Available online at www.sciencedirect.com
ScienceDirect
Pattern Recognition 41 (2008) 2034–2044
PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY
www.elsevier.com/locate/pr

Cancellable biometrics and annotations on BioHash

Andrew B.J. Teoh[a,*], Yip Wai Kuan[b], Sangyoun Lee[a]

[a]*Biometrics Engineering Research Center (BERC), Yonsei University, Seoul, South Korea*
[b]*Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia*

Received 14 February 2006; received in revised form 18 June 2007; accepted 3 December 2007

Abstract

Lately, the once powerful one-factor authentication which is based solely on either password, token or biometric approach, appears to be insufficient in addressing the challenges of identity frauds. For example, the sole biometric approach suffers from the privacy invasion and non-revocable issues. Passwords and tokens are easily forgotten and lost. To address these issues, the notion of cancellable biometrics was introduced to denote biometric templates that can be cancelled and replaced with the inclusion of another independent authentication factor. BioHash is a form of cancellable biometrics which mixes a set of user-specific random vectors with biometric features. In verification setting, BioHash is able to deliver extremely low error rates as compared to the sole biometric approach when a genuine token is used. However, this raises the possibility of two identity theft scenarios: (i) stolen-biometrics, in which an impostor possesses intercepted biometric data of sufficient high quality to be considered genuine and (ii) stolen-token, in which an impostor has access to the genuine token and used by the impostor to claim as the genuine user. We found that the recognition rate for the latter case is poorer. In this paper, the quantised random projection ensemble based on the Johnson–Lindenstrauss Lemma is used to establish the mathematical foundation of BioHash. Based on this model, we elucidate the characteristics of BioHash in pattern recognition as well as security view points and propose new methods to rectify the stolen-token problem.

Keywords: BioHash; Cancellable biometrics; Random projection; Johnson–Lindenstrauss lemma

1. Introduction

Although biometrics is a powerful tool against repudiation and has been widely deployed in various security systems, biometric characteristics (especially physiological biometrics) are largely immutable, resulting in permanent biometric compromise when stolen or leaked. The concept of cancellable biometrics was introduced [1,2] to denote biometric templates that can be cancelled and replaced, as well as being unique for every application. Cancellable biometrics requires storage of the transformed (not actual) version of the biometric template and hence provides higher privacy levels by allowing multiple templates to be associated with the same biometric data. This promotes non-linkability of user's biometric data stored across various databases.

Cancellable biometrics is a relatively new direction of research, spurred on by the privacy invasion and biometrics non-revocable issues. There are three principal criteria to be fulfilled before a cancellable biometric template can be considered useful [3]:

(i) Diversity: no same cancellable template can be used in two different applications.
(ii) Reusability: straightforward revocation and reissuance in the event of compromise.
(iii) One-way transformation: non-invertibility of template computation to prevent recovery of secret biometric data.

From a pattern recognition view point, the formulation should not deteriorate the recognition performance. There are several methods proposed by the research community and they will be further elaborated in Section 2.

Recently, works reported in [4–7] proposed a cancellable biometrics formulation known as BioHash which fulfilled the

* Corresponding author. Tel.: +82 2 2123 6609; fax: +82 2 362 5563.
E-mail addresses: bjteoh@ieee.org (A.B.J. Teoh), syleee@yonsei.ac.kr (Y.W. Kuan), yip.wai.kuan04@mmu.edu.my (S. Lee).

0031-3203/$30.00
doi:10.1016/j.patcog.2007.12.002

criteria above. BioHash combined the biometric template (face, fingerprint and palmprint biometrics which can be represented as a fixed-length and ordered feature vector) with user-specific tokenised random numbers (TRN) to produce a set of non-invertible binary bit strings. The BioHash is dependent on both biometric and TRN and it is irreproducible without presenting the two simultaneously. The inversion of BioHash to recover biometric data is impossible because factoring the inner products of biometrics feature and TRN is intractable. Furthermore, this method delivered extremely low error rates when the genuine token was used. The reported results have aroused great attention from researchers as seen in reports by Cheung et al. [8,9] and Kong et al. [10]. A group of researchers asserted that the outstanding performance of BioHash is actually based on the sole use of TRN; therefore they conjectured that the introduction of any forms of biometrics becomes meaningless since the system can solely rely on the tokens without a flaw [9,10]. They also commented that the non-invertibility of the random mixing process will destroy the optimality of most feature representations [8], thus deteriorating the recognition accuracy when the genuine token is stolen and used by an impostor (known as the *stolen-token* scenario).

In this paper, we address the two concerns of BioHash through its mathematical model. We show that BioHash is essentially an ensemble of quantised random projections (RPs) which preserves the intra-class variations while enhancing the inter-class variations when the genuine token is used. On the other hand, the result reverts to the original performance or slightly poorer in the stolen-token scenario. However, this problem can be easily rectified by using the techniques that will be discussed in this paper. We also considered another scenario that might occur in a real world application, namely the *stolen-biometrics* scenario—in which fraudulent verification is attempted using only intercepted biometric data associated with the genuine user, but without the associated token. In addition, we further solidify the security characteristics which were not addressed in the previous papers based on our established model. We utilized face biometrics as the subject of study in this paper since there is a known and standardized database for comparison.

The outline of the paper is as follows: Section 3 contains a literature survey on related research; Section 4 outlines the BioHash reformulation and its statistical analysis; and Section 4 presents the experimental results and the discussion. Section 5 discusses a variant of BioHash aimed at solving the stolen-token problem. Finally, Section 6 provides the security analysis of BioHash. Conclusions are drawn in Section 7.

2. Previous works on cancellable biometrics

The first attempt towards using indirect biometric templates was recorded by Davida et al. [11] but the concrete idea of cancellable biometrics was established by Ratha et al. [1] and Bolle et al. [2]. This research area is growing rapidly and many new techniques have been proposed since then. These methods generally fall into three categories: (1) error-correcting based, (2) integration of external factors and biometrics, and (3) non-invertible transforms.

2.1. Error-correcting based

In the error-correcting code scheme, codeword and decoding functions are established from the biometric templates during enrolment. The codeword value can be used either as a key or hash. At the authentication stage, the input biometric data are used to compute or recover the codeword. For instance, Davida et al. [11] proposed a majority decoding scheme for iris biometrics. In their scheme, a pair of related binary representations of iris code, the input, and test template which is 2048 bit in length was extracted through the majority decoding scheme and matched by using hamming distance (HD). Subsequently, algebraic decoding was applied in order to rectify the offset of the test data using offline checksums. In certain extent, the scheme may preserve user privacy as the biometric template was non-invertible. However, neither the issues of reusability/cancelability nor practical work as addressed. Juels et al. [12,13] generalized and improved the Davida et al. [11] scheme through a modification in error-correcting codes, and is hence reduced the code size and achieved higher resilience. Clancy et al. [14] implemented the technique that was proposed by Juels et al. [13]. In Clancy's work, a group of minutia points were extracted from the input fingerprint to bind in a locking set using polynomial-based secret sharing scheme. Subsequently, a set of non-related chaff points were added intentionally to 'shadow' the key to maximize the unlocking computational complexity, where the secret key could only be recovered if there is a substantial overlap between the input and test fingerprint. The method has been theoretically proven to be secure in protecting the secrecy of fingerprint, but is beyond the level of practical use due to high false reject rate (FRR) at 20–30% and huge storage requirement. Most recently, Hao et al. [15] proposed an improved Juels et al. [12,13] scheme based on the hybrid error-correction techniques. It reported a very low FRR around 0.47% and 0% false accept rate (FAR) using iris biometric data.

Linnartz and Tuyls [16] assumed that a noise-free template X is available at the enrolment time and use this to enrol a secret S to generate a helper data W. They assume that each dimension of the template is quantised at q resolution levels. In each dimension, the process of obtaining W is equivalent to finding residuals that must be added to X to fit into odd or even grid quantum depending upon whether the corresponding S bit is zero or one. At verification time, the (noise-prone) biometric template Y is used to obtain S', which is approximately the same as S. According to the paper, the relatively few errors in S' can be corrected using error-correction techniques. The proposed technique assumes that the noise in each dimension is relatively small compared to the quantisation Q. Tuyls et al. [17] described a practical system based on the proposed scheme, achieving equal error rates (EERs) around 5.3% and 4.5% in two datasets. However, the secret bit length generated (40 bits) is still low for most security applications.

