C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced Feature Level Fusion for Fuzzy Commitment Scheme. In *Proceedings of the 1st International Joint Conference on Biometrics (IJCB'11)*, 7 pages, Washington, DC, USA, October 10–13, 2011. © IEEE. http://dx.doi.org/10.1109/IJCB.2011.6117535. The original publication is available at http://www.ieeexplore.com.

Reliability-balanced Feature Level Fusion for Fuzzy Commitment Scheme

Christian Rathgeb, Andreas Uhl and Peter Wild*
Multimedia Signal Processing and Security Lab
Department of Computer Sciences, University of Salzburg, Austria
{crathgeb,uhl,pwild}@cosy.sbg.ac.at

Abstract

Fuzzy commitment schemes have been established as a reliable means of binding cryptographic keys to binary feature vectors extracted from diverse biometric modalities. In addition, attempts have been made to extend fuzzy commitment schemes to incorporate multiple biometric feature vectors. Within these schemes potential improvements through feature level fusion are commonly neglected.

In this paper a feature level fusion technique for fuzzy commitment schemes is presented. The proposed reliability-balanced feature level fusion is designed to re-arrange and combine two binary biometric templates in a way that error correction capacities are exploited more effectively within a fuzzy commitment scheme yielding improvement with respect to key-retrieval rates. In experiments, which are carried out on iris-biometric data, reliability-balanced feature level fusion significantly outperforms conventional approaches to multi-biometric fuzzy commitment schemes confirming the soundness of the proposed technique.

1. Introduction

Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric [3], offering solutions to secure biometric-based key management as well as biometric template protection. The fuzzy commitment scheme (FCS) [6] represents one of the most popular template protection schemes and has been applied to several biometric modalities. In FCSs keys prepared with error correction information are bound to binary biometric feature vectors, i.e. biometric variance is overcome by means of error correction. While different applications of error correction have been proposed (*e.g.* in [4, 2]) perfect error correction codes for desired code lengths have remained elusive. In addition, attempts have been made to adapt binary biometric feature vectors in order to provide a more efficient error correction decoding (*e.g.* in [2, 14]), yielding improved key-retrieval rates. In addition, multi-biometric FCSs have been proposed (*e.g.* in [17, 8]) in which different feature vectors are utilized at key-binding. However, so far feature level fusion (FLF) approaches within multi-biometric FCSs has been implemented by simple concatenations of biometric templates neglecting potential performance improvements resulting from a sensible re-arrangement of binary feature vectors.

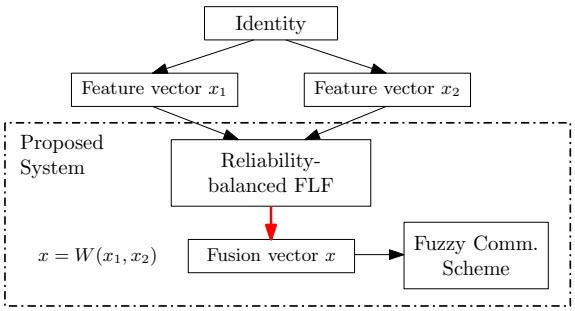


Figure 1. Basic operation mode of the proposed reliability-balanced FLF for FCS.

In this paper a FLF for FCSs is presented. Emphasis is put on the reliability, *i.e.* stability and driscriminativity, of single bits in biometric feature vectors. Based on a per-algorithm analysis of reliability distributions within feature vectors obtained from a small training set, FLF function W transforms two given biometric templates x_1 and x_2 into one template x, $x = W(x_1, x_2)$. The proposed approach, which is illustrated in Fig. 1, is designed to balance bit reliability of according chunks of the entire fused template at a maximum reachable level. Thereby, a more efficient error correction decoding within a FCS is achieved yielding improved key-retrieval rates. The generic reliability-based FLF is evaluated on iris biometric data employing two different feature extraction algorithms inappropriate for biometric fusion at score level. In experiments the proposed FLF yields a significant performance improvement, compared to existing methods.

The remainder of this paper is organized as follows: in Section 2 related work regarding (multi-biometric) FCSs is

*supported by the Austrian Science Fund FWF, project no. L554-N15 and FIT-IT Trust in IT-Systems, project no. 819382.

reviewed. Subsequently, the proposed FLF is described in detail in Section 3. Section 4 presents experiments employing an iris-biometric database. Finally, a conclusion is given in Section 5 .

