Fusing Binary Templates for Multi-biometric Cryptosystems

Guangcan Mai, Meng-Hui Lim and Pong C Yuen
Hong Kong Baptist University
{csgcmai, menghuilim, pcyuen}@Comp.HKBU.Edu.HK

Abstract

Biometric cryptosystem has been proven to be one of the promising approaches for template protection. Since most methods in this approach require binary input, to extend it for multiple modalities, binary template fusion is required. This paper addresses the issues of multi-biometrics' performance and security, and proposes a new binary template fusion method which could maximize the fused template discriminability and its entropy by reducing the bits dependency. Three publicly available datasets are used for experiments. Experimental results show that the proposed method outperforms the state of the art methods.

1. Introduction

Multi-modal biometric systems, consolidating multiple traits (*e.g.*, face, fingerprint, palmprint, voice, iris), address limitations of unimodal biometric systems in matching accuracy, spoofing difficulty, universality, and feasibility [27]. However, the template security in multi-biometric systems is more crucial than uni-biometric systems because they store and process information about multiple biometric traits per user. Once the system storage is compromised, the biometric templates that without protection could be revealed and used to construct the physical spoof [8, 26]. As the biometrics is unique and irrevocable, if the original biometric images corresponding to multiple traits of a user can all be reconstructed, it would cause permanent compromise of these user biometrics.

To date, there are three kinds of biometric template protection approaches. They are feature transformation [23], biometric cryptosystems [13, 14] and hybrid approaches [10]. In the feature transformation approach, templates are transformed through a one-way transformation method using a user-specific random key. This approach provides cancellability as a new user-specific key can be used to generate a new transformed output if the previous transformed output has been compromised. The biometric cryptosystems store a sketch that is generated from the enrolled template, where the security of these cryptosystems is based on the entropy of the templates. Hybrid approaches combine both feature transformation and biometric cryptosystems approaches to provide both security and template cancellability.

Biometric cryptosystems take query templates (features) and the auxiliary data as input, and produce the binary decisions (accept/reject). When employing biometric cryptosystems, multiple traits in multi-biometric systems can be fused at feature or score/decision level. Multi-biometric cryptosystems based on score/decision-level fusion are arguably less secure than those based on feature-level-fusion. In score/decision-level-fusion-based systems, the sketches generated from the unimodal templates are stored individually and can be attacked separately; while in feature-level-fusion-based systems, the stored sketch is generated from the multimodal template and much harder to be attacked because the multimodal template integrates multiple uncorrelated biometrics and hence has a higher entropy. The higher security of feature-level-fusion-based systems has also been justified in a recent work [19] using hill-climbing analysis.

Binary feature is the only acceptable form of input for typical biometric cryptosystems such as fuzzy commitment. To obtain a set of fused binary features via feature fusion, a typical approach is to convert distinct types of features to some unified representations, fuse them and convert these fused features into binary when such a biometric cryptosystem is concerned. However, when some of the modalities are inherently represented in binary (e.g., binary features extracted from commercial black-box feature extractors such as IrisCode [4]), converting these features to other forms is often infeasible because the quantization and encoding parameters used in the actual binarization process are not available. In this case, feature fusion can only be carried out after converting the unimodal features into binary [7, 9, 10, 18, 30].

In this paper, we focus on binary feature level fusion for multi-biometric cryptosystems, where biometric features from multiple biometric sources are converted individually to a unified binary representation before fusion. Generally, in multi-biometric cryptosystems, there are three criteria for fused binary biometric features:

- **Discriminability:** Fused binary features have to be dis-

criminative in order not to defeat the original purpose of recognizing users. Each bit of the fused feature should have small intra-user variations and large inter-user variations.

- **Security:** Entropy of the fused binary features have to be adequately high in order to thwart guessing attacks, even if the stored auxiliary data is revealed. Hence, the binary feature fusion should produce highly uniform bits and incur low dependency among bits in the fused binary representation.

- **Privacy:** The stored auxiliary data for feature extraction and fusion should not leak information on the corresponding raw biometrics of a target user.

To obtain a fused binary feature with high discriminability and high entropy, the dependency among bits in a binary representation should be reduced and each of the bits is made highly uniform, on top of having small intra-user variations and large inter-user variations.

The entropy of the extracted binary features from every biometric source is generally limited, because of the inherently high dependency among bits. This dependency can be used to facilitate guessing of the binary features of the target user(s) [11, 25, 31]. However, existing binary fusion techniques are limited to simple concatenation and bit selection. Most of them consider only the discriminability criterion without taking into account the dependency among bits, thus potentially producing fused binary representation with low entropy.

By combining information from multiple bits appropriately, it is more likely that a uniform and discriminative bit can be derived. We propose a binary feature fusion method to extract discriminative and high-entropy templates from multiple binary representations of unimodal biometric sources for multi-biometric cryptosystems. First, we use dependency reductive bit-grouping to extract a set of less dependent bit-groups. Then, for each bit group, we fuse the bits based on a discriminability and uniformity objective function.

