A Cancellable Face Template Scheme Based on Nonlinear Multi-Dimension Spectral Hashing

Xingbo Dong, KokSheik Wong, Zhe Jin
School of Information Technology
Monash University Malaysia
Bandar Sunway, Malaysia
{xingbo.dong, wong.koksheik, jin.zhe}@monash.edu

Jean-luc Dugelay
Department of Digital Security
EURECOM
Sophia-Antipolis, France
jld@eurecom.fr

***Abstract*—The exposure of face templates potentially leads to severe security and privacy risks. For example, the attacker can utilize the compromised face template to masquerade the template owner. In addition, these concerns are aggravated since face is irreplaceable and irrevocable. In this paper, we propose a cancelable transform, namely nonlinear multi-dimension spectral hashing (NMDSH) to protect face template. Essentially, NMDSH utilizes a many-to-one function to transform real-valued deep face feature vector into binary code. The transformed template thus possesses strong non-invertible property. Next, a highly nonlinear softmod function is further adapted into the scheme to provide an additional layer of protection against similarity-based attack. The accuracy performance of NMDSH is evaluated. Experiment results suggest that NMDSH can preserve the accuracy performance largely. Properties including non-invertibility, revocability and resistance to similarity-based attack are also evaluated.**

Keywords—biometric, face recognition, biometric template protection

I. INTRODUCTION

Biometric technology provides new mechanisms for identity management with higher level of security and greater convenience. It is evidenced that biometric technology has been largely deployed in various applications, which leads to the proliferation of databases that store biometric templates. However, when a biometric template is stolen, permanent compromise is inevitable due to the fact that biometric characteristics are largely immutable. Furthermore, the same unprotected biometric source enrolled in multiple databases for different applications are completely correlated. An adversary can perform cross match to track and potentially monitor personal activities if one biometric template is compromised. With such threat, a privacy invasion is of people's concern, and biometric template protection (BTP) schemes are suitable to address this challenge. Briefly, BTP aims to transform an unprotected biometric template into a protected one by using parameterized function. An effective BTP scheme should satisfy four requirements, i.e., non-invertibility, revocability, non-linkability and performance preservation.

The current BTP techniques in the literature can be broadly divided into feature transformation (a.k.a. cancellable biometrics) and biometric cryptosystems. In the feature transform scheme, the biometric template is transformed by a transformation function and then stored in the database. The parameters of the transformation function are normally derived from a random key or password. The identical transformation function with same parameters is applied to query features and the transformed query is matched against the transformed template. On the other hand, biometric cryptosystem is a process that either: (a) securely binds a secret key (e.g., PIN, private keys) to a biometric for generating the protected biometric template, or (b) directly generates the cryptographic key from biometric features so that neither the key nor the biometric can be retrieved from the protected biometric template. The key is retrieved only if the genuine biometric query is presented. In addition to the purpose of template protection, biometric cryptosystem is also utilized for the secret / key management purpose.

In this paper, we propose a many-to-one function embedded transformation, namely nonlinear multi-dimension spectral hashing (NMDSH), to secure deep face features. NMDSH is an extension of graph-based hamming embedding [1] for cancellable biometrics. Moreover, with a deliberated *softmod* function, NMDSH provides a higher level of security and privacy protection against similarity attack (SA) for biometric data. We have made the source code available at http://goo.gl/8EoLsp.

II. RELATED WORK

Several relevant schemes for cancellable face templates are reviewed in this section. Specifically, the review here focuses on cancellable biometric techniques since the proposed method falls under this category.

Random projection (RP) is a process of projecting feature vector from n dimensions to m dimensions ($n \gg m$) in the Euclidean space by utilizing random matrices [2]. RP is based on Johnson-Lindenstrauss lemma (J-L lemma) [3], which proves that points from a high-dimensional space can be embed into low-dimensional space while approximately preserving the distance. Orthogonal projection matrix is a projection f proposed in [4], [5]. Briefly, Gram-Schmidt orthogonalization is performed on a $n \times m$ random matrix to generate a matrix $\boldsymbol{R} \in \mathbb{R}^{n \times m}$. Then, the feature vector $\boldsymbol{x} \in \mathbb{R}^n$ is projected onto $\boldsymbol{y} \in \mathbb{R}^m$ as $\boldsymbol{y} = \sqrt{\mathrm{n/m}}\boldsymbol{R}^T\boldsymbol{x}$. Specifically, the projection matrix $\boldsymbol{R}$ could be generated easily from Gaussian distributed sequences, which are proven to have the characteristic of orthogonality [6], [7].