2. Previous Work

In 1999, Juels and Wattenberg [6] proposed the FCS, a bit commitment scheme resilient to noise. A FCS is formally defined as a function F, applied to commit a codeword $c \in C$ with a witness $x \in \{0,1\}^n$ where C is a set of error correcting codewords of length n. The witness x represents a binary biometric feature vector which can be uniquely expressed in terms of the codeword c along with an offset $\delta \in \{0,1\}^n$, where $\delta = x - c$. Given a biometric feature vector x expressed in this way, c is concealed applying a conventional hash function (e.g. SHA-3), while leaving δ as it is. The stored helper data is defined as,

$$F(c,x) = \big(h(x), x - c\big). \tag{1}$$

In order to achieve resilience to small corruptions in x, any x' sufficiently "close" to x according to an appropriate metric (e.g. Hamming distance), should be able to reconstruct c using the difference vector δ to translate x' in the direction of x. In case $\|x - x'\| \leq t$, where t is a defined threshold lower bounded by the according error correction capacity, x' yields a successful decommitment of $F(c,x)$ for any c. Otherwise, $h(c) \neq h(c')$ for the decoded codeword c' and a failure message is returned. In Fig. 2 the basic operation mode of the FCS is illustrated.

Key approaches to FCSs with respect to applied biometric modalities, performance rates in terms of false rejection rate (FRR) and false acceptance rate (FAR), extracted key sizes, and applied data sets are summarized in Table 2. The FCS was applied to iris-codes by Hao *et al.* [4]. In their scheme 2048-bit iris-codes are applied to bind and retrieve 140-bit cryptographic keys prepared with Hadamard and Reed-Solomon error correction codes. Hadamard codes are applied to eliminate bit errors originating from the natural biometric variance and Reed-Solomon codes are applied to correct burst errors resulting from distortions. In order to provide an error correction decoding in an iris-based FCS, which gets close to a theoretical bound, two-dimensional iterative min-sum decoding is introduced in [2]. A matrix formed by two different binary Reed-Muller codes enables a more efficient decoding, in addition, it was found that a random permutation of iris-code bits improves recognition rates due to a more uniform distribution of error occurrence. In [13], a systematic approach to the construction of iris-based FCS is presented. Different techniques to improve the accuracy of iris-based FCSs have been proposed in [19, 14].

In [18] a randomized dynamic quantization transformation is applied to binarize fingerprint features extracted from a multichannel Gabor filter. Subsequently, Reed-Solomon codes are applied to construct the FCS incorporating a non-invertible projection based on a user-specific token. A similar FCS based on face features is presented in [1]. In [11] a binary fixed-length minutiae representation obtained by quantizing the Fourier phase spectrum of a minutia set is applied in a FCS where alignment is achieved through focal points of high curvature regions. In [10] a FCS for on-line signatures is presented.

Several approaches have been proposed to extend biometric cryptosystem to incorporate multiple biometric characteristics. In [17] fingerprint and face templates are combined in a FCS. Real-valued fingerprint features and binary iris-codes are ultilized in [12]. Chunks of binary features are applied in a FCS and used as additional points within a fuzzy vault. In [8] 3D face templates obtained by different feature extraction methods are fused at feature level, score level and decision level in a FCS. Proposed FLFs in [17, 8] involve simple concatenations of binarized biometric templates. A review of biometric cryptosystem technologies can be found in [3].

3. Improving Reliability Distribution with Feature Level Fusion

In traditional FCSs, the witness as a bitstream $x \in \{0,1\}^n$ represents directly the binary output of some feature extractor. We adopt a new function W for the generation of witness data out of two binary feature vectors $x_1, x_2 \in \{0,1\}^n$, *i.e.* $x = W(x_1, x_2)$. This step is useful for two reasons:

1. In classic binary feature extraction, bits of a feature vector x are not ordered according to their reliability, *i.e.* the probability that the i-th bit comparison of the corresponding feature vectors correctly indicate whether believed B and observed X identities are equal:

$$R(i) = \frac{P(x[i] = b[i] \mid X = B) + P(x[i] \neq b[i] \mid X \neq B)}{2}. \tag{2}$$

But a balanced reliability distribution is a desirable property for FCSs, since error correction is designed to handle a fixed amount of errors within chunks of biometric feature vectors.

2. Multi-biometrics can be applied to enhance FCS performance without negative impact on the amount of bit comparisons (n remains fixed).

