UNIVERSITÄT SALZBURG

Template Protection under Signal Degradation: A Case-Study on Iris-Biometric Fuzzy Commitment Schemes

Christian Rathgeb Andreas Uhl

Technical Report 2011-04 November 2011

Department of Computer Sciences

Jakob-Haringer-Straße 2
5020 Salzburg
Austria
www.cosy.sbg.ac.at

Technical Report Series

Template Protection under Signal Degradation: A Case-Study on Iris-Biometric Fuzzy Commitment Schemes*

Christian Rathgeb and Andreas Uhl
Multimedia Signal Processing and Security Lab (WaveLab)
{crathgeb, uhl}@cosy.sbg.ac.at

Abstract

Low intra-class variability at high inter-class variability is considered a fundamental premise of biometric template protection, i.e. biometric traits need to be captured under favorable conditions in order to provide practical recognition rates. While performance degradations have been reported on less constraint datasets detailed studies based on a certain ground truth have remained evasive. The fuzzy commitment scheme, in which chosen keys prepared with error correction information are bound to binary biometric feature vectors, represents one of the most popular template protection schemes. In this work the impact of blur and noise to fuzzy commitment schemes is investigated. Iris textures are successively blurred and noised in order to measure the robustness of iris-biometric fuzzy commitment schemes.

1 Introduction

Biometric template protection schemes are designed to meet major requirements of biometric information protection (ISO/IEC FCD 24745), i.e. irreversibility (infeasibility of reconstructing original biometric templates from the stored reference data) and unlinkability (infeasibility of cross-matching different versions of protected templates). In addition, template protection schemes, which are commonly categorized as biometric cryptosystems (also referred to as helper data-based schemes) and cancelable biometrics (also referred to as feature transformation), are desired to maintain recognition accuracy [5]. Due to the sensitivity of template protection schemes it is generally conceded that deployments of biometric cryptosystems as well as cancelable biometrics require a constraint acquisition of biometric traits, in order to minimize any sort of signal degradation [3]. However, so far no studies about the actual impact of signal degradation on the recognition performance of template protection schemes have been proposed.

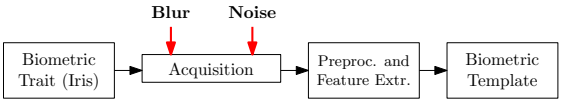


Figure 1: Supposed blur and noise occurrence within an (iris) biometric recognition system.

Biometric fuzzy commitment schemes (FCSs) [6], biometric cryptosystems which represent instances of biometric key-binding, have been proposed for several modalities (e.g. fingerprints, iris) achieving practical key retrieval rates at sufficient key sizes. While it is generally considered that template protection schemes, such as the FCS, are restricted to be operated under constraint environment detailed performance analysis in the presence of signal degradation have remained elusive. The contribution of this work is the investigation of the impact of signal degradation on the performance of FCSs. Two types of conditions, blur and noise, applied in the order illustrated in Figure 1, are investigated:

- **Blur:** focusing on image acquisition out of focus blur represents a frequent distortion.
- **Noise:** noise represents an undesirable but inevitable product of any electronic device.

*supported by the Autrian Science Fund, under project no. L554-N15.

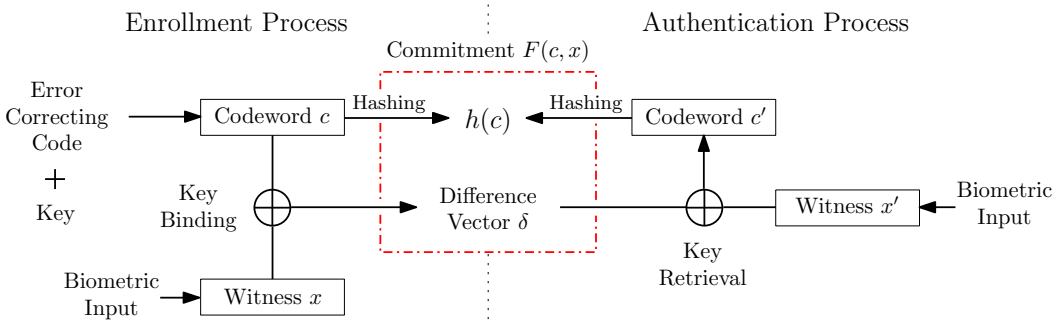


Figure 2: The FCS: keys prepared with error correction are XORed with biometric feature vectors in the key-binding process. biometric features are XORed with the commitment and error correction decoding is applied at key-retrieval. Keys are verified applying hashes.