BioHashing, an instance of RP, is a well-known salting based cancellable biometrics scheme applied to face [8]–[10]. Generally, BioHashing is a two-factor BTP technique based on user-specific token and biometric features, followed by a discretization procedure. The n-bit BioHash code $\boldsymbol{c}$ of a biometric feature vector $\boldsymbol{x} \in \mathbb{R}^N$ is computed as $\boldsymbol{c} = \mathrm{Sgn}(\sum \boldsymbol{x}\boldsymbol{b}_i - \tau)$, where $\mathrm{Sgn}(\cdot)$ is a signum function, τ is an empirically determined threshold, $\boldsymbol{b}_i \in \mathbb{R}^N$ and $i = 1, \ldots, n$ $(n \leq N)$ is an orthogonal pseudo-random vector. The Hamming distance is computed between two hash codes to indicate the similarity between two biometric vectors. New template for the identical biometric feature vector can be reissued by using a newly generated pseudo-random number.

However, BioHashing assumes that the pseudo-random numbers would never be compromised, which is impractical and hence BioHashing is of high risk under stolen key scenario. [11].

Random permutation is another common approach to generate cancellable biometric template [12], [13]. The feature vector is permuted according to a randomly generated key. For example in [12], permutation matrix is utilized as a parameterized transformation function to generate cancellable face template. In [13], the principal component analysis (PCA) and independent component analysis (ICA) coefficients are extracted from face images and permuted by ID specific parameters. A feature level fusion is then performed to generate the cancellable face templates. As for random permutation, the permutation key is assumed to be securely stored, which is impractical. In other words, if the key is stolen, the face template could be vulnerable. However, authentication accuracy is preserved since permutations are merely rearranging the feature vector.

Bloom filter is a generic transformation function applied to handle face template [14]. Specifically, the biometric feature is mapped to a bit array b with several independent hashing functions, where b is an array of length n. Specifically, k ($k \ll n$) independent hash functions denoted by $h_1, h_2, \dots, h_k$ are first defined, then each element of a data set $\boldsymbol{S}$ is hashed by using the hash functions and the resulting hash values are derived as k indices. Finally, all k indices of the bit-array b are set to unity. At the verification stage, the bit-array of the query element y is matched with the stored template by hamming distance to indicate the similarity between two biometric data.

Index-of-Max (IoM) is a recently proposed ranking-based locality sensitive hashing technique for template protection [15]. IoM transforms features from real value domain into index domain by computing the product between the feature vector $\boldsymbol{x}$ and Gaussian random generated matrices $\boldsymbol{W}$. The indices of the maximum value are output as the hash code.

III. Preliminary

Multidimensional Spectral Hashing (MDSH) is an instance of Locality Sensitive Hashing (LSH), which is proposed for image retrieval application based on spectral graph partitioning [16]. MDSH utilizes affinity matrix to indicate the similarity between the given data. The affinity between data points $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$ is defined as $\mathrm{W}(i,j) = e^{\frac{-\|x_i - x_j\|^2}{2\sigma^2}}$, where σ is the parameter set empirically by the user. To learn the binary codes, the typical cost function is given in terms of the Hamming distance $\|\boldsymbol{y_i} - \boldsymbol{y_j}\|^2$, computed between the binary hash codes of the data points i and j, where $\boldsymbol{y_i}$ is a binary vector of length k. The elements of $\boldsymbol{y_i}$ consists of 1 or -1 only, thus the Hamming distance or Hamming affinity can be defined as a simple dot product function $\boldsymbol{y_i}^T\boldsymbol{y_j}$ since $\|\boldsymbol{y_i} - \boldsymbol{y_j}\|^2 = 2k - \boldsymbol{y_i}^T\boldsymbol{y_j}$. The Hamming affinity is matched with the above defined affinity $\mathrm{W}(i,j)$ between data points $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$.

Based on the abovementioned assumption, MDSH can be regarded as a binary matrix factorization problem of the affinity matrix (see [16] for detailed information). To find the best binary code, the spectral relaxation is applied, the computation of the single dimension j-th eigen function $\boldsymbol{\phi}_{ij}(\boldsymbol{x}(i))$ with eigenvalue λ_{ij} is given by equations below:

$$\boldsymbol{\phi}_{ij}(\boldsymbol{x}(i)) = sin(\frac{\pi}{2} + \frac{j\pi}{b_i - a_i}\boldsymbol{x}(i)) \quad (1)$$

$$\lambda_{ij} = e^{-\frac{\delta^2}{2}\left|\frac{j\pi}{b_i - a_i}\right|^2} \quad (2)$$

where $\boldsymbol{x}(i)$ is a single-dimensional arbitrary real feature corresponding to the i-th coordinate of $\boldsymbol{x}$, and uniformly distributed in the range of $[a_i, b_i]$.