The FLF function W is computed as follows:

1. For each employed feature extraction method the corresponding reliability is approximated in a separate

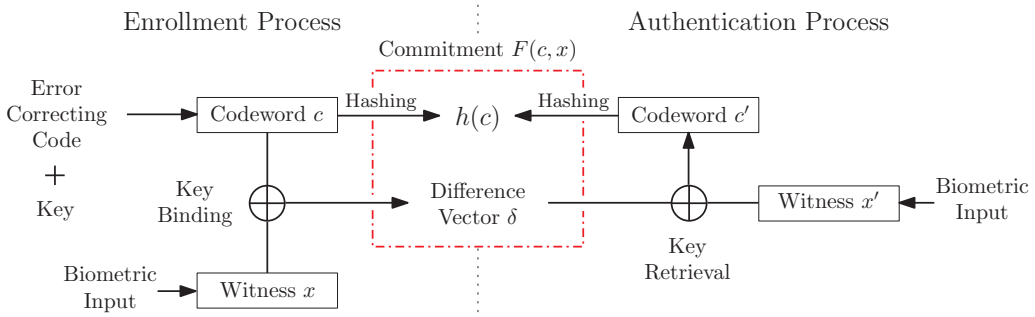


Figure 2. The FCS: keys prepared with error correction are XORed with biometric feature vectors in the key-binding process. biometric features are XORed with the commitment and error correction decoding is applied at key-retrieval. Keys are verified applying hashes.

Authors	Modality	FRR/ FAR (%)	Key Size (Bits)	Test Set	Remarks
Hao *et al.* [4]	Iris	0.47/ 0	140	70 subjects	ideal images
Bringer *et al.* [2]		5.62/ 0	42	ICE 2005	short key
Teoh and Kim [18]	Fingerprint	0.9/ 0	296	FVC 2002	user-specific tokens
Nandakumar [11]		12.6/ 0	327	FVC 2002	–
Ao and Li [1]	Face	7.99/ 0.11	>4000	294 subjects	user-specific tokens
Maiorana and Campisi [10]	Online Sig.	EER >9	>100	MCYT	>1 enroll. sam.
Sutcu *et al.* [17]	Fingerprint & Face	0.92/ $\ll$0.01	–	NIST DB 27 & Face94	–
Nandakumar and Jain [12]	Fingerprint & Iris	1.8/ 0.01	224	MSU-DBI & CASIAv1	use of fuzzy vault
Kelkboom *et al.* [8]	FLF for 3D Face	~22/ 0.25	155	FRGC	>1 enroll. sam.

Table 1. Experimental results of proposed fuzzy commitment schemes.

training stage from a set $G = \{(x, y)|X = Y\}$ of genuine feature vector samples and $I = \{(x, y)|X \neq Y\}$ of impostors:

$$R(i) \approx \frac{1}{2} \cdot \left(\frac{\parallel \{(x,y) \in G \,|x[i] = b[i]\} \parallel}{\parallel G \parallel} + \frac{\parallel \{(x,y) \in I \,|x[i] \neq b[i]\} \parallel}{\parallel I \parallel} \right). \quad (3)$$

2. Binary biometric samples can be ordered with respect to global reliability $R(i)$ to achieve even higher recognition accuracy when comparing only parts of biometric data [15]. Therefore, for each feature extraction method the set of permutations ordering feature vectors with respect to reliability is considered and an arbitrary $\sigma \in \mathcal{P}$ is selected (I_n is the index set $\{1, 2, \ldots, n\}$):

$$\mathcal{P} = \{\sigma : I_n \rightarrow I_n \,|\, \exists \sigma^{-1} \wedge \forall i < j : R(\sigma(i)) \geq R(\sigma(j))\} \quad (4)$$

3. Given two different features with reliabilities R_1 and R_2 and corresponding permutations σ_1, σ_2, we compute $W(x_1, x_2) \in \{0, 1\}^n$ from feature vectors x_1, x_2 as:

$$W(x_1, x_2)[i] = \begin{cases} x_1[\sigma_1(\lceil i/2 \rceil)] & \text{if } i \text{ is even} \\ x_2[\sigma_2(\lceil (n-i)/2 \rceil)] & \text{otherwise.} \end{cases} \quad (5)$$

Error correction codewords, bound to parts of binary bitstreams which are expected to contain a very small amount of errors, are not used efficiently since during decoding only a very small number of bit-errors is corrected. On the other side, error correction codewords, bound to parts of binary bitstreams which are expected to contain a very large amount of errors are not used efficiently either, since decoding will not succeed.