The structure of this paper is organized as follows. In the next section, we present related work of binary fusion techniques of biometric features. In Section 3, we describe proposed two-stage binary feature fusion. We present our experimental results to justify the effectiveness of our fusion approach in Section 4. Finally, concluding remarks are drawn in Section 5.

2. Related Work

Only a few binary feature-level-fusion based multi-biometric cryptosystems can be found in the literature [15, 20, 28]. Furthermore, most of them only consider the discriminability of the fused binary feature, but lack of consideration on security. Sutcu *et al*. [28] combine binary string of fingerprint and face by concatenation, then the fuzzy commitment is applied on the combined feature immediately. However, concatenating binary strings might lead to a curse-of-dimensionality problem due to the large increase in feature dimensionality and limited training data [27]. In addition, feature concatenation cannot remove redundant or unstable feature introduced during feature extraction.

Bit selection is applied to avoid the curse-of-dimensionality problem by selecting discriminative or reliable features. Kelkboom *et al*. [15] selected a subset of most reliable bits according to a criteria named z-score at feature level fusion, which measures the regularized distance between the real-value corresponding to these quantized bits and the quantization threshold. Nagar *et al*. [20] present a discriminability based bit selection method to select a subset of bits from each biometric trait individually and combine the selected bits together via concatenation. They compute the discriminability from the genuine and impostor bit-error probability. In most cases, there are insufficient bits that fulfill all three requirements (i.e., high uniformity, small intra-user variations and large inter-user variations). In addition, most bits are mutually dependent and the dependency among them cannot be reduced through bit selection.

3. Proposed binary feature level fusion

3.1. Overview of proposed method

A discriminative and high-entropy binary representation necessitates lowly-dependent and highly-uniform bits with small intra-user and large inter-user variations. We propose a two-stage binary feature-level fusion method to achieve this objective: (i) dependency reductive bit-grouping and (ii) discriminative and uniform within-group fusion. We first reduce the dependency among the fused bits by assigning the bits into groups so that the groups have low inter-dependency. With these bit groups, we extract an output fused bit per group through a mapping that maximizes uniformity, minimizes intra-user variation and maximizes inter-user variation of the fused bit. By concatenating these fused bits, we obtain the fused representation of a user. The block diagram of proposed method is shown in Fig.1.

Suppose we have extracted a multimodal binary feature $\boldsymbol{b} = \{b_1, b_2, \cdots, b_N\}$, which is obtained by concatenating binary features from multiple modalities (*e.g*., face, fingerprint, iris, *etc*.). Here, N denotes the size of the concatenated binary feature. Our two stages in testing phase for fusing the bits of $\boldsymbol{b}$ to an L-bit binary feature $\boldsymbol{z} = \{z_1, z_2, \cdots, z_L\}$ are described as follows:

(1) **Dependency reductive bit-grouping**: Input bits of $\boldsymbol{b}$ are grouped into a set of weakly-dependent disjoint