The MDSH algorithm generally consists of four steps:

1) Compute the single-dimension eigen functions denoted by $\boldsymbol{\phi}_{ij}(\boldsymbol{x}(i))$. Specifically, $\boldsymbol{\phi}_{ij}(\boldsymbol{x}(i))$ is the j-th eigen function of the i-th coordinate, while λ_{ij} is the corresponding eigenvalue.

2) Sort λ_{ij} in ascending order, and selected the top k indices to form the set $A = \{(i_1, i_1), (i_2, i_2), \dots, (i_k, i_k)\}$.

3) Each data point $\boldsymbol{x}$ is encoded by using $y_{ij}(\boldsymbol{x}) = \mathrm{sign}(\boldsymbol{\phi}_{ij}(\boldsymbol{x}))$ for all $(i,j) \in A$.

4) Compute the Hamming affinity between $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$ by using the below equation:

$$H(i,j) = -1 + \prod_d \left(1 + H_d(i,j)\right), \quad (3)$$

where the weighted Hamming affinity is given by:

$$H_d(i,j) = \sum_{d,l \in \mathrm{A}} \lambda_{dl} sign(\boldsymbol{\phi}_{dl}(\boldsymbol{x(i)})) sign(\boldsymbol{\phi}_{dl}(\boldsymbol{x(j)})). \quad (4)$$

IV. Proposed Method

Despite deep face feature is showing excellent accuracy in the face recognition task, its vulnerability in terms of privacy and security are of great concern to the public. In [17], a neighborly de-convolutional neural network (NbNet) is designed to reconstruct face images from their deep face features. Experiment results show that NbNet can reconstruct the face images with high accuracy, leading to privacy and security risks. Therefore, in this paper, a nonlinear multi-dimensional spectral hashing (NMDSH) is proposed to generate secure face template from the deep features. An overview of the system is depicted in Fig 1. First, the face features are extracted by using a deep model, namely, InsightFace. Random projection is then performed on the feature vector to achieve cancelability. With the mainly-to-one sine(·) function embedded, NMDSH transformation is able to provide the strong non-invertible property to the randomized feature vector. Furthermore, a *softmod* function is included to resist SA. Finally, the binary hash code is generated by the sign(·) function with zero threshold, and stored in the database as the template.

A. Performing RP to achieve cancelability

Random projection is used for the purpose of cancelability or revocability. When a template is compromised, a new protected template can be generated by performing the proposed method with different random projection seed. Let the feature matrix $\boldsymbol{v} \in \mathbb{R}^n$ $(n = 512)$ represents the deep face

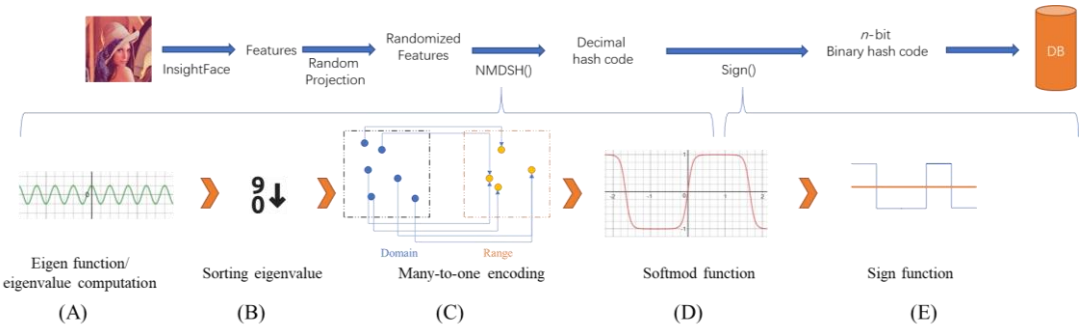


Fig 1. Overview of the secured face protection process

features defined in the Euclidean space. The procedure of RP can be described as a 2-step algorithm as follows:

- Step (1) Use a token to generate a pseudo random matrix and transform the matrix into an orthonormal matrix by applying the Gram–Schmidt process [18]. With this, an orthonormal matrix $\boldsymbol{R} \in \mathbb{R}^{n\times n}$ can be formed.
- Step (2) Compute the randomized feature vector $\boldsymbol{x}$ by using the following equation:

$$\boldsymbol{x} = \boldsymbol{v}\boldsymbol{R} \in \mathbb{R}^{n}. \tag{5}$$

B. Adopting MDSH to achieve non-invertibility

MDSH, which is introduced in section III, is employed to hash the randomized feature vector. As shown in Fig 1 (A), the single-dimension eigen functions denoted by $\boldsymbol{\phi}_{ij}(\boldsymbol{x}(i))$ and the corresponding eigenvalue λ_{ij} are first computed according to (1) and (2) on the training dataset. Secondly, λ_{ij} is sorted in ascending order and a set of top k indices A is obtained, which is depicted in Fig 1 (B). Finally, as shown in Fig 1 (C) and (E), the face feature vector $\boldsymbol{x}$ in the testing dataset is encoded by $\boldsymbol{y}_{ij}(\boldsymbol{x}) = \text{sign}(\boldsymbol{\phi}_{ij}(\boldsymbol{x}))$ for all $(i,j) \in A$. Note that the MDSH adopted in this paper is different from the original one in [16] because step 4 of MDSH is ignored, and the similarity of different face images is calculated directly from the Hamming distance of the binary codes. The modified version of the multi-dimension spectral hashing is called SMDSH, which utilizes a many-to-one function $\text{sign}(\boldsymbol{\phi}_{ij}(\cdot))$ to transform deep face feature vector into binary code. The transformed template thus possesses strong non-invertible property.

C. Utilizing Softmod to resist against similarity attack

Although MDSH preserves the accuracy of the deep face feature and achieves non-invertibility, it is vulnerable under SA due to the distance preserving property [19]. SA is a new kind of attack that essentially exploits the property of similarity-preserving hashing in reverting biometric. Conceptually, SA tries to optimize the reconstruction problem, i.e.arg $\min\|x - \hat{x}\|$,where $\hat{x}$ is the attacker's estimation of the original biometric x. we could estimate $\|x - \hat{x}\| \approx \|y - \hat{y}\|$ from their hashes through the similarity preserving property, If such an estimation is accurate enough, a similar $\hat{x}$ can be reconstructed. In a nutshell, the distance-preserving property can lead to information leakage, thus the original distance can likely be retrieved from the hashed space. The leakage of MDSH can be quantified by the mutual information among the normalized distance in the original space d, and the normalized distance in the hashed space s. In order to withstand this attack, the system should ensure that

$$I(d-;\, s-) \leq \delta \tag{6}$$

where the symbol '$-$' denote the inter cases, and $I(\cdot)$ indicates the mutual information. The upper bound of $I(d-;\, s-)$, which can be represented as entropy, is $H(d-)$ since $I(d-;\, s-) \leqslant H(d-) \leqslant H(s-)$. Assuming that $d-$ follows a unimodal distribution, then $H(d-)$ can be represented by the variance of $d-$, denoted by $V[d-]$[19]. Hence, (6) can be expressed as:

$$V[d-] \leq \delta. \tag{7}$$

(7) suggests that most inter-class distances in the hashed space should be made as similar as possible (i.e., equidistant among classes) to resist SA. Therefore, a *softmod* activation layer is added to MDSH to create a nonlinear MDSH as indicated in Fig. 1 (D), namely NMDSH:

$$y = q(\boldsymbol{\phi}_{ij}(\boldsymbol{x})), \tag{8}$$

where $q(\cdot)$is a nonlinear *softmod* activation function defined as:

$$q(x) = \frac{2}{1 + e^{-8\sin(\alpha\pi x)}} - 1. \tag{9}$$

Here, α is an empirical parameter (nonlinear rate) defined by user. We will demonstrate NMDSH' resistance against SA in Section V.

In a nutshell, the generated binary template enjoys several merits: (1) strong concealment of the face deep features extracted by InsightFace due to the many-to-one function and *softmod* function; (2) accuracy of deep features is well preserved; (3) template is revocable due to user-specific random projection; (4) speedy matching attributed to bit-wise operations; (5) binary hash code can also be used as indexing, and; (6) NMDSH is an unsupervised method based on statistic theory, which can be easily implemented.