To achieve a uniform distribution of errors per bit-block (with respect to the training set) bits at bit positions with low reliability have to be arranged in bit-blocks together with bits originating from bit positions which exhibit high reliability and vice versa. For this purpose the first $n/2$ bits of reliability-ordered binary biometric data of both algorithms are combined in a single template of length n. The fusion is performed in a way such that alternating single bits of each algorithm are set (bits are interleaved), while the first $n/2$ bits of reliability-ordered feature vector bits of the first algorithm are read from left to right and the first $n/2$ bits of reliability-ordered feature vector bits of the second algorithm are read from right to left. The proposed bits fusion process is illustrated in Fig. 3.

The reliability-balanced FLF technique which provides a more efficient error correction decoding represents the main contribution of the proposed scheme.

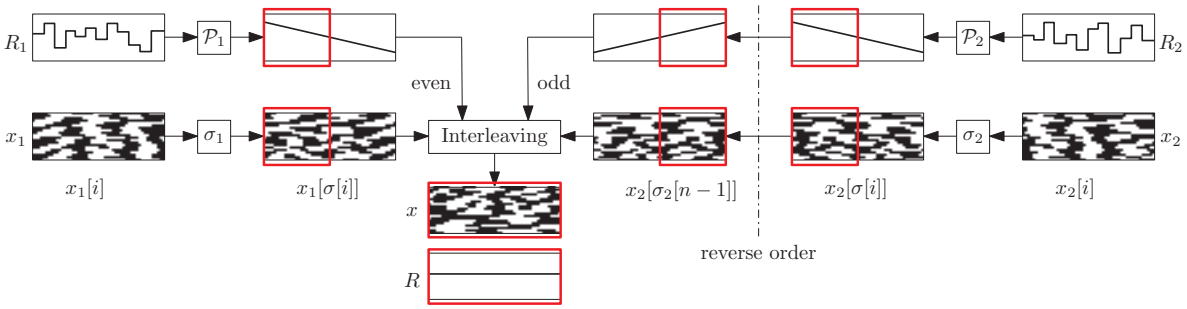


Figure 3. Reliability-balanced FLF: two binary biometric templates, x_1 and x_2, are fused into one template x of same size. Based on reliability distributions, R_1 and R_2, obtained from a training set, bits of templates are reordered (in addition one templated is reverse ordered) and the final template is generated from interleaving the $n/2$ most reliable bits of both.

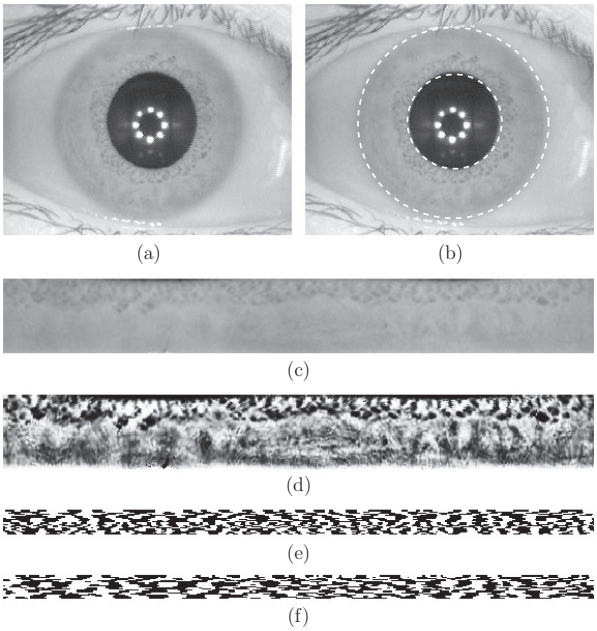


Figure 4. Preprocessing and feature extraction: (a) image of eye (b) detection of pupil and iris (c) unwrapped and (d) preprocessed iris texture, iris-code of (e) Masek and (f) Ma *et al*.

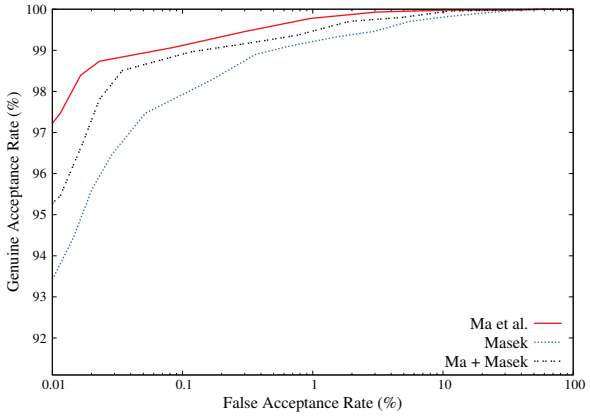


Figure 5. ROC curves for the algorithm of Ma *et al*., Masek and score level fusion of both applying the Hamming distance.