2.2. Integration of external factors and biometrics

The second approach of integrating an independent factor with biometric features was first proposed by Soutar et al. [18]. They described a different approach for generating cancellable biometrics from fingerprints using optical computing techniques. With a few fingerprint images and a set of random numbers for training, the algorithm creates a complex-valued correlation filter function which is mathematically optimised to possess both distortion tolerance and discrimination properties. An output pattern c_0 is also generated via correlation between the training fingerprint image and the correlation filter. This output pattern will then be binarised using a simple threshold-based decision and used to derive cryptographic key using redundant error correction code resulting in a lookup table T. However, the method did not carry rigorous security guarantees and the resulting FAR and FRR are unknown. Similarly, Savvides et al. [19] proposed a cancellable biometrics scheme that encrypts the training images used to synthesize the correlation filter for biometrics authentication. They demonstrated that convolving the training images with any random convolution kernel prior to building the biometric filter does not change the resulting correlation output peak-to-sidelobe ratios, thus preserving the authentication performance. However, the security will be jeopardised via a deterministic deconvolution with a known random kernel. Another method that falls under this category is the BioHash scheme.

2.3. Non-invertible transforms

In non-invertible transformed-based approach, instead of storing the original biometric, the biometric is transformed using a one-way function. The transformation occurs in the same signal or feature space as the original biometric. For example, Bolle et al. [2] introduced an intentional distortion of a biometrics signal based on a chosen transform function. The biometrics signal was distorted in the same fashion at each presentation, that is, during enrolment and for every subsequent authentication. With this approach, every instance of enrolment can use a different transform function thus rendering cross-matching impossible. Furthermore, if one variant of the biometrics is compromised, then the transformation can simply be changed to create a new variant for re-enrolment. However, it is not an easy task to design such a function due to the limiting characteristics of the feature vector. Generally, extracted features take different values changing in some range depend to the type of biometrics used and feature extractor, rather than taking precise values, and therefore transform function has to satisfy some smoothness criteria. While providing robustness against to variability of same user's biometric data, that transformation must also distinguish different users successfully. Sutcu et al. [20] realised this idea by proposing a sum of weighted and shifted Gaussian functions as a non-invertible and scalable transformation function. However, their preliminary results showed that the method was not favourable in terms of recognition performance. Ang et al. [21] proposed the similar technique with the key-dependent transformation so that the matching can be done in the transformed domain. Yet, both transforms degrade the matching accuracy significantly in the altered domain.

3. BioHash revisited and reformulation

The initial BioHashing [6] scheme is simplified and described as follows:

(i) Feature extraction is used to extract the biometric feature from the raw input. The biometric feature is represented as a fixed-length vector, $\Gamma \in \Re^n$, with n being the length of Γ.
(ii) Random basis generation using a user-specific TRN to generate m orthonormal pseudo-random vectors, $\{\boldsymbol{r}_{\perp i} \in \Re^n | i = 1, \ldots, m\}$ and $m \leqslant n$.
(iii) Token and biometric mixing via $\{< \Gamma | \boldsymbol{r}_{\perp i} > | i = 1, \ldots, m\}$ with $\langle \cdot | \cdot \rangle$ indicating the inner product operation.
(iv) Binary discretisation to compute an m bit BioHash template, $b = \{b_i | i = 1, \ldots, m\}$ from

$$b_i = \begin{cases} 0 & \text{if } \langle \Gamma \| \boldsymbol{r}_{\perp i} \rangle \leqslant \tau, \\ 1 & \text{if } \langle \Gamma \| \boldsymbol{r}_{\perp i} \rangle > \tau, \end{cases}$$

with τ being an empirically determined threshold.

Fig. 1 illustrates the progression of BioHashing.

For implementation, the BioHash template can be stored in a centralised database at enrolment. During verification, the extracted feature is combined with the genuine TRN and the resulting BioHash template is compared with the enrolled template by using HD (the difference in the number of bits).

Mathematically, the BioHash can be reformulated as

$$\boldsymbol{b} = \mathrm{Sig}\left(\sum_j \Gamma \boldsymbol{r}_{\perp j} - \tau \right), \tag{1}$$

where $\mathrm{Sig}(\cdot)$ is defined as a signum function and τ is the preset threshold, which is normally set to $\tau = 0$. Alternatively, Eq. (1) can be represented as

$$\boldsymbol{b} = \mathrm{Sig}(\boldsymbol{R}\Gamma - \tau). \tag{2}$$

The matrix $\boldsymbol{R}$ being the $m \times n$ orthonormal random matrix and $m < n$. Its columns are the realizations of independent and identically distributed (i.i.d.) zero-mean normal variables.

In the literature, $\boldsymbol{R}\Gamma$ is known as random projection (RP) [22]. RP is a simple yet powerful dimension reduction technique that uses random matrices, $\boldsymbol{R}$ to project the biometric feature, Γ, into low-dimensional spaces. For BioHashing, RP is quantised to binary bit string by thresholding τ such that on average 50% of the projections have absolute value greater than τ, while the remaining 50% have absolute value less than τ. Eq. (2) only applies to a user who holds $\boldsymbol{R}$ (the user-specific random vectors), and thus the formulation can be extended to introduce an ensemble of random subspaces, where each

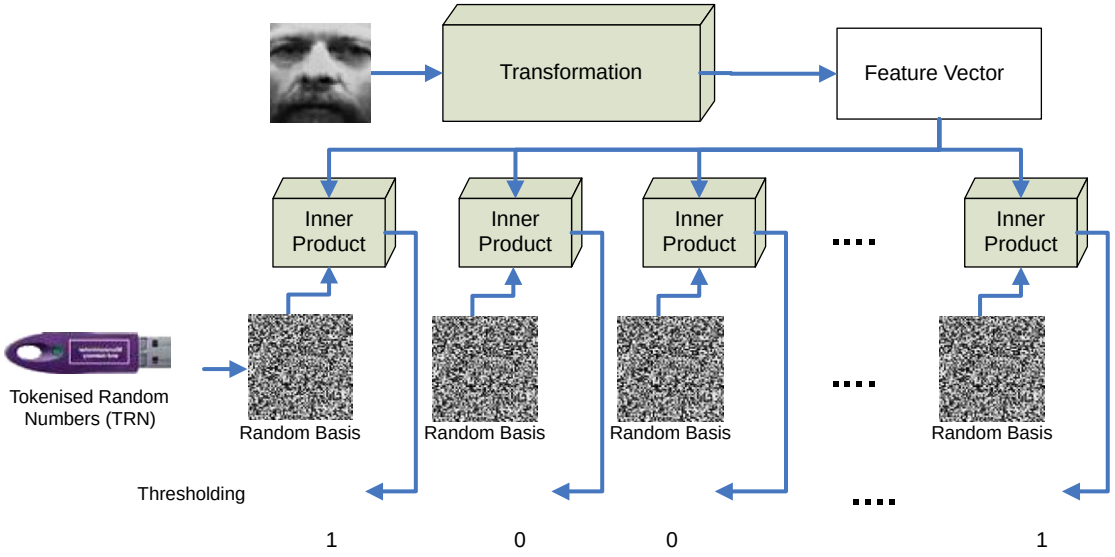

Fig. 1. The progression of BioHashing.

subspace represents different individual k. The resulting bit string, BioHash is given as follows:

$$\boldsymbol{b}^k = \mathrm{Sig}(\boldsymbol{R}^k \boldsymbol{I}^k - \tau) \quad \text{with } k = 1, \ldots, g, \tag{3}$$

where g is the total number of users in the system.