Experimental studies are carried out on iris-biometric data employing different feature extraction algorithms to construct FCSs. Various combinations of different intensities of blur and noise are applied to simulate signal degradation. It is demonstrated that, opposed to current opinions, signal degradation, within a restricted extent, does not necessarily effect the key retrieval performance of a template protection scheme, even if this is the case for original recognition algorithms.

This paper is organized as follows: in Section 2 related work regarding biometric cryptosystems and FCSs is reviewed. Subsequently, a comprehensive case study on iris-biometric FCS is presented in Section 3. A conclusion is given in Section 4 .

2 Related Work

In past year numerous template protection schemes have been proposed (a review can be found in [3] and in [5]). 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 Figure 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 1. The FCS was applied to iris-codes in [4]. In the 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. Different techniques to improve the accuracy of iris-based FCSs have been proposed in [11, 15]. In [9] 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

Ref.	Modality	FRR/ FAR	Key Bits	Test Set	Remarks
Hao *et al.* [4]	Iris	0.47/ 0	140	70 subjects	ideal images
Bringer [2]		5.62/ 0	42	ICE 2005	short key
Rathgeb and Uhl [11]		4.64/ 0	128	CASIAv3	–
Teoh and Kim [13]	Fingerprint	0.9/ 0	296	FVC 2002	user-specific tokens
Nandakumar [9]		12.6/ 0	327	FVC 2002	–
Van der Veen *et al.* [14]	Face	3.5/ 0.11	58	FERET/ Caltech	>1 enroll. sam.
Ao and Li [1]		7.99/ 0.11	>4000	294 subjects	user-specific tokens
Maiorana and Campisi [8]	Online Sig.	EER >9	>100	MCYT	>1 enroll. sam.
Sutcu *et al.* [12]	Fingerprint & Face	0.92/ 0.01	–	NIST DB 27/ Face94	–
Nandakumar and Jain [10]	Fingerprint & Iris	1.8/ 0.01	224	MSU/ CASIAv1	use of fuzzy vault

Table 1: Experimental results of proposed FCSs in literature according to applied biometric modalities, obtained performance rates, number of bound key bits, and used test sets.

through focal points of high curvature regions. In [13] 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 a face features is presented in [1]. A FCS based on face biometrics is presented in [14] in which real-valued face features are binarized by simple thresholding followed by a reliable bit selection to detect most discriminative features. In [8] a FCS for on-line signatures is presented. In [12, 10] multi-biometric FCSs are proposed. It has been found that FCSs (template protection schemes in general) reveal worse performance on non-ideal data sets (e.g. in [2]), however, this is the case for underlying recognition algorithms, too. To our knowledge, so far, no detailed investigations about the impact of signal degradation based on a certain ground truth have been proposed.

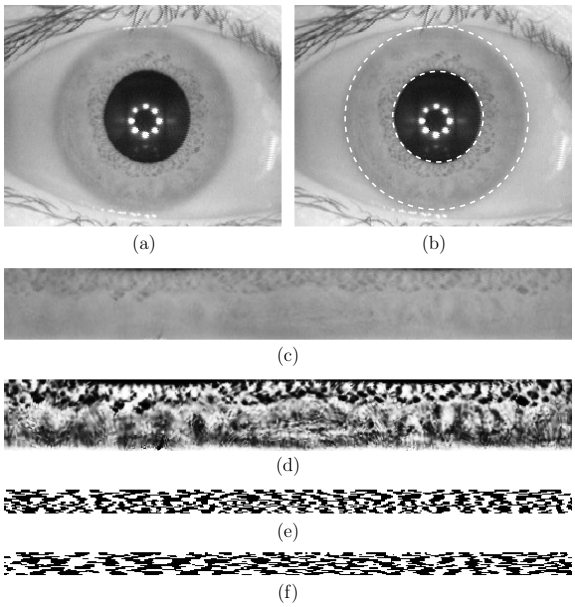


Figure 3: Preprocessing and feature extraction: (a) image of eye (b) detection of pupil and iris (c) unwrapped and (d) preprocessed iris texture, iris-code of (e) Masek and (f) Ma *et al.*.

