Cancelable Multi-Biometrics: Mixing Iris-Codes based on Adaptive Bloom Filters

C. Rathgeb and C. Busch

da/sec Biometrics and Internet Security Research Group
Hochschule Darmstadt, Germany
{christian.rathgeb,christoph.busch}@h-da.de

***Abstract*—In this work adaptive Bloom filter-based transforms are applied in order to mix binary iris biometric templates at feature level, where iris-codes are obtained from both eyes of a single subject. The irreversible mixing transform, which generates alignment-free templates, obscures information present in different iris-codes. In addition, the transform is parameterized in order to achieve unlinkability, implementing cancelable multi-biometrics. Experiments which are carried out on the IITD Iris Database version 1.0 confirm the soundness of the proposed approach, (1) maintaining biometric performance at equal error rates below 0.5% for different feature extraction methods and fusion scenarios and (2) achieving a compression of mixed templates down to 10% of original size.**

I. Introduction

Research confirms an extraordinarily high level of statistical reliability for iris recognition systems [1], [2]. Daugman's algorithm [3], which forms the basis of the vast majority of today's iris recognition systems comprises four stages: (1) image acquisition, in which an image of a subject's eye is captured; (2) pre-processing, which involves the detection of the iris and un-rolling of the iris to a normalized texture (3) feature extraction, in which binary feature vectors, i.e. iris-codes, are generated; and (4) feature comparison, where iris-codes are aligned applying circular bit shifts, and dis-similarity scores are estimated based on the fractional Hamming distance. Biometric recognition represents the strongest form of personal identification, however, physiological biometric characteristics are not secret and cannot be revoked or reissued causing several vulnerabilities that violate individuals' privacy, e.g. tracking subjects without consent. In addition, it has been demonstrated that spoofed iris images can be re-constructed from stored iris-codes [4].

Biometric template protection schemes [5] which are categorized as biometric cryptosystems [6] and cancelable biometrics [7] offer solutions to privacy preserving biometric authentication. Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transforms that provide a comparison of biometric templates in the transformed domain, i.e. biometric templates are permanently protected. In accordance with the ISO/IEC IS 24745 [8] on biometric information protection, technologies of cancelable biometrics meet the two major requirements of irreversibility and unlinkability. On the one hand knowledge of the protected template can not be used to determine any information about the original biometric sample, while it should be easy to generate the protected template (irreversibility). On the other hand different versions of protected biometric templates can be generated based on the same biometric data, while protected templates should not allow cross-matching (unlinkability). The majority of existing approaches to cancelable biometrics report a significant decrease in biometric performance which is caused by two issues: (1) local neighborhoods of feature elements are obscured and (2) transformed enrollment templates are not "seen", i.e. alignment can not be performed properly at the time of comparison [5]. This implies, that low intra-class variability at high inter-class variability is considered a fundamental premise for biometric template protection schemes which can only be achieved in case biometric traits are acquired under favorable environmental conditions. In order to overcome this restriction, multi-biometric template protection schemes [9], [10] have been introduced, since a combination of different biometric characteristics generally leads to higher accuracy [11]. Within a conventional biometric system a fusion of different biometric information can be performed at various stages yielding feature level, score level, and decision level fusion [12], as defined in the ISO/IEC TR 24722 [13] on multimodal and other multi-biometric fusion. While preliminary scores are not available within the vast majority of biometric cryptosystems, cancelable multi-biometric systems based on score level fusion can be constructed analogue to conventional biometric systems. For both technologies biometric fusion based on decision level can easily be implemented combining final decisions. However, score and decision level fusion require a separate storage of protected templates, i.e., with respect to template protection, feature level has been identified as the only suitable level of fusion [14]. Performing multi-biometric template protection at feature level represents a great challenge since it requires a generic framework in order to establish a common representation of biometric features [9]. In addition, feature alignment turns out to be a critical issue since protected templates, which comprise information of more than one biometric instance, are expected to require a complex alignment process. So far, hardly any alignment-free (multi-biometric) template protection schemes have been proposed.

A. Contribution of Work

The proposed work builds upon the approach we proposed in [15] and the concept of mixing multiple instances of a

single biometric characteristic, which has been introduced in [16] for fingerprints. In [15] the basic concept of Bloom filter-based cancelable iris biometrics has been introduced, however, within the presented work emphasis is put on cancelable multi-biometrics which represents a more challenging task [10], i.e. we significantly exented existing work according to several aspects, tackling the aforementioned issues. We demonstrate the feasibility of multi-biometric Bloom filter-based template protection by introducing the recently proposed concept of mixing biometric features, which originate from different biometric characteristics, into a single protected template, to iris biometrics. For this purpose we asses multi-instance single-algorithm and multi-instance multi-algorithm fusion scenarios in order to obtain alignment-free mixed templates. Binary iris-biometric feature vectors extracted from both eyes of a subject are mixed to a single protected template at feature level, which highly increases security while at the same time biometric performance is maintained. Implementing cancelable biometrics the proposed technique exhibits the properties of irreversibility and unlinkability [8].

B. Organization of Article

The remainder of this article is organized as follows: related work with respect cancelable iris biometrics and multi-biometric template protection is briefly summarized in Sect II. In Sect. III the proposed mixing approach is described in detail. Experimental results are presented in Sect. IV. Finally, conclusions are drawn in Sect. V.

II. Related Work

Biometric template protection schemes [5] are commonly classified as biometric cryptosystems and cancelable biometrics. Since the presented approach represents an instance of cancelable multi-biometrics, in this section we will merely focus on these technologies. Ratha *et al.* [7] were the first to introduced the concept of cancelable biometrics. In their work the authors apply image-based block permutations and surface-folding in order to obtain revocable biometric templates. In further work [17] the authors propose different techniques to generate cancelable iris biometrics based on non-invertible transforms and biometric salting, which are applied in image and feature domain. In order to preserve a computational efficient alignment of resulting iris-codes based on circular bit-shifting, iris textures and iris-codes are obscured in a row-wise manner, which means adjacency of pixels and bits is maintained along x-axis in image and feature domain, respectively. In [18] block re-mapping and image wraping have been applied to normalized iris textures. For both types of transforms a proper alignment of resulting iris-codes is infeasible causing a significant decrease of biometric performance. In [19] several enrollment templates are processed to obtain a vector of consistent bits. Revocability is provided by encoding the iris-code according to a subject-specific random seed. In case subject-specific transforms are applied in order to achieve cancelable biometrics, these transforms have to be considered compromised during inter-class comparisons [20]. Subject-specific secrets, be it transform parameters, random numbers, or any kind of passwords are easily compromised, i.e. performance evaluations have to be performed under the "stolen-secret scenario", where each impostor is in possession of valid secrets. In [21] cancelable iris templates are achieved by applying sector random projection to iris images. Again, recognition performance is only maintained if subject-specific random matrices are applied. In [22] non-invertible iris-codes are computed by thresholding inner products of the feature vector with randomly generated vectors. The random vectors are created by using a per-subject secret and a pseudo random number generator. Several normalized iris textures are multiplied with a random kernel in [23] to create concealed feature vectors. In [15] we proposed cancelable iris biometrics based on adaptive Bloom filters. The application of Bloom filter-based transforms is shown to be irreversible and achieves an alignment-free representation of features, at the same time biometric performance is maintained for different feature extraction algorithms.