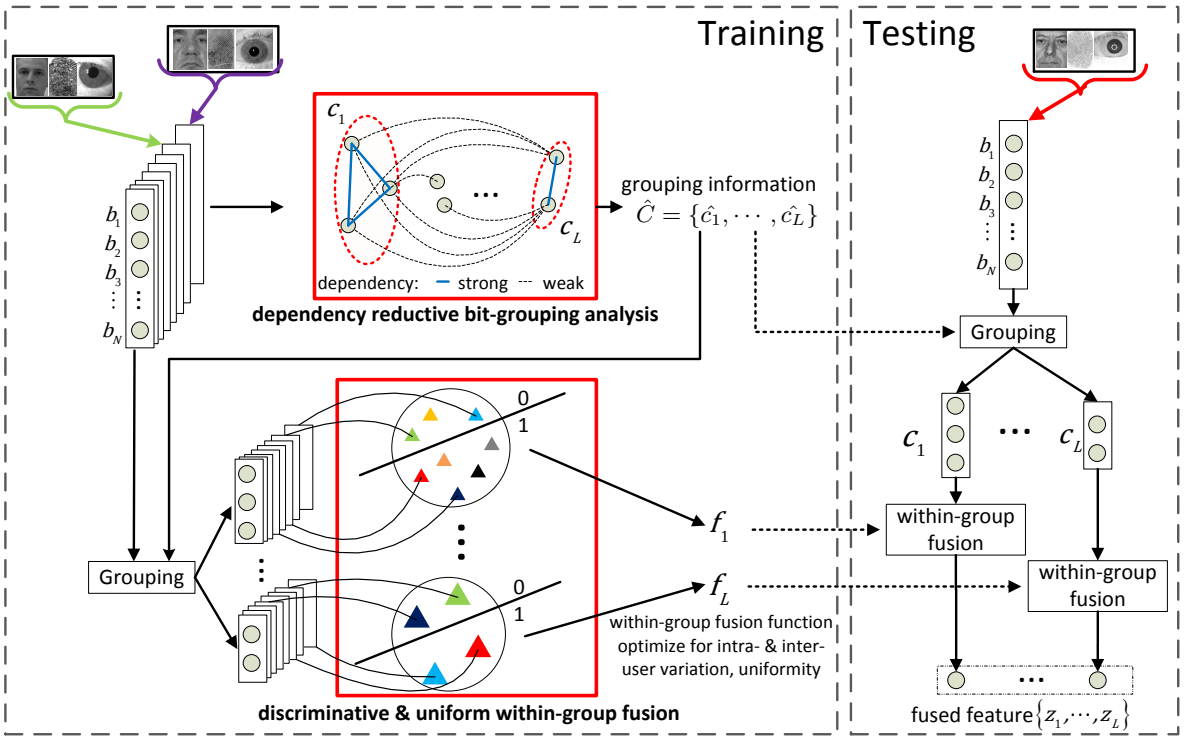


Figure 1: The proposed binary feature level fusion algorithm

bit-groups $C = \{c_1, c_2, ..., c_L\}$ such that $\forall l_1, l_2 \in [1, L], c_{l_1} \cap c_{l_2} = \emptyset, \bigcup_{l=1}^{L} c_l \subseteq \{b_1, \cdots, b_n, \cdots, b_N\}$.

(2) **Discriminative and uniform within-group fusion**: Bits in each group c_l are fused to a single bit z_l using a group-specific mapping f_l that maximizes the discriminability and uniformity of z_l.

The output bit z_l of all groups are concatenated to produce the final bit string $\boldsymbol{z}$. To realize these two stages, the optimum grouping function $c_l = \{b_n, n \in \hat{\zeta}_l\}$ that is based on grouping information $\hat{C} = \{\hat{c_1}, \cdots, \hat{c_l}, \cdots, \hat{c_L}\}$ in stage one and the mapping function f_l in stage two need to be sought. Here, the grouping information $\hat{c_l}$ specifies bits of $\boldsymbol{b}$ that should be grouped. The mapping function f_l specifies to which output bit value is for the bits in group c_l are mapped.

3.2. Dependency reductive bit-grouping

To extract a set of lowly dependent bit-groups C from $\boldsymbol{b}$, the bits with strong dependency should be grouped together, and the ones with weak dependency should be grouped into different groups. We adopt clustering with dependency as the similarity metric to perform such dependency reductive bit-grouping. However, dependency, typically measured by mutual information(MI), is not a common metric in clustering that is based on spatial domain. This causes the desired bit-groups unable to be extracted via partitioning the bits directly according to their distribution or density. Inspired by [17], we overcome this limitation by using agglomerative hierarchical clustering.

The basic idea of the agglomerative hierarchical clustering is to first initialize all the objects as a one-point (singleton) cluster, and then merge the cluster pair with the highest similarity iteratively. We express the dependency measure using MI [17] as

$$I(c_{l_1}, c_{l_2}) = H(c_{l_1}) + H(c_{l_2}) - H(c_{l_1}, c_{l_2}) \qquad (1)$$

where $H(c_{l_1})$ and $H(c_{l_2})$ denote the joint entropy of bits in cluster c_{l_1} and c_{l_2}, respectively, and $H(c_{l_1}, c_{l_2})$ denotes the joint entropy of bits in both of them.

Performing agglomerative hierarchical clustering using MI as similarity metric might not group the bits with strong pairwise dependency together. This is because the MI does not provide a fair comparison when involving cluster of different sizes. When ignoring the high order dependency (higher than second order) of the bits, the MI between two clusters is roughly equal to the MI sum of their corresponding bit-pairs (each of bits from different clusters). For a specific cluster, its MI with a large-size cluster is mostly higher than a small-size cluster, even though the bits of this cluster have higher dependency with the bits in the small-size cluster than the ones in large-size cluster. The large-size cluster would be merged with the specific cluster, which

Algorithm 1 AMI based hierarchical clustering

Inputs:
α training samples $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_\alpha\}$,
number of clusters L, maximum cluster size t_{size}

Outputs:
grouping information $\hat{C} = \{\hat{c_1}, \cdots, \hat{c_l}, \cdots, \hat{c_L}\}$