3 A Case Study on Iris-FCSs

3.1 Experimental Setup

Experiments are carried out using the CASIA-v3-Interval iris database[1]. In experiments only left-eye images (1332 instances) are evaluated. At preprocessing the iris of a given sample image is detected, un-wrapped to a rectangular texture of 512×64 pixel, and lighting across the texture is normalized as shown in Figure 3 (a)-(d).

In the feature extraction stage we employ custom implementations of two different algorithms used to extract binary iris-codes. The first one was proposed by Ma et al. [7]. 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 dyadic wavelet transform is then performed on each of the resulting 10 signals, and two fixed subbands are selected from each transform resulting in a total number of 20 subbands. In each

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

subband all local minima and maxima above a 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 then $512 \times 20 = 10240$ bit. The second feature extraction method follows an implementation by Masek[2] in which filters obtained from a Log-Gabor function are applied. Here a row-wise convolution with a complex Log-Gabor filter is performed on the texture pixels. The phase angle of the resulting complex value for each pixel is discretized into 2 bits. To have a code comparable to the first algorithm, we use the same texture size and row-averaging into 10 signals prior to applying the one-dimensional Log-Gabor filter. The 2 bits of phase information are used to generate a binary code, which therefore is again $512 \times 20 = 10240$ bit. Sample iris-codes of both algorithms are shown in Figure 3 (e)-(f).

3.2 Iris-Biometric FCSs

The applied fuzzy commitment scheme follows the approach in [4]. For the applied algorithm of Ma et al. and the Log-Gabor feature extraction we found that the application of Hadamard codewords of 128-bit and a Reed-Solomon code $RS(16, 80)$ reveals the best experimental results for the binding of 128-bit cryptographic keys. At key-binding, a $16 \cdot 8 = 128$ bit cryptographic key R 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. In a Hadamard code codewords of length n are mapped to codewords of length 2^{n-1} in which up to 25% of bit errors can be corrected. Hence, 80 8-bit codewords are mapped to 80 128-bit codewords resulting in a 10240-bit bitstream which is bound with the iris-code by XORing both. Additionally, a hash of the original key $h(R)$ is stored as second part of the commitment. At authentication key retrieval is performed by XORing an extracted iris-code with the first part of the commitment. The resulting bitstream is decoded applying Hadamard decoding and Reed-Solomon decoding afterwards. The resulting key R' is then hashed and if $h(R') = h(R)$ the correct key R is released. Otherwise an error message is returned.

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

Blur		Noise	
Abbrev.	Description	Abbrev.	Description
B-0	no blur	N-0	no noise
B-1	$\sigma = 0.6$	N-1	$\sigma = 10$
B-2	$\sigma = 1.0$	N-2	$\sigma = 20$
B-3	$\sigma = 1.2$	N-3	$\sigma = 30$

Table 2: Blur and noise conditions considered for signal degradation (different denotations of σ are defined in 3.3.1 and 3.3.2).

In [2] it was found that a random permutation of bits in iris-codes improves key retrieval rates since a more uniform distribution of error occurrence is obtained. We consider two types of FCSs, one in which iris-codes are left unaltered and one in which a single random permutation is applied to each iris-code of the entire database, denoted by FCS RP.