Focusing on multi-biometric template protection [10] the vast majority of approaches implement biometric cryptosystems. A multi-biometric cryptosystem based on the fuzzy commitment scheme [24] was proposed in [25], in which binary fingerprint and face features are combined. In [14] two different feature extraction algorithms are applied to 3D face data yielding a single sensor scenario. The authors provide results for feature level, score level and decision level fusion. In order to obtain a comparison score the number of errors corrected by the error correction code are estimated. Best results are obtained for the multi-algorithm fusion at feature level. In [26] a fuzzy vault scheme [27] based on fingerprint and iris is presented. The authors demonstrate that a combination of biometric modalities leads to increased accuracy of the template protection scheme. In [28] two different feature extraction methods are combined to achieve cancelable face biometrics. PCA (principal component analysis) and ICA (independent component analysis) coefficients are extracted and both feature vectors are randomly scrambled and added in order to create a transformed template. A sensible rearrangement of bits in iris-codes in order to provide a uniform distribution of error probabilities within a fuzzy commitment scheme is introduced in [29]. The rearrangement allows a more efficient execution of error correction codes combining the most reliable bits generated by different feature extraction algorithms. In rather recent work [9] results on multi-biometric fuzzy commitment schemes and fuzzy vault schemes based on fingerprint, face and iris are reported. In order to obtain a common feature representation for each type of template protection scheme the authors propose different embedding algorithms, e.g. for mapping a binary string to a point set. In [30] a multi-biometric template protection system employing decision level fusion of multiple protected fingerprint templates is proposed.

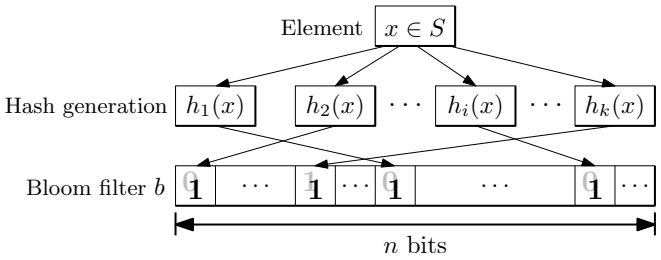


Fig. 1. Insertion of an element $x \in S$ into a generalized Bloom filter b of length n where k different hash functions are applied.

III. Bloom Filter-based Mixing of Binary Biometric Templates

A Bloom filter [31] is a space-efficient probabilistic data structure representing a set in order to support membership queries. In addition to an efficient storage and rapid processing of queries, Bloom filters convince by their wide field of applications, e.g. database applications [32] or network applications [33]. Basically, a Bloom filter b is a bit array of length n, where initially all bits are set to 0. In order to represent a set S a Bloom filter traditionally utilizes k independent hash functions $h_1, h_2, ..., h_k$ with range $[0, n-1]$. For each element $x \in S$, bits at positions $h_i(x)$ of Bloom filter b are set to 1, for $1 \leq i \leq k$, as shown in Fig. 1. A bit can be set to 1 multiple times, but only the first change has an effect. In order to test whether an element y is in S, it has to be checked whether all position of $h_i(y)$ in b are set to 1. If this is the case, it is assumed that y is in S with a certain probability of false positive. If not, clearly y is not a member of S.

We adapt the original concept of a Bloom filter in two ways:

1) One trivial transform h is applied to each element $x \in S$ instead of multiple hash functions. We exploit the transform h to incorporate an application and potentially also subject-specific auxiliary data AD , which are XORed with the element. In the context of biometric template protection hash functions would not be resistant to brute force attacks since feature elements are expected to be small, consisting only of a few bits;
2) Given a Bloom filter b of length n we restrict to inserting l elements, where $l \leq n$. In case of uniformly distributed data, for inserting a total of l elements $1-(1-1/n)^l$ bits are expected to be set to 1. In order to meet this requirement parts of feature elements are mapped to different Bloom filters, i.e. a set of Bloom filters represents the protected template. Since we focus on a multi-biometric scenario, l represents the sum of elements generated by at least one biometric feature extractor, which is applied to multiple biometric characteristics (e.g. two eye instances). In the proposed approach, iris-biometric feature vectors of two different eyes are extracted, i.e. $l = l_1 + l_2$. In case the same feature extractor is applied to both eyes of a subject it is expected that $l_1 = l_2$. The approach can be generalized, incorporating M different feature vectors where $l = \sum_{i=1}^{M} l_i$. In order to avoid an inbalanced distribution of features, binary feature vectors of similar size are recommended.

The proposed mixing approach comprises three major steps which are depicted as part of Fig. 2: (1) the extraction of feature vectors from both eyes of a subject; (2) the proposed Bloom filter-based mixing transform which is utilized to merge two given feature vectors into a single protected template; (3) the storage and comparison of cancelable mixed templates. In the following subsections the Bloom filter-based mixing transform, according multi-biometric template protection, comparison of protected templates, and biometric data compression are described in detail.

A. Bloom Filter-based Mixing Transform

In the proposed system Bloom filters are utilized in order to achieve an alignment-free representation of iris-codes. Generic iris recognition systems [2] extract binary feature vectors based on a row-wise analysis of normalized iris textures, i.e. iris-codes typically represent two-dimensional binary feature vectors of width W and height H (see Fig. 5 (e)-(f)). In the proposed scheme iris-codes are divided into K blocks of equal size, where each column consists of $w \leq H$ bits. In case $w < H$, columns consist of the w upper most bits, i.e. features originating from outer iris bands, which are expected to contain less discriminative information, are ignored. Subsequently, the entire sequence of columns of each block is successively transformed to corresponding locations within Bloom filters, that is, a total number of K separate Bloom filters of length $n = 2^w$ form the template of size $K \cdot 2^w$. The transform h is implemented by mapping columns within 2D iris- codes to the indexes of their decimal value, which is shown for two different codewords (=columns stemming from left and right eye) as part of Fig. 2, for each column $x \in \{0,1\}^w$, the mapping is defined as,

$$b[h(x) \oplus AD] = 1, \text{ with } h(x) = \sum_{j=0}^{w-1} x_j \cdot 2^j, \qquad (1)$$

where AD represents an application-specific secret which is incorporated in order to provide unlinkability. As shown in Fig. 2 codewords of different iris-codes which originate from equal parts in the iris texture are mapped to identical Bloom filters, implementing the concept of mixing biometric characteristics at feature level [16].

One major advantage of the proposed transform is that it is alignment-free to a certain degree, i.e. generated templates (=sets of Bloom filters) do not need to be aligned at the time of comparison. Equal columns within certain blocks (=codewords) are mapped to identical indexes within Bloom filters, i.e. self-propagating errors caused by an inappropriate alignment of iris-codes are eliminated (radial neighborhoods persist). The rotation-compensating property of the proposed system comes at the cost of location information of iris-code columns. At block boundaries miss-alignment of iris-codes will distribute a certain amount of potentially matching codewords among different blocks, which would be mapped