3.1. Random projection

The underlying behaviour of BioHash or quantised RP can be explained by using Johnson–Lindenstrauss Lemma (JL Lemma) [23]:

For any $0 < \varepsilon < 1$ and any integer k, let m be a positive integer such that $m \geqslant \frac{4 \log k}{\varepsilon^2/2 - \varepsilon^3/3}$. Then for any set S of $k = |S\|$ data points in $\Re^n$, there is a map $f: \Re^n \to \Re^m$, such that for all $\boldsymbol{x}, \boldsymbol{y} \in S$:

$$(1-\varepsilon)\|\boldsymbol{x}-\boldsymbol{y}\|^2 \leqslant \|f(\boldsymbol{x}) - f(\boldsymbol{y})\|^2 \leqslant (1+\varepsilon)\|\boldsymbol{x}-\boldsymbol{y}\|^2. \tag{4}$$

JL Lemma states that a set of k points in a high dimensional Euclidean space can be mapped down onto an $m \geqslant O(\log(k)/\varepsilon^2)$ dimensional subspace such that the distances between the points are approximately preserved (i.e. not distorted more than a factor of $1 \pm \varepsilon$, for any $0 < \varepsilon < 1$).

The effectiveness of RP depends on how well the pair-wise distances of the two feature vectors from the same user with random vectors, $\boldsymbol{r_i} \in \boldsymbol{R}$, are preserved. Since $\boldsymbol{r_i}$ is often standard-normally distributed, it is sufficient to use matrices with independent column vector entries chosen from a distribution with bound support [22].

Given two feature vectors, $\boldsymbol{x}$ and $\boldsymbol{y}$, and let $\tilde{\boldsymbol{x}} = \boldsymbol{R}\boldsymbol{x}$ *and* $\tilde{\boldsymbol{y}} = \boldsymbol{R}\boldsymbol{y}$, *where* $\|\tilde{\boldsymbol{x}}\| = \|\tilde{\boldsymbol{y}}\| = 1$, *hence* $\|\tilde{\boldsymbol{x}} - \tilde{\boldsymbol{y}}\|^2 = \|\boldsymbol{x} - \boldsymbol{y}\|^2$.

Proof.

$$\|\tilde{\boldsymbol{x}} - \tilde{\boldsymbol{y}}\|^2 = \|\tilde{\boldsymbol{x}}\|^2 + \|\tilde{\boldsymbol{y}}\|^2 - 2\tilde{\boldsymbol{x}}^T\tilde{\boldsymbol{y}} = 2(1 - \tilde{\boldsymbol{x}}^T\tilde{\boldsymbol{y}})$$

Let

$$\begin{aligned}\alpha &= 1 - \tilde{\boldsymbol{x}}^{\mathrm{T}}\tilde{\boldsymbol{y}} \\ &= 1 - \boldsymbol{x}^T\boldsymbol{R}^T\boldsymbol{R}\boldsymbol{y}, \quad 0 < \alpha < 1\end{aligned} \tag{5}$$

with α in Eq. (5) as correlation and it will be used as the classification metric.

The matrix $\boldsymbol{R}^{\mathrm{T}}\boldsymbol{R}$ can be decomposed as follows:

$$\boldsymbol{R}^{\mathrm{T}}\boldsymbol{R} = \boldsymbol{I} + \delta_{ij}, \quad i \neq j,$$

where $\delta_{ij} = \boldsymbol{r}_i^{\mathrm{T}}\boldsymbol{r}_j$, $\boldsymbol{r_i}\boldsymbol{r_j} \in \boldsymbol{R}$, $\delta_{ii} = 0$ for $\forall i$ and $\boldsymbol{I}$ is an identity matrix.

If $\boldsymbol{R}$ is orthonormal and $\delta_{ij} = 0$; hence, $\boldsymbol{R}^{\mathrm{T}}\boldsymbol{R} = \boldsymbol{I}$ and $\tilde{\boldsymbol{x}}^{\mathrm{T}}\tilde{\boldsymbol{y}} = \boldsymbol{x}^{\mathrm{T}}\mathbf{y}$. □

This concludes that the pair-wise distances between the feature vectors are preserved in the random subspace. Note that the pair-wise distances can be described collectively in terms of their statistical measures, such as the mean and standard deviation. In short, the statistical characteristics of the feature topology are preserved under RP.

It is worth noting that the degree of preservation of the pair-wise distances increases with the random projected feature dimension, m, until the maximum limit is reached when $m = n$.

The effect of m on the preservation power of the pair-wise distances can be analysed statistically through the small perturbations of $\delta_{ij} = \boldsymbol{r}_i^{\mathrm{T}}\boldsymbol{r}_j$, where $i \neq j$ [22], $\boldsymbol{r}_i$ and $\boldsymbol{r}_j$ are two normalized random vectors independently drawn from a standard normal distribution, $N(0, 1)$. The variable δ_{ij} can be regarded as an estimator of the correlation coefficient between two zero-mean unit-variance normally distributed random variables. Due to the Fisher transformation [24], δ_{ij} becomes $0.5\ \ln(1+\delta_{ij})/(1-\delta_{ij})$, which is normally distributed with variance $1/(m-3)$. As m becomes larger, $\boldsymbol{\sigma}_{\boldsymbol{\delta}}^2 \approx 1/m$ and $\delta_{ij} \sim N(0, 1/m)$. In other words as m increases, the entries of δ_{ij} become smaller; thus $\boldsymbol{R}^{\mathrm{T}}\boldsymbol{R} \approx \boldsymbol{I}$. The RP of the same

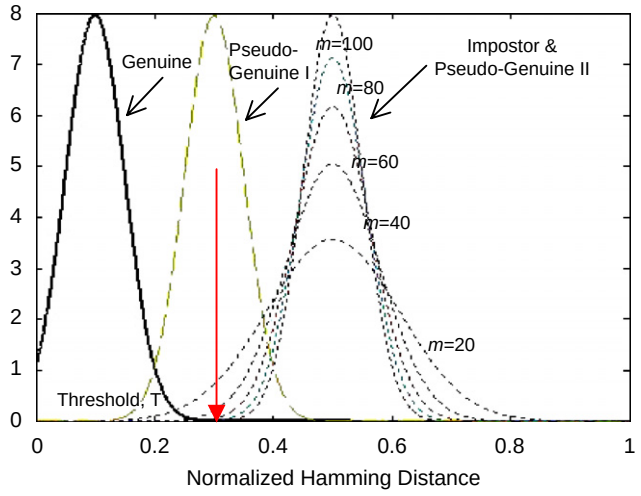

Fig. 2. Theoretical genuine, impostor, pseudo-genuine Types I and II distributions for BioHash.

class implies that the genuine distribution (when different BioHashes of the same individual are compared) can be preserved by transforming a random subspace subjected by $\boldsymbol{R}$ which is orthonormal and standard-normally distributed, and $m \approx n$.

Since BioHash is actually a quantised RP, the genuine distribution of BioHash could not be identical (in terms of its mean and standard deviation) to the genuine distribution of Γ due to the loss of information. Nonetheless, the deviation is not great. This will be empirically shown in Section 4.

3.2. Genuine and impostor distribution analysis for BioHash

BioHash authentication is essentially the *failure of a test of statistical independence*, similar to the Daugman IrisCode [25] prescription. This test is statistically inclined to succeed when templates computed from different individuals are compared, and to fail when templates of the same individual are compared. The statistical property of g BioHashes, which are constructed using uncorrelated and distinctive $\boldsymbol{R}^k$, is the outcome of a Bernoulli trial. Therefore, the impostor distribution corresponds to a binomial distribution having mean HD, $d_{HD}=0.5$, and degree of freedom, $\gamma = m$:

$$f(x) = \frac{\gamma!}{\lambda!(\gamma-\lambda)!} p^{\lambda}(1-p)^{(\gamma-\lambda)}, \tag{6}$$

with expectation $=p$ and standard deviation $=\sqrt{\frac{p(1-p)}{m}}$, where $x=\lambda/\gamma$ is the outcome fraction of γ Bernoulli trials and $p=0.5$. In our case, x is the HD, the fraction of bits that happens to agree when two different BioHashes from two different individuals are compared. This implies that the impostor distribution will be centred at 0.5, and the standard deviation will decrease as m increases to yield a steeper slope as shown in Fig. 2.