4. Experiments on Biometric Data

4.1. Experimental Setup

Experiments are carried out using the CASIA-v3-Interval iris database[1]. In experiments only left-eye images (1332 instances) are evaluated, since the estimated global distribution of reliable bits is highly influenced by natural distortions [15]. At preprocessing the iris of a given sample image is detected, un-wrapped to a rectangular texture of 512×64 pixel, and illumination across the texture is normalized as shown in Fig. 4 (a)-(d).

In the feature extraction stage custom implementations of two different iris recognition algorithms are employed. The first feature extraction method follows an implementation by Masek[2] in which filters obtained from a one-dimensional Log-Gabor function are utilized to generate iris-codes of 10240 bit. The second one was proposed by Ma *et al.* [9]. Within this algorithm a dyadic wavelet transform is performed based on which two fixed subbands are selected. Local minima and maxima above a adequate threshold are located an encoded extracting 10240 bit. Sample iris-codes generate by both feature extraction methods are shown in Fig. 4 (e)-(f). The receiver operating characteristic (ROC) curves of each algorithm and the score level fusion of both are plotted in Fig. 5 where the Hamming distance is applied as dis-similarity measure and alignment is achieved applying up to 8-bit circular shifts in each direction. The score level fusion of both algorithms does not improve the recognition accuracy.

In the training stage the first 20 classes are applied for parameter estimation. Remaining subjects of the database

[1]The Center of Biometrics and Security Research, CASIA Iris Image Database, http://www.sinobiometrics.com

[2]L. Masek: Recognition of Human Iris Patterns for Biometric Identification, Master's thesis, University of Western Australia, 2003

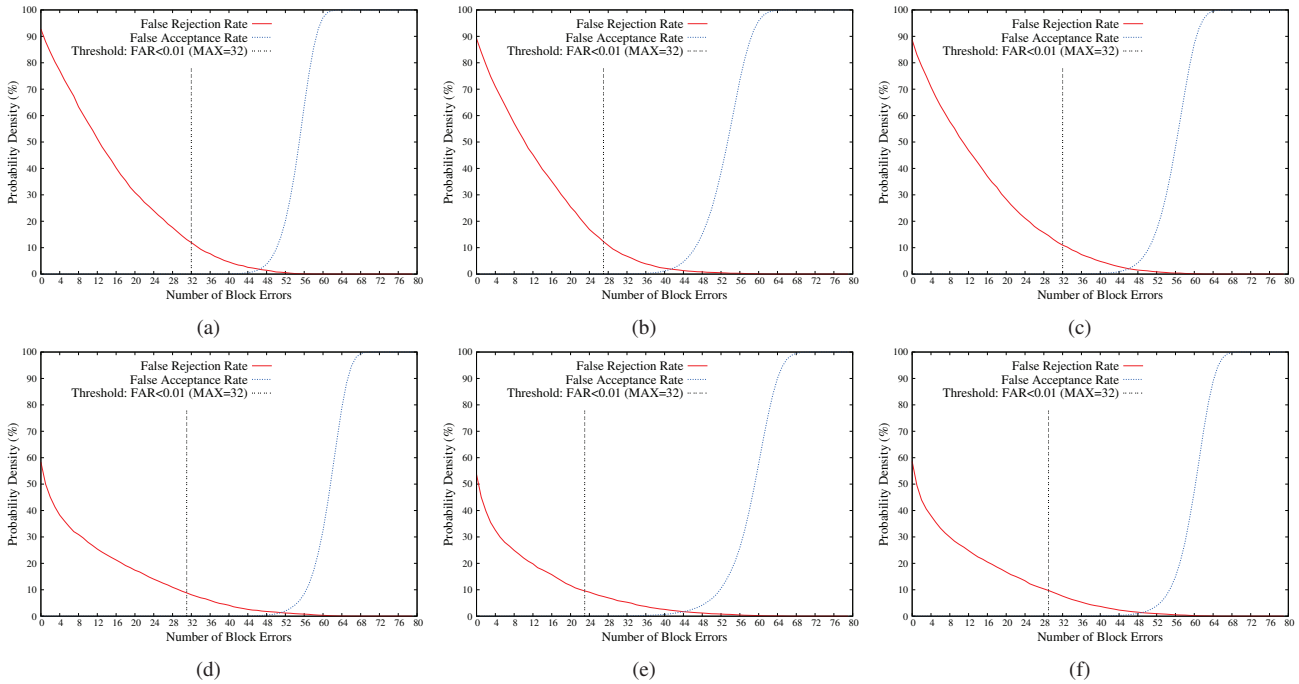


Figure 6. Experimental results of the original FCSs of (a) Ma *et al.*, (b) Masek, (c) a fusion of both (every second bit of each algorithm), the randomized FCSs of (d) Ma *et al.*, (e) Masek and (f) a fusion of both (interleaved randomized bits of each algorithm).