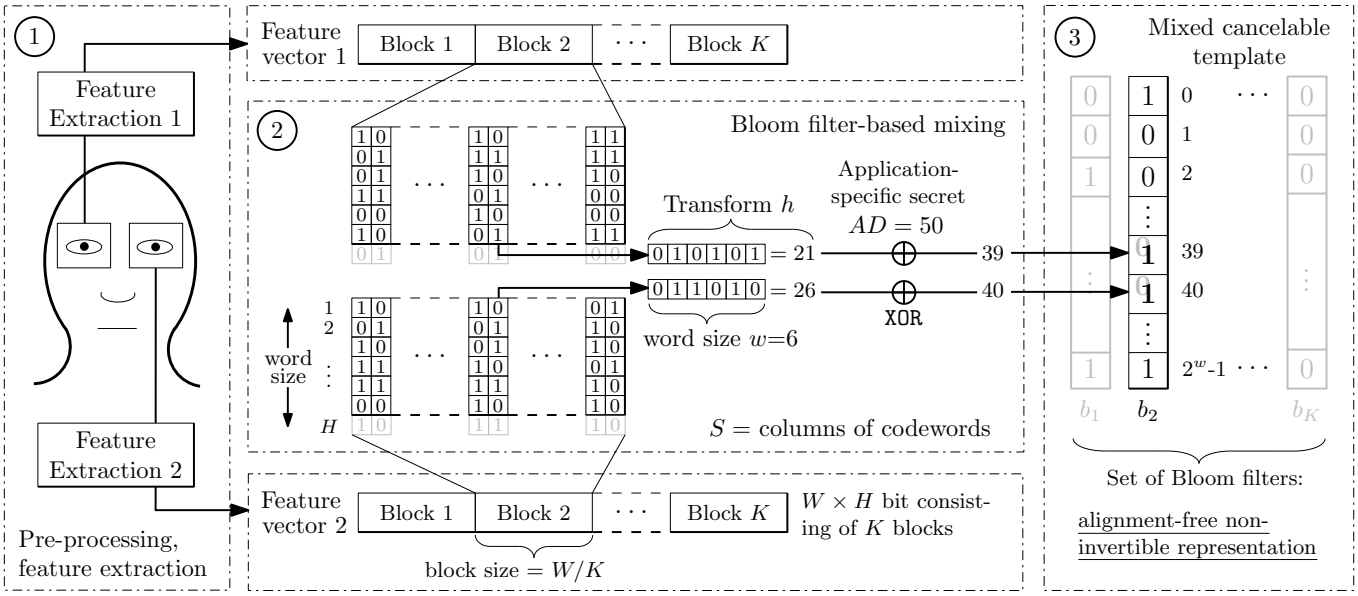


Fig. 2. The Bloom filter-based transform which mixes codewords of different biometric feature vectors in according Bloom filters. The highlighted codewords of different iris-codes are transformed to 21 and 26, XORed with AD and mixed in Bloom filter b_2, changing element at index 39 and also index 40 to 1.

to neighbored Bloom filters. In experiments where ± 8 bit shifts are required to align iris-codes properly, miss-alignment did not affect biometric performance. In case larger rotation angles need to be anticipated, multiple columns of right and left neighbor-block can be mapped to the Bloom filter under construction in order to overcome this drawback.

The proposed Bloom filter-based mixing transform is designed to fulfill the two major requirements of biometric information protection [8], irreversibility and unlinkability. Protected biometric templates, for which no formal model exists, are considered secure in case these requirements are achieved.

1) Irreversibility: original positions of codewords within iris-codes are concealed, i.e. given a Bloom filter b it is not clear from which column a distinct 1-bit in the protected template originated. By mixing codewords of different biometric feature vectors, it is not even clear which feature vector a distinct 1-bit in the protected template originated from. In addition, high correlation between codewords, especially neighboring ones, is expected. Consequently, a significant amount of codewords are mapped to identical positions in Bloom filters even for small values of l. Assume $|b|$ bits are set to 1 within a Bloom filter after inserting l codewords, i.e. $|b|$ different codewords occur in the concatenation of l_1 and $_2$ columns of bits. Hence, the probability of re-mapping a bit to a certain position is $1 - |b|/l$. For a potential attacker the reconstruction of the original iris-code part involves an arranging of $|b|$ codewords to l positions. For $|b| \leq l$ the theoretical amount of possible sequences is recursively defined by $f(|b|, l)$ where each of the $|b|$ codewords have to appear at least once within l columns,

$$f(|b|,l) = \begin{cases} 1, & \text{if } |b| = 1, \\ |b|^l - \sum_{i=1}^{|b|-1} \binom{|b|}{i} \cdot f(i,l) & \text{otherwise.} \end{cases} \quad (2)$$

In other words, all sequences where less than $|b|$ codewords appear are subtracted from the number of all possible sequences, $|b|^l$. With respect to the nature of a given biometric input Fig. 3 theoretically indicates the security based on Eq. (2), which is formally proven in Appendix A, for diverse system configurations. Note the rapid increase of possible sequences even for small values of $|b|$ (logarithmic scales of both axis). Peaks are located around $3l/4$, in case of $l = |b|$ we get $f(l,l) = l!$ and $f(1,l) = 1$. For instance, for $l = 4$ and $|b| = 2$ we get $f(2,4) = 2^4 - \binom{2}{1} \cdot f(1,4) = 16 - 2 \cdot 1 = 14$ possible sequences, for $l = 4$ and $|b| = 3$ we get $f(3,4) = 3^4 - \binom{3}{1} \cdot f(1,4) - \binom{3}{2} \cdot f(2,4) = 81 - 3 \cdot 1 - 3 \cdot 14 = 36$ possible sequences and for $l = 4$ and $|b| = 4$ we get $f(4,4) = 4! = 24$ possible sequences and so forth.

2) Unlinkability: unlinkability is provided by incorporating an application and subject specific bit vector, denoted by $AD \in \{0,1\}^w$, which is XORed with a processed codeword x prior to mapping it to a Bloom filter b, $b[h(x) \oplus AD] = 1$. Alternatively, different types of hash functions could be applied in different applications, or a single hash function could be applied based on an application specific seed. In experiments it will be demonstrated that for randomly generated bit vectors it is infeasible for potential attackers, that have access to the reference database of two or more protected systems, to cross-match pairs of protected templates extracted from a single subject.

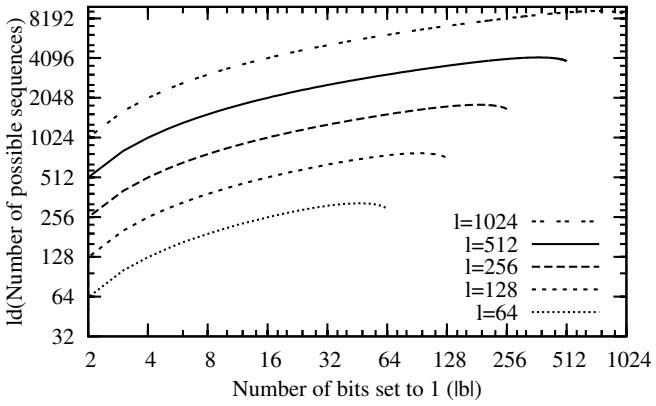


Fig. 3. Amount of possible sequences (per block) for different numbers of transformed codewords and proportions of re-mapped codewords.

B. Multi-biometric Template Protection

In accordance with ISO/IEC TR 24722 [13] multi-biometric fusion is yielded where we consider two scenarios:

- *Multi-instance single-algorithm mixing:* a single feature extraction algorithm is applied to different instances (i.e., eyes). Since feature extraction is applied to normalized iris textures of fixed size in this scenario the number of codewords per block (of both iris-codes), which are mixed in a distinct Bloom filter, is l, where $l_1 = l_2 = l/2$.
- *Multi-instance multi-algorithm mixing:* different feature extraction algorithms are applied to different instances, which is expected to cause fewer collision within Bloom filters in case constitutions of feature vectors significantly differ. Again, feature extraction algorithms are applied to normalized iris textures of fixed size, while the size of resulting iris-codes and, thus, the number of codewords per block, may differ, $l_1 \neq l_2$. Still codeword which originate from the same area within the iris texture are mixed in distinct Bloom filters.