V. Experiment

A. Face datasets

Two popular dataset LFW [20] and VGG2 (VGGFace2) [21] are used in our experiment. LFW is designed to study the problem of unconstrained face recognition. The data set contains 13,233 face images from 5749 individuals collected from the web. Each face has been labeled with the name of the pictured person. 1680 of the pictured people have two or more distinct photos in the data set. On the other hand, VGG2 is large-scale face recognition dataset, where the images are

TABLE 1. EER AND INTER-CLASS VERIATIONS UNDER DIFFERENT NONLINEAR RATE $\boldsymbol{\alpha}$

α	0.10	0.20	0.30	0.40	0.50	**0.60**	0.70	0.80	0.90	1.00
V [d^-]	451.31	451.31	451.31	380.12	373.19	**286.05**	295.09	337.04	402.10	483.05
EER	0.42	0.42	0.42	0.44	0.44	1.05	1.84	6.61	12.43	17.27

TABLE 2. EER AND INTER-CLASS VERIATIONS WITH DIFFERENT HASHING ALGORITHM

	$NMDSH_{0.6}$[a]	**SMDSH**	**BioHashing**	**IoM**
V [d −]	**286.05**	501.10	1064	608.73
EER	1.05	**0.37**	0.44	0.48

[a] Subscript value indicates the nonlinear rate α in (9).

downloaded from Google Image Search. These images are having large variations in pose, age, illumination, ethnicity and profession. There are 9131 subjects in VGG2, and 3.31 Million images are included.

B. Deep model features extraction

InsightFace (a.k.a. ArcFace), a latest deep model for face images, utilizes a new loss function named additive angular margin loss for learning and it has achieved excellent performance on public benchmarks [20]. In this work, we utilize the InsightFace open source code from github[1].

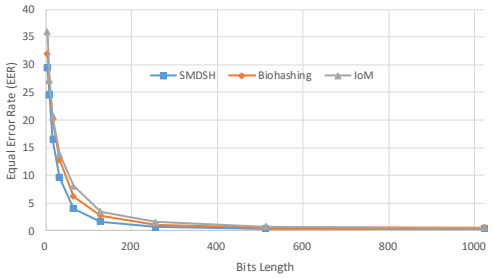
All images are firstly aligned by MTCNN [22]. Specifically, images are aligned and cropped to 112×112. Images that cannot be aligned will be discarded since we only focus on biometric template protection. Next, the InsightFace[2] models pre-trained by MS-Celeb-1M [23] are employed to generate the 512-dimension embeddings.

C. SMDSH parameter optimization on accuracy

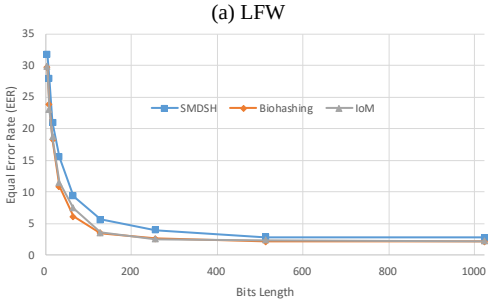
The bit-length parameter of SMDSH is investigated in terms of accuracy using equal error rate (EER) as indicator. The protocol is described as follow: training set, gallery set, and probe set are generated for LFW and VGG2. For LFW, face images are classified into three classes according to [24], and only Known (subjects included in the gallery), Known unknowns (subjects used for training but not included in the gallery) are utilized to compute EER under close-set situation since we want to focus on close-set only in this research. The training dataset is generated by collecting the first 3 images of Known and first image of Known unknowns. The first 3 images of Known are taken also as gallery set, and the remaining images of Known is taken as the probe set, thus we ensure that all subjects in the probe has corresponding user in the gallery. The results for SMDSH, BioHashing and IoM on LFW are depicted in Fig. 2(a).

As for VGG2, the first 2000 users are denoted as Known, and the next 2000 users are taken as Known unknowns. To generate the training set, first 2 images of known and first images of known unknowns are selected. The first 3 images from Known are taken as gallery while the 4th to 6th images from Known are taken as the probe set. The result of SMDSH, BioHashing and IoM on VGG2 are depicted in Fig. 2(b).

Fig. 2 suggests that SMDSH shows comparable performances for all bit lengths. For both LFW and VGG2, when the bit length is larger than 512, the EER stabilizes. Based on this observation, we set the bit length of SMDSH and NMDSH to 1024 for accuracy and security purposes in the following experiment. It is also observed in Fig. 2(a) that the proposed SMDSH outperforms two similar hashing on



(a) LFW



(b) VGG2

Fig 2. EER vs bits length on (a) LFW and (b) VGG2.

LFW, namely, BioHashing and IoM. However, SMDSH slightly inferior on VGG2 when compared with IoM and BioHashing as observed in Fig. 2(b). This is possibly due to the fact that VGG2 has 2000 users in the gallery while LFW only has 610 users in the gallery. From such observations, the adaptation of SMDSH in large gallery will be investigated in our future work. All in all, SMDSH hash code with length 1024 bits and beyond show consistent performance in terms of accuracy.