are registered applying a randomly generated cryptographic key. Commitments are generated from every iris image and key retrieval is processed for all pairs of stored commitments and iris-codes. Key binding and retrieval is performed according to the approach of Hao *et al.* [4]. At key binding a $16 \cdot 8 = 128$ bit cryptographic key k is first prepared with a $RS(16, 80)$ Reed-Solomon code. The Reed-Solomon error correction code operates on block level and is capable of correcting $(80 - 16)/2 = 32$ block errors. Then, the 80 8-bit blocks are Hadamard encoded resulting in 80 128-bit codewords (=10240-bit) and bound to the iris-code by XORing both, *i.e.* codewords of length n are mapped to codewords of length 2^{n-1} where up to 25% of bit errors can be corrected. Best experimental results were obtained for this configuration. Since balanced reliability distributions are estimated based on a training set burst errors may still occur at key retrieval, *i.e.* block level error correction remains essential. Additionally, a hash of the original key $h(k)$ is stored. Key retrieval is performed by XORing an extracted iris-code with the commitment. The resulting bitstream is decoded applying Hadamard decoding and Reed-Solomon decoding afterwards. The resulting key k' is then hashed and if $h(k') = h(k)$ the correct key k is released.

4.2. Performance Evaluation

Focusing on the applied iris recognition algorithms FRRs of 2.54% and 6.59% are obtained at according FARs less than 0.01% using the Hamming distance as dissimilarity measure. The score level fusion of both algorithms results in a FRR of 4.58% (see Fig. 5). The FRR of a FCS defines the percentage of incorrect keys returned to genuine subjects. By analogy, the FAR defines the percentage of correct keys returned to non-genuine subjects. In case iris-codes of both algorithms are applied in FCSs leaving bit orders unaltered FRRs of 11.93% and 10.87% are achieved at FARs less than 0.01%. Again, using each second bit of according iris-codes within a FCS does not improve the key-retrieval rate. FRRs and FARs for both FCSs and the fusion scenario are plotted in Fig. 6 (a)-(c). If random permutations of iris-code bits are applied, as suggested

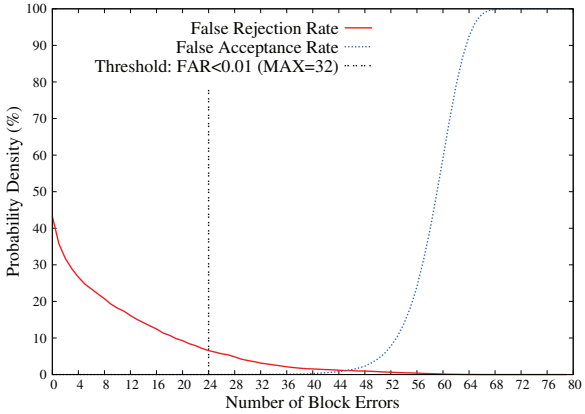
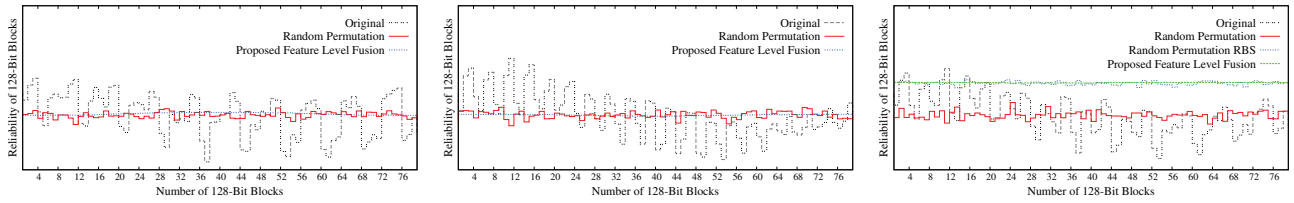
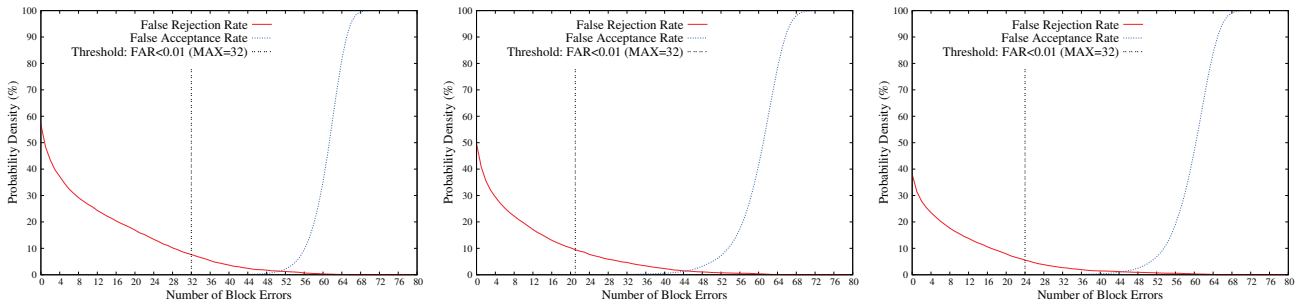