Initialize:
$\hat{C_{tmp}} = \{\hat{c_1}, \cdots, \hat{c_n}, \cdots, \hat{c_N}\}$, where $\hat{c_n} = \{n\}$
$En_{tmp} \leftarrow kThMaxEtp(\hat{C_{tmp}}, L)$[1]
$\hat{C} \leftarrow \hat{C_{tmp}}$; $En \leftarrow 0$
$S = \{s_{ij}\}_{i \neq j}$; s_{ij}: AMI between cluster c_i, c_j

while $|\hat{C_{tmp}}| > L$ **do**
  search for largest s_{ab}
  if $|\hat{c_a}| + |\hat{c_b}| > t_{size}$ **then**
    $s_{ab} \leftarrow -1$
    Continue
  end if
  merge $\hat{c_a}$ and $\hat{c_b}$ to $\hat{c_z}$ and form the new $\hat{C_{tmp}}$
  $En_{tmp} \leftarrow kThMaxEtp(\hat{C_{tmp}}, L)$
  if $En_{tmp} > \min(En, 1)$ **then**
    $\hat{C} \leftarrow \hat{C_{tmp}}$, $En \leftarrow En_{tmp}$
  end if
  for each $\hat{c_j} \in \hat{C_{tmp}}$, $j \neq z$ **do**
    update all s_{zj}
  end for
end while
find L highest-entropy clusters from $\hat{C}$ and return

is unwanted because bits with strong dependency are not grouped together.

To cluster the bits with strong pairwise dependency together, normalization of MI on cluster size is required to alleviate the effect of cluster size on clustering. Treating each cluster as a set, the number of pairwise bit-dependency involved in the MI between two clusters equals the cardinality product of these two clusters. To obtain a fair comparison on pairwise bit-dependency involving cluster of different sizes, we normalize the MI using the cardinality product, which is named as average mutual information (AMI)

$$I_{avg}(c_{l_1}, c_{l_2}) = \frac{I(c_{l_1}, c_{l_2})}{|c_{l_1}||c_{l_2}|} \tag{2}$$

where $|c_{l_1}|$ and $|c_{l_2}|$ denotes the cardinality of cluster c_{l_1} and c_{l_2}, respectively. Therefore, we design our AMI based clustering algorithm, which is shown in Algorithm 1.

We prevent the clusters to be merged to a cluster with size larger than t_{size} in Algorithm 1 by setting their similarity to -1. This is because the within-group fusion function sought in stage two is based on the estimation of the bit-combination distribution of each groups. However, the estimation for a group with large size require large number of training data, which is generally limited in biometrics. To ensure the estimation accuracy, the cluster size has to be limited. The maximum size we used is the binary logarithm of number of training samples.

The merging of the cluster pair with the maximum dependency yields the updated cluster configuration $\hat{C_{tmp}}$. This configuration will be assigned to the current output cluster set $\hat{C}$ based on their L-th largest cluster entropy. As the entropy of the fused bit is dominated by the cluster entropy, all of the L extracted clusters should have at least one-bit entropy. If some of the clusters could not achieve at least one-bit entropy, their entropy should be as high as possible. Therefore, we update the cluster set $\hat{C}$ to $\hat{C_{tmp}}$ when one of following conditions is satisfied: i) The L-th largest cluster entropy of both $\hat{C}$ and $\hat{C_{tmp}}$ are greater than one-bit; ii) The L-th largest cluster entropy of $\hat{C}$ less than one-bit and less than the one of $\hat{C_{tmp}}$.

3.3. Discriminative-uniform within-group fusion

The objective of this step is to search for a within-group fusion function $f(c) = z$ for each group c to fuse its bits to a bit z with maximum uniformity, minimum intra-user variations and maximum inter-user variations. For a bit-group c that consist of m bits, there are at most 2^m possible bit-combinations. This can be expressed as $c = \{x_1, \cdots, x_i, \cdots, x_{2^m}\}$, where x_i denotes i-th probable bit-combination of c. Then, the within-group fusion is analogous to a binary-label assignment process, where each bit-combination is assigned a binary output label (a fused bit value). More specifically, the fusion function for group c could be described using a binary vector $\boldsymbol{g} = \{g_1, \cdots, g_i, \cdots, g_{2^m}\}, g_i \in \{0, 1\}$, such that $f(x_i) = g_i$.

Maximizing the uniformity, minimizing the intra-user variations and maximizing the inter-user variations in the within-group fusion could be achieved even though the maximization of the uniformity is removed. The uniformity of a bit means how close the probability of this bit takes value '0/1' approach to 0.5, which will be maximized automatically during the maximization of the inter-user variation. To maximize the inter-user variation, bits from different users should have highest probability to take different values. This implies that the bit could equally separate all of the users into two sets, one set of users take value '0' and the another take value '1'. Therefore, the bits have equal probability 0.5 across the population to take value '0/1' when their inter-user variation is maximized.