3.3 Signal Degradation

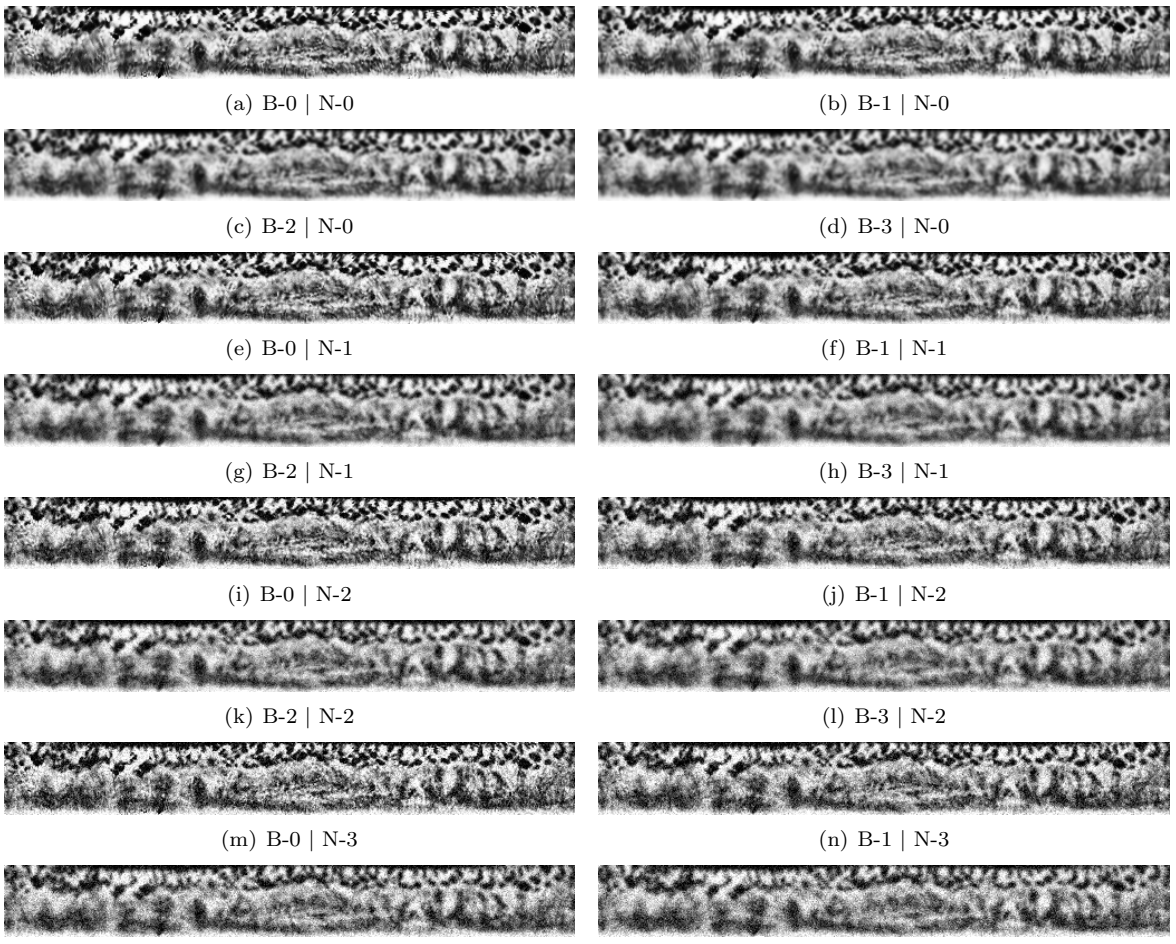
Signal degradation is simulated by means of blur and noise where blur is applied prior to noise (out of focus blur is caused before noise occurs). For different intensities (including absence) of blur and noise, which are summarized in Table 2, are considered, and combinations of these. In order to avoid segmentation errors blur and noise is incorporated after preprocessing (deformation of blur and noise caused by an unwrapping of the iris is ignored, however, signal degradation still decreases recognition accuracy of the applied algorithms). Examples of adding according signal degradation to a sample iris texture are shown in Figure 4 (a)-(p). is Blur and noise conditions are described in detail as follows:

3.3.1 Blur Conditions

Out of focus blur represents a frequent distortion in image acquisition mainly caused by an inappropriate distance of the camera to the eye (another type of blur is motion blur caused by rapid movement which is not considered in this work). We simulate the point spread function of the blur as a Gaussian

$$f(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}, \qquad (2)$$

which is then convoluted with the specific image.



(a) B-0 | N-0 (b) B-1 | N-0
(c) B-2 | N-0 (d) B-3 | N-0
(e) B-0 | N-1 (f) B-1 | N-1
(g) B-2 | N-1 (h) B-3 | N-1
(i) B-0 | N-2 (j) B-1 | N-2
(k) B-2 | N-2 (l) B-3 | N-2
(m) B-0 | N-3 (n) B-1 | N-3
(o) B-2 | N-3 (p) B-3 | N-3

Figure 4: Signal degradation: (a)-(p) different intensities of blur and noise applied to a sample iris texture.