D. NMDSH parameter optimization on SA resistance

Although SMDSH shows comparable accuracy performance, it is still not safe to conclude SMDSH is the ideal hashing for BTP. Therefore, NMDSH's resistance to SA, as discussed in section IV, is evaluated by the inter-class variation $V[d-]$. Since *softmod* is use in NMDSH, and the distance correlation between Hamming and original Euclidean space can achieve a nonlinearly correlation. Table 1 records the result of $V[d-]$ using different nonlinear rate $\boldsymbol{\alpha}$ values in (9), while Table 2 presents the result for different hashing methods.

From Table 1, it is observed that both large and small $\boldsymbol{\alpha}$ can lead to large inter-class variations, while a large $\boldsymbol{\alpha}$ leads to dramatical drop in accuracy. It is also observed $\boldsymbol{\alpha} = 0.6$ achieves the optimal performance for LFW, where $V[d-]$ is small and EER is still generally preserved. In Table 2, we can see that $NMDSH_{0.6}$ achieves significantly smaller inter-class

[1] https://bit.ly/2LTTjj3

[2] https://bit.ly/2RnF8WR

TABLE 3. ACCURACY PERFORMANCE BY LFW STANDARD PROTOCOL

	Original	SMDSH	$NMDSH_{0.6}$	BioHashing	IoM
AUC:	99.92 %	**99.90% ± 0.01%**	99.37% ± 0.03%	99.89% ± 0.02%	99.89% ± 0.01%
EER:	0.50%	**0.75 ± 0.07%**	3.51%± 0.13%	0.88± 0.12%	0.83± 0.05%
TPR001:	99.53 %	**99.31% ± 0.07%**	94.67% ± 0.47%	99.17% ± 0.15%	99.21% ± 0.07%
TPR0001:	99.23 %	**98.61% ± 0.29%**	91.86%±1.24%	98.39% ± 0.15%	98.54% ± 0.15%

TABLE 4. ACCURACY PERFORMANCE BY BLUFR PROTOCOL

	Original	SMDSH	$NMDSH_{0.6}$	BioHashing	IoM
VR (FAR0.1%)	99.70% ± 0.07%	99.34%±0.16%	90.01%±2.16%	99.29%±0.20%	**99.53%±0.12%**
DIR (Rank1, FAR1%)	98.04% ± 0.46%	95.54%±0.58%	68.38%±2.81%	95.48%±0.51%	**96.29%±0.75%**

variation when compared to two popular cancelable BTP techniques, viz., BioHashing and IoM. This implies that $NMDSH_{0.6}$ is more secure than other methods in terms of resistance against SA.

It is expected that the accuracy performance of $NMDSH_{0.6}$ to degrade since its EER increases from 0.37 to 1.05 according to Table 2. This is due to the trade-off between security and accuracy. Specifically, if high accuracy is desired, the transformed template should contain more discriminate information. However, when more information is included in the template, it will also undesirably facilitate attackers to retrieve the original biometric data, and eventually information leakage.

Overall, our results showed that NMDSH achieves a well-balanced performance between accuracy and security when $\boldsymbol{\alpha} = 0.6$. In addition, NMDSH also shows higher security level than BioHashing and IoM.

E. Accuracy performance evaluation on LFW

After deciding the parameters of SMDSH/NMDSH, the accuracy performance of SMDSH/NMDSH are performed on public face dataset LFW. There are two popular protocols available for LFW accuracy performance evaluation, namely, the standard LFW protocol [20] and the BLUFR protocol [25]. For the standard evaluation protocol, a 10-fold cross-validation verification experiment is required, where each fold consists of 300 genuine and 300 impostor comparisons. The results collected under the standard protocol are recorded in Table 3, including AUC (area under curve), EER, and true positive rate (TPR). It should be noted that the standard LFW protocol has some limitations, for example only 3000 genuine and 3000 impostor matches for classification, and the performance evaluation at low false accept rates (FARs) is not appropriate due to the limited number of impostor matches. Therefore, BLUFR protocol is utilized to further evaluate the proposed models [25]. BLUFR defines both 10-fold cross-validation face verification and identification tests involving larger number of genuine and impostor comparisons. Table 4 reports the true accept rate at FAR of 0.1% for face verification, as well as the detection and identification rate (DIR) at Rank-1 with 1% FAR for open-set identification.

