Iris-Biometric Fuzzy Commitment Schemes under Signal Degradation*

C. Rathgeb and A. Uhl

Multimedia Signal Processing and Security Lab.

Department of Computer Sciences

University of Salzburg, A-5020 Salzburg, Austria

{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. it is believed that biometric traits need to be captured under favorable conditions in order to provide practical recognition rates. In this work the impact of blur and noise to fuzzy commitment schemes is investigated and is compared to the impact observed on the accuracy of the underlying recognition scheme. 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 and cancelable biometrics, are desired to maintain recognition accuracy [1]. 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.

Biometric fuzzy commitment schemes (FCSs) [2], 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 Fig. 1, are investigated:

* This work has been supported by the Austrian Science Fund, project no. L554-N15.

Fig. 1. Supposed blur and noise occurrence within a biometric recognition system

Fig. 2. Basic operation mode of the Fuzzy Commitment Scheme

- **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.

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. Finally, a conclusion is given in Section 4.

2 Fuzzy Commitment Schemes

In past year numerous template protection schemes have been proposed [1]. In 1999, Juels and Wattenberg [2] 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

Table 1. Experimental results of proposed Fuzzy Commitment Scheme

Author(s)	Modality	FRR/ FAR	Key Bits	Remarks
Hao <i>et al.</i> [3]	Iris	0.47/ 0	140	ideal images
Bringer <i>et al.</i> [4]		5.62/ 0	42	short key
Rathgeb and Uhl [5]		4.64/ 0	128	–
Teoh <i>et al.</i> [6]	Fingerprint	0.9/ 0	296	user-specific tokens
Nandakumar [7]		12.6/ 0	327	–
Van der Veen <i>et al.</i> [8]	Face	3.5/ 0.11	58	>1 enroll. sam.
Ao and Li [9]		7.99/ 0.11	>4000	user-specific tokens

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,

$$F(c, x) = (h(x), x - c). \quad (1)$$

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 1. The FCS was applied to iris-codes in [3]. In this 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 [4]. 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 [5,10]. In [7] a binary fixed-length minutiae representation obtained by quantizing the Fourier phase spectrum of a minutiae set is applied in a FCS where alignment is achieved through focal points of high curvature regions. In [6] 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 [9]. A FCS based on face biometrics is presented in [8] in which real-valued face features are binarized by simple thresholding followed by a reliable bit selection to detect most discriminative

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

features. It has been found that FCSs (template protection schemes in general) reveal worse performance on non-ideal data sets (e.g. in [4]), 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.

3 A Case Study on Iris-Biometric FCSs

3.1 Experimental Setup

Experiments are carried out using the CASIA-v3-Interval iris database¹. 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 Fig. 3 (a)-(d).

In the feature extraction stage custom implementations of two different iris recognition algorithms are employed. The first one was proposed by Ma *et al.* [11]. Within this algorithm a dyadic wavelet transform is performed based on

¹ The Center of Biometrics and Security Research, <http://www.idealtest.org>

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

which two fixed subbands are selected. Local minima and maxima above a adequate threshold are located an encoded extracting 10240 bit. The second feature extraction method follows an implementation by Masek² in which filters obtained from a one-dimensional Log-Gabor function are utilized to generate iris-codes of 10240 bit. Sample iris-codes of both algorithms are shown in Fig. 3 (e)-(f).

3.2 Iris-Biometric FCSs

The applied fuzzy commitment scheme follows the approach in [12]. 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.

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). 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

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

Table 2. Blur and noise conditions considered for signal degradation (different denotations of σ are defined in Eq. 2 and Eq. 3)

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	$\sigma = 30$

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 Fig. 4 (a)-(d). Out of focus blur represents a frequent distortion in image acquisition mainly caused by an inappropriate distance of the camera to the acquired 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

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

which is then convoluted with the specific image. 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 position x, y with N being the noisy image, for an original image I as

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

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. Obtained performance rates for FCSs under various forms of signal degradation for the feature extraction of Ma *et al.* are plotted in Fig. 5 (a)-(d). For the recognition algorithm of Ma *et al.* and Masek in verification mode (columns “HD” in Table 3), 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 a FRR of 5.90%. With respect to the feature extraction of Masek a FRR of 8.01% is obtained.

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

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 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 $\sim 6.50\%$ are obtained compared to a FRR of 5.90% without signal degradation. It is found that incorporating a certain amount of blur even improves key retrieval rates obtaining FRRs of $\sim 5.00\%$, 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 $\sim 10.00\%$ are obtained (partially outperforming the original recognition algorithm), compared to 8.01% without signal degradation. Again, in case of a slight blur performance is improved or retained. For both feature extraction methods, characteristics of FCS's FRRs and FARs remain almost unaltered in presence of signal degradation, i.e. all types of investigated FCSs appear rather robust to a certain extent of signal degradation based on blur and noise.