As illustrated in Fig. 2, the genuine and impostor distributions tend to separate better as m increases, thus decreasing the $\mathrm{FAR} = 100\int_0^T P_{\mathrm{Im}}(x)\,\mathrm{d}x\%$ and $\mathrm{FRR} = 100\int_T^1 P_{\mathrm{Ge}}(x)\,\mathrm{d}x\%$ simultaneously, where T is a decision threshold and P_{Ge} and P_{Im} refer to genuine and impostor distribution, respectively. The impostor distribution is shifted to the right and centred at 0.5, while the standard deviation (the impostor distribution profile) shrinks according to $0.5/\sqrt{m}$. On the other hand, the genuine distribution is roughly preserved when m is large. The clear separation indicates that BioHash results in dramatically reduced error rates in comparison to genuine vs impostor distribution based on measurement of continuously valued differences (before BioHashing) in feature space.

Conversely, when the token is stolen, it means that a different I^k is projected onto the single random subspace, $\boldsymbol{R}$. It is obvious that the impostor (*pseudo-genuine Type I* hereafter) distribution will revert to its original state (or become poorer due to quantisation process) as the pair-wise distances are only preserved to a certain extent, as indicated in Fig. 2. Again, this is only true for $m \approx n$, where n is biometrics feature dimension.

On the other hand, for the stolen-biometrics scenario, the net effect is essentially equivalent to the projection of the compromised biometrics features onto multiple random subspaces, and hence the impostor distribution (*pseudo-genuine Type II* hereafter) is expected to peak at 0.5 while its standard deviation would be $0.5/\sqrt{m}$. We verify these assertions in the next section.

4. Experiments and discussions

In the experiment, EigenFace [26] is adopted as the face feature extractor and the metrics defined in Eq. (5) is used as dissimilarity measure. For the eigenbasis training, we use 400 images (40 subjects, each with 10 images) from ORL Face Database (http://www.uk.research.att.com/facedatabase.html). We evaluate the assertions by using the publicly available FERET Face database [27]. FERET contains face images associated with 1196 individuals; however, a substantial number of these (i.e. left- and right-profile views) are unsuitable for our experiments. For the experiment, we randomly selected a subset of 400 users, each having six essentially normalised frontal images with variations in pose (i.e. within ±25 angles), scale and illumination. Many of these images were taken over an extended period, and are highly varied, i.e. in terms of eyewear (absence and presence thereof) and illumination.

To generate the impostor distribution, the first BioHash of each subject is matched against the first BioHash of all other subjects, and the same matching process was repeated for subsequent BioHashs, leading to $(400\times399)/2\times6$=478, 800 impostor attempts. For the genuine distribution, each BioHash of each subject is matched against all other BioHashes of the same subject, leading to 6000 ($(5\times6)/2$ attempts of each subject$\times$400). For the pseudo-genuine I distribution, we assume the worst case scenario where the impostors always manage to steal the same genuine token. In other words, only a set of TRN is mixed with all the facial images and the matching is performed according to the impostor match described above. Pseudo-genuine II distribution is generated by taking other biometrics features from the data set mixed with the corresponding impostor TRN (impostor own token). The genuine vs impostor distributions and the genuine vs pseudo-genuine I and II distributions enable us

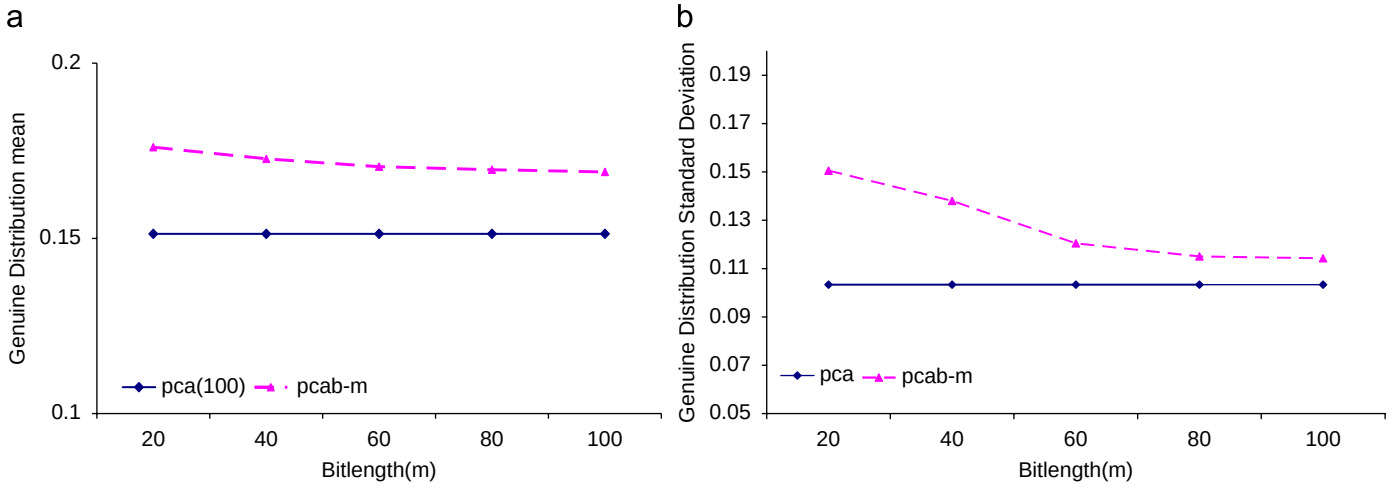

Fig. 3. Genuine distribution (a) means and (b) standard deviation variations according to BioHash bitlength, m.

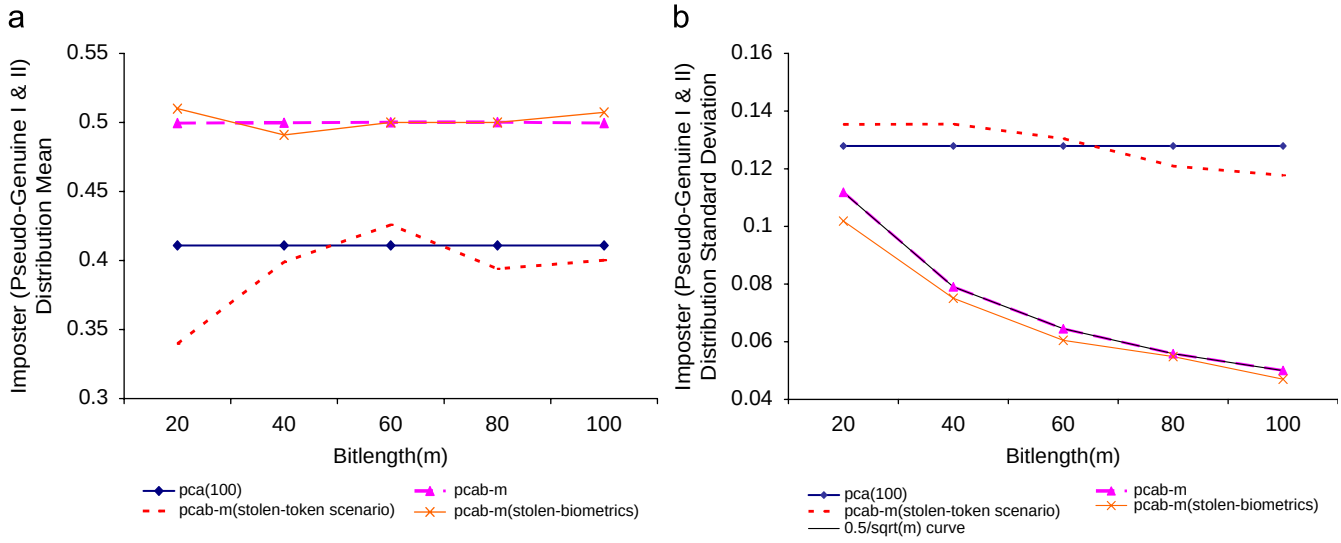

Fig. 4. Impostor (pseudo-Genuine I and II) distribution (a) mean and (b) standard variation variations according to BioHash bit length, m.

to calculate the EER for the genuine-token, stolen-token, and stolen-biometrics scenarios. EER refers to the average value of two error rates, i.e. FAR and FRR. We repeat the same process 10 times and the results are averaged to reduce the statistical fluctuation caused by the different random numbers. In this paper, pca and pcab-m denote EigenFace and BioHash, respectively, with m bit length. Note that the feature length of pca, n is 100 for this experiment. The experimental data are acquired for BioHash with length 20, 40, 60, 80, and 100.