In case iris-codes exhibit a significantly different amount of bits weights are automatically assigned to according feature vectors since more codewords of a single algorithm are mapped to all Bloom filters. In order to avoid an automatic assignment of weights the amount of mixed codewords can be balanced by reducing the amount of transformed codewords of the iris-code of greater size, e.g. by incorporating only most reliable columns. In experiments different feature extraction algorithms are utilized, which are applied after performing the same segmentation process to both eyes and extract the same amount of bits, i.e. $l_1 = l_2 = l/2$ holds for conducted evaluations. The choice of different feature extraction algorithms which generate iris-codes of same size maximizes the security of the proposed scheme. Since, in the proposed multi-algorithm fusion scenario, information of two iris-codes is obscure within a single protected template the reconstruction of one of these iris-codes is lower-bounded by the number of codewords within blocks of the shorter iris-code, which are mapped to according Bloom filters.

C. Comparison of Protected Templates

Typically, comparisons between binary biometric feature vectors are implemented by the simple XOR operator applied to a pair of binary biometric feature vectors. The sum of all detected disagreements between any corresponding pairs of bits divided by the amount of compared bits yields the fractional Hamming distance (HD) as a measure of dissimilarity between pairs of binary biometric feature vectors [3]. Let $|b|$ denote the amount of bits within a Bloom filter b, which are set to 1. Then the dissimilarity DS between two Bloom filters b_i and b_j is defined as,

$$DS(b_i, b_j) = \frac{HD(b_i, b_j)}{|b_i| + |b_j|} \qquad |b_i|, |b_j| \neq 0. \tag{3}$$

If pairs of Bloom filters would be compared by merely estimating Hamming distances between these, mis-matching bits between Bloom filters in which fewer bits are set to 1 would be weighted less and vice versa. Obviously, DS is computed as efficient as HD while DS does not have to be computed at numerous shifting positions. In order to incorporate masking bits obtained at the time of pre-processing, columns of iris-codes which are mostly affected by occlusions must not be mapped to Bloom filters, i.e. a separate storage of bit masks is not required.

D. Biometric Data Compression

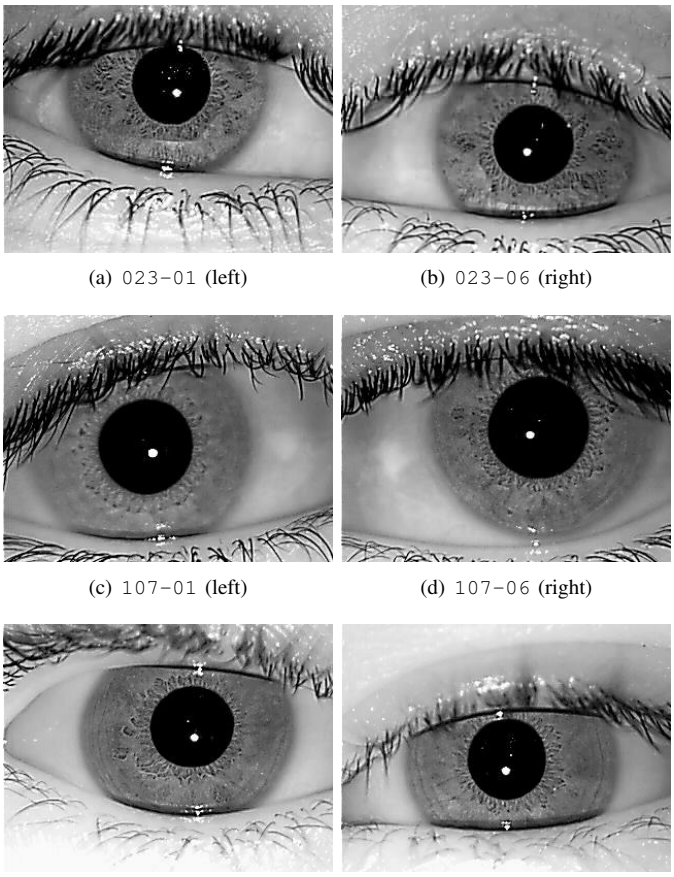
The original template sizes are $W_1 \times H_1$ and $W_2 \times H_2$ bits. In the proposed scheme the template is divided into $W_1/l_1 = W_2/l_2 = K$ blocks of length l_1 and l_2 resulting in a template size of $2^w \cdot K = 2^w \cdot W_1/l_1 = 2^w \cdot W_2/l_2$ where $w \leq H_1$ and $w \leq H_2$. A compression is achieved if,

$$K \cdot 2^w < W_1 \cdot H_1 + W_2 \cdot H_2 \tag{4}$$

applies. In case $l_1 = l_2 = l/2$ and we set $l = 2^q$ we get,

$$K \cdot 2^w < 2W \cdot H \Leftrightarrow 2^{w-q+1}/H < 1, \tag{5}$$

which is most likely the case as we will demonstrate in experiments. For instance, for two given iris-codes of size 2048 with $W_1 = W_2 = 256$ and $H_1 = H_2 = 8$, and the setting $l = 128$ and $w = 8$ we get $256/64 \cdot 2^8 = 1024 < 2048$, i.e. a compression down to 50% of the original size is achieved ($2^{8-7+1}/8 = 0.5$). Sizes of transformed templates are operated by setting parameters l and w. Both, increasing l and decreasing w reduces the overall size of the resulting template, see Eq. 5. Again the major advantage of the proposed transform is that compared to existing approaches to biometric template compression, e.g. [34], a comparison of compressed templates does not require an optimal alignment within the presented scheme. It is important to note that algorithms may extract binary templates where distinct parts comprise features which should not be arranged in single columns, e.g. in [35] different parts of iris-codes represent real and complex values or in [36] different parts of iris-codes represent minima and maxima extracted from different wavelet subbands.



(a) 023-01 (left) (b) 023-06 (right)

(c) 107-01 (left) (d) 107-06 (right)

(e) 218-01 (left) (f) 218-06 (right)

Fig. 4. Sample pairs of left and right 320 × 240 pixel NIR eye images of the IITD Iris Database version 1.0, numbers in captions refer to identifiers.

IV. Experiments

Performance is estimated in terms of false non-match rate (FNMR) at a targeted false match rate (FMR) and equal error rate (EER). The FNMR of a biometric system defines the proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample. By analogy, the FMR defines the proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template. As score distributions overlap EERs are obtained, i.e the system error rate where FNMR = FMR.

A. Experimental Setup

Experiments are carried out using the IITD Iris Database version 1.0[1] which comprises 2 240 320×240 NIR images from 224 different subjects where for each subject the first five iris images were acquired from the left eye while the rest five images were acquired from the right eye. For each subject five pairs of eye images are formed for genuine comparisons, and one pair of eye images is applied within imposter comparisons leading to a total number of 5· 4/2 · 224 =2 240 genuine comparisons and 224·223/2=24 976 imposter comparisons. Sample images of left and right eyes of three different subjects are shown in Fig. 4. It is important to note that images of left and right eyes are not acquired using the JIRIS camera where only single eyes are captured, i.e. optimal alignments between pairs of left and right eyes must not be expected to be achieved at identical shifting positions. At pre-processing the iris of a given sample image is detected, un-wrapped to an enhanced rectangular texture of 512×64 pixel, shown in Fig. 5 (a)-(d) applying the weighted adaptive Hough algorithm proposed in [37]. The two-stage segmentation algorithm employs a weighted adaptive Hough transform iteratively refining a region of interest to find an initial center point, which is utilized to polar transform the image and extract polar and limbic boundary curves one after another from an (ellipso-) polar representation.