Table 3. Results for both FCSs under various signal degradation conditions

			Ma <i>et al.</i>			Masek		
Blur	Noise	$\emptyset$ PSNR	HD	FCS		HD	FCS	
			FRR at FAR $\leq$ 0.01	FRR at FAR $\leq$ 0.01	Corr. Blocks	FRR at FAR $\leq$ 0.01	FRR at FAR $\leq$ 0.01	Corr. Blocks
B-0	N-0	—	2.54 %	5.90 %	32	6.59 %	8.01 %	28
B-1	N-0	26.47 dB	3.82 %	5.69 %	32	9.92 %	7.86 %	28
B-2	N-0	21.04 dB	3.75 %	4.88 %	32	10.62 %	7.59 %	26
B-3	N-0	19.62 dB	4.36 %	5.22 %	32	10.94 %	8.61 %	27
B-0	N-1	28.32 dB	4.25 %	5.94 %	32	9.51 %	8.75 %	27
B-1	N-1	24.27 dB	3.36 %	5.76 %	32	10.15 %	9.02 %	27
B-2	N-1	20.21 dB	3.84 %	5.56 %	32	10.80 %	8.95 %	27
B-3	N-1	19.07 dB	4.15 %	6.30 %	31	10.69 %	8.88 %	27
B-0	N-2	22.54 dB	4.88 %	6.51 %	32	9.92 %	9.22 %	27
B-1	N-2	20.99 dB	4.09 %	5.76 %	32	10.62 %	9.17 %	28
B-2	N-2	18.58 dB	3.86 %	5.76 %	32	9.97 %	9.02 %	27
B-3	N-2	17.70 dB	4.27 %	5.83 %	32	10.69 %	10.44 %	26
B-0	N-3	19.14 dB	4.36 %	6.44 %	32	10.33 %	9.86 %	28
B-1	N-3	18.28 dB	4.43 %	6.37 %	32	10.49 %	10.37 %	26
B-2	N-3	16.82 dB	4.56 %	6.24 %	32	10.96 %	9.43 %	27
B-3	N-3	16.19 dB	4.27 %	6.58 %	32	9.54 %	9.29 %	27

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.

References

1. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security* 2011 (2011)
2. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: *Sixth ACM Conference on Computer and Communications Security*, pp. 28–36 (1999)
3. Hao, F., Anderson, R., Daugman, J.: Combining Cryptography with Biometrics Effectively. *IEEE Trans. on Computers* 55, 1081–1088 (2006)
4. Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Zémor, G.: Theoretical and practical boundaries of binary secure sketches. *IEEE Trans. on Information Forensics and Security* 3, 673–683 (2008)

5. Rathgeb, C., Uhl, A.: Adaptive fuzzy commitment scheme based on iris-code error analysis. In: Proc. of the 2nd European Workshop on Visual Information Processing (EUVIP 2010), pp. 41–44 (2010)
6. Teoh, A., Kim, J.: Secure biometric template protection in fuzzy commitment scheme. *IEICE Electron. Express* 4, 724–730 (2007)
7. Nandakumar, K.: A fingerprint cryptosystem based on minutiae phase spectrum. In: Proc. of IEEE Workshop on Information Forensics and Security, WIFS (2010)
8. Van der Veen, M., Kevenaar, T., Schrijen, G.J., Akkermans, T.H., Zuo, F.: Face biometrics with renewable templates. In: SPIE Proc. on Security, Steganography, and Watermarking of Multimedia Contents, vol. 6072, pp. 205–216 (2006)
9. Ao, M., Li, S.Z.: Near Infrared Face Based Biometric Key Binding. In: Tistarelli, M., Nixon, M.S. (eds.) *ICB 2009. LNCS*, vol. 5558, pp. 376–385. Springer, Heidelberg (2009)
10. Zhang, L., Sun, Z., Tan, T., Hu, S.: Robust Biometric Key Extraction Based on Iris Cryptosystem. In: Tistarelli, M., Nixon, M.S. (eds.) *ICB 2009. LNCS*, vol. 5558, pp. 1060–1069. Springer, Heidelberg (2009)
11. Ma, L., Tan, T., Wang, Y., Zhang, D.: Efficient Iris Recognition by Characterizing Key Local Variations. *IEEE Trans. on Image Processing* 13, 739–750 (2004)
12. Rathgeb, C., Uhl, A.: Systematic Construction of Iris-Based Fuzzy Commitment Schemes. In: Tistarelli, M., Nixon, M.S. (eds.) *ICB 2009. LNCS*, vol. 5558, pp. 940–949. Springer, Heidelberg (2009)