Figure 7. Experimental results of FCS obtained from a fusion of randomly chosen bits of 5120 most reliable bits of both algorithms.



(a) (b) (c)

Figure 8. Distributions of reliability within 128-bit blocks according to unaltered templates, randomized templates, and the proposed FLF for (a) Ma *et al*., (b) Masek, and (c) a fusion of both feature extraction methods (applied to the training set of 20 subjects).



(a) (b) (c)

Figure 9. Experimental results of the proposed FLF FCS for (a) Ma *et al*., (b) Masek, and (c) both algorithms.

in [2], a more uniform distribution of errors is achieved and performance rates are improved. For the feature extraction of Ma *et al*. and Masek a FRR of 8.81% and 9.56% are obtained at FARs less than 0.01% (one random permutation is applied to all iris-codes). Like in the original iris recognition scenario the FCS based on the algorithm of Ma *et al*. outperforms the FCS based on the algorithm of Masek since error correction capacities are exploited more effectively. In the fusion scenario templates are generated by interleaving randomly chosen bits of according iris-codes. Again, FLF does not improve the key-retrieval rate resulting in a FRR of 9.74%. FRRs and FARs of both algorithms and the according fusion based on a random permutation are plotted in Fig. 6 (d)-(f). However, if fused templates are constructed by randomly choosing bits of parts of iris-codes detected as most reliable ones, *i.e*. interleaving randomly permuted 5120 most reliable bits after reliable bit selection (RBS) of both feature extraction methods, the key-retrieval rate is improved resulting in a FRR of 6.53% at a FAR less than 0.01%. In Fig. 7 the obtained FRR and FAR are plotted.

Reliability distributions of the applied training set averaged over 128-bit blocks are shown in Fig. 8 (a)-(c). Reliability distributions of unaltered iris-codes appear periodic due to a line-wise processing of feature extractions exhibiting high variation. In case a random permutation of bits is applied the variation of reliability is significantly decreased, yielding a significant performance improvement. The proposed FLF achieves a balanced (near uniform) distribution of reliability for single feature vectors (a fusion of half templates of one feature extraction) as well as the fusion of both biometric templates. In Fig. 8 a significant improvement of the average reliability within fused templates is observed resulting in a FRR of 5.56% at a FAR less than 0.01%. If the proposed FLF is applied within biometric feature vectors of one template a FRR of 7.64% and a FRR of 9.47% is obtained for the algorithm of Ma *et al*. and Masek, respectively. FRRs and FARs of the proposed technique for both algorithms and the according fusion are plotted in Fig. 9 (a)-(c). All obtained results are summarized in Table 2 including the number of corrected block errors after Hadamard decoding, *i.e*. error correction capacities may not handle the optimal amount of occurring errors within intra-class key retrievals. While a fusion of the applied feature extraction methods does not seem to pay off for simple FLF the proposed approach significantly improves key-retrieval rates.

System	Algorithm	FRR (FAR $<$ 0.01)	Corr. Blocks
Original (HD)	Ma *et al*.	2.54 %	–
	Masek	6.59 %	–
	Ma+Masek	4.58 %	–
Ordered FCS	Ma *et al*.	11.93 %	32
	Masek	10.87 %	28
	Ma+Masek	10.97 %	32
Random FCS	Ma *et al*.	8.81 %	31
	Masek	9.56 %	23
	Ma+Masek	9.74 %	29
	Ma+Masek (RBS)	**6.53 %**	24
Bits-Fusion FCS	Ma *et al*.	7.64 %	32
	Masek	9.47 %	21
	Ma+Masek	**5.56 %**	24

Table 2. Summarized experimental results.