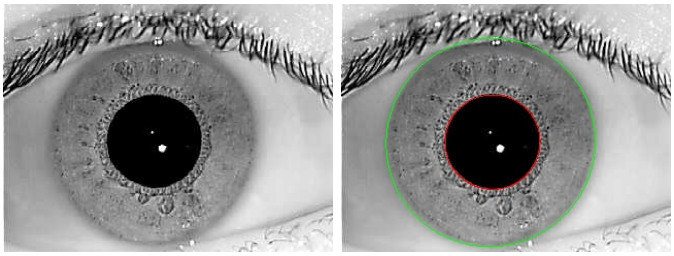
In the feature extraction stage custom implementations[2] of two different iris recognition algorithms are employed where normalized iris textures are divided into stripes to obtain 10 one-dimensional signals, each one averaged from the pixels of 5 adjacent rows (the upper 512×50 rows are analyzed). The first feature extraction method follows an implementation by Masek [35] in which filters obtained from a LogGabor function are applied. Within this approach the texture is divided into 10 stripes to obtain 5 one-dimensional signals, each one averaged from the pixels of 5 adjacent rows, hence, the upper 512×50 pixel of preprocessed iris textures are analyzed. A row-wise convolution with a complex LogGabor filter is performed on the texture pixels. The phase angle of the resulting complex value for each pixel is discretized into 2 bits. The 2 bits of phase information are used to generate a binary code, which therefore is $512 \times 20 = 10\,240$ bit. This algorithm is somewhat similar to Daugman's use of LogGabor filters, but it works only on rows as opposed to the 2-dimensional filters used by Daugman. The second feature extraction algorithm was proposed by Ma *et al.* [36]. Within this algorithm a dyadic wavelet transform is performed on 10 signals obtained from the according texture stripes, and two fixed subbands are selected from each transform resulting in a total number of 20 subbands. In each subband all local minima and maxima above an adequate threshold are located, and a bit-code alternating between 0 and 1 at each extreme point is extracted. Using 512 bits per signal, the final code is again $512 \times 20 = 10\,240$ bit. Sample iris-codes generate by both feature extraction methods are shown in Fig. 5 (e)-(f). For the choice of feature extraction algorithms $W_1 = W_2$ and $H_1 = H_2$, which implies that $l_1 = l_2 = l/2$ applies.

B. Performance Evaluation

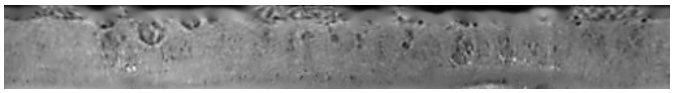
The performance rates of the original systems are summarized in Table I. Without a doubt a combination of both eyes, where we applied a simple sum-rule fusion at score-level, significantly improves the biometric performance of the

[1]IITD Iris Database version 1.0, http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm

[2]USIT – University of Salzburg Iris Toolkit v1.0, http://www.wavelab.at/sources/



(a) Acquisition (b) Detection



(c) Iris texture

(d) Enhanced iris texture

(e) Iris-code 1-D Log-Gabor filter

(f) Iris-code Ma *et al.*

Fig. 5. Iris detection, pre-processing, and applied feature extraction for image `001-02` of the IITD Iris Database version 1.0.

TABLE I
ORIGINAL SYSTEMS: NATIVE PERFORMANCE RATES (IN %) FOR SINGLE- AND MULTI-INSTANCE SCENARIOS FOR BOTH FEATURE EXTRACTORS (FNMRS ARE OBTAINED AT FMR=0.01%).

Scenario	Left/ right eye ø		Both eyes	
	1-FNMR	EER	1-FNMR	EER
Single-algorithm 1D LogGabor	95.448	1.746	99.239	0.451
Single-algorithm Ma *et al.*	94.587	1.875	98.703	0.495
Multi-algorithm	95.053	1.793	99.016	0.477

system leading to EERs of ≈0.5%. While the 1D LogGabor feature extraction slightly outperforms the algorithm of Ma *et al.* a fusion of both algorithms does not improve the overall biometric performance.

A common way to estimate the average entropy ($\simeq$ amount of mutually independent bits) of biometric feature vectors is to measure the provided "degrees-of-freedom" which are defined by $d = p(1-p)/\sigma^2$, where p is the mean *HD* and σ^2 the corresponding variance between comparisons of different pairs of binary feature vectors. In case all bits of each binary feature vector of length z would be mutually independent, comparisons of pairs of different feature vectors would yield a binomial distribution, $\mathcal{B}(z,k) = \binom{z}{k} p^k (1-p)^{z-k} = \binom{z}{k} 0.5^z$ and the expectation of the Hamming distance would be $1/z \cdot \mathbb{E}(X \oplus Y) = zp \cdot 1/z = p = 0.5$, where X and Y are two independent random variables in $\{0,1\}$. In reality p decreases to $0.5 - \epsilon$ while Hamming distances remain binomially distributed with a reduction in z in particular, $\mathcal{B}(d, 0.5)$ [38]. The 1D Log-Gabor feature extractor achieves a total of 592 degrees of freedom for a mean of 0.493 and an according standard deviation of 0.021. The algorithm of Ma *et al.* yields 1291 degrees of freedom for a mean of 0.498 and a standard deviation of 0.013. From the estimated degrees-of-freedom an average iris-code extracted by the algorithm of Ma *et al.* exhibits an average length of $\simeq$8 (10240/1291) bit. By analogy, for the 1D LogGabor feature extractor according sequences exhibit an average length of $\simeq$17 (10240/592) bit (cf. Fig. 5(e)-(f)).

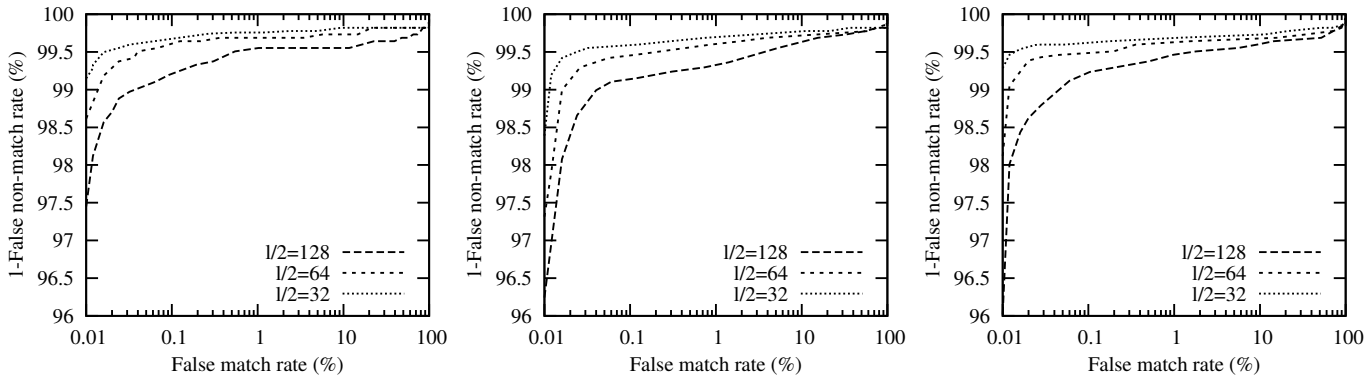
TABLE II
1-FNMRS (IN %) AT FMR=0.01% FOR DIFFERENT CONFIGURATIONS OF THE BLOOM FILTER-BASED MIXING TRANSFORM.