3.3.2 Noise Conditions

Amplifier noise is primarily caused by thermal noise. Due to signal amplification in dark (or underexposed) areas of an image, thermal noise has a high impact on these areas. Additional sources contribute to the noise in a digital image such as shot noise, quantization noise and others. These additional noise sources however, only make up a negligible part of the noise and are therefore ignored during this work.

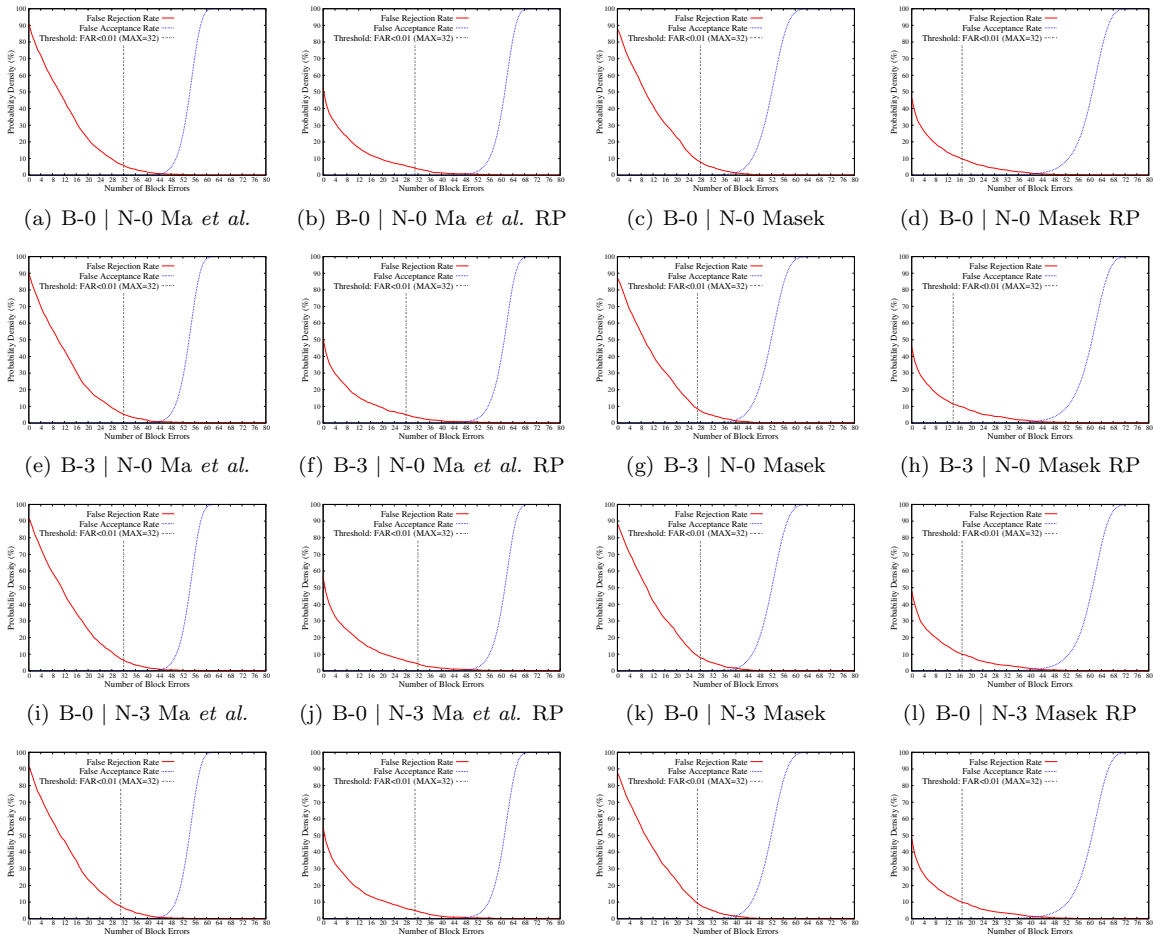
Let P be the set of all pixels in image $I \in \mathbb{N}^2$, $\omega = (\omega_p)_{p \in P}$, be a collection of independent identically distributed real-valued random variables following a Gaussian distribution with mean m and variance σ^2. We simulate thermal noise as additive Gaussian noise with $m = 0$, variance σ^2 for pixel p at x, y as

$$N(x, y) = I(x, y) + \omega_p, \quad p \in P, \tag{3}$$

with N being the noisy image, for an original I.