From Figs. 3a and b, the mean and standard deviation of the genuine distribution for pcab-m are close to pca at $m = 100$. This suggests that the genuine distributions of BioHash are preserved when $m \approx n$. On the contrary, the large deviation in the genuine's means (16% of difference) and standard deviations (51% of difference) for small m ($m = 20$) indicates great distortion in the feature topology as discussed in Section 2.1.

On the other hand, the experimental values of the impostor and pseudo-genuine II distribution means peaked around theoretical mean of 0.5 regardless of m (Fig. 4a). The empirical values of the standard deviation for impostor distribution for various m are also tightly tagged to the theoretical value, $0.5/\sqrt{m}$ and closely followed by pseudo-genuine II's standard deviations, as indicated in Fig. 4b. The observation leads to the conclusion that the impostor distribution and the pseudo-genuine II of BioHash are independent of the feature extractor, and it is solely dependent on the BioHash bit length, m. This implies that the amplification of the inter-class variation (the impostor/pseudo-genuine II distribution) of BioHash is controllable as long as $m < n$.

For the stolen-token scenario, we see that the pseudo-genuine I distribution's mean is close to pca and the $0.5/\sqrt{m}$ rule is not obeyed for the standard deviation as depicted in Fig. 4.

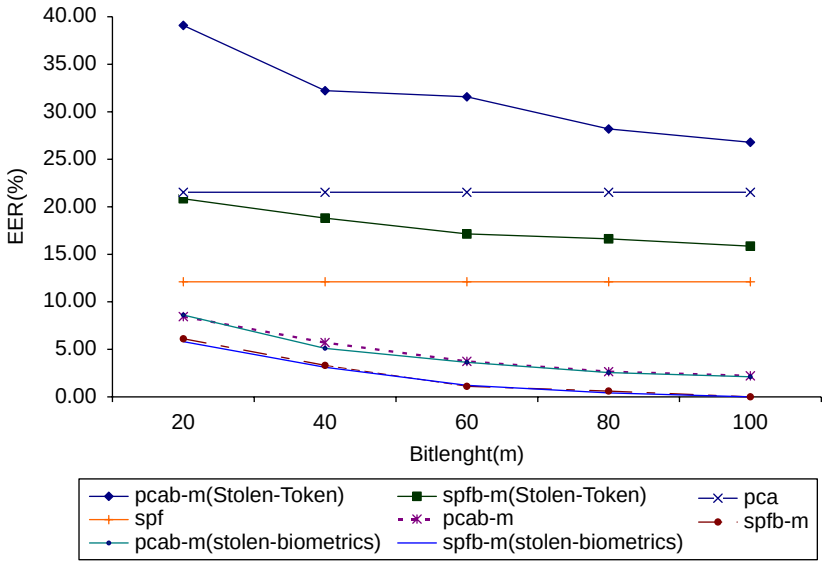

Fig. 5. The performance comparisons for pca and spf and their BioHash counterparts, pcab-*m*, spfb-*m* in genuine-token, stolen-token, and stolen-biometrics scenarios.

This vindicated the contention described in Section 2.2—the performance reverts back (or poorer) to its original. For this experiment, the recognition performance of the stolen-token scenario (EER = 26.79%) is poorer than pca (EER = 21.53%). This is due to the genuine distribution's mean of pcab-*m* is higher than pca (as depicted in Fig. 3a), thus inducing larger overlapping in the genuine vs pseudo-genuine I distribution as genuine distribution is right shifted.

A straightforward solution is to use a better feature extractor, as the recognition performance for stolen-token scenario is proportional to the quality of the feature extractor. We repeat the experiments with the better feature extractor such as spectroface which combined the wavelet and Fourier transforms [28] (spf and spfb-*m* henceforth for spectroface and its BioHash). For the experiments, we use a wavelet base with Daubechies filter order 7, level 1 is selected for spf and spfb-*m*. Note that the feature length for spf is 240 but we limit spfb-*m* to $m = 100$ for the fair comparisons with pcab-*m*. From Fig. 5, we notice that spf (EER = 12.11%) is superior than pca (EER = 21.53%), and same to their BioHash counterparts, EER = 15.86% for spfb-100 and EER = 26.79% for pcab-100. On the other hand, pcab-100 and spfb-100 with genuine token is superior, EER = 2.21% and EER = 0%, respectively. Fig. 6 illustrates the genuine vs impostor and genuine vs pseudo-genuine I and II distributions for genuine-token, stolen-token, and stolen-biometrics scenarios, respectively. Note that if intra-class variation of biometrics (mean and standard deviation of genuine distribution) is large (Fig. 6a), then BioHash could not achieve zero EER in genuine-token scenario since quantised RP preserves the intra-class variation of biometrics feature.

For stolen-biometrics scenario, we observe that EER for pcab-*m* (2.11%) and spfb-*m* (0%) is very low, as in the genuine-token case. This is favourable for practical application since stolen-token attack is the worst case scenario that we considered.

In a nutshell, BioHash can be viewed as quantised RPs that preserve the intra-class variations (the genuine distribution) while it enhances the inter-class variations (the impostor distribution) when users are well behaved (use their corresponding tokens). However, the result reverts to the original performance (or become poorer) when the genuine token is stolen and used by the impostor to claim as the genuine user.

We point out that both components (TRN + biometrics) play equally important roles in BioHash. For instance, if the TRN overtakes biometrics as conjectured by Cheung et al. [8] and Kong et al. [10], the most apparent effect is the zero (or near zero) mean and standard deviation occurrences in the genuine distribution. However, our findings in Section 3.1 and experimental results in Section 4 revealed that their claim is not true and not justified. The TRN and biometric components both have significant and equal contribution to the final BioHash output. Aside from the good recognition capabilities, we also note that our construction has the advantages of security (revocable templates) and privacy protection not realisable if only biometric feature is considered.

5. Multi-stage BioHash

The performance of BioHash in stolen-token scenario is often poorer than its original counterpart due to high information lost when transforming from real to binary space. This is because as shown in early paragraph in Section 3, the discretisation method is just a simple binary thresholding scheme. In order to enhance the distinguishability of random projected features, $\boldsymbol{v} = \boldsymbol{R}\Gamma$ such that each transformed feature is discernible to separate the genuine user from potential impostor users, we transform $\{v_i \in \boldsymbol{v} | i = 1, \ldots, m\}$ from the real into the 2^N index space before the final representation using Grey binary representation. Specifically, we assume that v_i is distributed according to standard normal distribution, $v_i \sim N(0, 1)$ and

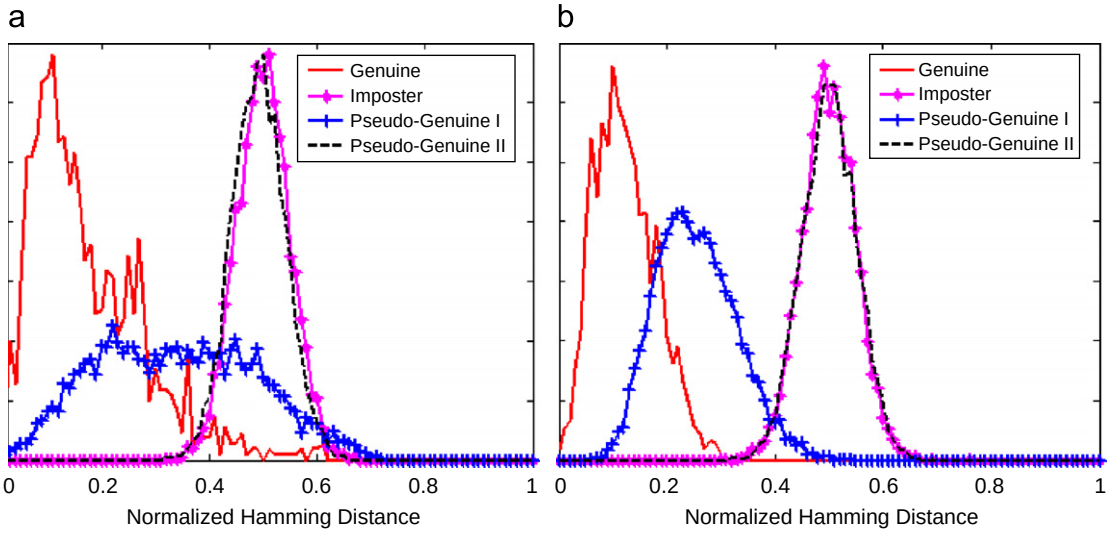

Fig. 6. Genuine, impostor, and pseudo-genuine I and II distributions for (a) pcab-100 and (b) spfb-100.

the element values fall within twice of user-dependent standard deviation from the mean value to be in the genuine segment to compensate for the noisy nature of biometric data. The feature element space is next divided into 2^N segments by adjusting the user-dependent standard deviation. By using this method, each v_i can render multiple bits instead of 1 bit in the original BioHash, and thus provides higher entropy in the resulting bit string. Fig. 7 depicts the idea of multi-state discretisation.