The intra-user variations and inter-user variations of the fused bit z corresponding to group c could be measured by the genuine bit-error probability p_g^e and the impostor bit-

[1] $kThMaxEtp(\hat{C}, k)$ returns the k-th largest cluster entropy of $\hat{C}$

error probability p_i^e, respectively. Let y_s and y_t denote the corresponding bit-combination of s-th and the t-th training sample in group c, where $s \neq t$ and s, t range from 1 to number of training samples α. The genuine probability of bit-combination-pairs (x_i, x_j) is defined as their occurrence probability across bit-combination-pairs that each of their bit-combinations come from same user. Mathematically,

$$\Pr_G(x_i, x_j) = \Pr(y_s = x_i, y_t = x_j | L_s = L_t) \quad (3)$$

where L_s and L_t denote the label of s-th and t-th training sample, x_i and x_j denotes the i-th and j-th possible bit-combination of group c, resp., and i, j range from 1 to 2^m.

Genuine bit-error probability of the fused bit is the probability where samples from the same user take different values/bit patterns. From the view of the pattern-pairs, it is the probability of pattern-pairs where two patterns come from the same user but are associated with different fused bit value. Let $K^{(0)}$ and $K^{(1)}$ denote the sets of patterns in group c to be fused to bit value '0' and '1', respectively. This implies that $g_i = 0$ when $x_i \in K^{(0)}$ and $g_j = 1$ when $x_j \in K^{(1)}$. Mathematically, the genuine bit-error probability of the fused bit z corresponding to group c is the summation of all genuine pattern-pair probability where the patterns in the pair are associated with different fused results. We have

$$\begin{aligned} p_g^e &= \Pr(y_s \in K^{(0)}, y_t \in K^{(1)} | L_s = L_t) \\ &= \sum_{x_i \in K^{(0)}} \sum_{x_j \in K^{(1)}} \Pr(y_s = x_i, y_t = x_j | L_s = L_t) \\ &= \sum_{g_i=0} \sum_{g_j=1} \Pr_G(x_i, x_j) \end{aligned} \quad (4)$$

The impostor probability of pattern-pairs (x_i, x_j) is the occurrence probability of pattern-pairs where both patterns come from different users,

$$\Pr_I(x_i, x_j) = \Pr(y_s = x_i, y_t = x_j | L_s \neq L_t) \quad (5)$$

Similarly, the impostor bit-error probability of fused bit z corresponding to group c is the probability of pattern-pairs where their patterns come from different users and have different fused results, which can be expressed as

$$\begin{aligned} p_i^e &= \Pr(y_s \in K^{(0)}, y_t \in K^{(1)} | L_s \neq L_t) \\ &= \sum_{x_i \in K^{(0)}} \sum_{x_j \in K^{(1)}} \Pr(y_s = x_i, y_t = x_j | L_s \neq L_t) \\ &= \sum_{g_i=0} \sum_{g_j=1} \Pr_I(x_i, x_j) \end{aligned} \quad (6)$$

We have obtained the expressions of genuine and impostor bit-error probability of the fused bit z in terms of the bit-patterns in cluster c and their corresponding fused results $\boldsymbol{g}$. To seek the $\boldsymbol{g}$ for the within-group fusion with minimum genuine and maximum impostor bit-error probability, we solve the following minimization problem using integer genetic algorithm [5, 6],

$$\begin{aligned} \min_{\boldsymbol{g}} F(\boldsymbol{g}) &= \left(p_g^e - p_i^e\right) \\ &= \sum_{g_i=0} \sum_{g_j=1} \left(\Pr_G(x_i, x_j) - \Pr_I(x_i, x_j)\right) \end{aligned} \quad (7)$$

subject to

$$\boldsymbol{g} = \{0, 1\}^{2^m}$$

A unique $\boldsymbol{g}$ has to be sought for every group.