Fusion Scenario: Multi-instance-	Word size w (bits)	Block size $l/2$ (bits) 2^5	2^6	2^7	2^8	2^9
Single-algorithm 1D Log Gabor	10	98.97	98.47	97.45	95.66	81.48
	9	99.28	98.43	97.31	88.64	–
	8	99.28	98.34	93.69	–	–
Single-algorithm Ma *et al.*	10	98.38	97.31	96.24	92.62	62.34
	9	98.74	96.51	95.21	74.46	–
	8	98.74	95.84	82.06	–	–
Multi-algorithm	10	99.28	98.12	96.01	95.25	73.47
	9	98.97	97.89	94.05	78.44	–
	8	98.83	97.45	88.72	–	–

TABLE III
EERS (IN %) FOR DIFFERENT CONFIGURATIONS OF THE BLOOM FILTER-BASED MIXING TRANSFORM.

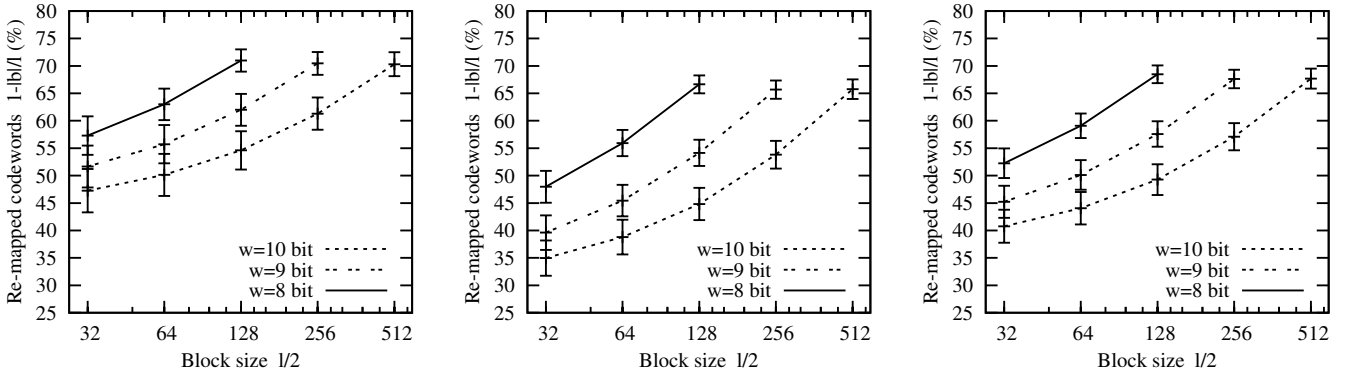
Fusion Scenario: Multi-instance-	Word size w (bits)	Block size $l/2$ (bits) 2^5	2^6	2^7	2^8	2^9
Single-algorithm 1D Log Gabor	10	0.430	0.455	0.495	0.969	4.744
	9	0.495	0.499	0.733	3.257	–
	8	0.493	0.560	2.514	–	–
Single-algorithm Ma *et al.*	10	0.477	0.497	0.499	1.478	7.930
	9	0.483	0.499	1.332	6.447	–
	8	0.495	0.731	4.130	–	–
Multi-algorithm	10	0.428	0.453	0.521	1.663	6.678
	9	0.430	0.453	0.975	5.499	–
	8	0.453	0.743	3.870	–	–

Focusing on the Bloom filter-based mixing approach we merely focus on multi-instance fusion scenarios. For the proposed system extracted iris-codes are divided in an upper 512×10 bit half and a lower 512×10 bit half as these represent real and complex values or minima and maxima extracted from different wavelet subbands, respectively. Table II and Table III summarize obtained 1-FNMRs and EERs for different word sizes w and block sizes $l/2$ for all fusion scenarios. Clearly, rotations of ± 8 bits are compensated. Throughout experiments best result were achieved for the maximum word size of 10 bits, i.e. $K = 10240/(32 \cdot 10) = 32$ blocks of $l = 64$ codewords which are mapped to 32 Bloom filters of size $n =$



(a) 1D LogGabor,$w = 10$ (b) Ma *et al.*, $w = 10$ (c) Fusion, $w = 10$

Fig. 6. ROC curves in the multi-instance fusion scenario for (a) 1D LogGabor feature extractor (b) algorithm of Ma *et al.*, and (c) a fusion of both algorithms.



(a) 1D LogGabor (b) Ma *et al.* (c) Fusion

Fig. 7. Proportion of re-mapped codewords, 1-$|b|/l$, for different block sizes $l/2$ and word sizes w and different multi-instance fusion scenarios.

$2^w = 2^{10}$. The receiver operation characteristic (ROC) curves for $w = 10$ are depicted in Fig. 6. Biometric performance is maintained (or improved) for small block sizes, in contrast to the original systems the combination of different algorithms improves biometric performance, e.g. for the setting $w = 10$ and $l/2 = 2^5$. Biometric performance is also maintained for a single-instance scenarios as we have shown in [15] based on a different dataset. Obviously, the applied DS metric represents an improved biometric comparator. For greater block sizes (e.g. $l/2 = 2^8$) biometric performance decreases. While an increase of block sizes provides a higher degree of rotation-invariance, it increases the chance that identical codewords occur within blocks, i.e. local information is lost leading to a greater overlap of intra- and inter-class score distributions.

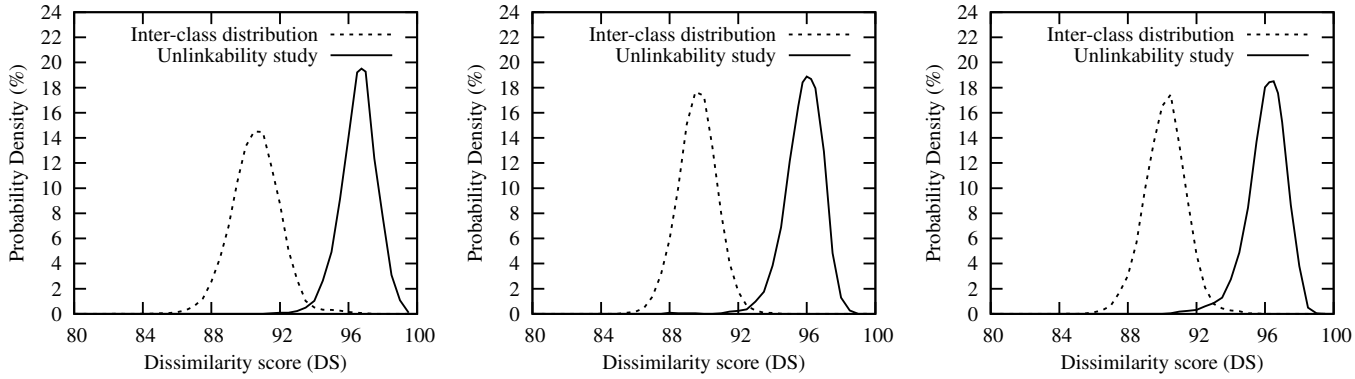
C. Privacy Threats and Adversary Model

Since biometric data is considered as personally identifiable information, privacy threats, for which the predefined properties of irreversibility and unlinkability represent appropriate countermeasures, comprise: (1) retrieval or analysis of properties of the data subject that are not required or intended for biometric identification and verification; (2) the linkage of biometric references to subjects across different applications in the same database or across different databases [8]. Focusing on the proposed system, the former requires a reconstruction of the original biometric feature vector.

In accordance with [39] and [8] we assume that a potential impostor has full knowledge of the algorithm (Kerckhoffs' principle) and has access to the database in which protected templates are stored, which corresponds to a union of advanced model and collision model. That is, we investigate whether it is possible for an impostor to re-construct the original biometric templates from the mixed protected template and to link protected templates which have been obscured applying different ADs.