Our implementation is outlined below:

(a) At enrolment, we compute the standard deviation of v_i of user j,

$$\sigma_{ij} = \sqrt{\left(\sum_{k=1}^{r}(v_{ijk} - \bar{v}_{ij})^2\right)/r}, \quad i = 1, \ldots, m$$

where r is the number of training samples and $\bar{v}_{ij}$ is the mean of v_{ij}.

(b) For each jth user, the feature space is divided into 2^N segments which cover the range $[L, R]$ by adjusting to each user standard deviation. The number of bits in each segment, n_i, can be determined by first enumerating a set of N values, $\psi_j = \{\text{abs}(\frac{R-L}{2^N} - 2\sigma_{ij}) | i = 1, \ldots, m \text{ and } N = 1, \ldots, 10\}$. n_i is one of the values of N that provides the smallest value in set ψ. In this case, L and R are the right and left boundaries of entire feature space and in our case, they take the values -1 and 1, respectively, due to the observation that $v_i \sim N(0, 1)$. Hence, $n_i = N_{\min(\psi_j)}$, where $\psi_j = \{\text{abs}(2^{1-N} - 2\sigma_{ij}) | i = 1, \ldots, m \text{ and } N = 1, \ldots, 10\}$. Maximum value of N is arbitrarily limited to 10 to avoid too many bits being used for a single representation. Then, n_i for each user j is stored.

(c) At verification, the *genuine segment index* of v_i of user j can be obtained from $d_i = \lfloor (\frac{v_i - L}{R-L}) 2^{n_i} \rfloor$ or $d_i = \lfloor (v_i + 1) 2^{n_i - 1} \rfloor$ and its binary representation of v_i is given by Grey Coding, $b_i = \text{grey}(d_i)$, the final BioHash is $b_1 \| b_2 \| b_3 \| \ldots \| b_m$.

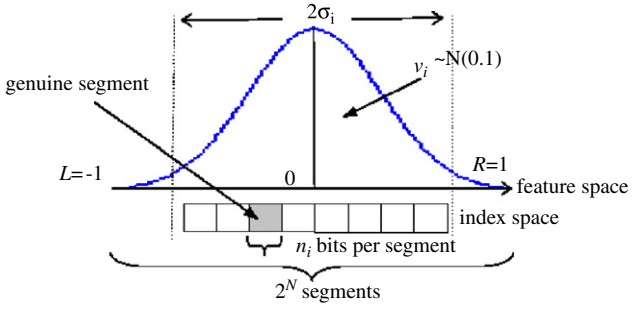

Fig. 7. Illustration of multi-state discretisation on ith element of v_j of user j.

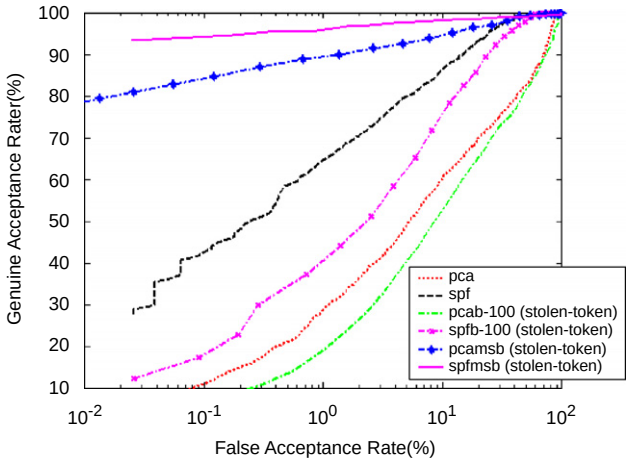

Fig. 8. Receiving operating characteristic (ROC) curve.

With the above procedure, a BioHash with length $\sum_{i=1}^{m} n_i$ can be generated by cascading all Grey encoded indices of genuine segments from the m-dimensional $\boldsymbol{v}$.

For the experiments, we randomly select $r = 3$ templates among six samples of each subject to be the training samples for

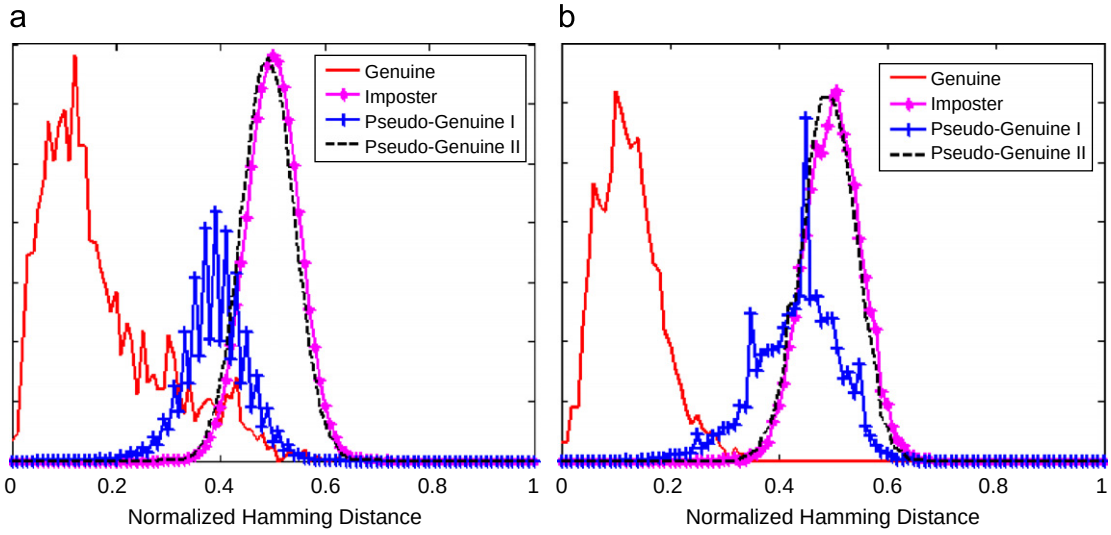

Fig. 9. Genuine, impostor and pseudo-genuine I & II distributions for (a) pcamsb and (b) spfmsb.

multi-state discretisation and the other for testing purposes. ${}^6C_3$ runs are performed with different partitions between the training and testing. The same procedures are performed as described in Section 4. The association of BioHash (pcab-100 and spfb-100) and multi-state discretisation—pcamsb (EER = 5.71%) and spfmsb (EER = 1.77%)—depicts prominent performance improvement in stolen-token scenario, as indicated in the receive operating characteristic curve in Fig. 8. This is a vital improvement for practical concerns. In this instance, BioHash allows the genuine user (his own biometric and genuine token) to access the system, whereas the impostor, even with his own biometric combined with either the stolen token or his own token, would deny access at least 98.23% of the time. In terms of genuine vs pseudo-genuine I distributions (Fig. 9), we observe that the pseudo-genuine I distribution is right shifted compared to earlier results without multi-state discretisation shown in Fig. 6, and resulting in EER reduction. It is worth noting that the genuine vs impostor/pseudo-genuine II distributions are only slightly altered (relative to the ordinary BioHash) by the multi-state discretisation prescription, thus retaining the good performances of BioHash in genuine-token and stolen-biometrics scenario. Previous efforts that have been attempted to remedy this problem are fusion techniques [29], error correction code, i.e. algebraic codes [33] and modular polynomial interpolation [30], but the improvement in recognition rate was not as significant.