4. Experimental Results

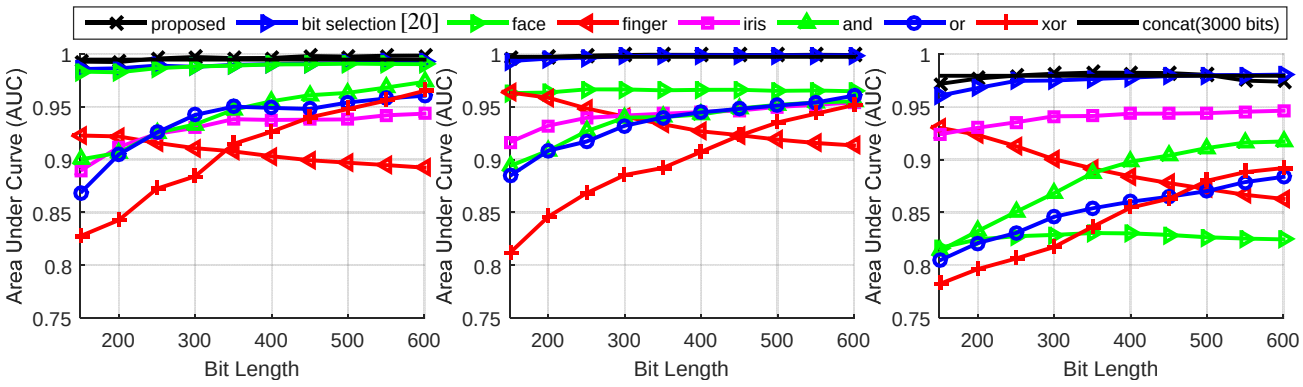
4.1. Database and feature extraction

We evaluated the discriminability and entropy of the fused binary feature generated by the proposed fusion algorithm using one real and two chimeric multi-modal databases containing three modalities: face, fingerprint and iris. The real multi-modal database, WVU[12], contains images of 106 subjects where each subject has five multi-modal samples, with three samples are used for training and the remaining two for testing. Both two chimeric multi-modal database are obtained by randomly matching images from a face, a fingerprint and an iris database. These databases contain image of 100 subjects where each subject has eight multi-modal samples, with four samples are used for training and the remaining four are used for testing. The first chimeric multi-modal database, named as Chimeric A, consists of face from FERET[22], fingerprint from FVC2000-DB2 and iris from CASIA-Iris-Thousand [1]. The second one, named as Chimeric B, consists of face from FRGC[21], fingerprint from FVC2002-DB2 and iris from ICE2006[3]. Our testing protocol is described as follows. For the genuine attempts, we use the first sample as enrollment and the remaining samples as query. For the impostor attempts, the i-th sample of each subject is matched against the i-th sample of remaining subjects, while each pair of samples will be matched against once to avoid the correlation.

Prior to evaluate binary fusion algorithms, we extract the binary features of face, fingerprint and iris. The images of each modality is first processed as follows:

Face Proper face alignment is first applied based on the standard face landmark. To eliminate effect from variations such as hair style and background, the face region of each sample is cropped and resized to 61×73 pixels in FERET and FRGC, resp., 15×20 pixels in WVU.

Fingerprint We first extract minutiae from each fingerprint using Verifinger SDK 4.2 [2]. The extracted minutiae are converted into an ordered binary feature using the



(a) WVU Multimodal (b) Chimeric A (c) Chimeric B

Figure 2: Comparison of area under ROC curve on (a) WVU multi-modal, (b) Chimeric A, (c) Chimeric B databases.

method proposed in [7] without randomization. Following parameters in [7], each fingerprint image is represented by a vector with length 2^{24}.

Iris The weighted adaptive hough and ellipsopolar transform (WAHET) [29] is employed to segment the iris with size 512×64, then the real features with size 480×1 are extracted from the segmented iris using extractor of Ko *et al.* [16]. Both segmentation and extraction algorithm we used are implemented using the iris toolkit (USIT) [24].

After the preprocessing, we use the PCA on face and LDA on fingerprint and iris to reduce the feature dimension to 50. Then, for features from all of the three modalities, we encode each feature component to a 20-bit binary vector using LSSC [18] and obtain a 1000-bit binary feature.

In this comparative study, we compared the proposed method with the bit selection in [20] by varying the length of fused features. The baseline comparisons of our experiment include the uni-biometric features (i.e., face, fingerprint and iris), and the most straightforward fusion methods, i.e., concatenation and the bit-wise-operation based methods (AND, OR, XOR). To have a fair comparison, features given by each baseline method should have the same length with the proposed method. However, each of the uni-biometric binary feature is originally with length 1000. We obtained the comparable uni-biometric binary features by selecting the most discriminative bits from features of each modality using the discriminability criteria as in [20]. The features of bit-wise-operation are obtained by performing the AND, OR, XOR operation on the obtained uni-biometric binary features. It is noted that the feature of concatenation is obtained by concatenating the three original (without selection) uni-biometric binary features and has length 3000 (1000 × 3), which will be shown as a straight line in the experimental results when varying the bit length.

4.2. Fused binary template discriminability

This section evaluates the discriminability of the fused binary template given by the proposed fusion algorithm on verification using area under curve (AUC) of receiver operating characteristic (ROC). By varying the bit length of the fused binary template from 150 to 600, we plot the AUC of ROC for three databases in Fig.2.

