148–157.
[20] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. Sixth ACM Conf. Comp. and Commun. Security*, 1999, pp. 28–36.
[21] A. Juels and M. Sudan, "A fuzzy vault scheme," in *IEEE Int. Symp. Information Theory*, 2002, p. 408.
[22] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcard-based fingerprint authentication," in *Proc. ACMSIGMM Multimedia, Biometrics Methods and Applications Workshop*, 2003, pp. 45–52.
[23] U. Uludag and A. K. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Proc. Computer Vision and Pattern Recognition Workshop*, 2006, pp. 163–163.
[24] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, Mar. 2005, vol. 5, pp. 609–612.
[25] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Proc. Int. Conf. Pattern Recognition*, 2008, pp. 1–4.
[26] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," in *Proc. 2nd Int. Conf. Biometrics*, Aug. 2007, pp. 800–808.
[27] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Advances in Cryptology—Eurocrypt*, 2004, pp. 523–540.
[28] 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.
[29] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," in *Proc. 2nd Int. Conf. Biometrics*, Aug. 2007, pp. 760–769.
[30] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Proc. Sixth Int. Conf. Audio and Video-Based Biometric Person Authentication*, 2005, pp. 310–319.
[31] F. Hao, R. Anderson, and J. Daugman, Combining Cryptography with Biometric Effectively University of Cambridge, Tech. Rep. UCAM-CL-TR-640, 2005, ISSN 1476-2986.
[32] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. Yedidia, "Using distributed source coding to secure fingerprint biometric," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, 2007, pp. 129–132.
[33] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric template with sketch: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pt. 2, pp. 503–512, Sep. 2007.
[34] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *ECCV Workshop BioAW*, 2004, pp. 158–170.
[35] T. Kevenaar, G. Schrijen, M. Veen, A. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in *Proc. Fourth IEEE Automatic Identification Advanced Technologies*, 2004, pp. 21–26.
[36] Y. Sutcu, S. Rane, J. Yedidia, S. Draper, and A. Vetro, "Feature extraction for a slepian-wolf biometric system using ldpc codes," in *Proc. IEEE Int. Symp. Information Theory*, 2008, pp. 6–11.
[37] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on key stroke dynamics," in *Proc. ACM Conf. Computer and Communication Security*, 1999, pp. 73–82.
[38] F. Monrose, M. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Proc. IEEE Symp. Security and Privacy*, 2001, pp. 202–213.
[39] A. Teoh, D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.
[40] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," in *Proc. 7th IFIP TC6/TC11 Conf. Commun. Multimedia Security*, 2003, vol. 22, pp. 1–13.
[41] D. Ngo, A. 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.
[42] A. Teoh, A. Goh, and D. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.
[43] Y. Sutcu, H. Sencar, and N. Nemon, "A secure biometric authentication scheme based on roubst hashing," in *Proc. Seventh Workshop Multimedia and Security*, 2005, pp. 111–116.
[44] S. Tulyakov, V. Chavan, and V. Govindaraju, "Symmetric hash functions for fingerprint minutiae," in *Proc. Int. Workshop Pattern Recognition for Crime Prevention, Security, and Surveillance*, 2005, pp. 30–38.
[45] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *ACISP 2005*, pp. 242–252.
[46] N. Ratha, J. Connell, R. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *Proc. Int. Conf. Pattern Recognition*, 2006, pp. 370–373.
[47] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–752, Apr. 2007.
[48] Y. C. Feng and P. C. Yuen, "Protecting face biometric data on smartcard with Reed–Solomon code," in *Proc. IEEE Computer Vision and Pattern Recognition Workshop on Biometrics*, 2006, pp. 29–34.
[49] Y. C. Feng and P. C. Yuen, "Class-distribution preserving transform for face biometric data security," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP)*, 2007, pp. 141–144.
[50] Y. C. Feng and P. C. Yuen, "Selection of distinguish points for class distribution preserving transform for biometric template protection," in *Proc. IEEE Int. Conf. Biometrics (ICB)*, 2007, pp. 636–645.
[51] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.* 2008 [Online]. Available: http://www.hindawi.com/journals/asp/2008/579416.abs.html
[52] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for face template protection," in *Proc. Int. Society for Optical Engineering (SPIE)*, 2008, vol. 6944, pp. 1–11.

Yi C. Feng received the Bachelor of Engineering degree from Tsinghua University, in 2004, and the Mphil. degree in computer science from Hong Kong Baptist University, in 2007. He is currently working toward the Ph.D. degree at Hong Kong Baptist University.

His research interests are in pattern recognition, biometric security, and privacy.



Pong C. Yuen (S'92–M'93) received the B.Sc. degree in electronic engineering with first class honours from City Polytechnic of Hong Kong, in 1989, and the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong, in 1993.

He joined the Department of Computer Science, Hong Kong Baptist University, in 1993, as an Assistant Professor and currently is a Professor. He was a recipient of the University Fellowship to visit The University of Sydney in 1996. He was associated with the Laboratory of Imaging Science and Engineering, Department of Electrical Engineering and worked with Prof. Hong Yan. In 1998, he spent a six-month sabbatical leave at The University of Maryland Institute for Advanced Computer Studies (UMIACS), University of Maryland at College Park. He was associated with the Computer Vision Laboratory. From June 2005 to January 2006, he was a visiting professor at GRAVIR Laboratory (GRAphics, VIsion and Robotics) of INRIA Rhone Alpes, France. He was associated with PRIMA Group. He was the director of Croucher Advanced Study Institute (ASI) on biometric authentication in 2004 and is the director of Croucher ASI on Biometric Security and Privacy in 2007. He has been actively involved in many international conferences as an organizing committee and/or technical program committee member. Recently, he was the track cochair of the International Conference on Pattern Recognition 2006.

Dr. Yuen is an editorial board member of *Pattern Recognition*. His current research interests include human face processing and recognition, biometric security and privacy, and human activity recognition.

Anil K. Jain (S'70–M'72–SM'86–F'91) is a University Distinguished Professor in the Department of Computer Science and Engineering at Michigan State University, East Lansing. His research interests include pattern recognition and biometric authentication.

Dr. Jain received the 1996 IEEE TRANSACTIONS ON NEURAL NETWORKS Outstanding Paper Award and the Pattern Recognition Society best paper awards in 1987, 1991, and 2005. He served as the Editor-in-Chief of the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE (1991–94). He is a fellow of the AAAS, ACM, IAPR, and SPIE. He has received Fulbright, Guggenheim, Alexander von Humboldt, IEEE Computer Society Technical Achievement, IEEE Wallace McDowell, and IAPR King-Sun Fu awards. He holds six patents in the area of fngerprints and is the coauthor of a number of books, including *Handbook of Biometrics* (2007), *Handbook of Multibiometrics* (2006), *Handbook of Face Recognition* (2005), *Handbook of Fingerprint Recognition* (2003), *BIOMETRICS: Personal Identification in Networked Society* (1999), and *Algorithms For Clustering Data* (1988). ISI has designated him as a highly cited researcher. According to Citeseer, his book *Algorithms for Clustering Data* (Prentice-Hall, 1988) is ranked #93 in Most Cited Articles in Computer Science. He is currently serving as an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and *ACM Transactions on Knowledge Discovery in Data*. He served as a member of the Defense Science Board and served on The National Academies committees on Whither Biometrics and Improvised Explosive Devices.