6. Security analysis

In this section, we prove the non-invertible property of BioHash, so that it is computationally difficult to recover the biometric feature from the BioHashes. This property ensures that only the combination of TRN and biometrics feature can contribute to the authentication process. We also consider possible ways the BioHash may be attacked and discuss how the new BioHash construction circumvents these attacks.

6.1. Non-invertible property of BioHash

The security analysis of non-invertible property can by considering earlier description of the RP, $\boldsymbol{v} = \boldsymbol{R}\Gamma$ where $\boldsymbol{R}$ is an $m \times n$ orthonormal random matrix and $m < n$. The vector $\boldsymbol{v}$ can be regarded as a set of underdetermined systems of linear equations (more unknowns than equations). Therefore, it is impossible to find the *exact values of all the elements* in $\boldsymbol{\Gamma}$ by solving an underdetermined linear equation system in $\boldsymbol{v} = \boldsymbol{R}\Gamma$ if $m < n$, based on the premise that the possible solutions are infinite.

We adopt a formal proof that is described in Ref. [34] and [35]. Assuming both $\boldsymbol{R}$ and Γ are known, the system can be analysed by the QR factorisation of $\boldsymbol{R}^{\mathrm{T}}$ such that

$$\boldsymbol{R}^{\mathrm{T}} = Q\begin{pmatrix}\bar{\boldsymbol{R}}\\ \boldsymbol{0}\end{pmatrix}, \tag{7}$$

where Q is an $n \times n$ orthogonal matrix and $\bar{\boldsymbol{R}}$ is a $m \times m$ upper triangular matrix. If $\boldsymbol{R}$ is full rank, i.e rank$(\boldsymbol{R}) = m$, there is a unique solution $\Gamma_{\min\_\mathrm{norm}}$ that minimizes $\|\Gamma\|_2$:

$$\begin{aligned}\Gamma_{\min\_\mathrm{norm}} &= Q\begin{pmatrix}\bar{\boldsymbol{R}}^{\mathrm{T}^{-1}} & \boldsymbol{v}\\ \boldsymbol{0} & \end{pmatrix}\\ &= Q\begin{pmatrix}\bar{\boldsymbol{R}}\\ \boldsymbol{0}\end{pmatrix}\left(\bar{\boldsymbol{R}}^{\mathrm{T}}\ \bar{\boldsymbol{R}}\right)^{-1}\boldsymbol{v}\\ &= \boldsymbol{R}^{\mathrm{T}}(\boldsymbol{R}\boldsymbol{R}^{\mathrm{T}})^{-1}\boldsymbol{v}\\ &= \boldsymbol{R}^{\dagger}\boldsymbol{v},\end{aligned}$$

where $\boldsymbol{R}^{\dagger}$ is the pseudo-inverse of $\boldsymbol{R}$. $\Gamma_{\min\_\mathrm{norm}}$ may serve as a starting point to the underdetermined system, $\boldsymbol{v} = \boldsymbol{R}\Gamma$. The complete solution set can be characterised by adding an arbitrary vector from the null space of $\boldsymbol{R}$, which can be constructed by the national basis for the null space of $\boldsymbol{R}$, denoted by $\boldsymbol{\Psi}$. It can be confirmed that $\boldsymbol{R}\boldsymbol{\Psi} = 0$ and that any vector $\boldsymbol{v}$, where

$$\Gamma = \Gamma_{\min\_\mathrm{norm}} + \boldsymbol{\Psi}\boldsymbol{v} \tag{8}$$

for an arbitrary vector $\boldsymbol{v}$ satisfies $\boldsymbol{v} = \boldsymbol{R}\Gamma$.

This result proves that even if the random matrix, $\boldsymbol{R}$, is known to the adversary, it is impossible to find the exact values of all the elements in vector Γ of each underdetermined system of linear equations. The best effort that can be attempted is the computation of the minimum norm solution [22]. Note also that the conversion of the real-valued RP also undergoes a lossy discretisation step which is not easily inverted.

Furthermore, the inclusion of multi-stage discretisation strengthened the non-invertible property of BioHash. This is because no additional information is leaked from the number of bits in each segment, n_i, as we do not store the statistics of feature elements, i.e. σ_{ij}. Therefore it is not possible to estimate the randomly projected feature values, $\{v_i \in \boldsymbol{v} | i = 1, \ldots, m\}$ based on n_i, and the fixed boundary $[-1\ 1]$.

6.2. Security attacks

(a) *Brute-force attack*: The impostor does not have any knowledge of the genuine BioHash or token. He performs a brute-force attack by trying out all possible combination of the key. The computational complexity to guess the key is 2^m where m is the BioHash's bit length due to the bit output of BioHash is independent of each other. This property can be easily verified as $\boldsymbol{R}$ is an $m \times n$ orthonormal random matrix. There is no a priori restriction on the value of m provided $m < n$, where n denotes feature length of biometrics feature extractor.

(b) *Multiple key attacks without compromising genuine tokens*: The impostor eavesdrops on a genuine user to collect multiple BioHashes. If the genuine token is not compromised, the non-invertible property of BioHash ensures that recovery of the biometrics feature is infeasible.

(c) *Substitution token with intercepted biometrics attack*: In this scenario, the impostor uses his own token and intercepted biometrics feature to generate acceptance into the system. The experimental results are shown in Fig. 5 as stolen-biometrics scenario, with zero EER indicating that using the BioHash, this attack will not be successful.

(d) *Known token attack*: This represents the situation whereby the impostor has access to the genuine token. He attempts to combine the stolen token with his own biometrics to enter the system. From the experimental results that are shown in Section 5, the probability of him succeeding is about 1.77% if multi-state discretisation BioHash is used.

7. Concluding remarks

In this paper, we undertook a formal statistical analysis of the previously published cancellable biometrics-BioHash in terms of the ensemble of the quantised RPs. This process involves transformation of raw biometrics data into a low-dimensional feature space representation, then subsequently re-projecting these user-specific feature vectors onto a sequence of random subspaces specified by the tokenised random vectors, and finally quantising these projections to yield the binary bit string.

The end result is an extremely powerful two-factor authenticator which integrates biometric data with tokens in a non-invertible manner, thereby protecting sensitive biometric data in a manner equivalent to a cryptographic cipher or hash input. These BioHashes are cancellable via straightforward revocation and then refreshment of the token, thereby protecting against interception of biometric data or even physical fabrication of the biometric feature.

In terms of recognition performance, BioHash also offers a significant advantage, namely the possibility of achieving zero error rates when the genuine tokens are used. This is accomplished through the ensemble of the quantised RPs capable of preserving intra-class variations, while amplifying inter-class variations via projecting onto uncorrelated random subspaces. Recognition performance improves with the BioHash bit length, m, up to the maximum of $m = n$, i.e. the feature space dimension. Large BioHash bit length is desirable in some cryptographic applications in order to resist brute force random guessing attacks. Large m suppresses inter-class correlations in the bit string outcomes, as can be seen from the predicted standard deviation of $0.5/\sqrt{m}$ for the impostor distribution, resulting in more pronounced shifting away from the genuine distribution. There is an important proviso, namely that recognition effectiveness also depends on the quality of the feature extractor.

The performance of BioHash reverted to the original state (or slightly poorer) when the genuine token was stolen and used by the impostor to claim as the genuine user. In the paper, we demonstrate the use of multi-state BioHash to resolve the stolen-token problem. As a result, the multi-state discretised BioHash could function as an effective cancellable biometrics to protect the privacy of the biometrics without compromising the recognition performance in the event of compromised token.

The BioHash is hence a substantive improvement over recognition based purely on biometric feature extraction and complex classifier. The other promising research area is the further stabilisation of the bit string outputs via error correction techniques. This enables BioHash to be used as cryptographic keys, thereby addressing application scenarios beyond identity verification [30–33].

Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University.

References

[1] N. Ratha, J. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40 (3) (2001) 614–634.

[2] R.M. Bolle, J.H. Connel, N.K. Ratha, Biometrics perils and patches, Pattern Recognition 35 (2002) 2727–2738.