4.3. Privacy Aspects

Recently, template protection schemes based on FCS have been exposed vulnerable to several attacks. Despite privacy leakage in FCS [5], *i.e*. the information that the stored commitment contains (leaks) about biometric data, attacks based on error correction code histograms [16] and decodability attacks [7] have been proposed. These attacks utilize structures of applied error correction codewords bound to chunks of binary biometric feature vectors. Since bits of biometric templates are obscured within the proposed approach, yielding a balanced distribution of reliability, these attacks are aggravated and it is expected that committed codewords are more difficult to identify, *e.g*. by analyzing error correction code histograms. A more sophisticated analysis of a potential privacy enhancement provided presented approach is subject to future work.

5. Conclusion

Diverse biometric modalities have been applied in FCSs, even in multi-biometric scenarios. However, applied FLFs for FCSs only involved a concatenation of binary biometric feature vectors. In this paper a reliability-balanced FLF is proposed which aims at fusing binary biometric templates of two feature extraction methods into one single template of the same size. Reliability-balanced FLF is designed to balance average reliability across chunks of entire biometric templates based on a small training set. It is demonstrated that the proposed technique achieves a more balanced distribution of reliability yielding improved recognition rates in a FCS (although a FLF of the applied algorithms does not pay off for trivial approaches), since error correction is applied more effectively. Experiments are carried out on iris biometric data obtaining a significant improvement of key retrieval rates.

References

[1] M. Ao and S. Z. Li. Near infrared face based biometric key binding. *In Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558*, pages 376–385, 2009.

[2] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security*, 3:673–683, 2008.

[3] A. Cavoukian and A. Stoianov. Biometric encryption. In *Encyclopedia of Biometrics*. Springer Verlag, 2009.

[4] F. Hao, R. Anderson, and J. Daugman. Combining Cryptography with Biometrics Effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.

[5] T. Ignatenko and F. M. J. Willems. Information leakage in fuzzy commitment schemes. *Trans. on Information Forensics and Security*, 5(2):337–348, 2010.

[6] A. Juels and M. Wattenberg. A fuzzy commitment scheme. *Sixth ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[7] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *Trans. on Information Forensics and Security*, 2010. in Press.

[8] 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)*, pages 1–7, 2009.

[9] L. Ma, T. Tan, Y. Wang, and D. Zhang. Efficient Iris Recogntion by Characterizing Key Local Variations. *IEEE Transactions on Image Processing*, 13(6):739–750, 2004.

[10] E. Maiorana and P. Campisi. Fuzzy commitment for function based signature template protection. *IEEE Signal Processing Letters*, 17:249–252, 2010.

[11] K. Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *Proc. of IEEE Workshop on Information Forensics and Security (WIFS)*, 2010.

[12] K. Nandakumar and A. K. Jain. Multibiometric template security using fuzzy vault. In *IEEE 2nd International Conference on Biometrics: Theory, Applications, and Systems, BTAS '08*, pages 1–6, 2008.

[13] C. Rathgeb and A. Uhl. Systematic construction of iris-based fuzzy commitment schemes. *In Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558*, pages 947–956, 2009.

[14] C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis. In *Proc. of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, pages 41–44, 2010.

[15] C. Rathgeb, A. Uhl, and P. Wild. Incremental iris recognition: A single-algorithm serial fusion strategy to optimize time complexity. In *Proc. 4th IEEE International Conference on Biometrics: Theory, Application, and Systems.*, pages 1–6, 2010.

[16] A. Stoianov, T. Kevenaar, and M. van der Veen. Security issues of biometric encryption. In *Proc. of the Toronto Int. Conf. Science and Technology for Humanity (TIC-STH)*, pages 34–39, 2009.

[17] Y. Sutcu, Q. Li, and N. Memon. Secure biometric templates from fingerprint-face features. In *IEEE Conference on Computer Vision and Pattern Recognition, CVPR '07*, pages 1–6, 2007.

[18] A. Teoh and J. Kim. Secure biometric template protection in fuzzy commitment scheme. *IEICE Electron. Express*, 4(23):724–730, 2007.

[19] L. Zhang, Z. Sun, T. Tan, and S. Hu. Robust biometric key extraction based on iris cryptosystem. *In Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558*, pages 1060–1070, 2009.