Based on the results recorded in Table 3, SMDSH shows superior performance when compared with IoM and BioHashing on the LFW standard protocol, while NMDSH falls short in terms of accuracy performance. On the other hand, under the BLUFR protocol in Table 4, SMDSH is marginally inferior to IoM, but its accuracy is still similar to that of IoM. This suggests that SMDSH can preserve the biometric accuracy performance. As expected, the accuracy of NMDSH is lower when compared with SMDSH. However, NMDSH is still practical and desirable, considering its resistance against SA.

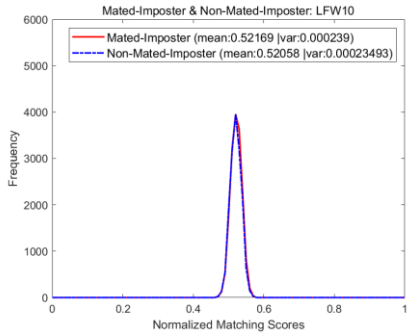
As a summary, our proposed SMDSH exhibits superior accuracy performance on LFW using the standard protocol. On the other hand, SMDSH outperforms BioHashing but is marginally inferior to IoM using the BLUFR protocol. Regarding NMDSH, results suggest that the accuracy will degrade, but the degradation is traded for security.

VI. REVOCABILITY AND UNLINKABILITY

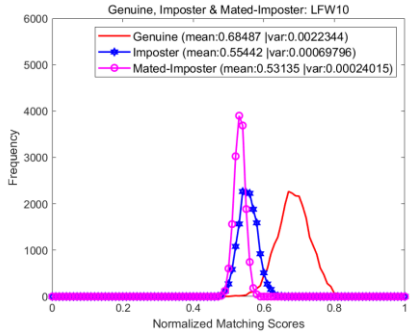
To validate the requirement of non-linkability and revocability, several simulations are conducted. Specifically, unlinkability is achieved when the attacker is incapable of retrieving any information by matching the hashed codes generated from an identical face by employing different random projection matrices (e.g., two hash codes are from same identity), given that templates from several databases or applications are compromised and the attacker knows well about the hashing algorithm in use. On the other hand, cancelability allows the generation of new template (by means of using new random projection keys) when the template in question is compromised. In addition, it should also be infeasible to attack a renewed template or retrieve any useful information from any of the revoked templates.

Two scores are considered to evaluate the revocability and unlikability, namely: (a) Mated-Imposter score - the matching score between two NMDSH hashed codes from the same face computed by employing two different random projection matrices, and; (b) Non-Mated-Imposter - the matching scores between two hashed codes from two different faces using two different random projection matrices. Genuine scores are the matching scores from the same person and the same random projection matrix, while imposter scores are the matching scores from different person faces. For verification purpose, a protocol based on LFW is adopted to compute the abovementioned scores under different scenarios. In LFW, the identity having ≥ 10 images are selected and the first 10 images are chosen to form a new small dataset denoted as LFW10 (total 158 users).

To resist the linkability attack, the matching score distribution from mated user and non-mated user in two different application should be indistinguishable. Fig. 3(a) shows that the distribution for Non-Mated-Imposter scores and Mated-Imposter scores are overlapped, which indicates that even an attacker can obtain all matching scores between the compromised templates from different sources, it is still



(a) non-linkability analysis



(b) revocability analysis

Fig 3. NMDSH matching score distributions for (a) non-linkability analysis, (b) revocability analysis.

infeasible to identify any hashed code pairs from the same individual. Hence, the unlikability property is achieved by NMDSH.

To evaluate the revocability property of NMDSH and demonstrate the security of renewed template, the distributions of Mated-Imposter, Genuine and Imposter scores are considered. As observed in Fig. 3(b), the distribution of Mated-Imposter and imposter scores are largely overlapped, and the Mated-Imposter distribution is far from the distribution of genuine score. Under the revocation situation, the score distribution shows no difference between the templates generated from same individual face or different individual face by different random matrices. Thus, the revocability property is justified.

Overall, our analysis and results show that the proposed NMDSH satisfies the BTP requirements, viz., unlinkability and revocability. SMDSH, which is of higher accuracy, can also be regarded as a valid cancellable BTP scheme with a limited robust to SA.

VII. Conclusion

In this paper, we proposed a nonlinear hashing method based on MDSH, namely NMDSH, to secure the face deep features. Notably, by incorporating many-to-one and *softmod* functions, the generated binary template can be securely protected against template inversion and SA. The accuracy of the NMDSH is preserved largely when considering the public face datasets such as LFW and VGG2. In addition, unlinkability and revocability are also demonstrated experimentally to vindicate the feasibility of NMDSH. As future work, transforming the NMDSH into a supervised method will be explored, and this may lead to higher accuracy with the help of supervised learning.