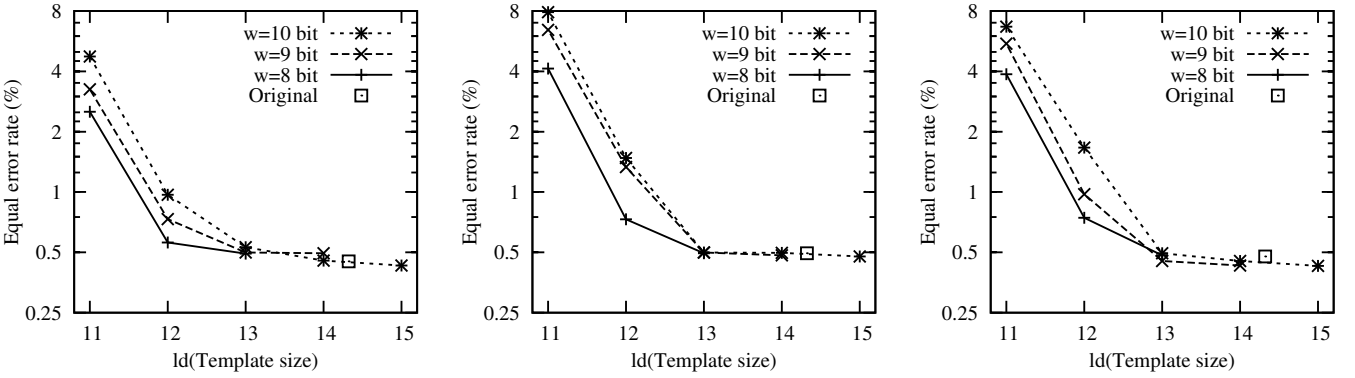
D. Multi-biometric Template Protection

The security of the mixing approach relies on the non-invertible mapping of codewords to a Bloom filter. W.l.o.g. this transform obscures the original position of the codeword, the number a codeword occurs, as well as from which iris-code a 1-bit in the Bloom filter originates from. For different configurations certain amounts of codewords are mapped to an identical position within according Bloom filters. Fig. 7 depicts the average percentage of re-mapped codewords and according standard deviations for all fusion scenarios



(a) 1D LogGabor (b) Ma *et al.* (c) Fusion

Fig. 8. Score distributions for inter-class comparisons and according unlinkability test for different multi-instance fusion scenarios.



(a) 1D LogGabor (b) Ma *et al.* (c) Fusion

Fig. 9. EERs according to resulting sizes of protected templates compared to the original systems for different multi-instance fusion scenarios.

and applied configurations, according to Fig. 3 remapping $1 - |b|/l \simeq 1 - 3/4 = 25\%$ would be optimal in terms of security. As expected, more codewords are re-mapped for larger block sizes, i.e. for all configurations of w, the amount of re-mapped codewords increases with the block size l. In addition, the amount of re-mapped codewords increases with smaller word sizes w, i.e. more information is lost compared to larger values of w. As a result, in general, biometric performance decreases with the word size w (see Table II and Table III).

For best performing configurations (w.r.t. accuracy), mapping $l = 64$ codewords of length $w = 10$ to a $n = 2^{10}$ bit Bloom filters, for the 1D LogGabor feature extraction $\sim$ 48% of codewords are re-mapped, $1 - |b|/l \simeq 0.48$ (see Fig. 7(a)). By analogy, for the algorithm of Ma *et al.* on average $\sim$35% of codewords are re-mapped (see Fig. 7(b)), while in the multi-instance multi-algorithm scenario on average $\sim$41% of codewords are re-mapped (see Fig. 7(c)). Focusing on the 1D LogGabor feature extractor, according to the previously estimated amount of possible sequences (see Fig. 3, $l = 64$) a potential attacker would have to try $\sim 2^{314}$ different sequences, $|b| = 64 \cdot (1 - 0.48) = 33.28$, for each pair of blocks. For the algorithm of Ma *et al.* the average amount of re-mapped codewords is even lower resulting in $\sim 2^{324}$ different sequences for $|b| = 64 \cdot (1 - 0.35) = 41.6$. For a fusion of both algorithms we get $|b| = 64 \cdot (1 - 0.41) = 37.76$ resulting in $\sim 2^{320}$ possible sequences. By increasing block sizes security is significantly increased, e.g. for the 1D LogGabor feature extractor a total number of $\sim 2^{753}$ possible sequences have to be tried for each pair of blocks in order to guess the two original iris-code parts for $w = 10$ and $l = 128$, with $|b| = 128 \cdot (1 - 0.49) = 65.28$, while the system still reveals a practical EER of 0.455%. Obviously, the presented cancelable biometric mixing approach is operated through a natural trade-off between security and biometric performance. In addition, it is important to note that an adversary has no criteria for the correctness of inverse iris-codes, even in case he gains access to the system.

Unlinkability, i.e. the infeasibility of cross-matching different protected templates of a single subject, represents a major issue of biometric template protection, however, experimental studies on unlinkability are commonly ignored [40]. In the proposed cancelable scheme unlinkability is achieved by incorporating an application-specific bit vector AD, which is XORed with iris-code columns prior to transforms. In order to investigate the unlinkability of the presented approach

we focus on the best performing configuration in terms of accuracy, i.e. $l = 64$ columns comprising $w = 10$ bits of two different iris-codes are successively mapped to according Bloom filters of size $n = 2^{10}$. Subsequently, obtained inter-class distributions (where a single bit vector is applied) are compared to distributions yielded by comparing Bloom filters originating from a single iris-code which are obscured by different bit vectors. Obtained score distributions are depicted in Fig. 8 for all multi-instance fusion scenarios, where unlinkability studies have been obtained from more than 10 000 genuine comparison with randomly chosen bit vectors. The comparison of different mixed templates generated from pairs of iris-codes does not allow cross-matching since resulting dissimilarity scores are generally higher than that of impostor comparisons within a single application. That is, an adversary will not be able to cross-match protected templates of a single subject if these are generated employing different auxiliary data.

E. Compressed Templates

Regarding resulting template sizes, for the majority of configurations $K \cdot 2^w < 2 \cdot W \cdot H = 10 \cdot 2^{11}$ applies, which means a compression w.r.t. the original pair of templates is achieved. Again, a trade-off is observed, between template size and biometric performance. Obtained EERs and resulting template sizes are plotted in Fig. 9 for all multi-instance fusion scenarios. Smallest template sizes (10% of original size), e.g. for the configuration of $w = 9$ and $l = 2^9$, result in rather unpractical performance rates of EERs $\sim$5%, while compressions down to 20% or 40% of the original size almost maintain accuracy. Extracted codes which represent mixed protected templates which enables an alignment-free comparison and a highly compact storage of iris-codes, e.g. 2D barcodes, smart cards of magnetic stripes [34].

V. Conclusions

In this work a multi-biometric template protection scheme based on multiple instances of iris images is proposed. Based on the concept of mixing biometric information [16], iris-codes obtained from different eyes are mixed in an alignment-free protected template based on adaptive Bloom filters [15], i.e. the scheme represents an instance of cancelable multi-biometrics. In experiments the muti-biometric template protection scheme is evaluated in an multi-instance single-algorithm and multi-instance multi-algorithm configuration where biometric performance is maintained (or even improved) for all scenarios, yielding EERs below 0.5%. At the same time protected templates are highly compressed down to $\sim$20% of the original size of mixed iris-codes. In addition, the proposed scheme provides a fast comparison of protected templates suitable for biometric recognition in identification mode.

Acknowledgment

This work has been partially funded by the European FP7 FIDELITY project (SEC-2011-284862) and the Center of Applied Security Research Darmstadt (CASED).