3.4 Performance Evaluation

Experimental results for both feature extraction methods and FCSs according to different intensities of blur and noise are summarized in Table 3, including average peak signal-to-noise ratios (PSNRs) caused by signal degradation and 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). The FRR of a FCS defines the percentage of incorrect keys returned to genuine



(a) B-0 | N-0 Ma *et al.* (b) B-0 | N-0 Ma *et al.* RP (c) B-0 | N-0 Masek (d) B-0 | N-0 Masek RP

(e) B-3 | N-0 Ma *et al.* (f) B-3 | N-0 Ma *et al.* RP (g) B-3 | N-0 Masek (h) B-3 | N-0 Masek RP

(i) B-0 | N-3 Ma *et al.* (j) B-0 | N-3 Ma *et al.* RP (k) B-0 | N-3 Masek (l) B-0 | N-3 Masek RP

(m) B-3 | N-3 Ma *et al.* (n) B-3 | N-3 Ma *et al.* RP (o) B-3 | N-3 Masek (p) B-3 | N-3 Masek RP

Figure 5: Performance rates: (a)-(p) FCSs based on the algorithm of Ma *et al.* and Masek under various signal degradation conditions.

subjects. By analogy, the FAR defines the percentage of correct keys retrieved by non-genuine subjects. Obtained performance rates for FCSs under various forms of signal degradation are plotted in Figure 5 (a)-(p). It is assumed that all subjects are registered under favorable conditions, i.e. commitments constructed using unaltered templates are decommited applying degraded templates. For the recognition algorithm of Ma *et al.* and Masek FRRs of 2.54% and 6.59% are obtained at a FAR of 0.01% where the Hamming distance is applied as dis-similarity metric. Focusing on the feature extraction of Ma *et al.* FCSs provide FRRs of 5.90% and 3.73%, in the case case a random permutation is applied. FRRs are lower bounded by error correction capacities, i.e. bit-level error correction is applied more effectively if errors are distributed rather uniformly (see Figure 5 (a) and (b)). With respect to the feature extraction of Masek, applying a random permutation does not improve the key retrieval rate obtaining FRRs of 8.01% and 9.15%, respectively. Due to a more uniform distribution of errors Hadamard decoding succeeds more often for significant amount of impostor attempts, causing a decrease of the error correction threshold (see Fig 5 (c) and (d)).

Simulating signal degradation, recognition accuracy is significantly effected for both recognition algorithms leading to FRRs above 4% and 10% at a FAR of 0.01%, respectively. In contrast, FCSs