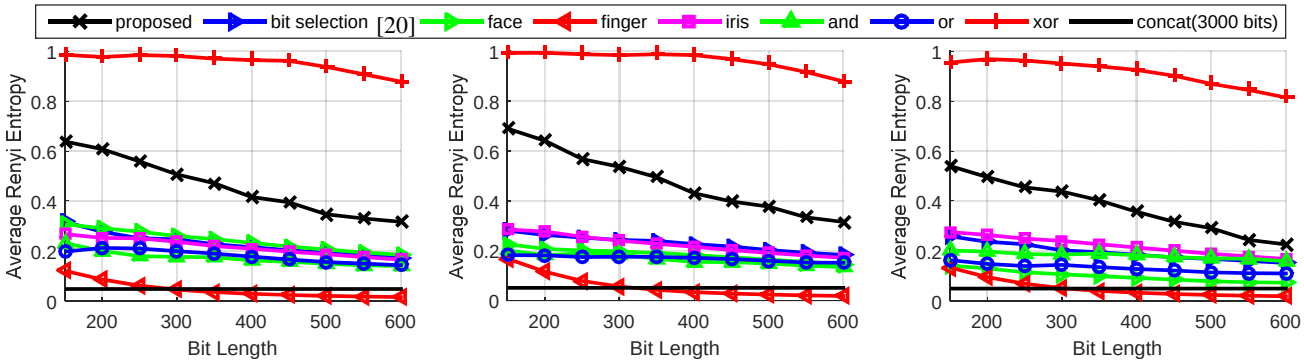
It can be observed that the proposed method is comparable with bit selection and concatenation on all of three databases. Excepting that face on WVU multi-modal database is as discriminative as the proposed method and bit selection, the proposed method and bit selection outperform remaining methods. It is noted that the curve for bit selection is overlapped with the curve for face feature in Fig.2(a) and curve for proposed method is overlapped with the bit selection in Fig.2(b).

The results shows that the features of both the proposed method and bit selection are more discriminative than remaining comparative methods even though biometrics of different qualities are involved. The differences between the AUC of face and fingerprint are around $7 \sim 10\%$ and $2 \sim 5\%$ on WVU multimodal and Chimeric A, resp., while the difference between the AUC of iris and face is around 10% on Chimeric B.

The fingerprint discriminability decreases as the bit length increases on all of three databases. This is because the most discriminative bits will be firstly selected to construct the feature of different bit lengths. When the bit length goes large, there are insufficient discriminative bitscan be selected out. Eventually, the non-discriminative (even noise) bits are used, which cause the discriminability decreases.

4.3. Fused binary template entropy

This section evaluates the entropy of the fused binary template given by the proposed fusion algorithm using



(a) WVU Multimodal (b) Chimeric A (c) Chimeric B

Figure 3: Comparison of average Renyi entropy on (a) WVU multi-modal, (b) Chimeric A, (c) Chimeric B databases.

quadratic Renyi entropy as in [11], which measures the content of biometric information as the complexity for successfully guessing a target template. Specifically, the quadratic Renyi entropy measures the effort for searching an identified sample of the target template, implying that they have zero hamming distance. Assuming that the average impostor hamming distance (impostor hamming distance per bit, aIHD) obeys binomial distribution with expectation p and standard deviation σ, the entropy of the template is estimated as

$$\begin{aligned} H &= -\log_2 \Pr(\text{IHD} = 0) \\ &= -\log_2 p^0 (1-p)^{N_*} = -N_* \log_2 (1-p) \end{aligned} \tag{8}$$

where $N_* = p(1-p)/\sigma^2$ is the estimated number of independent Bernoulli trials. Longer binary feature usually has higher entropy. To neglect the effect of bit length, we plotted the average Renyi entropy (entropy per bit) versus bit length for the three databases in Fig.3.

It can be observed that the templates given by XOR-fusion rule and the proposed fusion method rank first and second in terms of average entropy in all of three databases, respectively. The main reason for the fused template given by XOR-fusion rule have such high entropy is the uniformity of their fused bit higher than any of the corresponding input bits, which results in reducing of the dependency among fused bits.

It can be observed that the security curve of both the proposed method and bit selection method keep decreasing as the system length increases. For the proposed method, this is because we extracted the groups with high entropy first and then fused them together. For the other methods, the bits with high discriminability (implicitly high uniformity) will be selected out firstly. Therefore, the bit extracted later has lower entropy than the one extracted first, which causes security curves keep decreasing.

5. Conclusion

We have proposed a binary feature fusion algorithm for multi-biometric systems that can give a discriminative and high-entropy binary templates. The fused template of multiple traits using the proposed method can be used directly as the input of popular biometric cryptosystems, *e.g.*, fuzzy extractor and fuzzy commitment. The proposed binary feature level fusion algorithm consist of two stages, i.e., dependency reductive bit-grouping analysis, discriminative and uniform within-group fusion. The first stage aims to reduce the dependency among the fused bits in the output feature, and the second stage is to try to achieve that each fused bit with high uniformity, small intra and large inter-user variation. Experiments on three multi-modal database (WVU multi-modal and two Chimeric) show that the proposed binary feature fusion method can optimize fused template with high discriminability and entropy simultaneously. The future work of this paper is the analysis of trade-off between discriminability and security on the fused template when adopting biometric cryptosystems.

Acknowledgment

This project is partially supported by the Hong Kong RGC grant HKBU 211612.

References

[1] CASIA Iris Image Database , http://biometrics.idealtest.org/.

[2] VeriFinger SDK , http://www.neurotechnology.com/.

[3] K. W. Bowyer and P. J. Flynn. The ND-IRIS-0405 iris image dataset, 2009.

[4] J. Daugman. High confidence visual recognition of persons by a test of statistical independence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(11):1148–1161, 1993.