[3] B.J. Andrew Teoh, A. Goh, C.L. David Ngo, Random multispace quantisation as an analytic mechanism for biohashing of biometric and random identity inputs, IEEE Trans. Pattern Anal. Mach. Intell. 28 (12) (2006) 1892–1901.

[4] B.J. Andrew Teoh, C.L. David Ngo, Cancellable biometrics featuring with tokenised random number, Pattern Recognition Letter 26 (10) (2005) 1454–1460.
[5] Y.H. Pang, B.J. Andrew Teoh, C.L. David Ngo, Cancellable palmprint authentication system, Int. J. Signal Process. 1 (2) (2005) 98–104.
[6] B.J. Andrew Teoh, C.L. David Ngo, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognition 37 (11) (2004) 2245–2255.
[7] C. Tee, B.J. Andrew Teoh, A. Goh, C.L. David Ngo, PalmHashing: A novel approach for dual factor authentication, Pattern Anal. Appl. 7 (3) (2004) 255–268.
[8] K.H. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, H.W. Lam, An analysis on accuracy of cancellable biometrics based on BioHashing. KES 2005, Lecture Notes on Aritificial Intelligence, vol. 3683, pp. 1168–1172.
[9] K.H. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, Revealing the secret of FaceHashing, ICB 2006, Lecture Notes on Computer Science, vol. 3832, Springer, Berlin. pp. 106–112.
[10] A. Kong, K.H. Cheung, D. Zhang, M. Kamel, J. You, An analysis of BioHashing and its variants, Pattern Recognition 39 (7) (2005) 1359–1368.
[11] G. Davida, Y. Frankel, B.J. Matt, On enabling secure applications through off-line biometrics identification, in: Proceeding Symposium on Privacy and Security, 1998, pp. 148–157.
[12] A. Juels, M.A. Wattenberg, Fuzzy commitment scheme, in: ACM Conference on Computer and Communications Security, 1999, pp. 28–36.
[13] A. Juels, M. Sudan, A fuzzy vault scheme, in: ACM Conference on Computer and Communications Security, 2002, pp. 408.
[14] T.C. Clancy, N. Kiyavashand, D.J. Lin, Secure smartcard-based fingerprint authentication, in: ACM SIGMM 2993 Multimedia, Biometrics Methods and Applications Workshop, 2003, pp. 45–52.
[15] F. Hao, R. Anderson, J. Daugman, Combining crypto with biometrics effectively, IEEE Trans. Comput. 55 (9) (2006) 1081–1088.
[16] J.P. Linnartz, P. Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates, in: Proceedings of the 4th International Conference on Audio-and Video-Based Biometric Person Authentication, Lecture Notes on Computer Science, vol. 2688, Springer, Berlin, 2003, pp. 393–402.
[17] P. Tuyls, A. Akkermans, T. Kevenaar, G.J. Schrijen, A. Bazen, R. Veldhuis, Practical biometric template protection system based on reliable components, in: Proceedings of the 5th International Conference on Audio-and Video-Based Biometric Person Authentication, Lecture Notes on Computer Science, vol. 3546, Springer, Berlin, 2005, pp. 436–446.
[18] C. Soutar, D. Roberge, A.R. Stoianov, Gilroy, B.V.K. Vijaya Kumar, Biometrics encryption, in: R.K. Nichols (Ed.), ICSA Guide to Cryptography, McGraw-Hill, New York, 1999, pp. 649–675.
[19] M. Savvides, B.V.K. Vijaya Kumar, P.K. Khosla, Cancellable biometrics filters for face recognition, in: International Conference of Pattern Recognition, vol. 3, 2004, pp. 922–925.
[20] Y. Sutcu, H.T. Sencar, N. Memon, A secure biometric authentication scheme based on robust hashing, in: Proceedings of the 7th Workshop on Multimedia and Security, New York, USA, 2005, pp. 111–116.
[21] R. Ang, S.N. Rei, L. McAven, Cancellable key-based fingerprint templates, in: Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4–6, 2005, pp. 242–252.
[22] S. Kaski, Dimensionality reduction by random mapping: fast similarity computation for clustering, in: Proceedings of the International Joint Conference on Neural Networks, vol. 1, 1998, pp. 413–418.
[23] S. Dasgupta, A. Gupta, An elementary proof of the Johnson–Lindenstrauss Lemma, UTechnical Report TR-99-006, International Computer Science Institute, Berkeley, CA, 1999.
[24] F.N. David, The moments of the z and F distributions, Biometrika 36 (1949) 394–403.
[25] J. Daugman, The important of being random: statistical principles of iris recognition, Pattern Recognition 36 (2003) 279–291.
[26] M. Turk, A. Pentland, Eigenfaces for recognition, J. Cognitive Neurosci. 13 (1) (1991) 71–86.
[27] P. Phillips, H. Moon, P. Rauss, S. Rizvi, The FERET database and evaluation methodology for face recognition algorithms, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 1997, pp. 137–143.
[28] H.L. Lai, P.C. Yuen, G.C. Feng, Face recognition using holistic Fourier invariant features, Pattern Recognition 34 (2001) 95–109.
[29] D. Maio, L. Nanni, MultiHashing, human authentication featuring biometrics data and tokenised random number: a case study FVC2004, Neurocomputing, 2005, to appear.
[30] A. Goh, C.L. David Ngo, Computation of cryptographic keys from face biometrics, Lecture Notes on Computer Science, vol. 2828, Springer, Berlin, 2003, pp. 1–13.
[31] B.J. Andrew Teoh, C.L. David Ngo, A. Goh, Personalised cryptographic key generation based on FaceHashing, Comput. Secur. J. 23 (7) (2004) 606–614.
[32] W.K. Yip, A. Goh, C.L. David Ngo, B.J. Andrew Teoh, Generation of replaceable cryptographic keys from dynamic handwritten signatures, Lecture Notes on Computer Science, vol. 3832, Springer, Berlin, pp. 509–515.
[33] W.K. Yip, A. Goh, C.L. David Ngo, B.J. Andrew Teoh, Cryptographic keys from dynamic handsignatures with biometric secrecy preservation and replaceability, in: 4th IEEE Workshop On Automatic Identification Advanced Technologies (AutoID'05), October 17–18, 2005, Buffalo, New York, USA, 2005, pp. 27–32.
[34] K. Liu, H. Kargupta, J. Ryan, Random projection-based multiplicative data perturbation for privacy preserving distributed data mining, IEEE Trans. Knowl. Data Eng. 18 (1) (2006) 92–106.
[35] J.W. Demmel, N.J. Higham, Improved error bounds for underdetermined system solvers, Computer Science Department, University of Tennessee, Knoxville, TN, Technical Report CS-90-113, August 1990.

About the author—ANDREW TEOH BENG Jin obtained his B.Eng. (Electronic) in 1999 and Ph.D degree in 2003 from National University of Malaysia. He is currently a senior lecturer and Associate Dean of Faculty of Information Science and Technology, Multimedia University Malaysia. He held the post of chairman in Center of Excellent in Biometrics and Bioinformatics in the same university. He also serves as a research consultant for Corentix Technologies in the research of Biometrics system development and deployment. His research interest is in multimodal biometrics, pattern recognition, multimedia signal processing and Internet security. He has published over 100 international journals and conference papers.

About the author—YIP WAI KUAN received her B.S. and M.S. degrees in computer science from University Science of Malaysia in 1999 and 2003, respectively. Currently, she works as an Analytic Solutions Development Engineer in Intel Malaysia and is completing her Ph.D. degree in information technology from Multimedia University, Malaysia. Her research interests cover the areas of dynamic hand signatures, signal processing, and information security.

About the author—SANGYOUN LEE received B.S. and M.S. degrees in Electronic Engineering from Yonsei University, Seoul, South Korea in 1987 and 1989, respectively. He received the Ph.D. degree in Electrical & Computer Engineering from Georgia Tech., Atlanta, Georgia, in 1999. He was a senior researcher in Korea Telecom from 1989 to 2004. He is now an assistant professor in Electrical & Electronic Engineering Department, Yonsei University. His research interests include pattern recognition, computer vision, video coding, and biometrics.