Acknowledgment

This research was partly supported by EU Horizon 2020 - Marie Sklodowska-Curie Actions through the project entitled Computer Vision Enabled Multimedia Forensics and People Identification (Project No. 690907, Acronym: IDENTITY), Fundamental Research Grant Scheme (FRGS/1/2018/ICT02/MUSM/03/3).

References

[1] Z. Jin, M.-H. Lim, A. B. J. Teoh, and B.-M. Goi, "A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template," Pattern Recognition Letters, vol. 42, pp. 137–147, Jun. 2014.

[2] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and Robust Iris Recognition Using Random Projections and Sparse Representations," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.

[3] W. B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," in Contemporary Mathematics, vol. 26, R. Beals, A. Beck, A. Bellow, and A. Hajian, Eds. Providence, Rhode Island: American Mathematical Society, 1984, pp. 189–206.

[4] S. D. A. Gupta, "An elementary proof of the Johnson-Lindenstrauss Lemma," p. 6.

[5] P. Frankl and H. Maehara, "The Johnson-Lindenstrauss lemma and the sphericity of some graphs," Journal of Combinatorial Theory, Series B, vol. 44, no. 3, pp. 355–362, Jun. 1988.

[6] D. Achlioptas, "Database-friendly Random Projections," in Proceedings of the Twentieth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, New York, NY, USA, 2001, pp. 274–281.

[7] R. I. Arriaga and S. Vempala, "An algorithmic theory of learning: Robust concepts and random projection," Mach Learn, vol. 63, no. 2, pp. 161–182, May 2006.

[8] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[9] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, "An Integrated Dual Factor Authenticator Based on the Face Data and Tokenised Random Number," in Biometric Authentication, vol. 3072, D. Zhang and A. K. Jain, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 117–123.

[10] D. C. L. Ngo, A. B. J. Teoh, and A. Goh, "Eigenspace-Based Face Hashing," in Biometric Authentication, vol. 3072, D. Zhang and A. K. Jain, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 195–199.

[11] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants," Pattern Recognition, vol. 39, no. 7, pp. 1359–1368, Jul. 2006.

[12] J. Kang, D. Nyang, and K. Lee, "Two-factor face authentication using matrix permutation transformation and a user password," Information Sciences, vol. 269, pp. 1–20, Jun. 2014.

[13] M. Jeong, C. Lee, J. Kim, J.-Y. Choi, K.-A. Toh, and J. Kim, "Changeable Biometrics for Appearance Based Face Recognition," in 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, Baltimore, MD, USA, 2006, pp. 1–5.

[14] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, and C. Busch, "Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters," in 2014 22nd International Conference on Pattern Recognition, 2014, pp. 4483–4488.

[15] Z. Jin, J. Y. Hwang, Y. Lai, S. Kim, and A. B. J. Teoh, "Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[16] Y. Weiss, R. Fergus, and A. Torralba, "Multidimensional Spectral Hashing," in Computer Vision – ECCV 2012, vol. 7576, A. Fitzgibbon, S. Lazebnik, P. Perona, Y. Sato, and C. Schmid, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 340–353.

[17] G. Mai, K. Cao, P. C. Yuen, and A. K. Jain, "On the Reconstruction of Face Images from Deep Face Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1–1, 2018.

[18] A. George, Mathematical Methods for Physicists - 3rd Edition. 1985.

[19] Y. Chen, Y. Wo, R. Xie, C. Wu, and G. Han, "Deep Secure Quantization: On secure biometric hashing against similarity-based attacks," Signal Processing, vol. 154, pp. 314–323, Jan. 2019.

[20] G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database forStudying Face Recognition in Unconstrained Environments," presented at the Workshop on Faces in "Real-Life" Images: Detection, Alignment, and Recognition, 2008.

[21] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A Dataset for Recognising Faces across Pose and Age," in 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, 2018, pp. 67–74.

[22] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks," IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.

[23] Y. Guo, L. Zhang, Y. Hu, X. He, and J. Gao, "MS-Celeb-1M: A Dataset and Benchmark for Large-Scale Face Recognition," arXiv:1607.08221 [cs], Jul. 2016.

[24] M. Günther, S. Cruz, E. M. Rudd, and T. E. Boult, "Toward Open-Set Face Recognition," in 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2017, pp. 573–582.

[25] S. Liao, Zhen Lei, Dong Yi, and S. Z. Li, "A benchmark study of large-scale unconstrained face recognition," in IEEE International Joint Conference on Biometrics, Clearwater, FL, USA, 2014, pp. 1–8.