[5] K. Deb. An efficient constraint handling method for genetic algorithms. *Computer methods in applied mechanics and engineering*, 186(2):311–338, 2000.

[6] K. Deep, K. P. Singh, M. Kansal, and C. Mohan. A real coded genetic algorithm for solving integer and mixed integer optimization problems. *Applied Mathematics and Computation*, 212(2):505–518, 2009.

[7] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha. Anonymous and revocable fingerprint recognition. In *Computer Vision and Pattern Recognition, IEEE Conference on*, pages 1–7, 2007.

[8] Y. C. Feng, M.-H. Lim, and P. C. Yuen. Masquerade attack on transform-based binary-template protection based on perceptron learning. *Pattern Recognition*, 47(9):3019–3033, 2014.

[9] Y. C. Feng and P. C. Yuen. Binary discriminant analysis for generating binary face template. *Information Forensics and Security, IEEE Transactions on*, 7(2):613–624, 2012.

[10] Y. C. Feng, P. C. Yuen, and A. K. Jain. A hybrid approach for generating secure and discriminating face template. *Information Forensics and Security, IEEE Transactions on*, 5(1):103–117, 2010.

[11] S. Hidano, T. Ohki, and K. Takahashi. Evaluation of security for biometric guessing attacks in biometric cryptosystem using fuzzy commitment scheme. In *Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–6. IEEE, 2012.

[12] L. Hornak, A. Ross, S. G. Crihalmeanu, and S. A. Schuckers. A protocol for multibiometric data acquisition storage and dissemination. Technical report, West Virginia University, https://eidr. wvu. edu/esra/documentdata. eSRA, 2007.

[13] A. Juels and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

[14] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36, 1999.

[15] E. Kelkboom, X. Zhou, J. Breebaart, R. Veldhuis, and C. Busch. Multi-algorithm fusion with template protection. In *Biometrics: Theory, Applications, and Systems, IEEE 3rd International Conference on*, pages 1–8, 2009.

[16] J.-G. Ko, Y.-H. Gil, J.-H. Yoo, and K.-I. Chung. A novel and efficient feature extraction method for iris recognition. *ETRI journal*, 29(3):399–401, 2007.

[17] A. Kraskov and P. Grassberger. Mic: mutual information based hierarchical clustering. In *Information theory and statistical learning*, pages 101–123. Springer, 2009.

[18] M.-H. Lim and A. B. J. Teoh. A novel encoding scheme for effective biometric discretization: Linearly separable subcode. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 35(2):300–313, 2013.

[19] E. Maiorana, G. Hine, and P. Campisi. Hill-climbing attacks on multibiometrics recognition systems. *Information Forensics and Security, IEEE Transactions on*, 10(5):900–915, May 2015.

[20] A. Nagar, K. Nandakumar, and A. K. Jain. Multibiometric cryptosystems based on feature-level fusion. *Information Forensics and Security, IEEE Transactions on*, 7(1):255–268, 2012.

[21] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. Overview of the face recognition grand challenge. In *Computer vision and pattern recognition, IEEE Conference on*, volume 1, pages 947–954, 2005.

[22] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss. The feret evaluation methodology for face-recognition algorithms. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 22(10):1090–1104, 2000.

[23] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4):561–572, 2007.

[24] C. Rathgeb, Andreas Uhl, and P. Wild. Iris recognition: from segmentation to template security. *Adv. Inf. Secur.*, 59, 2012.

[25] C. Rathgeb and A. Uhl. Statistical attack against iris-biometric fuzzy commitment schemes. In *Computer Vision and Pattern Recognition Workshops, IEEE Conference on*, pages 23–30, 2011.

[26] R. N. Rodrigues, N. Kamat, and V. Govindaraju. Evaluation of biometric spoofing in a multimodal system. In *Biometrics: Theory Applications and Systems, Fourth IEEE International Conference on*, pages 1–5, 2010.

[27] A. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of multibiometrics*, volume 6. Springer Science & Business Media, 2006.

[28] Y. Sutcu, Q. Li, and N. Memon. Secure biometric templates from fingerprint-face features. In *Computer Vision and Pattern Recognition, IEEE Conference on*, pages 1–6, 2007.

[29] A. Uhl and P. Wild. Weighted adaptive hough and ellipsopolar transforms for real-time iris segmentation. In *Biometrics (ICB), 5th IAPR International Conference on*, pages 283–290. IEEE, 2012.

[30] A. Vij and A. Namboodiri. Learning minutiae neighborhoods: A new binary representation for matching fingerprints. In *Computer Vision and Pattern Recognition Workshops, IEEE Conference on*, pages 64–69, 2014.

[31] X. Zhou, A. Kuijper, and C. Busch. Retrieving secrets from iris fuzzy commitment. In *Biometrics (ICB), 5th IAPR International Conference on*, pages 238–244. IEEE, 2012.