			Ma *et al.*					Masek				
			HD	FCS		FCS RP		HD	FCS		FCS RP	
			FRR at	FRR at	Corr.	FRR at	Corr.	FRR at	FRR at	Corr.	FRR at	Corr.
Blur	Noise	∅ PSNR	FAR≤0.01	FAR≤0.01	Blocks	FAR≤0.01	Blocks	FAR≤0.01	FAR≤0.01	Blocks	FAR≤0.01	Blocks
B-0	N-0	–	2.54 %	5.90 %	32	3.72 %	31	6.59 %	8.01 %	28	9.15 %	17
B-1	N-0	26.47 dB	3.82 %	5.69 %	32	3.66 %	32	9.92 %	7.86 %	28	9.29 %	17
B-2	N-0	21.04 dB	3.75 %	4.88 %	32	3.32 %	32	10.62 %	7.59 %	26	10.78 %	15
B-3	N-0	19.62 dB	4.36 %	5.22 %	32	3.93 %	28	10.94 %	8.61 %	27	11.32 %	14
B-0	N-1	28.32 dB	4.25 %	5.94 %	32	3.79 %	32	9.51 %	8.75 %	27	9.32 %	19
B-1	N-1	24.27 dB	3.36 %	5.76 %	32	3.86 %	32	10.15 %	9.02 %	27	9.15 %	18
B-2	N-1	20.21 dB	3.84 %	5.56 %	32	3.25 %	32	10.80 %	8.95 %	27	9.56 %	17
B-3	N-1	19.07 dB	4.15 %	6.30 %	31	4.54 %	29	10.69 %	8.88 %	27	10.51 %	15
B-0	N-2	22.54 dB	4.88 %	6.51 %	32	3.93 %	32	9.92 %	9.22 %	27	9.39 %	18
B-1	N-2	20.99 dB	4.09 %	5.76 %	32	3.59 %	32	10.62 %	9.17 %	28	9.83 %	18
B-2	N-2	18.58 dB	3.86 %	5.76 %	32	3.66 %	32	9.97 %	9.02 %	27	12.00 %	14
B-3	N-2	17.70 dB	4.27 %	5.83 %	32	3.73 %	31	10.69 %	10.44 %	26	10.85 %	15
B-0	N-3	19.14 dB	4.36 %	6.44 %	32	4.20 %	32	10.33 %	9.86 %	28	9.97 %	17
B-1	N-3	18.28 dB	4.43 %	6.37 %	32	4.07 %	32	10.49 %	10.37 %	26	9.97 %	17
B-2	N-3	16.82 dB	4.56 %	6.24 %	32	4.32 %	32	10.96 %	9.43 %	27	9.76 %	18
B-3	N-3	16.19 dB	4.27 %	6.58 %	32	4.40 %	32	9.54 %	9.29 %	27	10.04 %	17

Table 3: Summarized experiments for both feature extraction methods and FCSs under various signal degradation conditions.

based on both feature extraction methods appear rather robust to signal degradation. Focusing on FCSs based on the algorithm of Ma *et al.* FRRs do not significantly increase, for drastic signal degradation FRRs of $\sim$ 6.50% and $\sim$ 4.00% (RP) are obtained compared to a FRR of 5.90% and 3.72% (RP) without signal degradation. It is found that incorporating a certain amount of blur even improves key retrieval rates obtaining FRRs of $\sim$ 5.00% and 3.50% (RP), since, on average, extracted iris-codes are even more alike (iris-codes extracted from blurred textures do not encode detailed features), i.e. slight blurring is equivalent to denoising. Focusing on the algorithm of Masek a more predominant decrease in key retrieval rates is observed, however, results are still comparable to those obtained in the absence of blur and noise. In case of drastic signal degradation FRRs of $\sim$ 10.00% (original and RP) are obtained (partially outperforming the original recognition algorithm), compared to 8.01% and 9.15% (RP) without signal degradation. Again, in case of a slight blur performance is improved or retained.

For both feature extraction methods and both types of FCSs characteristics of FRRs and FARs remain almost unaltered in presence of signal degradation (see rates within columns of Figure 5), i.e. all types of investigated fuzzy commitment schemes appear rather robust to a certain extent of signal degradation based on blur and noise.

4 Conclusion

In this paper we investigate the impact of signal degradation on the performance of template protection schemes, in particular, the effect of blur and noise to FCSs based on iris. Based on different feature extraction methods FCSs are constructed and a significant amount of blur and noise is added successively to iris biometric data to simulate out of focus blur and thermal noise. It is found that, opposed to current opinions, FCSs appear rather resilient to a certain amount of signal degradation within biometric data obtaining key retrieval rates comparable to those achieved in the absence of signal degradation, even if this is not the case for underlying recognition algorithms. Future work will comprise studies on the impact of image compression to template protection.

References

[1] M. Ao and S. Z. Li. Near infrared face based biometric key binding. *In Proc. of the 3rd Int. Conf. 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 Trans. on Information Forensics and Security*, 3:673–683, 2008.

[3] A. Cavoukian and A. Stoianov. Biometric encryption: The new breed of untraceable biometrics.

In *Biometrics: fundamentals, theory, and systems*. Wiley, 2009.

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

[5] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP J. Adv. Signal Process*, 2008:1–17, 2008.

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

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

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

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

[10] 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.

[11] 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.

[12] 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.

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

[14] M. Van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo. Face biometrics with renewable templates. In *SPIE Proc. on Security, Steganography, and Watermarking of Multimedia Contents*, volume 6072, pages 205–216, 2006.

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