References

[1] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[2] K. Bowyer, K. Hollingsworth, and P. Flynn, "Image understanding for iris biometrics: A survey," *Computer Vision and Image Understanding*, vol. 110, no. 2, pp. 281–307, 2007.

[3] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[4] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 385–395, 2011.

[5] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 3, 2011.

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

[7] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[8] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection*, International Organization for Standardization, 2011.

[9] A. Nagar, K. Nandakumar, and A. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 255–268, 2012.

[10] C. Rathgeb and C. Busch, "Multibiometric template protection: Issues and challenges," in *New Trends and Developments in Biometrics*. In-Tech, 2012, pp. 173–190.

[11] A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115–2125, 2003.

[12] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics (International Series on Biometrics)*. Springer-Verlag, 2006.

[13] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC TR 24722:2007. Information Technology – Multimodal and other multibiometric fusion*, International Organization for Standardization and International Electrotechnical Committee, 2007.

[14] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. S. Veldhuis, and C. Busch, "Multi-algorithm fusion with template protection," in *Proc. of the 3rd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'09)*, 2009, pp. 1–7.

[15] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Proc. 6th Int'l Conf. on Biometrics*, 2013, to appear.

[16] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 260–267, 2013.

[17] J. Zuo, N. K. Ratha, and J. H. Connel, "Cancelable iris biometric," *Proc. 19th Int'l Conf. on Pattern Recognition*, pp. 1–4, 2008.

[18] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Proc. 12th Int'l Information Security Conf.*, ser. LNCS, P. Samarati, M. Yung, F. Martinelli, and C. Ardagna, Eds., vol. 5735. Springer, 2009, pp. 135–142.

[19] O. Ouda, N. Tsumura, and T. Nakaguchi, "Bioencoding: A reliable tokenless cancelable biometrics scheme for protecting iriscodes," *IEICE Transactions on Information and Systems*, vol. E93.D, pp. 1878–1888, 2010.

[20] A. Kong, K.-H. Cheunga, D. Zhanga, M. Kamelb, and J. Youa, "An analysis of BioHashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[21] 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 Intellegence*, vol. 33, no. 9, pp. 1877–1893, 2011.

[22] S. C. Chong, A. T. B. Jin, and D. N. C. Ling, "High security iris verification system based on random secret integration," *Computer Vision and Image Understanding*, vol. 102, no. 2, pp. 169–177, 2006.

[23] ——, "Iris authentication using privatized advanced correlation filter," in *Proc. 1st Int'l Conf. on Biometrics*, ser. LNCS, D. Zhang and A. Jain, Eds., vol. 3832. Springer, 2006, pp. 382–388.

[24] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. on Computer and Communications Security*. ACM, 1999, pp. 28–36.

[25] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proc. IEEE Conf. on Computer Vision and Pattern Recognition*. IEEE, 2007, pp. 1–6.

[26] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proc. IEEE 2nd Int'l Conf. on Biometrics: Theory, Applications, and Systems*. IEEE, 2008, pp. 1–6.

[27] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int'l Symp. on Information Theory*. IEEE, 2002, p. 408.

[28] M. Y. Jeong, C. Lee, J. Kim, J. Y. Choi, K. A. Toh, and J. Kim, "Changeable biometrics for appearance based face recognition," in *Proc. Biometric Consortium Conf.* IEEE, 2006, pp. 1–5.

[29] C. Rathgeb, A. Uhl, and P. Wild, "Reliability-balanced feature level fusion for fuzzy commitment scheme," in *Proc. Int'l Joint Conf. on Biometrics*. IEEE, 2011, pp. 1–7.

[30] B. Yang, C. Busch, K. de Groot, H. Xu, and R. N. J. Veldhuis, "Performance evaluation of fusing protected fingerprint minutiae templates on the decision level," *Sensor-Journal, Special Issue: Hand-Based Biometrics Sensors and Systems*, vol. 2012, no. 12, pp. 5246–5272, 2012.

[31] B. Bloom, "Space/time tradeoffs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[32] J. Mullin, "Optimal semijoins for distributed database systems," *IEEE Transactions on Software Engineering*, vol. 16, no. 5, pp. 558 –560, may 1990.

[33] A. Broder and M. Mitzenmacher, "Network Applications of Bloom Filters: A Survey," *Internet Mathematics*, vol. 1, no. 4, pp. 485–509, 2005.

[34] J. E. Gentile, N. Ratha, and J. Connell, "Slic: Short-length iris codes," in *Proc. IEEE 3rd Int'l Conf. on Biometrics: Theory, Applications, and Systems*. IEEE, 2009, pp. 1–5.

[35] L. Masek, "Recognition of human iris patterns for biometric identification," Master's thesis, University of Western Australia, 2003.

[36] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Efficient iris recognition by characterizing key local variations," *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 739–750, 2004.

[37] A. Uhl and P. Wild, "Weighted adaptive hough and ellipsopolar transforms for real-time iris segmentation," in *Proc. 5th Int'l Conf. on Biometrics*, 2012, pp. 1–8.

[38] R. Viveros, K. Balasubramanian, and N. Balakrishnan, "Binomial and negative binomial analogues under correlated bernoulli trials," *The American Statistician*, vol. 48, no. 3, pp. 243–247, 1984.

[39] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *Proc. 5th Int'l Conf. on Biometrics*, 2012, pp. 498–505.

[40] E. Maiorana, "Biometric cryptosystem using function based on-line signature recognition," *Expert Systems with Applications*, vol. 37, no. 4, pp. 3454–3461, 2010.

APPENDIX

***Proof** (by induction):* for all $|b|, l \in \mathbb{N}$, $l \geq |b| > 1$, the theoretical amount of possible sequences is defined by $f(|b|, l)$, where each of the $|b|$ codewords have to appear at least once within l columns,

$$f(|b|, l) = |b|^l - \sum_{i=1}^{|b|-1} \binom{|b|}{i} \cdot f(i, l). \tag{6}$$

***Base case**:* $f(1, l) = 1$, and for $|b| = 2$, the number of possible sequences is $2^l - 2$, i.e. all possible sequences minus the two sequences where only one codeword occurs,

$$f(2, l) = 2^l - \sum_{i=1}^{1} \binom{2}{i} \cdot f(i, l) = 2^l - \binom{2}{1} \cdot f(1, l) = 2^l - 2.$$

(6) is true for the base case, $|b| = 2$.

***Induction step**:* $|b| \rightarrow |b|+1$, suppose (6) is true for $|b|$. For $|b| + 1$ the number of all possible sequences is $(|b| + 1)^l$, the subtracted number of possible i-element subsets are now of a set containing $|b| + 1$ elements, and sequences comprising $|b|$ codewords are subtracted. We get,

$$\begin{aligned}
f(|b|+1, l) = \; & (|b|+1)^l - \binom{|b|+1}{|b|} \cdot f(|b|, l) \\
& - \sum_{i=1}^{|b|-1} \binom{|b|+1}{i} \cdot f(i, l) \\
= \; & (|b|+1)^l - \binom{|b|+1}{|b|+1-|b|} \cdot f(|b|, l) \\
& - \sum_{i=1}^{|b|-1} \binom{|b|+1}{i} \cdot f(i, l) \\
= \; & (|b|+1)^l - (|b|+1) \cdot f(|b|, l) \\
& - \sum_{i=1}^{|b|-1} \binom{|b|+1}{i} \cdot f(i, l) \\
= \; & (|b|+1)^l - \sum_{i=1}^{|b|} \binom{|b|+1}{i} \cdot f(i, l)
\end{aligned}$$

***Conclusion**:* by the principle of induction, (6) is true for all $|b|, l \in \mathbb{N}$, $l \geq |b| > 1$.

■